L-Proxy

CEA-709 Gateway

User Manual

LOYTEC electronics GmbH

Contact

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

Version 3.1

Document № 88065706

Contents

Abbreviations

100Base-T	100 Mbps Ethernet network with RJ-45 plug
Aggregation	Collection of several CEA-709 packets into a single CEA-852 packet
BOOTP	Bootstrap Protocol, RFC 1497
CC	Configuration Client, also known as CN/IP Device
CEA-709	Protocol standard for LONWORKS networks
CEA-852	Protocol standard for tunneling CEA-709 packets over IP channels
CN	Control Network
COV	Change-of-Value
CP	Configuration Property
CR	Channel Routing
CS	Configuration Server that manages CEA-852 IP devices
DHCP	Dynamic Host Configuration Protocol, RFC 2131, RFC 2132
DNS	Domain Name Server, RFC 1034
DST	Daylight Saving Time
GMT	Greenwich Mean Time
IP	Internet Protocol
LSD Tool	LOYTEC System Diagnostics Tool
MAC	Media Access Control
MD5	Message Digest 5, a secure hash function, see Internet RFC 1321
NAT	Network Address Translation, see Internet RFC 1631
NV	Network Variable
RTT	Round-Trip Time
SCPT	Standard Configuration Property Type
SL	Send List
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
SNVT	Standard Network Variable Type
UCPT	User-defined Configuration Property Type
UI	User Interface
UNVT	User-defined Network Variable Type
XML	eXtensible Markup Language

1 Introduction

1.1 Overview

The L-Proxy is a high performance network infrastructure component for CEA-709 networks. It is the first device that allows network variable bindings across multiple domains, SNVT translation, address table expansion for CEA-709 nodes, firewall security etc. The L-Proxy provides **five** communication ports and it translates packets between these ports. Available ports are two FT ports, and three IP-852 ports. The three IP-852 ports are connecting to an IP-852 backbone channel. The L-Proxy's unique architecture very much supports well defined interfaces between various subsystems like HVAC, lighting, and security in a typical building. Easy to understand diagnostic LEDs allow installers and system integrators to install and troubleshoot this device without expert knowledge and dedicated troubleshooting tools.

The basic operation of L-Proxy is to take an input network variable (NV) or configuration property (CP) on one side, interpret the data in the variable and transmit a corresponding output network variable on the other side. This concept is used to solve a great amount of today's communication problems in CEA-709 networks as explained in the following chapters. The device is fully compliant with ANSI/CEA-709, and ANSI/CEA-852-A, EN 14908.

Network variables (NVs) in the CEA-709 network can also be operated as "external NVs". External NVs are polled or explicitly written to without allocating static or dynamic NVs on the L-Proxy. In this case, address information is supplied by the configuration software by importing e.g., a CSV file. User-defined network variable types (UNVTs) can be used as dynamic or external NVs. Configuration properties (CPs) on other devices can be accessed through file transfer. To transfer CPs, the device supports both the LONMARK file transfer and the read memory access method. For CPs, the standard SCPTs and user-defined UCPTs are supported.

L-Proxy is configured over the network with an easy-to-use configuration tool. This configuration tool can be used as a plug-in for LNS-based network installation tools or as a standalone tool.

The built-in Web server allows convenient device configuration through a standard Web browser such as the Internet Explorer or Firefox. The Web interface also provides statistics information for system installation and network troubleshooting.

The L-Proxy is used for:

- Binding of network variables (NVs) across multiple domains (up to 5 with a single device),
- mapping configuration properties (CPs) to network variables (NVs),

- using static, dynamic, or external (polled) network variables,

- supporting standard (SNVT, SCPT) and user-defined (UNVT, UCPT) types,

- translation between different SNVT types,

- overcoming the 15 destination addresses limit by expanding the address table in Neuron Chip based network nodes (up to 512 address table entries on each port),

- saving group addresses by breaking up groups into individual NV updates,

- a firewall for CEA-709 networks,

- supporting up to 512 network variables on each port,

- supporting up to 512 alias-network variables on each port,

- supporting up to 512 address table entries on each port,

- browsing data points on the Web interface,

- communicating on CEA-709 with either FT or IP-852 (IP channel on the Intranet/Internet).

1.2 Scope

This document covers L-Proxy devices with firmware version 3.1 and the L-Proxy Configurator 3.1 and higher. See Section 14 for differences between the different L-Proxy firmware versions. For L-Proxy devices with firmware versions before 3.0 please refer to L-Proxy User Manual version 2.2 [2]. Also note, that firmware and configuration files of L-Proxy 3.0 and higher are not compatible with 2.2.

2 Quick-Start Guide

This Chapter shows step-by-step instructions on how to configure the L-Proxy for a simple network architecture, mapping CEA-709 network variables from different ports of the L-Proxy.

2.1 Hardware Installation

Connect power (12-35 VDC or 12-24 VAC), the CEA-709 network, and the Ethernet cable as shown in Figure 1. More detailed instructions are shown in Chapter 3.

Important: ***Do not connect terminal 17 with Earth-ground!***
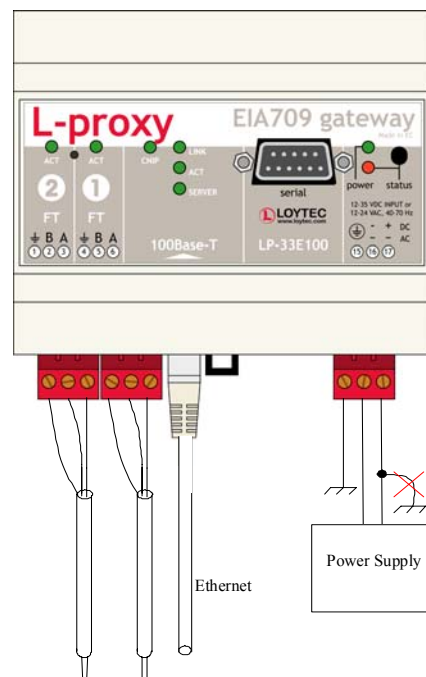
Figure 1: Basic Hardware Installation

2.2 Configuration with LNS-based Tools

This section describes a quick start scenario for the L-Proxy. In this scenario network variables are created on Port 1 (FT) and Port 2 (FT). The two ports can be in different LNS

databases and different domains. Then NVs are connected on L-Proxy by creating internal connections.

First, install the L-Proxy Configurator Software from the "setup.exe". This file can be downloaded from www.loytec.com. In your LNS-based tool, register the L-Proxy Configurator as LNS plug-in.

Open an LNS database and add an L-Proxy device for Port 1 (FT) using the device template, which has been created for the L-Proxy (e.g., L-Proxy_V3_0_FT-10.xif). Then create dynamic NVs on that L-Proxy port, e.g., "nviTemp" and "nvoSwitch". Close the LNS database. For detailed information on how to create dynamic NVs in LNS-based tools refer to Section 7.7.

Open another LNS database and add an L-Proxy device for Port 2 (FT) using the device template, which has been created for the L-Proxy (e.g., L-Proxy_V3_0_FT-10.xif). Then create dynamic NVs on that L-Proxy port, which are opposite to the NVs on port 1, e.g., "nvoTemp" and "nviSwitch".

To Create the Internal Connections

1. Open one of the two databases.

2. In LonMaker right-click on the L-Proxy device and select **Configure …** to launch the L-Proxy Configurator as plug-in.

3. This opens the data point manager screen of the software as shown in Figure 2. Note that the device status is displayed as "Configured" on the right-hand side below the speed button bar.
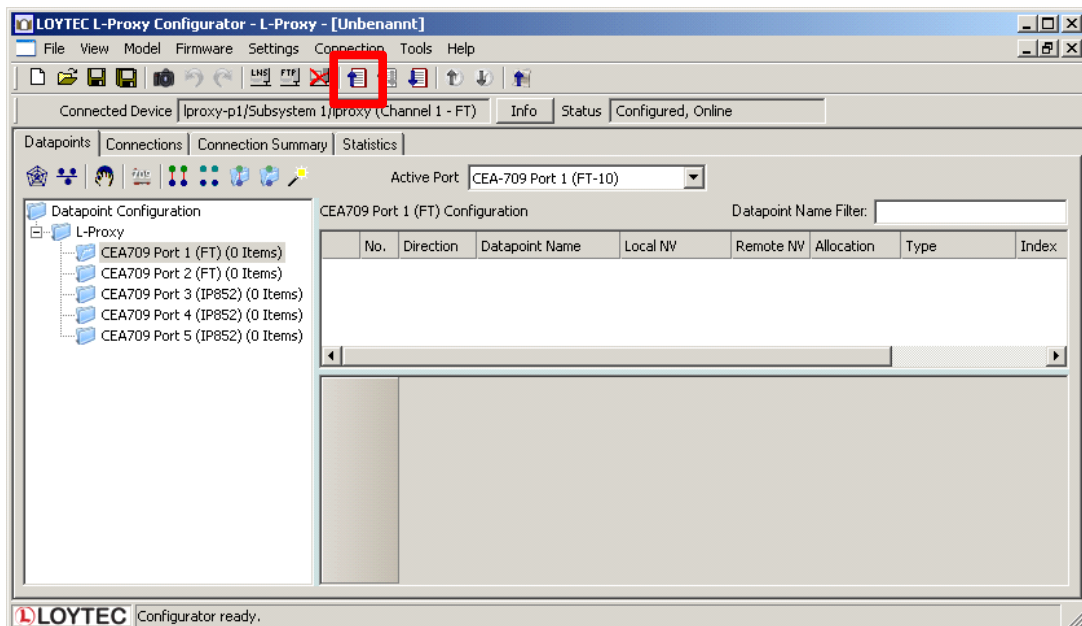
Figure 2: L-Proxy Configurator plug-in main screen.

4. Click on the **Upload Configuration** speed button as marked by the red rectangle in Figure 2.

5. This uploads all dynamic NVs from all ports of the L-Proxy. Figure 3 shows an example result of the upload.

Figure 3: Example result of synced dynamic NVs.

6. Click the magic wand button 🪄 **Auto-create connections** for auto-connecting the NVs. This creates internal connections for the NVs with the same base name. The prefix "nvi" and "nvo" are ignored. Therefore, two connections are created in our example, one named "nviTemp", and one named "nviSwitch".

7. Click on the **Connections** tab and view the generated connections as shown in Figure 4.
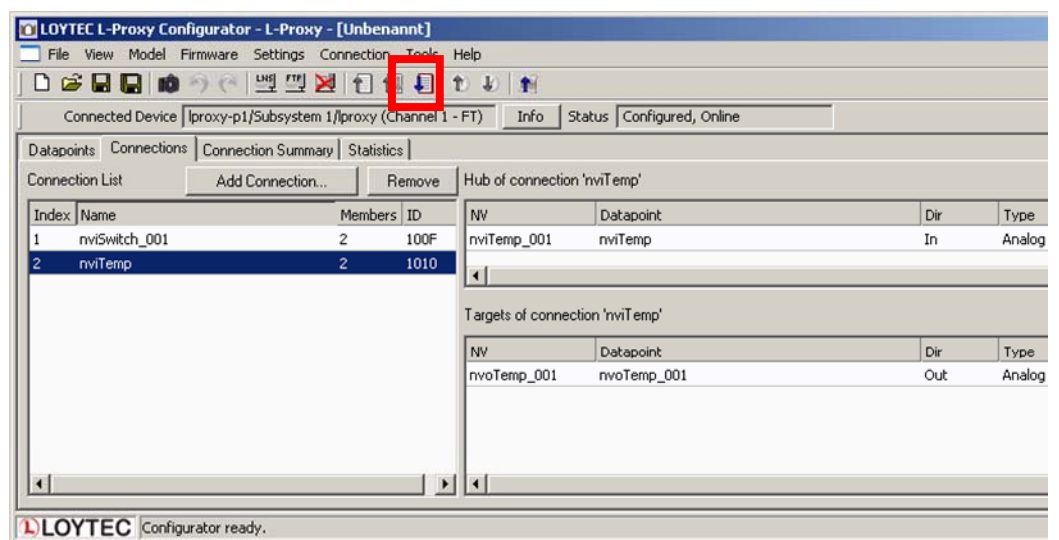
Figure 4: Generated connections.

8. Click on the **Download Configuration** button in the tool bar as indicated by the red rectangle in Figure 4. This opens the configuration download dialog as shown in Figure 5.
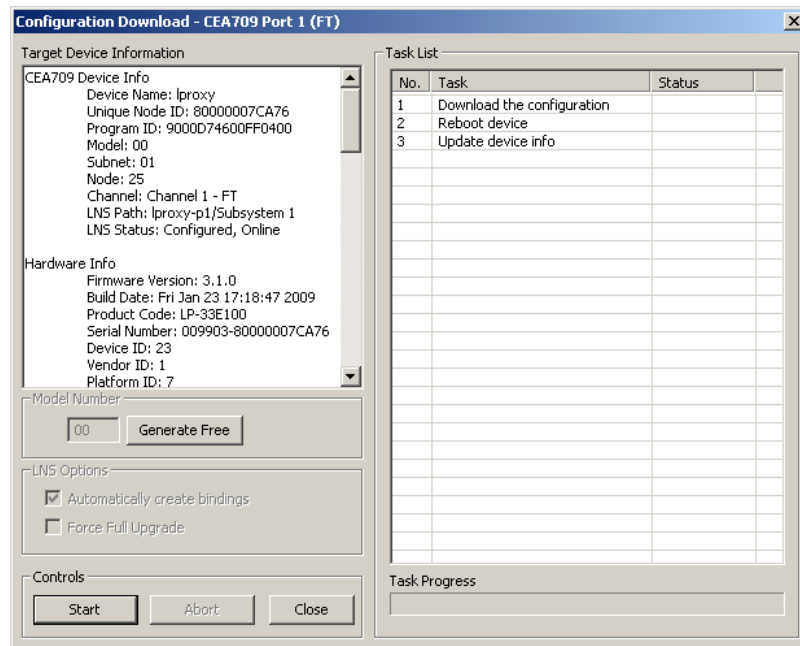
Figure 5: Download the configuration to the L-Proxy.

9. Click on **Start** to initiate the download process. The dialog shows the currently executed tasks.

10. Click **OK** when the download is finished and close the download dialog. It is recommended to save the L-Proxy project to a disk file.

11. Select **File → Save As …** and enter a suitable file name in the file requestor. The project file is stored as an '.lprxy' file.

After the configuration process, the NVs from Port 1 and Port 2 are connected over the internal connections. Any updates on the NVs of the devices connected to Port 1 are then propagated to Port 2 and vice-versa.

3 Hardware Installation

3.1 Enclosure

3.1.1 LP-33E100

The L-Proxy enclosure is 6 TE (1 TE = 17.5 mm) wide for DIN rail mounting, following DIN 43 880 (see Figure 6).
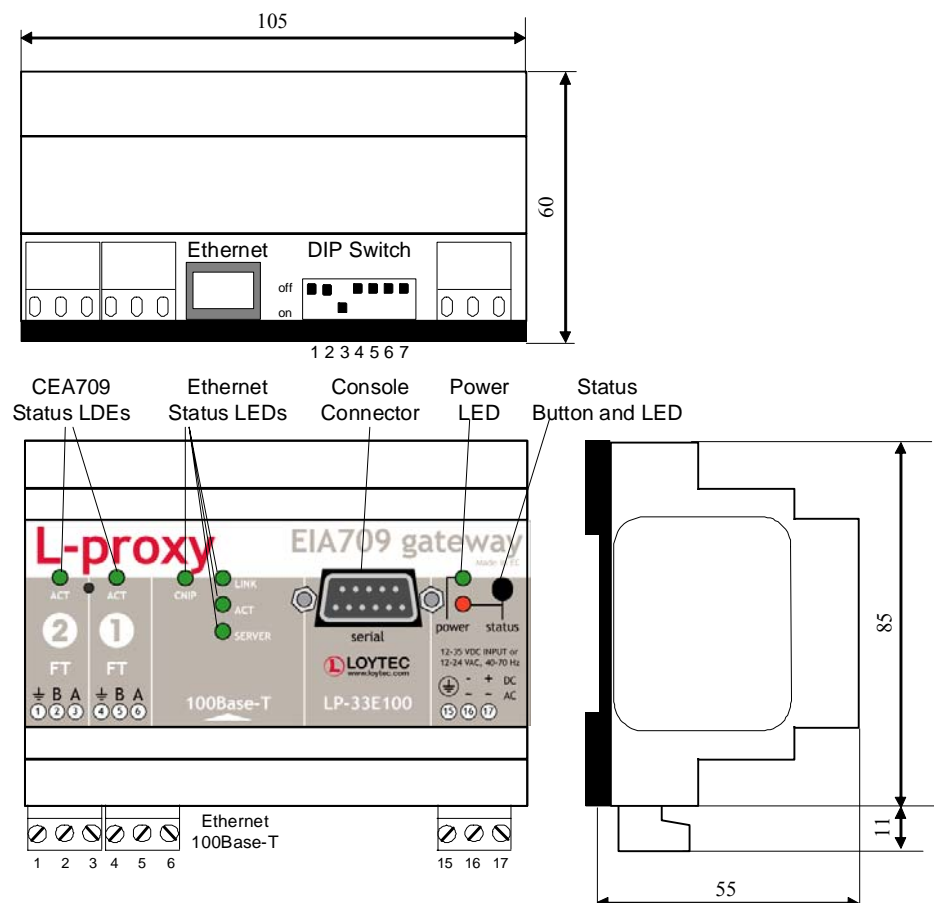
Figure 6: L-Proxy Enclosure (dimensions in mm).

3.2 Product Label

The product label on the side of the L-Proxy contains the following information (see Figure 7):

- L-Proxy order number with bar-code (e.g., LP-33E100),

- serial number with bar-code (Ser#),

- unique node ID and virtual ID of each port (NID1, VID1) with bar-code,

- Ethernet MAC ID with bar-code (MAC1).
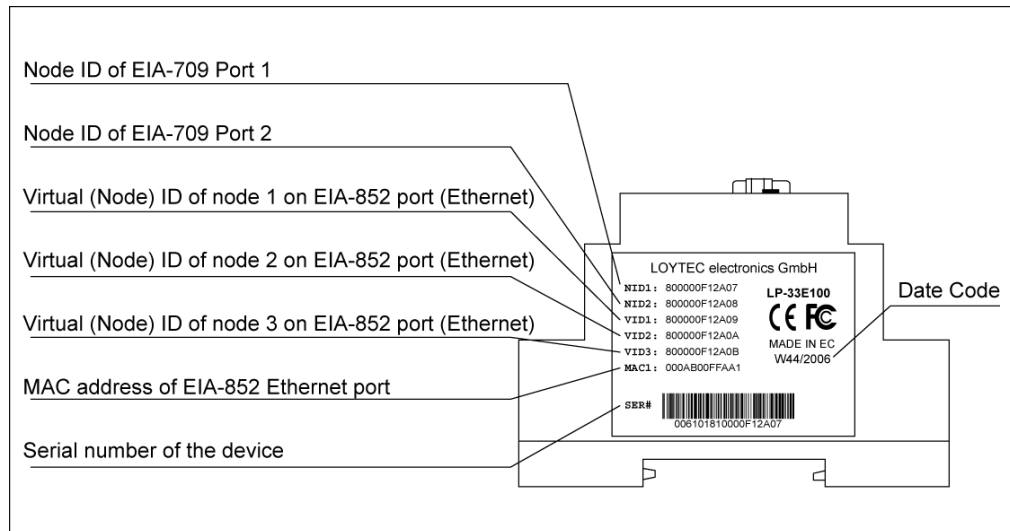
Figure 7: L-Proxy product label

Unless stated otherwise, all bar codes are encoded using "Code 128". An additional label is also supplied with the L-Proxy 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. The device can be mounted in any position. However, an installation place with proper airflow must be selected to ensure that the device's temperature does not exceed the specified range (see Chapter 15).

3.4 LED signals

3.4.1 Power LED

The L-Proxy power LED lights up green when power is supplied to terminals 16 and 17.

3.4.2 Status LED

The L-Proxy is equipped with a red status LED (see Figure 6). This LED is normally off. During boot-up the status LED is used to signal error conditions (red). If the fall-back image is executed the status LED flashes red once every second.

3.4.3 FT Activity LED

The FT port on the L-Proxy has a three-color LED (green, red, and orange, see Figure 6). Table 1 shows different LED patterns of the port and their meaning.

Behavior	Description	Comment
GREEN flashing fast	Traffic	
GREEN flashing at 1Hz	The L-Proxy's port is unconfigured	
RED permanent	Port damaged	
RED flashing fast	Traffic with high amount of errors	
RED flashing at 1 Hz (all ports)	Firmware image corrupt	Please upload new firmware.
ORANGE permanent	Port disabled	e.g., using LSD Tool
ORANGE flashing fast	Traffic on port configured as management port	e.g., using LSD Tool

Table 1: CEA-709 Activity LED Patterns

3.4.4 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.

3.4.5 Ethernet Activity LED

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

3.4.6 CNIP LED

The CNIP LED is a three color LED that indicates different operating states of the L-Proxy's CEA-852 device.

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

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

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

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

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

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

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

3.4.7 Config LED

This LED is green, if the L-Proxy is running with a valid proxy configuration.

3.4.8 Wink Action

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

3.5 Status Button

The L-Proxy is equipped with a status button (see Figure 6). When pressing the status button shortly during normal operation of the L-Proxy, it sends a "Service Pin Message" on the active CEA-709 network port (FT or CEA-852). As an alternative to pressing the status button, a service pin message can be sent via the Web interface (see Section 5.1).

The status button can also be used to switch the device back to factory default state. Press the service button and power-cycle the device. Keep the button pressed until the port LEDs illuminate orange permanently. Release the button within five seconds from that time on to reset the device to factory defaults. Alternatively, the device can be switched back to factory defaults over the console UI (see Section 4.3.7).

3.6 DIP Switch Settings

The DIP switch assignment for the L-Proxy is shown in Table 2. Please leave all switches at default state.

DIP Switch #	Function	Factory Default
1	Must be OFF	OFF
2	Must be OFF	OFF
3	Must be ON	ON
4	Must be OFF	OFF
5	Must be OFF	OFF
6	Must be OFF	OFF
7	Must be OFF	OFF

Table 2: DIP Switch Settings for L-Proxy

3.7 Terminal Layout and Power Supply

The L-Proxy provides screw terminals to connect to the network as well as to the power supply. The screw terminals can be used for wires of a maximum thickness of 1.5 mm^2/AWG12. The device can either be DC or AC powered.

Terminal	Function
1	Earth Ground
2, 3	CEA-709 A, B of FT Channel Port 2
4	Earth Ground
5, 6	CEA-709 A, B of FT Channel Port 1
8	Ethernet 100Base-T
15	Earth Ground
16, 17	Power Supply 12 – 35 VDC or 12 – 24 VAC ± 10 % **Do not connect terminal 17 to earth ground!**

Table 3: L-Proxy Terminals LP-33E100.

3.8 Wiring

The CEA-709 network segment connected to the L-Proxy needs to be terminated according to the rules found in the specification of the transceiver (see Section 10.1).

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

Important: *Never connect terminal 17 to earth ground!*
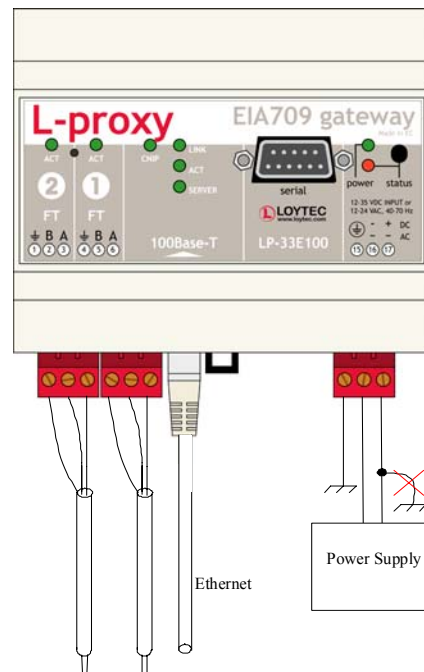
Figure 8: Connecting the L-Proxy

4 Console Interface

4.1 Console Connection

The L-Proxy is equipped with a serial interface to

- display the results of the self test,

- allow configuration via a console menu,

- upgrade the L-Proxy firmware.

To use the serial interface, the console connector (see Figure 6) of the L-Proxy can be connected to the RS-232 port of a PC. The PC can communicate with the L-Proxy using a standard terminal program with communication settings of 38,400 bps / 8 data bits / no parity / 1 stop bit. Use a standard null-modem cable with full handshaking to connect the L-Proxy serial console interface to your PC.

4.2 Self Test

Whenever the L-Proxy comes out of reset, it performs a self-test. The console output of a successful boot sequence on an L-Proxy reads as depicted in Figure 9. The duration of a successful boot sequence of an L-Proxy is typically 30 seconds.

```
LOYTEC electronics GmbH
www.loytec.com


Testing Board ID (3)                                        Passed
Testing RAM                                                 Passed
Testing boot loader                                         Passed
Testing fallback image                                      Passed
Testing primary image                                       Passed
Testing Flash                                               Passed

Loading primary image                                       Passed

Bootloader version 2
L-Proxy Primary Image loading...
Firmware version 3.1.0

Type bootshell to enter the boot shell...

Mounting file system                                        Passed
Starting TCP/IP networking                                  Passed
Starting CEA-852 device                                     Passed
Detecting CEA-709 port 1 (FT)                               Passed
Detecting CEA-709 port 2 (FT)                               Passed
Starting CEA-709 scanner                                    Passed
Starting CEA-709 networking                                 Passed
Starting FTP server                                         Passed
Starting Telnet server                                      Passed
Starting Web server                                         Passed

L-Proxy(c)
LOYTEC electronics GmbH
Fri Jan 23 17:18:47 2009 - V3.1.0
```
Figure 9: Console messages during the boot phase.

4.3 L-Proxy Device Main Menu

After booting has completed, the L-Proxy displays the console menu as shown in Figure 10.

```
Device Main Menu
================

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

[a]  Data Points

[0]  Reset device

Please choose:
```
Figure 10: L-Proxy Device Main Menu.

The menu items are described in the following sections.

4.3.1 Option 1 – Show device information

This menu item shows information about the L-Proxy and the current firmware version. The output should look like what is shown in Figure 11.

```
Device Information
==================

Product:        L-Proxy
Product code:   LP-33E100
Firmware:       L-Proxy Primary Image
Version:        3.1.0
Build date:     Fri Jan 23 17:18:47 2009
Serial number: 009903-80000007CA76
Free memory:    10077K,615K
Free flash:     4801K
CPU load:       0.4%
System temp:    36.7C
Supply volt:    15.4V


CEA-709 application unique node IDs
===================================

Port 1         : 80 00 00 07 CA 76 (Online)
Port 2         : 80 00 00 07 CA 77 (Online)
IP (node 1)    : 80 00 00 07 CA 78 (Online)
IP (node 2)    : 80 00 00 07 CA 79 (Offline)
IP (node 3)    : 80 00 00 07 CA 7A (Offline)

Press <RETURN> to continue
```

Figure 11: Device Information

4.3.2 Option 2 – Serial firmware upgrade

This menu item allows updating the L-Proxy firmware via the serial interface (console). See Section 11.2 for detailed instructions.

Note: *If you select this option accidentally, you can return to the main menu by sending a break signal. In case your terminal program does not offer an option to send a break signal, the device must be reset to return to the main menu.*

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 – CEA-709 configuration

Select this menu item to change the CEA-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, and MAC address. See Section 4.6 for details.

4.3.6 Option 6 – CEA-852 Device Configuration

Select this menu to change the CEA-852 device configuration. It allows changing settings like configuration server IP address, device name, SNTP server, escrow timeout, aggregation timeout and MD5 authentication secret. See Section 4.7 for details.

4.3.7 Option 8 – Reset configuration (factory defaults)

This menu item resets the L-Proxy to factory defaults. See Section 3.5 for details on how to load factory defaults by pressing the status button and Section 4.8 on how to load factory defaults through the console menu.

4.3.8 Option 9 – Device statistics

Select this menu item to display advanced IP, CEA-852 device, and statistics information like number of packets sent and received, number of channel members, etc. See Section 4.9 for details.

4.3.9 Option 0 – Reset Device

Select this menu item to reboot the L-Proxy. Some configuration changes require rebooting the device. Note that this option does not reset the configuration.

4.3.10 Option a – Data Points

This menu option takes the user to the data point menu. In this menu, the configured data points in the L-Proxy can be viewed and set. See Section 4.10 for details.

4.4 System Configuration Menu

The system configuration menu holds various system configuration settings. Typically, the system configuration menu looks like shown in Figure 12.

```
System Configuration Menu
=========================

[1]  Configure date/time : Mon Aug 11 18:38:47 2008 (GMT+02:00, DST)
[2]  Configure earth pos : 48:13:14 N 16:20:05 E 200 m
[7]  FTP server          : enabled
[8]  FTP server port     : 21 (default)
[9]  Web server          : enabled
[0]  Web server port     : 80 (default)
[a]  Telnet server       : enabled
[b]  Telnet server port  : 23 (default)

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

Please choose:
```

Figure 12: System Configuration Menu

4.4.1 Option 1 – Configure Date/Time

This menu item allows configuring L-Proxy's system time. It provides several sub-items as shown in Figure 13. With menu option **1**, the time source is defined. The following options are available: **auto**, **manual**, **NTP**, **LonMark**. In the **auto** mode, the device switches to the first external time source that is discovered. The option **manual** allows setting the time manually using menu items **2** and **3**. In **manual** mode, the device does not switch to an external time source. Note that if **NTP** is selected, the NTP servers have to be configured in the IP setting menu (see Section 4.3.5).

```
Date/Time Configuration Menu
============================

[1]  Set time sync source: manual
[2]  Set date            : 2008-01-29
[3]  Set time            : 10:58:56
[4]  Set timezone offset : +01:00
[5]  Set DST             : none

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

Please choose:
```

Figure 13: Configure Date/Time Menu

The time zone offset must be defined independently of the time source. It is specified in menu option **4** and defines the offset to GMT in hours and minutes (e.g., Vienna/Austria is +01:00, New York/USA is –06:00). Start and end of daylight savings time (DST) is defined in menu option **5**. Predefined choices are offered for Europe and USA/Canada. DST can be switched off completely, or set manually for other regions.

4.4.2 Option 2 – Configure Earth Position

This menu item allows configuring the L-Proxy's earth position. This setting defines the longitude, latitude, and absolute altitude of the device. This setting is used for an astronomical clock. For fixed locations such as a building, the position can be entered in this menu (see Figure 14). For moving locations, this setting can be updated over the network using the network variable nciEarthPos (see Section 9.1.2).

```
Earth Position Configuration Menu
=================================

[1]   Set latitude        : 48:13:14 N
[2]   Set longitude       : 16:20:05 E
[3]   Set altitude        : 200 m

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

Please choose:
```

Figure 14: Configure Earth Position

The latitude and longitude are entered through menu items **2** and **3** as degrees, minutes, and seconds. The altitude is entered in menu item **3** in meters height above sea level.

4.4.3 Option 7 – FTP server, 8 – FTP server port

This menu option allows enabling and disabling the FTP server and configuring the FTP server port. Press '7' to toggle between enabled and disabled. Press '8**'** to change the FTP server port. To use the default port, enter '0**'** when asked for the port number. The FTP server can be used to download a data point configuration or update the firmware (see Section 11.1).

4.4.4 Option 9 – Web server, 0 – Web server port

These menu items allow enabling and disabling the Web server and configuring the Web server port on the L-Proxy. You can disable the Web server if you do not want to provide access to the L-Proxy configuration via the Web interface. Press '9' to toggle between enabled and disabled. Press '0' to change the Web server port. To use the default port, enter '0' when asked for the port number.

4.4.5 Option a – Telnet server, b – Telnet server port

This menu option allows enabling and disabling the Telnet server and configuring the Telnet server port. Press 'a' to toggle between enabled and disabled. Press 'b**'** to change the Telnet server port. To use the default port, enter '0**'** when asked for the port number. The Telnet server is used to connect the Configurator software to the device via IP (see Section 7.9.2).

4.5 CEA-709 Configuration Menu

This menu allows changing the settings of the CEA-709 port of the L-Proxy. The menu is only used for displaying information on the L-Proxy. And looks as shown in Figure 15.

```
CEA-709 Configuration Menu
==========================

    Port 1                  : FT
    Port 2                  : FT
    IP                      : IP-852

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

Please choose:
```

Figure 15: CEA-709 Configuration Menu on the L-Proxy.

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:

- Enter '0.0.0.0' to clear an IP address.

- Enter '0' to select the default port number.

- Enter '0' to disable a time setting.

- Press **Return** to keep the current setting.

The IP configuration menu, when DHCP is disabled, is shown in Figure 16.

```
IP Configuration Menu
=====================

[1]   DHCP                  : disabled
[2]   IP Address            : 192.168.24.99
[3]   IP Netmask            : 255.255.192.0
[4]   IP Gateway            : 192.168.1.1
[5]   Hostname              : test-lproxy
[6]   Domainname            : <unset>
[7]   DNS Servers           : 10.101.17.2
[9]   MAC Address           : 00:0A:B0:01:0A:4C (factory default)
[0]   NTP Servers           : <unset> (out-of-sync)
[b]   Link Speed & Duplex   : Auto Detect

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

Please choose:
```

Figure 16: IP Configuration Menu when DHCP is disabled

The IP configuration menu, when DHCP is enabled, is shown in Figure 17.

```
IP Configuration Menu
=====================

[1]   DHCP                  : enabled
      IP Address            : 192.168.24.99
      IP Netmask            : 255.255.192.0
      IP Gateway            : 192.168.1.1
[5]   Hostname              : test-lproxy
      Domainname            : <unset>
      DNS Servers           : 10.101.17.2
[9]   MAC Address           : 00:0A:B0:01:0A:4C (factory default)
[0]   NTP Servers           : <unset> (out-of-sync)
[b]   Link Speed & Duplex   : Auto Detect

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

Please choose:
```

Figure 17: IP Configuration Menu when DHCP is enabled

4.6.1 Option 1 – DHCP

This option switches between manual entry of the IP address, netmask, and gateway address or automatic configuration from a DHCP server. If DHCP is disabled, one must enter the configuration data described in the following sections. If DHCP is enabled, please skip menu items **2** through **7**.

Press '1' to toggle between **DHCP enabled** and **DHCP disabled**.

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

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

Important! ***The default IP address 192.168.1.254 is only set for configuration access. It must be changed in order to make the device functional.***

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 on how to configure DHCP to acquire an IP address.

4.6.3 Option 7 – DNS Servers

You can configure up to 3 Domain Name Servers. On the L-Proxy these settings are not required and purely optional.

4.6.4 Option 9 – MAC Address

The L-Proxy 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.

4.6.5 Option 0 – NTP Servers

You can configure up to 2 NTP servers. Select '0' and when prompted

```
Enter new address of NTP server 1:
```

enter the first NTP server's IP address. Press **Enter**. When prompted, enter the IP address of the second NTP server and press **Enter**. To clear an NTP server's address, leave the respective IP address blank and press **Enter**.

The NTP server information will be used to synchronize the system time if the NTP time source has been selected in the system configuration menu (see Section 4.3.3). The text appended to this menu item displays the current NTP synchronization status (**out-of-sync** or **in-sync**).

4.6.6 Option b – Link Speed & Duplex

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

```
          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 CEA-852 Device Configuration Menu

This menu holds relevant information regarding the configuration of the CEA-852 device. In principle, there are two ways to add the L-Proxy to an IP channel. The recommended method is to enter the information at the configuration server. The configuration server will then contact the L-Proxy and configure the relevant information. If for some reason the L-Proxy shall contact the configuration server on its own behalf (e.g., as an auto-member), one can enter the configuration data directly into this menu. In this case L-Proxy tries to register with the configuration server. The device configuration menu is shown in Figure 18.

```
CEA-852 Device Configuration Menu
=================================

[2]   Config server address    : <unset>
[3]   Config server port        : 1629 (default)
[4]   Config client port        : 1628 (default)
[5]   Device name               :
      Channel mode              : Standard
      Pri. SNTP server          : <unset>
      Sec. SNTP server          : <unset>
      Channel timeout           : off
[6]   Escrow timeout            : on (64 ms)
[7]   Aggregation timeout       : on (16 ms)
[8]   MD5 authentication        : off
[9]   MD5 secret                : not displayed
[0]   Location string           : unknown
[a]   NAT address               : Auto (no NAT)
[b]   Multicast address         : <unset>

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

Please choose:
```

Figure 18: CEA-852 Device Configuration Menu

In case that the configuration server contacts the L-Proxy, only the MD5 secret in menu item **8** must be entered if authenticated communication is required. In networks that communicate over the Internet, one may also have to experiment with the escrow timeout in menu item **5**.

4.7.1 Option 2 – Config server address, 3 – Config server port

Please enter the IP address and port of the configuration server if the L-Proxy 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 4 – Config client port

If only one L-Proxy is used in an IP-852 channel behind a NAT router, this field should be left at the default setting (1628). If changed, it must not be the same as the configuration server port.

4.7.3 Option 5 – 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-Proxy behind one NAT router), the channel switches to **Extended NAT mode**. Please refer to the L-IP User Manual [1] to learn more about configuring the Extended NAT mode in the configuration server.

4.7.5 SNTP server, channel timeout

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

4.7.6 Option 6 – Escrow timeout

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

4.7.7 Option 7 – Aggregation Timeout

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

4.7.8 Option 8 – MD5 authentication

This menu item enables or disables MD5 authentication. Note that MD5 authentication cannot be used together with the Echelon's *i*.LON 1000 since the *i*.LON 1000 is not fully compliant with the CEA-852 authentication method. MD5 can be used with the *i*.LON 600.

4.7.9 Option 9 – MD5 secret

Enter the 16-byte MD5 secret. Note that for security purposes the active MD5 secret is not displayed. You may enter the 16 bytes as one string or with spaces between each byte,

e.g., 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.

4.7.10 Option 0 – Location string

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

4.7.11 Option a – NAT Address

If the CEA-852 device on the L-Proxy 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 CEA-852 device of the L-Proxy behind a NAT router or firewall, which has a dynamic public IP address, and determines the correct NAT address from a Configuration Server. This is the default setting.

```
Enable automatic NAT router discovery (y/n):
```
Figure 19: Enable/Disable automatic NAT Router Discovery

To enable/disable automatic NAT router discovery select this menu option. The question in Figure 19 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.

If an L-Proxy uses automatic NAT router discovery and the NAT address is known beforehand, the L-Proxy can simply be added to the channel in the L-IP configuration server by specifying the NAT address and correct port. If the NAT address is not known, take the following steps to add the L-Proxy to a CEA-852 IP channel in the configuration server:

1. On the L-Proxy turn on **automatic NAT router discovery** (this is the default setting). The NAT address should read 'Auto (no NAT)'.

2. Enter the IP address of the configuration server in the CEA-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-Proxy to the configuration server using this IP address.

4.7.12 Option b – Multicast Address

This menu option allows the user to add the CEA-852 device of the L-Proxy into a multi-cast group for the CEA-852 IP channel. Enter the channel's IP multi-cast address here. Please contact your system administrator on how to obtain a valid multi-cast address. Refer to the L-IP User Manual [1] to learn when it is beneficial to use multi-cast addresses in your channel.

4.8 Reset configuration (load factory defaults)

This menu item allows resetting the device into its factory default state. The menu appears as shown in Figure 20.

```
Reset Configuration Menu
========================

[1]  Reset everything to factory defaults
[3]  Reset all passwords
[4]  Clear data point configuration

[q]  Quit

Please choose:
```

Figure 20: Reset to Factory Defaults Menu

4.8.1 Option 1 – Reset everything to factory defaults

Select this menu item to reset the complete device to factory defaults (including error log, configuration files, passwords etc.).

4.8.2 Option 3 – Reset all passwords

Select this menu item to reset all passwords (Web interface, FTP server etc.) to factory defaults.

4.8.3 Option 4 – Clear data point configuration

Select this option to clear all configured data points, such as CEA-709 network variables or user registers. This effectively clears the entire port configuration. The L-Proxy must be rebooted to let the changes take effect.

4.9 Device Statistics Menu

This menu holds relevant information regarding the device statistics of the L-Proxy. The device statistics menu is shown in Figure 21. Use this menu only for debugging purposes. There is no need to access this menu if the network is running smoothly.

```
Statistics Menu
===============

[1]   Show CEA-852 statistics
[2]   Show CEA-709 application statistics
[4]   Show IP statistics
[6]   Enhanced communications test

[q]   Quit

Please choose:
```

Figure 21: Device Statistics Menu on the L-Proxy.

4.9.1   Option 1 – CEA-852 device statistics

A sample console output is shown in Figure 22. The first part displays CEA-852 device statistics, which are part of the standard and are comparable to e.g., the *i*.LON 600. Enter 'y' to go on to extended statistics.

```
CEA-852 Device Statistics
=========================

Seconds since cleared          : 261
Date/Time of clear (GMT)       : Wed Sep 27 16:18:19 2006
No. of members                 : 0
LT Packets received            : 0
LT Bytes received              : <unknown>
LT Packets sent                : 0
LT Bytes sent                  : <unknown>
IP Packets sent                : 0
IP Bytes sent                  : 0
IP Packets received            : 0
IP Bytes received              : 0
IP Packets data sent           : 0
IP Packets data received       : 0
LT Stale packets               : 0
RFC Packets sent               : 0
RFC Packets received           : 0
Avg. aggregation to IP         : <unknown>
Avg. aggregation from IP       : <unknown>
UDP Packets sent               : 0
TCP Packets sent               : 0
Multi-cast Packets sent        : 0

Show extended CEA-852 device statistics (y/n)?
```

Figure 22: CEA-852 Device Statistics

A sample console output of the extended CEA-852 device statistics is shown in Figure 23. At the end the user is prompted if the statistics shall be cleared. Enter 'y' to reset all counters to 0.

```
Extended CEA-852 Device Statistics
==================================

Session ID                           : 0x4dce9e98
SNTP synchronized                    : no
Number of CR member infos            : 0
Current channel routing mode         : CR
Message alloc count                  : 0
Dropped failed authentication        : 0
Dropped invalid frame                : 0
Dropped out-of-sequence              : 0
Dropped duplicates                   : 0
Dropped missing timestamp            : 0
Active DC datetime                   : 0x00000000
Active CM datetime                   : 0x00000000
Active SL datetime                   : 0x00000000
Stale DC messages                    : 0
Stale CM messages                    : 0
Stale SL messages                    : 0
Stale CR messages                    : 0
Number of DC updates                 : 0
Number of CM updates                 : 0
Number of SL updates                 : 0
Number of CR updates                 : 0
CR packets sent to CS                : 0

Clear CEA-852 device 1 statistics (y/n)?
```

Figure 23: Extended CEA-852 Device Statistics

4.9.2 Option 2 – CEA-709 Application Statistics

First, choose a port which the statistics shall be displayed for. A sample console output is shown in Figure 24.

```
CEA-709 application statistics
==============================

Device                 : CEA-709 (FT)
Node state             : unconfigured (0x02)

Transmission errors    : 0
Transmit TX failures   : 0
Receive TX full        : 0
Lost messages          : 0
Missed messages        : 0
Layer 2 received       : 0
Layer 3 received       : 0
Layer 3 transmitted    : 0
Transmit TX retries    : 0
Backlog overflows      : 0
Late acknowledgments   : 0
Collisions             : 0

Out buffers used       : 0
In buffers used        : 0

TCL active             : 0/0
TSPs used              : 0
TSPs deleted           : 0
No TSP available       : 0

L-Chip read error      : 0
L-Chip write error     : 0

Slow mode used         : 0
Active outgoing        : 0/0
Waiting outgoing       : 0/0
Blocked outgoing       : 0/0
Slow mode outgoing     : 0/0

Authentication failed  : 0
Authentication attempts : 0

Missed preambles       : 0
Packet RCV interrupted : 0
Long packets           : 0
Packet XMT failed      : 0
RCV buffer full        : 0
RCV packet lost        : 0
```

Figure 24: CEA-709 Application Statistics

4.9.3 Option 4 – IP statistics

A sample console output is shown in Figure 25.

```
*********** 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 25: IP Statistics

The IP statistics menu has the additional feature of displaying any IP address conflicts. If the L-Proxy's IP address conflicts with another host on the network, the banner shown in Figure 26 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 26: IP Address Conflict

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

4.9.4 Option 6 – Enhanced Communications Test

This menu item allows testing the communication path between the CEA-852 device of the L-Proxy and other CEA-852 devices on the IP channel. It tests the CEA-852 data communication. This test can be used to determine if there is a working TCP/IP connection as well as a working CEA-852 connection between the individual devices. The test thoroughly examines the paths between individual members and the configuration server in each direction.

A typical console output is shown in Figure 27.

```
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 27: 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 CEA-852 device of the L-Proxy. It is a measure for general network delay. If the test to a specific member fails, a text is displayed to describe the possible source of the problem. The reasons for failure are summarized in Table 4.

A warning **Incorrect NAT configuration detected!** is displayed if the enhanced communications test determines that the CEA-852 device of the L-Proxy 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.

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

Table 4: Possible Communication Problems

4.10 Data Point Menu

The L-Proxy data point menu as shown in Figure 28 allows the user to list data points, get, and set values of the data points. Note that the Console data point UI is kept very simple. For more convenient access to data points, the user may also consult the Web UI (see Section 5.2.6).

```
Data Point Menu
=================================

[1]  Data Points
[2]  Get Value
[3]  Set Value

[q]  Quit without saving

Please choose:
```

Figure 28: L-Proxy Data Point Menu.

4.10.1 Option 1 – List Data Points

Select this option to list all data points on the L-Proxy. The list is flat and displays the values and status of each data point. An example is shown in Figure 29.

```
Data Points:
----------------------------------------
CEA709 Port: (node)
NV_node1Ctrlnvi17state_bit0: invalid value (input) invalid value
NV_node1Ctrlnvo16state_bit0: 0 (output)
NV_node1Ctrlnvi15fire_test: invalid value (input) invalid value
NV_node1Ctrlnvo14fire_test: 2 (output)
NV_node1Ctrlnvi13amp: invalid value (input) invalid value
NV_node1Ctrlnvo12amp: -773.200000 (output)
CEA709 Port: (node)
-> NV_node1Ctrlnvi17state: invalid value (output) inactive
bit0: invalid value (output) invalid value
-> NV_node1Ctrlnvo16state: 8000000000000000 (input) inactive
bit0: 1 (input)
NV_node1Ctrlnvi15fire_test: invalid value (output) invalid value
NV_node1Ctrlnvo14fire_test: 2 (input)
NV_node1Ctrlnvi13amp: invalid value (output) invalid value
NV_node1Ctrlnvo12amp: -773.200000 (input)
```

Figure 29: Example data point listing.

4.10.2 Option 2 – Get Value

This option allows retrieving the value of a specific data point. When selecting this option the user is prompted to enter the complete data point name, e.g., 'NV_node1Ctrlnvi13amp'. Then hit **Enter**.

4.10.3 Option 3 – Set Value

This option allows setting the value of a specific data point. When selecting this option the user is prompted to enter the complete data point name, e.g., 'NV_node1Ctrlnvi13amp'. Then hit **Enter** and enter the desired value when prompted and press **Enter** again.

5 Web Interface

The L-Proxy comes with a built-in Web server and a Web interface to configure the L-Proxy and extract statistics information. The Web interface allows configuring the IP settings, CEA-852 and CEA-709 settings.

5.1 Device Information and Account Management

In a Web browser, enter the default IP address 192.168.1.254 of the L-Proxy. Make sure that the Web server has not been disabled in the console interface (see Section 4.4.4). Note that if your PC has an IP address in a subnet other than 192.168.1.xxx, you must open a command tool and enter the following route command to add a route to the L-Proxy.

To Add a Route to the Device

1. Windows **START → Run...**

2. Enter 'cmd' and click **OK**.

3. In the command window enter the command line
   ```
   route add 192.168.1.254 %COMPUTERNAME%
   ```

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

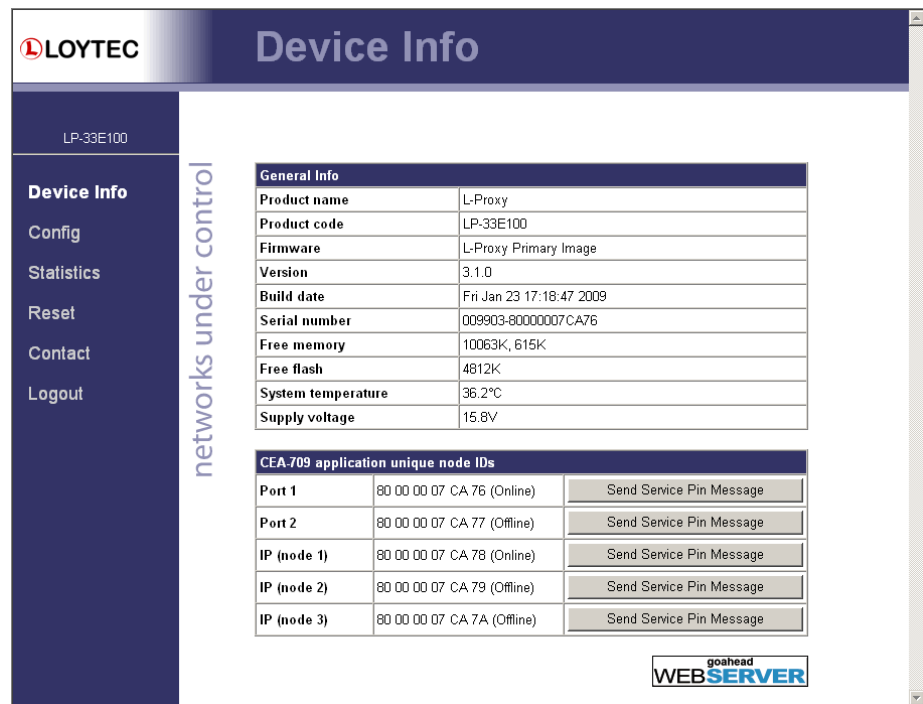5. The device information page should appear as shown in Figure 30.

Figure 30: Device Information Page

The device information page shows information about the L-Proxy and the current firmware version. It includes the unique node IDs ("Neuron IDs") of the CEA-709 network interfaces. This page can also be used to send the CEA-709 service pin messages. This is a useful feature when commissioning the L-Proxy, since it is not necessary to be on-site to press the device's status button.

Click through the menus on the left hand side to become familiar with the different screens. If you click on **Config** in the left menu, you will be asked to enter the administrator password in order to make changes to the settings as shown in Figure 31. Enter the default administrator password 'admin' and select **Login**.
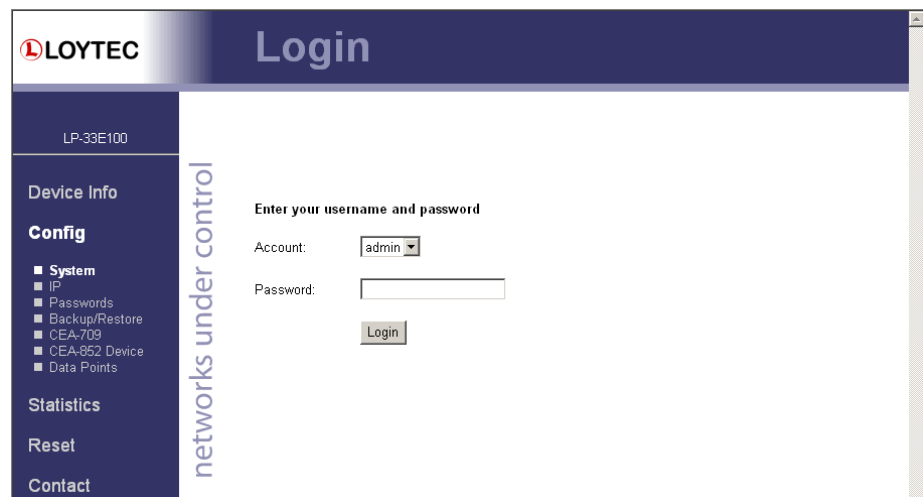
Figure 31: Enter 'admin' as the default administrator password.

The Config menu opens. Click on **Passwords** in the Config menu, which opens the password configuration page as shown in Figure 32. The L-Proxy has three user accounts: (1) **guest** allows the user to view certain information only, e.g., the device info page. By default the guest user has no password. (2) **operator** is able to read more sensible

information such as calendar data. (3) **admin** has full access to the L-Proxy and can make changes to its configuration. Note that the user accounts are also used to log on to the FTP and Telnet server.

Figure 32: Password Configuration Screen

Please change the administrator password in order to protect yourself from unwanted configuration changes by anyone else. To do so, select the **admin** account in the drop-down box and enter the new password. If the administrator password is left empty, password protection is turned off and everyone can access the L-Proxy without entering a password. Click on **Change password** to activate the change.

5.2 Device Configuration

The device configuration pages allow viewing and changing the device settings of the L-Proxy. 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.

5.2.1 System Configuration

The system configuration page is shown in Figure 33. This page allows to configure the L-Proxy's system time. The time sync source can be set to **auto**, **manual**, **NTP**, or **LonMark**. In the **auto** mode, the device switches to the first external time source that is discovered. The option **manual** allows setting the time manually in the fields **Local Time** and **Local Date**. In **manual** mode, the device does not switch to an external time source. Note, that if **NTP** is selected, the NTP servers have to be configured in the IP Configuration page (see Section 5.2.2).

The time zone offset must be defined independently of the time source. It is specified as the offset to GMT in hours and minutes (e.g., Vienna/Austria is +01:00, New York/USA is -06:00). For setting the daylight saving time (DST) predefined choices are offered for Europe and USA/Canada. DST can be switched off completely by choosing **none** or set manually for other regions. In that case, start and end date of DST must be entered in the fields below.

Figure 33: System Configuration Page, e.g., for Vienna, Austria

The next section on the page allows configuring the L-Proxy's earth position. This setting defines the longitude, latitude and elevation of the device. The latitude and longitude are entered as degrees, minutes, and seconds. The altitude is entered in meters height above sea level. This setting is used for an astronomical clock. For fixed locations such as a building, the position can be entered on this page.

The FTP server can be enabled and disabled and the FTP server port can be configured. The FTP server is used for instance to update the firmware (see Section 11.1) or to upload a new data point configuration. Further, the Web server port and the delimiter for CSV files can be configured. Note that the Web server can only be disabled on the console interface.

5.2.2 IP Configuration

Figure 34 shows the IP configuration page with DHCP disabled, while Figure 35 shows the IP configuration page with DHCP enabled. The mandatory IP settings, which are needed to operate the device, are marked with a red asterisk (IP address, netmask, gateway). The **Enable DHCP** checkbox switches between manual entry of the IP address, netmask, and gateway address, and automatic configuration from a DHCP server.

Hostname and **Domainname** are optional entries and can be left empty. For some DHCP configurations it may be necessary to enter a hostname. Please contact your system

administrator on how to configure DHCP to acquire an IP address. Further, you can configure up to 3 Domain Name Servers. Currently these entries are not used.

Figure 34: IP Configuration Page with DHCP disabled

Figure 35: IP Configuration Page with DHCP enabled

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

The device can be configured to synchronize its clock with NTP time. Enter the IP address of a primary and, optionally, a secondary NTP server. The L-Proxy will use NTP as a time source if the time sync source in the system configuration page is set to **NTP** (see Section 5.2.1). The field **NTP status** below the NTP server settings displays the current NTP synchronization status (**out-of-sync**, or **in-sync**).

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

5.2.3 Backup and Restore

A configuration backup of the L-Proxy device can be downloaded via the Web interface. Press the **Backup/Restore** link as shown in Figure 36 to start the download. The L-Proxy device assembles a single file including all required files. A file requestor dialog allows specifying the location where the backup file shall be stored.

To restore the device settings, simply select a previously generated backup file in the **Restore Configuration** section of the page by clicking the button next to the **Filename** field. Then press the **Restore** button.

The backed up configuration data consists of:

•   Device settings (Passwords, IP settings, e-mail config, etc.),

•   Data point configuration,
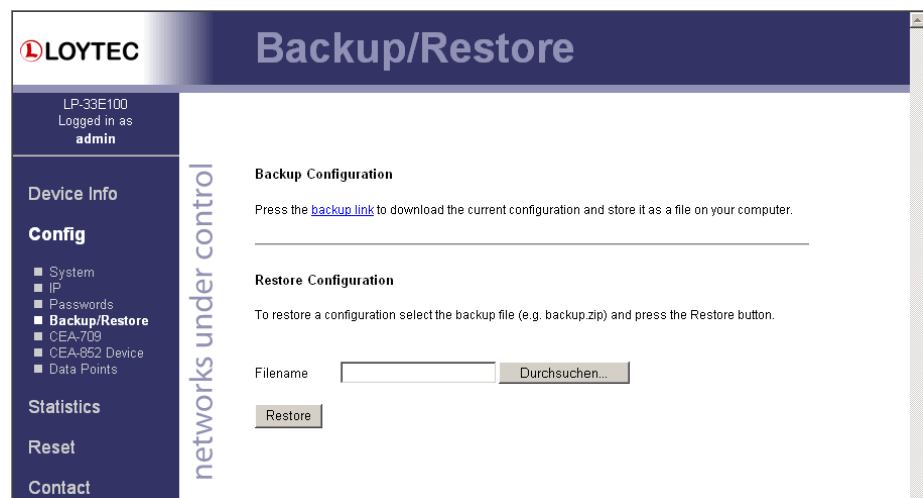
•   CEA-709 binding information.

Figure 36: Backup/Restore page.

5.2.4 CEA-709 Configuration

On the CEA-709 configuration page (shown in Figure 37) the user can view the L-Proxy's port and transceiver settings. Currently, there is nothing to configure.
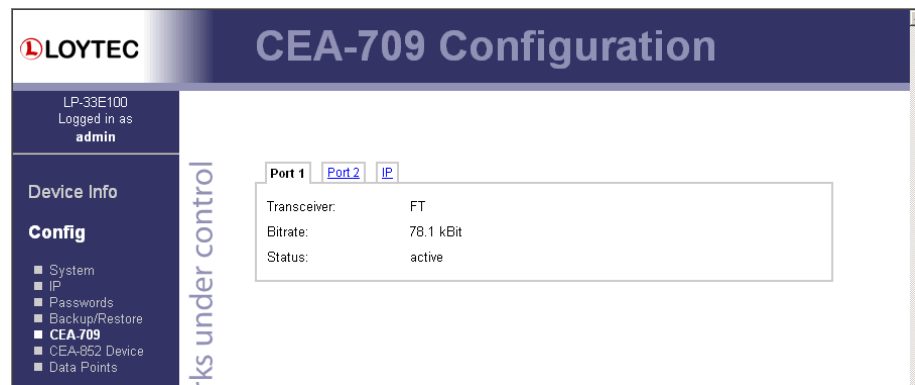
Figure 37: CEA-709 Configuration Page.

5.2.5 CEA-852 Device Configuration

The CEA-852 device of the L-Proxy can be configured in the CEA-852 device configuration page, which is depicted in Figure 38. Typically, the L-Proxy is added to an IP channel by entering the relevant information on a configuration server. The configuration server then contacts the CEA-852 device of the L-Proxy and sends its configuration.

The field **Config server address** and **Config server port** display the IP address and port of the configuration server, which manages the L-Proxy and the IP channel. The field **Config client port** represents the IP port of the L-Proxy's CEA-852 device. This setting should be left at its default (1628) unless there are more than one CEA-852 devices operating behind a single NAT router. Please refer to the L-IP User Manual [1] to learn more about NAT configuration.

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

The **Channel mode** field reflects the current channel mode of the CEA-852 device. It is configured by the configuration server. If there are any two devices in the channel which use the same IP address but different ports (e.g., multiple L-Proxy behind one NAT router) the channel switches to **Extended NAT mode**. Please refer to the L-IP User Manual [1] to learn more about configuring the Extended NAT mode in the configuration server.

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

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

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

The field **MD5 authentication** enables or disables MD5 authentication. Note that MD5 authentication cannot be used together with the Echelon's *i*.LON 1000 since the *i*.LON 1000 is not fully compliant with the CEA-852 authentication method. MD5 can be used with the *i*.LON 600. In the following field **MD5 secret** enter the 16-byte MD5 secret. Note that for security purposes the active MD5 secret is not displayed. You may enter the 16 bytes as one string or with spaces between each byte,

e.g., 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.

Also note that entering the MD5 secret on the Web interface may pose a security risk. Since the information is transmitted over the network it can be subject for eavesdroppers on the line. It is recommended to either use a cross-over cable or enter the secret on the console UI (see Section 4.7).

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

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

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

Figure 38: CEA-852 Device Configuration Page.

5.2.6 Data Points

The device's Web interface provides a data point page, which lists all configured data points on the device. An example is shown in Figure 39. The data point page contains a tree view. Clicking on a particular tree item fills the right part of the page with a data point list of that tree level and all levels below. Thus, one can get an easy overview of all data points.

The data point list displays the data point name, direction, type, current value, and data point state. Inactive points are displayed in gray. If the data point list does not fit on one page, there are page enumerator links at the bottom. Important data point states and their implications are listed in Table 5.
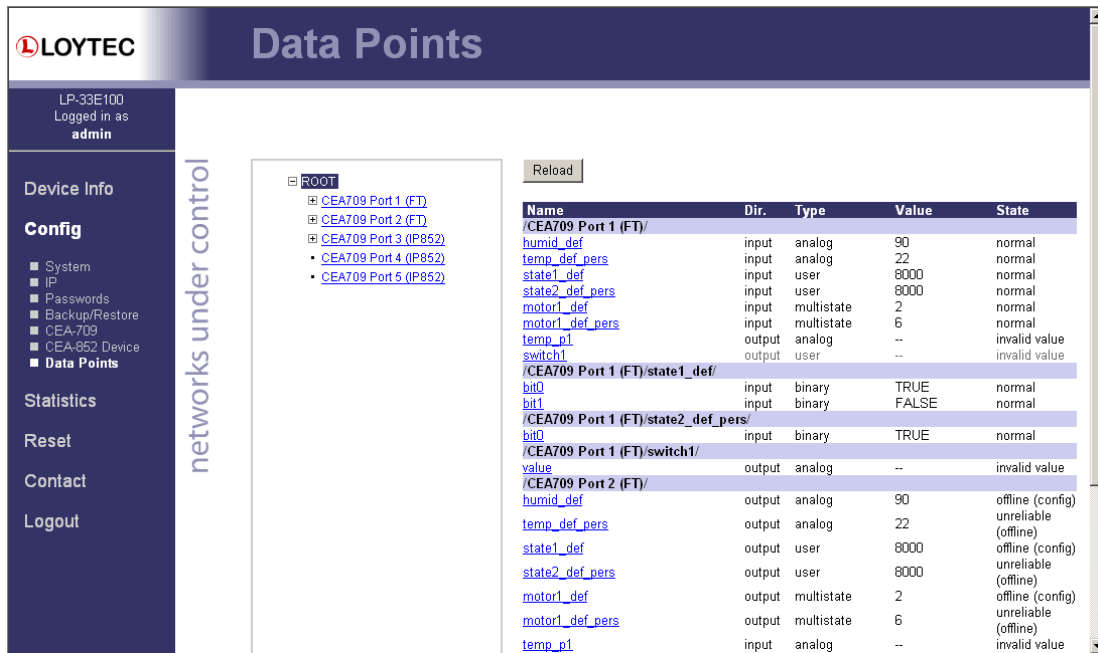
Figure 39: Data point page

Data Point Status	Description
normal	The data point is in normal operation state and possesses a value.
invalid value	The data point has no valid value.
offline (config)	The data point has a value but it is not reflected on the network due to a configuration error (not commissioned, no binding, no client mapping, etc.)
offline	The data point has a value but it is not reflected on the network due to a communication error (e.g., the peer node is not online).
unreliable (offline)	The data point has a value but it is considered unreliable because it was derived from a source, which was offline (e.g., the value was fed from a connection, where the source is offline).
unreliable (range)	The data point has a value but it is considered unreliable because the value source specified an out-of-range value. The value is limited to the supported range.
unreliable	The data point has a value but it is considered unreliable for an unspecified reason.
not configured	The data point is mapped to a port, which is not configured (e.g., the port is disabled).
Line grayed-out	The data point is inactive. Values can be written but no network communication is triggered. This can be the case, if a data point is not used in the configuration or it is connected to a dynamic NV, which is not present on the device.

Table 5: Data Point States

The data point names are links. Clicking on such a link opens a detailed page on that data point. If the data point supports it, the user can also enter a new data point value as depicted in Figure 40. The status field is discussed in Table 5. The flags, pollcycle, min/max send time and max age fields are the common timing parameters for the data point. See Section 6.3.2 for a closer discussion on timing parameters.

Figure 40: Data point details page.

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

- **Successfully set value**: The new value has been successfully set in the data point and the update has been sent on the network, if it is a network data point.

- **Could not send value update**: The new value has been set but it has not been sent out on the network. The reason can be that the peer node is currently offline or there is a configuration error. The data point status reflects this error.

- **Could not set value (error code)**: The new value has not been set because of an internal error. Please contact LOYTEC with the error code.

5.3 Device Statistics

The device statistics pages provide advanced statistics information about the CEA-709 device, the CEA-852 device, the System Log, and the Ethernet interface.

5.3.1 IP Statistics

Figure 41 shows the IP statistics page. It allows finding possible problems related to the IP communication. Specifically, any detected IP address conflicts are displayed (if the L-Proxy's IP address conflicts with a different host on the network).
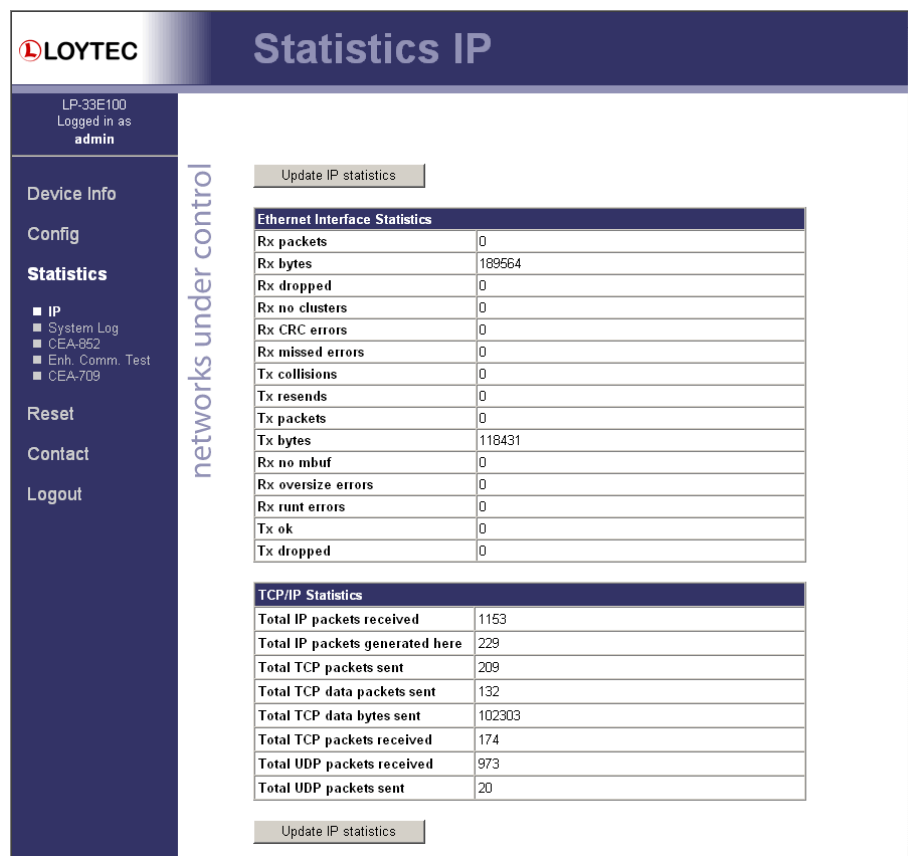
Figure 41: IP Statistics Page

5.3.2 CEA-852 Statistics

The CEA-852 statistics page displays the statistics data of the CEA-852 device on the L-Proxy. It is only displayed if the CEA-852 interface is enabled. The contents are the same as available through the console UI (see Section 4.9.1). The upper part of the CEA-852 statistics page is depicted in Figure 42. To update the statistics data, press the button **Update all CEA-852 statistics**. To reset all statistics counters to zero, click on the button **Clear all CEA-852 statistics**. The field **Date/Time of clear** will reflect the time of the last counter reset.
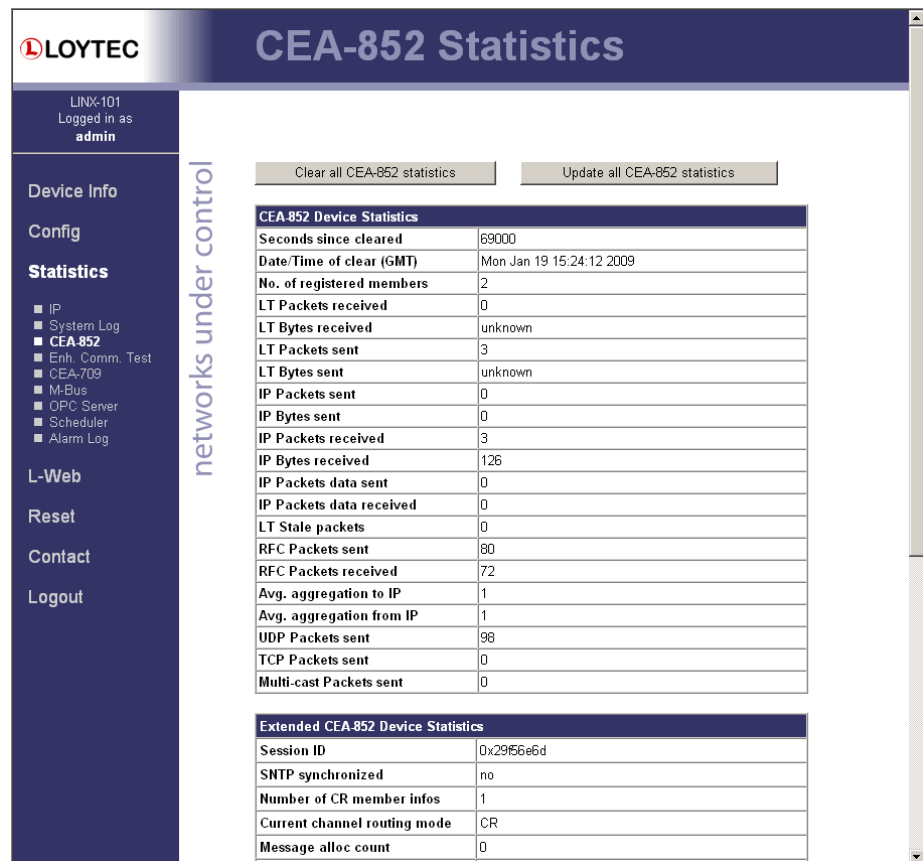
Figure 42: Part of the CEA-852 Statistics Page

5.3.3 Enhanced Communications Test

The Enhanced Communications Test allows testing the CEA-852 communication path between the CEA-852 device on the L-Proxy and other CEA-852 devices as well as the configuration server. The test thoroughly diagnoses the paths between individual members of the IP channel and the configuration server in each direction. Port-forwarding problems are recognized. For older devices or devices by other manufacturers, which do not support the enhanced test features, the test passes as soon as a device is reachable, but adds a comment, that the return path could not be tested. A typical output is shown in Figure 43.
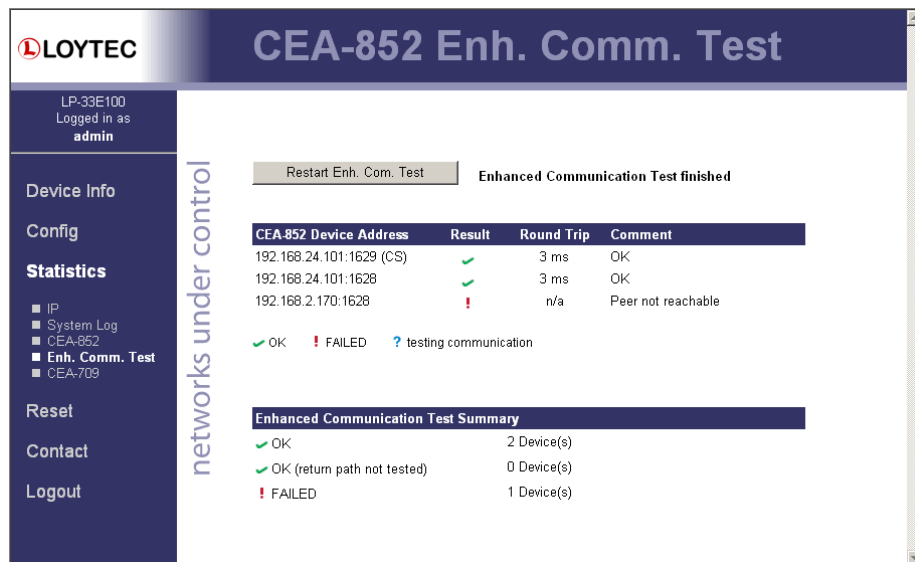
Figure 43: Enhanced Communication Test Output

The Round Trip Time (RTT) is measured as the time a packet sent to the peer device needs to be routed back to the L-Proxy. It is a measure for general network delay. If the test to a specific member fails, a text is displayed to describe the possible source of the problem. The reasons for failure are summarized in Table 4.

5.3.4 CEA-709 Statistics

The CEA-709 statistics page displays statistics data of the CEA-709 port on the L-Proxy as shown in Figure 44. This data can be used to troubleshoot networking problems. To update the data, click on the button **Update CEA-709 statistics**.
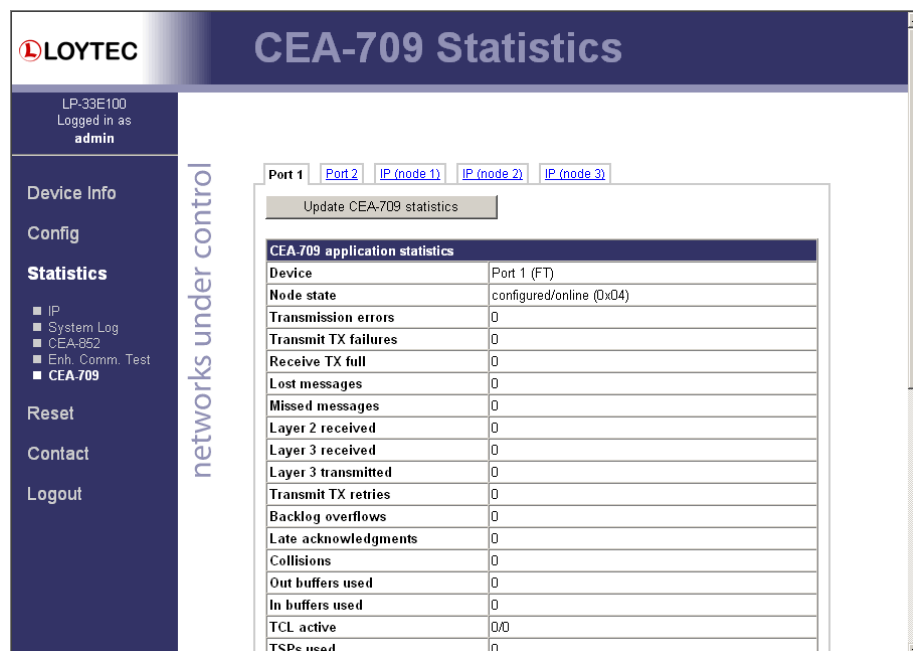
Figure 44: CEA-709 Statistics Page

5.3.5 System Log

The System Log page prints all messages stored in the system log of the L-Proxy. An example is shown in Figure 45. This log data is important for trouble-shooting. It contains

log entries for reboots and abnormal operating conditions. When contacting LOYTEC support, have a copy of this log ready.
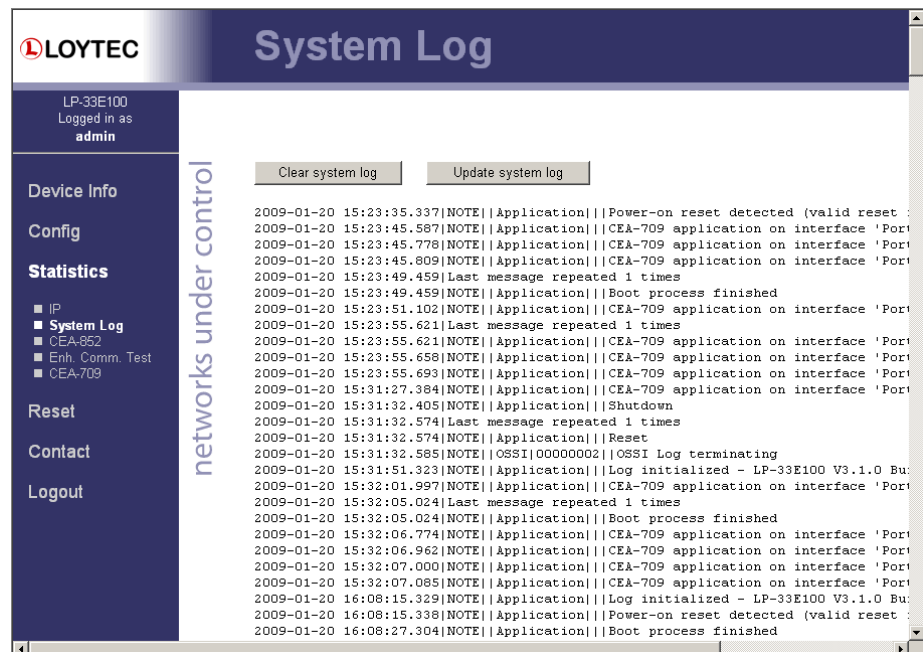
Figure 45: System Log Page

5.4 Reset, Contact, Logout

The menu item **Reset** allows two essential operations:

- Rebooting the L-Proxy from a remote location, or

- reset the data point configuration from a remote location (see also Section 4.8.3). This option clears all data points and the entire port configuration. It leaves the IP settings intact.

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 Concepts

6.1 What is a Proxy?

Webster's Revised Unabridged Dictionary (1913) lists the following entries for *Proxy*:

Proxy \Prox"y\, n.; pl. Proxies. [Contr. from procuracy. Cf. Proctor.]

1. The agency for another who acts through the agent; authority to act for another, esp. to vote in a legislative or corporate capacity.

2. The person who is substituted or deputed to act or vote for another.

3. A writing by which one person authorizes another to vote in his stead, as in a corporation meeting.

The L-Proxy follows this definition. It acts on behalf of somebody else. For L-Proxy the "somebody else" is another node in the network. As shown in Figure 46 the L-Proxy hardware offers 3 physical network ports, two FT and one IP-852, which represent 5 individual nodes, one on each FT port and three on the IP-852 port. One can think of L-Proxy as being 5 individual nodes that are somehow internally connected. Whenever an input network variable on L-Proxy is being updated, L-Proxy updates a corresponding output network variable. Also if a network variable poll is received on the output network variable this poll can be forwarded to the input network variable. It doesn't matter if the output network is on the same node or on one of the other four nodes as the input network variable. Since the 5 nodes can be configured in different domains, it is now possible to bind network variables across domains.

Figure 46: L-Proxy offers five network ports, which represent 5 individual nodes.

We have listed use cases for L-Proxy that are typical in network installations. We use these use cases to explain the fundamental operation of L-Proxy. Remember that input and output network variables can reside on the same node or different nodes, in the same domain or in different domains. The behavior of L-Proxy is always the same.

6.1.1 Update-Update Use Case

Figure 47 shows an Update-Update use case. In this use case the input network variable of the L-Proxy is bound to an output network variable of Node 1. This output network variable is periodically updated. On the output side of L-Proxy the corresponding output network variable is also bound to an input network variable on Node 2, which is waiting for updates.

Figure 47: Update-Update use case

6.1.2 Poll-Poll Use Case

Figure 48 shows a Poll-Poll use case. In this use case the input network variable of L-Proxy is bound to an output network variable of Node 1. However, this output network variable on Node 1 is declared polled and never updated. Hence, Node 1 waits for incoming polls. On the output side of L-Proxy the corresponding output network variable is not bound. Node 2 periodically polls this network variable.

Figure 48: Poll-Poll use case

6.1.3 Update-Poll Use Case

Figure 49 shows an Update-Poll use case. In this use case the input network variable on L-Proxy is bound to an output network variable on Node 1. This output network variable on Node 1 is periodically updated. On the output side of L-Proxy the corresponding output network variable is not bound. Node 2 periodically polls this network variable.

Figure 49: Update-Poll use case

6.1.4 Poll-Update Use Case (Active Poll)

Figure 50 shows a Poll-Update use case. In this use case the input network variable on L-Proxy is bound to an output network variable on Node 1. However, this output network variable on Node 1 is declared polled and never updated; Node 1 waits for incoming polls. On the output side of L-Proxy the corresponding output network variable is bound to an

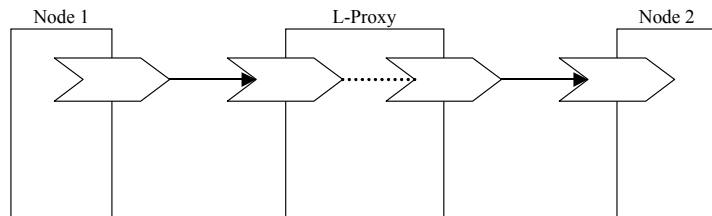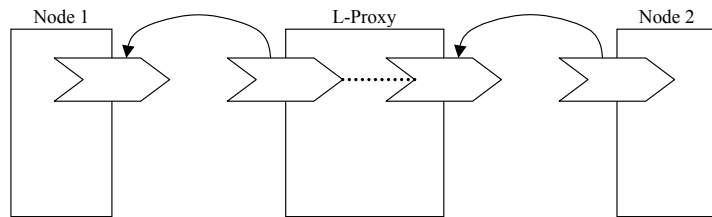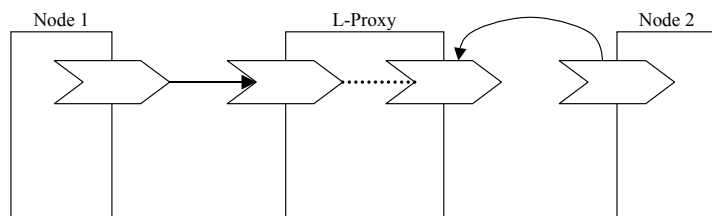input network variable on Node 2, which is waiting for updates. This use case is also called active poll use case since L-Proxy actively polls the output network variable on Node 1.
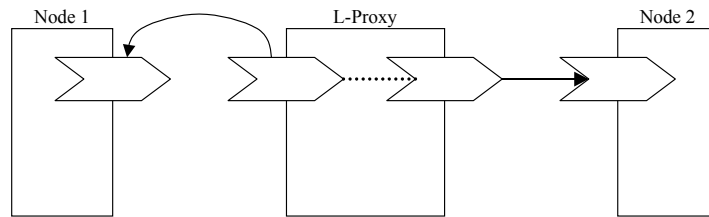
Figure 50: Poll-Update use case (active poll).

6.1.5 Use Case Combinations

There can be combinations of the different use cases. An example where Update-Update and Update-Poll are combined for one NV is shown in Figure 51. On the input side of L-Proxy an output NV is bound to the input NV of L-Proxy. Updates are received periodically. On the output side of L-Proxy an input network variable on Node 2 is bound to the output NV on L-Proxy (Update-Update use case). Further, an OPC server polls the same output NV periodically (Update-Poll use case).
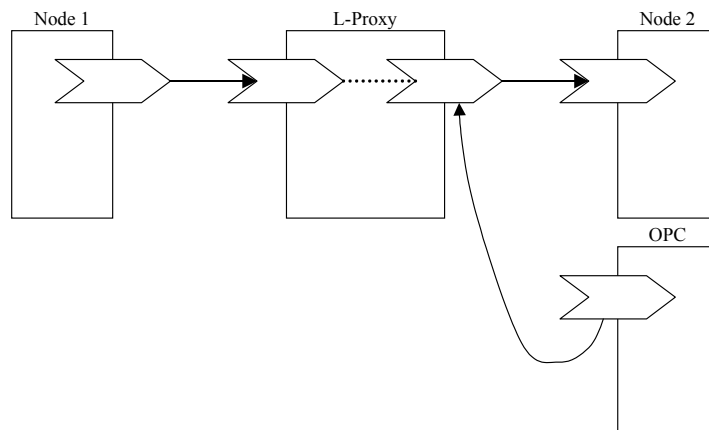
Figure 51: Combination of two basic use cases Update-Update and Update-Poll.

Another possible example for such a combination (Update-Update and Update-Poll) is shown in Figure 52. This use case is a variation of the Update-Update use case. The only difference is, that Node 2 does not wait for the first update to arrive after power-up or reset. Rather, it polls for an initial value after it was started and waits for updates thereafter.
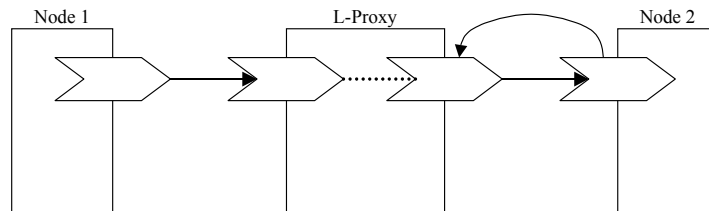
Figure 52: Combination where Node 2 gets an initial value through polling.

6.1.6 Poll Cache

If Node 2 doesn't receive network variable updates from the source node (Node 1) but rather polls Node 1 to update its input network variables, L-Proxy supports different network variable caching strategies in order to support a wide variety of desired behaviors.

Figure 53 shows the network variable *cache* memory inside L-Proxy. The cache can be used in different operating modes.

Figure 53: Poll cache inside L-Proxy. The cache is updated with every NV update and every poll response.

6.1.6.1 Passive Poll

Passive poll means that polling a network variable on Node 1 (see Figure 53) is always initiated by the destination node (Node 2) and never by L-Proxy itself. The behavior of this mode can be configured by the *maximum cache age* property, while having the *pollcycle* property set to zero. There are the following choices (a summary is given in Table 6):
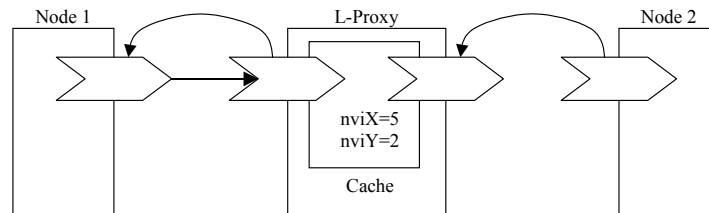
No Cache: Polls from Node 2 are directly forwarded to Node 1. A poll response is sent to Node 2 after the poll response was received from Node 1. If Node 1 doesn't respond to the poll request also L-Proxy doesn't respond to the poll request from Node 2. This behavior can be used to detect "dead" (not responding) nodes. This mode is typically used in poll-poll or update-update use cases. You can configure this behavior by setting "maximum cache age" to zero.

Poll on Startup: Polls from Node 2 are never forwarded to Node 1 except after power-up when the cache value is not valid. The cache content is updated with network variable updates (no polls) from Node 1. Only after power-up of L-Proxy, when the cache entry is not valid, L-Proxy will try to poll Node 1 until a valid value is received and stored in the cache. This behavior can be achieved by setting "maximum cache age" to '-1' and setting the "poll on startup" option to "yes".

Enable: The cache is enabled and a timeout in seconds must be specified. If the value in the cache is current (cache timeout has not expired since last update) the poll request from Node 2 reads the value from the cache. If the cache is expired the poll request from Node 2 will be forwarded to Node 1 and the L-Proxy will not respond to Node 2 until the poll response from Node 1 has been received. This mode can be used to detect dead nodes while keeping the network traffic low. For this mode *maximum age* must be set to the desired cache timeout value.

Behavior	Pollcycle	Poll-on-Startup	Max Cache Age
Passive Poll, no cache	0	No	0
Passive Poll, poll-on-startup	0	Yes	-1
Passive Poll, cache	0	No	>0
Active Poll, forward polls	>0	No	0
Active Poll, value from last poll cycle	>0	No	-1

Table 6: Timing Parameters.

6.1.6.2 Active Poll

Active poll means that L-Proxy actively polls the source node (Node 1) periodically at a specified poll rate. If in addition to the active polls from L-Proxy the destination node (Node 2) or some other node polls the source node (Node) 1, L-Proxy supports two strategies. This mode can be configured by setting the "poll cycle" property to the desired interval between the periodic polls and change the "maximum cache age" property to achieve one of the following behaviors (a summary is given in Table 6):

Forward polls: The poll request from Node 2 is interleaved with the active polls from L-Proxy in order to update the cache value right away. The poll response is sent to Node 2 after the poll response has been received from Node 1. This mode is configured by setting the "maximum cache age" property to zero.

Use value from last poll cycle: The poll request from Node 2 returns the current value from the cache (last active poll cycle). The cache value is not updated. This mode is configured by setting the maximum cache age property to '-1'.

Active polls can be used if a node cannot send updates (e. g. electrics meter) and the destination node (e. g. SCADA system) cannot poll a value. L-Proxy can then periodically poll the electric meter and send an NV update to the SCADA system.

6.1.6.3 Poll Strategy for Multiple Input Network Variables

In the case that multiple input network variables are connected to an output NV, the first input network variable in the connection is trying to send out a poll. In case this input NV is not configured for polling no poll will be sent out.

In the example in Figure 54 the poll request would only be forwarded to Node 1.
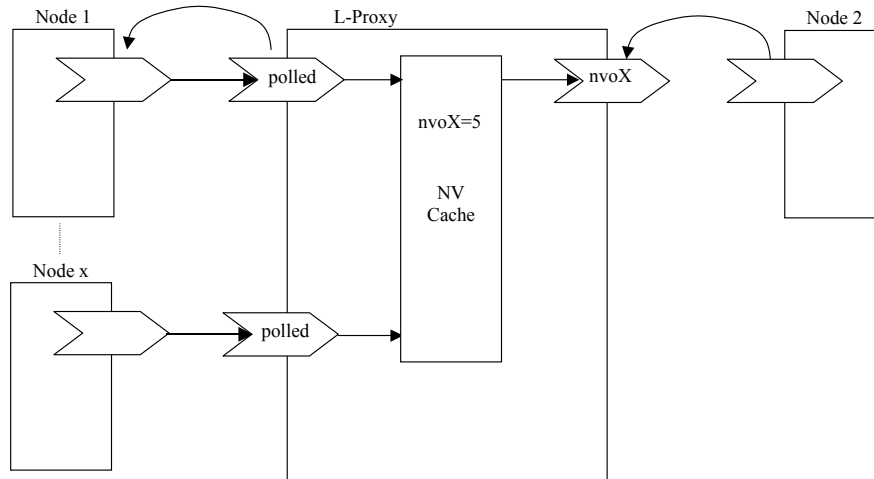
Figure 54 The first input NV with the polled attribute set updates the cache value.

6.1.7 SNVT Conversion

The L-Proxy starting with firmware version 3.0 supports automatic SNVT conversion for scalar types. In general there are the following requirements for SNVT conversion:

1. **Integer to Float conversion (I2F/F2I)**: This conversion type converts an integer value (signed or unsigned) to a float value (signed or unsigned) or vice versa. The type of both values must be a SNVT with the same SI unit (e.g. SNVT_temp to SNVT_temp_f).

2. **Integer to Integer conversion (I2I)**: This conversion type converts an integer value (signed or unsigned) to another integer value (signed or unsigned) or vice versa. The type of both values must be a SNVT with the same SI unit (e.g. SNVT_temp to SNVT_temp_p).

3. **Enumeration conversion:** This type converts one enumeration value to another enumeration value. If the value is outside the range of the target enumeration, the value is set to the first value of the target enumeration, which typically is the "invalid"-value.

4. **Structure conversion**: This type converts one or more structure values to one or more other structure values (e.g. multiple SNVT_switch to a single SNVT_state).

6.2 Network Interfaces on the L-Proxy

The L-Proxy as a physical device has 5 network ports. Port 1 and port 2 are FT-10 ports, port 3 through 5 are IP-852 ports. The FT-10 ports are physically available on terminals 1 through 6 (see Section 3.7) and can be connected to two separate FT-10 channels.

In the LNS database each L-Proxy port corresponds to a single device in the LNS database. These devices can be part of the same database (same domain) or live in different databases (different domains). Figure 55 shows an example in which all five ports of one physical L-Proxy are represented as separate devices in the same LNS database.

The three IP-852 ports deserve more explanation. They are logical ports on the physical Ethernet interface of the L-Proxy and connect to a single IP-852 channel. This means, that the L-Proxy is added as a single CEA-852 device to the configuration server (see Section 4.3.6). In the LNS database they are treated as three separate devices, with three different Node IDs. This means, that each of the IP-852 ports has to be added to an LNS database separately. Figure 55 depicts this situation for Port 3 to 5.
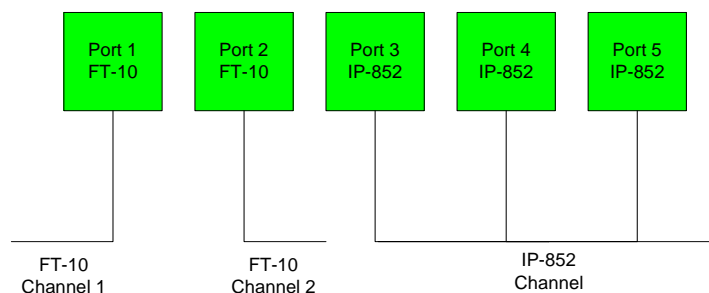

Figure 55: FT-10 and IP-852 ports on the L-Proxy

The IP-852 ports connected to the IP-852 backbone channel can be converted to more FT-10 channels in combination with CEA-852 routers such as the L-IP. Figure 56 shows a network diagram to illustrate this concept. Domains 2, 3, and 4 are attached via L-IPs to the L-Proxy's IP-852 ports.
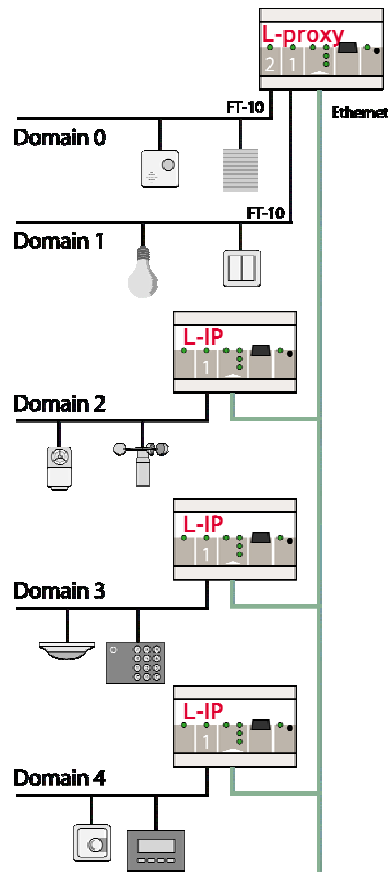
Figure 56: Connecting the IP-852 ports to other channels using L-IPs.

6.3 Data Points

6.3.1 Overview

Data points are part of the fundamental device concept to model process data. A data point is the basic input/output element on the device. Each data point has a value, a data type, a direction, and a set of meta-data describing the value in a semantic context. Each data point also has a name and a description. The entire set of data points is organized in a hierarchy.

At the data point level, the specific technological restrictions are abstracted and hidden from the user. Working with different technologies at this level involves common workflows for all supported technologies.

The direction of a data point is defined as the "network view" of the data flow. This means, an input data point obtains data from the network. An output data point sends data to the network. This is an important convention to remember as different technologies may define other direction semantics.

The basic classes of data points are:

- **Analog**: An *analog* data point typically represents a scalar value. The associated data type is a *double precision* machine variable. Meta-data for analog data points include information such as value range, engineering units, precision, and resolution.

- **Binary**: A *binary* data point contains a Boolean value. Meta-data for binary data points includes human-readable labels for the Boolean states (i.e., active and inactive texts).

- **Multi-state**: A *multi-state* data point represents a discrete set of states. The associated data type is a signed integer machine variable. Each state is identified by an integer value, the *state ID*. State IDs need not be consecutive. Meta-data of a multi-state data point includes human-readable descriptions for the individual states (state texts) and the number of available states.

- **String**: A *string* data point contains a variable-length string. The associated data type is a character string. International character sets are encoded in UTF-8. A string data point does not include any other meta-data.

- **User**: A *user* data points contains un-interpreted, user-defined data. The data is stored as a byte array. A user data point does not include any other meta-data. This type of data point also serves as a container for otherwise structured data points and represents the entirety of the structure.

6.3.2 Timing Parameters

Apart from the meta-data, data points can be configured with a number of timing parameters. The following properties are available to input or output data points, respectively:

- **Pollcycle** (input): The value is given in seconds, which specifies that this data point periodically polls data from the source.

- **Receive Timeout** (input): This is a variation on the poll cycle. When receive timeout is enabled, the data point actively polls the source unless it receives an update. For example, if poll cycle is set to 10 seconds and an update is received every 5 seconds, no extra polls are sent.

- **Poll-on-startup** (input): If this flag is set, the data point polls the value from the source when the system starts up. Once the value has been read, no further polls are sent unless a poll cycle has been defined.

- **Minimum Send Time** (output): This is the minimum time that elapses between two consecutive updates. If updates are requested more often, they are postponed and the last value is eventually transmitted after the minimum send time. Use this setting to limit the update rate.

- **Maximum Send Time** (output): This is the maximum time without sending an update. If no updates are requested, the last value is transmitted again after the maximum send time. Use this setting to enable a heart-beat feature.

- **Maximum Cache Age** (output): This parameter defines if a received poll request to an output can be answered from the data point cache. Setting it to '0' disables the cache. Then each poll request is repeated to the other side of the connection. Setting it to '-1' sets the cache age to infinite and polls are never forwarded. A value in milliseconds defines that a poll is only forwarded, if the last update to the output is older than this setting. If the polled data point does not respond to a request, the poll request on the primary side is not answered, either.

6.3.3 Default Values

Default values can be defined for data points when needed. The value of a data point will be set to the defined default value, if no other value source initializes the data point. Default values are beneficial, if certain input data points are not used by the network and need a pre-defined value, e.g., for calculations. Default values are overridden by persistent values or values determined by poll-on-startup.

6.3.4 Persistency

Data point values are by default not persistent. This means that their value is lost after a power-on reset. There exist different strategies for initializing data points with an appropriate value after the device has started.

For input data points, the value can be actively polled from the network when starting up. Use the Poll-on-Startup feature for this behavior. Polling the network values has the advantage that intermediate changes on the network are reflected. An input data point can be made persistent, if the last received value shall be available after a power-on reset before a poll-on-startup completes. This can be beneficial, if the remote device is temporarily offline and the last value is considered usable.

For output data points, the value can be restored after starting up by the application. For example, if the output data point's value is determined by an input data point and a math object, or the output data point is in a connection with an input, the input can poll its value on startup. If the output data point has no specific other value source, e.g., it is a configuration parameter set by the user, it can be made *persistent*.

To make a data point persistent, enable the Persistent property of the respective data point. The persistency option is only available for the base data point classes analog, binary, multi-state, string and user. More complex objects such as calendars, schedules, etc., have their own data persistency rules.

For structured data points, only all or none of the structure members can be made persistent. The configuration of the top-level data point, which represents the entire structure, serves as a master switch. Setting the top-level data point to be persistent enables persistency for all sub-data points. Clearing it disables persistency for all sub-data points.

6.3.5 Behavior on Value Changes

The value of a data point can change, if it is written by the application or over the network. For all data points (input and output) the application (connection, user control, etc.) can be notified, when the value is written to. The property **Only notify on COV** defines, whether the notification is done with each write or only if the value changes (change-of-value, COV). If only notify on COV is disabled, writing the same value multiple times will result in multiple notifications.

When the value of an output data point is updated, an update is usually sent out onto the network. The property **Send-On-Delta** decides how the update is reflected on the network. If send-on-delta is inactive, each update of the value is sent. If send-on-delta is active, value changes only are sent. The send-on-delta property is only valid for output data points.

For analog data points, the COV or send-on-delta takes an extra argument, which specifies by what amount the value must change to regard it as a change for action. Both, COV and send-on-delta for analog data points check the **Analog Point COV Increment** property. A change is detected, if the value increment is bigger or equal to the specified increment. If the property is zero, all updates are considered.

6.3.6 Custom Scaling

Custom scaling is applied to all analog data points when they communicate values to or from the network. This feature can be used, if a network data point has engineering units not suitable for the application (e.g., grams instead of kilograms). The scaling is linear and applied in the direction from the network to the application as:

$$A = k\,N + d,$$

where N is the network value, k the *custom scaling factor*, d the *custom scaling offset*, and A the application value. When sending a value to the network, the reverse scaling is applied. If this property is enabled, the analog values are pre-scaled from the technology to the data point. The custom scaling is in addition to any technology-specific scaling factors and can be applied regardless of the network technology.

6.4 Connections

With the use of connections data points can interact with each other. Connections specify which data points exchange values with each other. Both types of connections - "1:*n*" and "*m*:1" connections – are supported. The single data point is referred to as the *hub* data point, whereas the other data points are the *target* data points.

This means, the following connections are possible:

- 1 input data point is connected to *n* output data points,

- *m* inputs data points are connected to 1 output data point.

The most common connection will be the 1:1 connection. This is the type of connection that is auto-generated by the Configurator software. Other types must be created manually in the Configurator.

In the 1:*n* connection the input value is distributed to all n output data points. In the m:1 connection, the most current input value is written to the output data point. When polling the output data point in poll-through mode (maximum cache age is set on the output), the value from the first input data point is polled.

Connections can connect data points of different technologies with each other (also mixed among the target data points) but are restricted to the same class of data points. This means only data points of class *analog* can exchange values within a connection.

For certain classes of data points, additional restrictions exist:

- **Analog**: The value range is capped on the output data points. This means, if the input value in the hub does not fit into the range of an output data point, the value is capped to the biggest or smallest allowed value.

- **Binary**: No special restrictions exist.

- **Multi-state**: Only multi-state data points of an equal number of states can be placed into a connection. The actual state Ids need not be equal. They are ordered and the n-th state is propagated over a connection. For example, the 2nd state on the hub has the state ID '2', while on the target the 2nd state has the state ID '0'.

- **String**: No special restrictions exist.

- **User**: Only user data points of the same length can be placed in a connection.

6.5 CEA-709 Technology

6.5.1 CEA-709 Data Points

Data points in the CEA-709 network are known as network variables (NVs). They have a direction, a name, and a type, known as the standard network variable type (SNVT) or user-defined network variable type (UNVT). In addition to NVs, also configuration properties (CPs) in the CEA-709 network can be accessed as data points. Both standard CP types (SCPTs) and user-defined CP types (UCPTs) are supported.

The typical procedure in configuring the L-Proxy consists of the following steps:

1. Select the data points of the network to be used on the L-Proxy (e.g., select the NVs in the CEA-709 network nodes)

2. Create necessary data points on other ports

3. Select data points and create connections.

The CEA-709 NVs on the L-Proxy can be created in three different ways:

- **Static NV**: For each selected NV on the network there is a static NV created on the L-Proxy. This NV can be bound to the NV on the network. Note that adding static NVs to the L-Proxy results in a change to the default XIF file. The L-Proxy is assigned a new "model number" to reflect this change (see Section 6.5.2). Static NVs are the way to use NVs in non-LNS systems, where NVs shall be bound instead of using polling.

- **Dynamic NV**: For each selected NV on the network there is a dynamic NV created on the L-Proxy. Compared to static NVs, dynamic NVs do not change the XIF interface of the L-Proxy. The dynamic NVs are created by the network management tool. Currently, only LNS-based tools can manage dynamic NVs. As for static NVs, with dynamic NVs it is possible to use bindings instead of polling.

- **External NV**: The selected NVs on the network are treated as external NVs to the L-Proxy. The L-Proxy doesn't create any NVs on the device, but instead uses polling to read from those NVs and explicit updates to write to the NVs. Therefore, no bindings are necessary for external NVs. For input data points using external NVs however, a pollcycle must be configured. If not configured explicitly, a default pollcycle of 10 sec. is chosen. The default pollcycle can be changed in the project settings menu.

Based on the NV the data point is derived from, the following kinds of data points are created:

- Simple NVs that hold only one scalar value, e.g., SNVT_amp: Those kinds on NVs are represented as analog data points. The data points holds the current value, NV scaling factors are applied.

- Simple NVs based on an enumeration, e.g., SNVT_date_day: Enumeration types result in multistate data points. They represent the state of the NV.

- Structured NVs that consists of a number of fields, e.g., SNVT_switch: All structured NVs are represented as user point. That is, the data point is structured similar to the NV it is based on. Beneath the user data point, the individual structure fields are presented as "sub-data points".

For more information on the different types of network variables and their implications please refer to the application note in Section 13.2. For CPs the allocation type "File" is used.

6.5.2 Static Interface Changes

The L-Proxy can be configured to use static NVs. Unlike dynamic NVs, static NVs cannot be created in the network management tool. They are part of the static interface and are usually compiled into the device. When static NVs are used, the L-Proxy changes its static interface and boots with a new one.

Each time the static interface of the L-Proxy changes (i.e., static NVs are added, deleted, or modified), the model number is changed. The model number is the last byte of the program ID. Thus, a change in the static interface results in a change of the program ID and a new device template needs to be created in the network management tool. A new device template usually means that the device has to be deleted and added again in the database. All bindings and dynamic NVs have to be created again for the new device.

When the Configurator software is connected via LNS, it supports the process of changing the device template for the new static interface. It automatically upgrades the device template of the L-Proxy device in the LNS database and restores the previous bindings and dynamic NVs. If the L-Proxy is not configured with an LNS-based tool, this support is not available. The new static interface is only available in a new XIF file or by uploading the

new device template into the database. For more information on the static interface and device templates please refer to the application note in Section 13.2.

If the static interface of the device has been changed because a new configuration has been downloaded outside of the LNS database, the LNS database is out-of-sync with the device. The device appears offline in the LNS database and must be replaced with a new device template that matches the currently active static interface. The Configurator software can detect this situation when connected to the LNS database and provides a method to automatically fix the problem (see Section 7.9.16). As an alternative, the device can be manually deleted from the LNS database and a new device be created by uploading the static interface from the network.

6.5.3 Connections

With regard to the CEA-709 networking technology, it shall be noted that a connection is an internal mapping in the L-Proxy between input and output network variables. A connection always consists of *one* hub network variable and *one or multiple* target network variables. Hub NVs can be input or output network variables. If the hub NV is an input NV, then the target NVs must be output NVs and vice-versa.

Entire NVs, which are user data points, can be put in a connection with other NVs of the same SNVT. This is true for scalar NVs as well as for structured NVs. For example, an nviState64 can be connected to an nvoState64 in one connection. For other applications, single parts of structured NVs can be added to connections according to the rules for data points in connections of Section 6.4.

7 The L-Proxy Configurator

This Chapter gives step-by-step instructions on how to commission L-Proxy, create a data point configuration with input and output network variables, and how to create connections. We show the configuration steps using LonMaker TE but other LNS-based network management tools can be used as well to install and configure the L-Proxy. We also show how to configure the L-Proxy without LNS.

7.1 Installation

7.1.1 Software Installation

The L-Proxy Configurator must be used to setup the data point configuration of the L-Proxy. The Configurator is installed as a plug-in tool for all LNS-based network management tools as well as a stand-alone tool (for systems without LNS).

System requirements:

- LNS 3.1, Service Pack 8 or higher (for LNS mode),

- Windows 2000, Windows XP, Windows 2003 Server, or Windows Vista.

The L-Proxy Configurator can be downloaded from the LOYTEC Web site http://www.loytec.com. When asked for the type of installation, there are two options to choose from. Select **Typical** to install the required program files. Select **Full** to install the LONMARK resource files along with the software. This option is useful, when the system does not have the newest resource files.

7.1.2 Registration as a Plug-In

If the L-Proxy shall be configured using LNS-based tools (e.g., NL200 or LonMaker), the L-Proxy Configurator needs to be registered as an LNS plug-in. In the following, the process is described for LonMaker TE. Otherwise, please refer to the documentation of your network management tool on how to register an LNS plug-in.

To Register in LonMaker TE

1. Open LonMaker and create a new network.

2. Click **Next** until the plug-in registration tab appears in the Network Wizard. Select the **LOYTEC L-Proxy Configurator (Version X.Y)** from the list of **Not Registered** (see Figure 57).
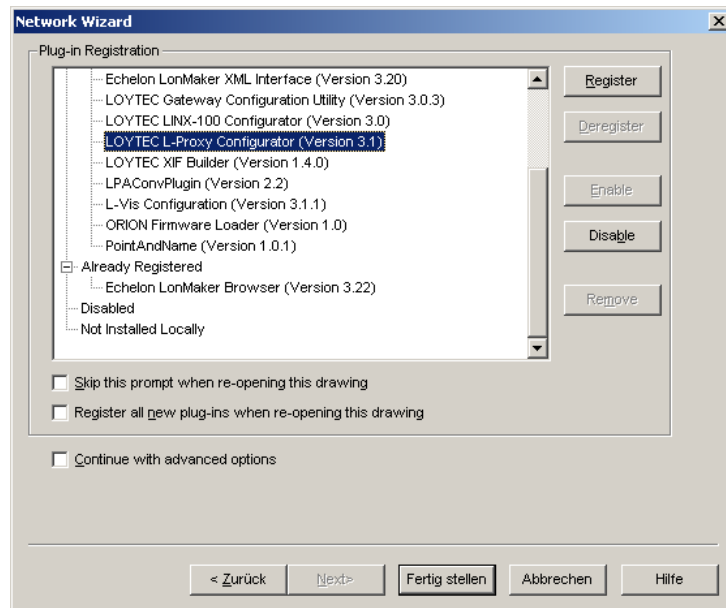
Figure 57: Select the Plug-in to be registered.

3. Click **Register**. The Configurator now appears in the **Pending** list.

4. Click **Finish** to complete the registration. Device templates for the L-Proxy 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.*

5. Under **LonMaker → Network Properties → Plug-In Registration** make sure that the **LOYTEC L-Proxy Configurator (Version X.Y)** shows up under **Already Registered**.
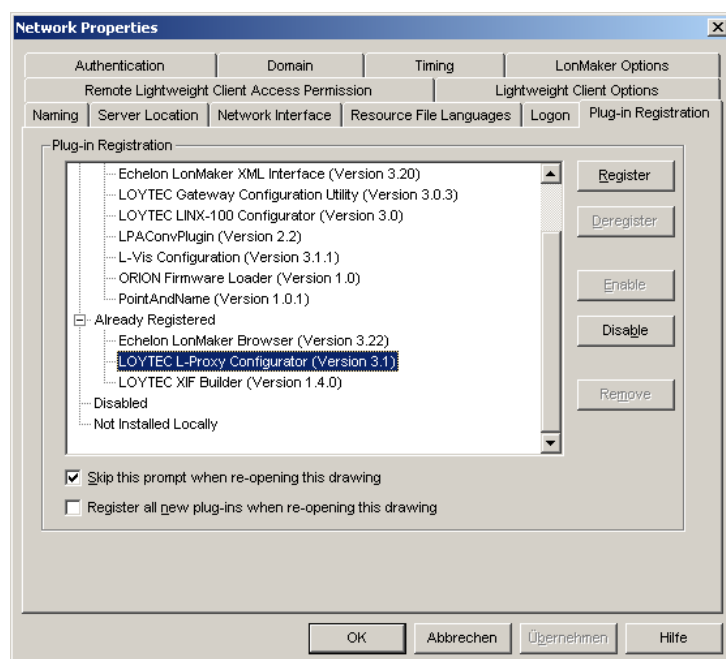
Figure 58: Check that the L-Proxy Configurator is properly registered.

7.1.3 Operating Modes

The Configurator 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 LNS network management software.

- **On-line Mode**: This is the preferred method to use the configuration utility. 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 add the device, commission the device, extract the port interface definition, and download the configuration into the device.

- **Off-line Mode**: In off-line mode, the network management software is not attached to the network or the device is not attached to the network, respectively. This mode can be used to add the device using the device templates, create the port interface definition and to make the internal connections.

- **Stand-alone Mode**: The Configurator can also be executed as a stand-alone program. This mode is useful for the engineer who doesn't want to start the configuration software as a plug-in from within network management software (e.g., NL-220, LonMaker or Alex). Instead the engineer can work directly with the device when online or engineer it offline.

7.1.4 Language Selection

The Configurator software uses the system default language. If the system language is not available, the English language support is enabled. The language support can also be manually changed to the user's preference.

To Change the Language

1. Go to the menu **Settings → Select Language …**.

2. In the dialog choose the preferred language.
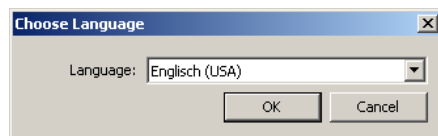
3. Click **OK**.

4. Another dialog prompts the user to restart the Configurator to let the changes take effect. Click **OK** and restart the application.

7.2 Data Point Manager

The Configurator uses a central concept to manage data points. The data point manager is located on the **Datapoints** tab as shown in Figure 59. It is used to select, create, edit and delete data points. The dialog is divided into three sections:

- The folder list (number 1 in Figure 59),

- The data point list (number 2 in Figure 59),
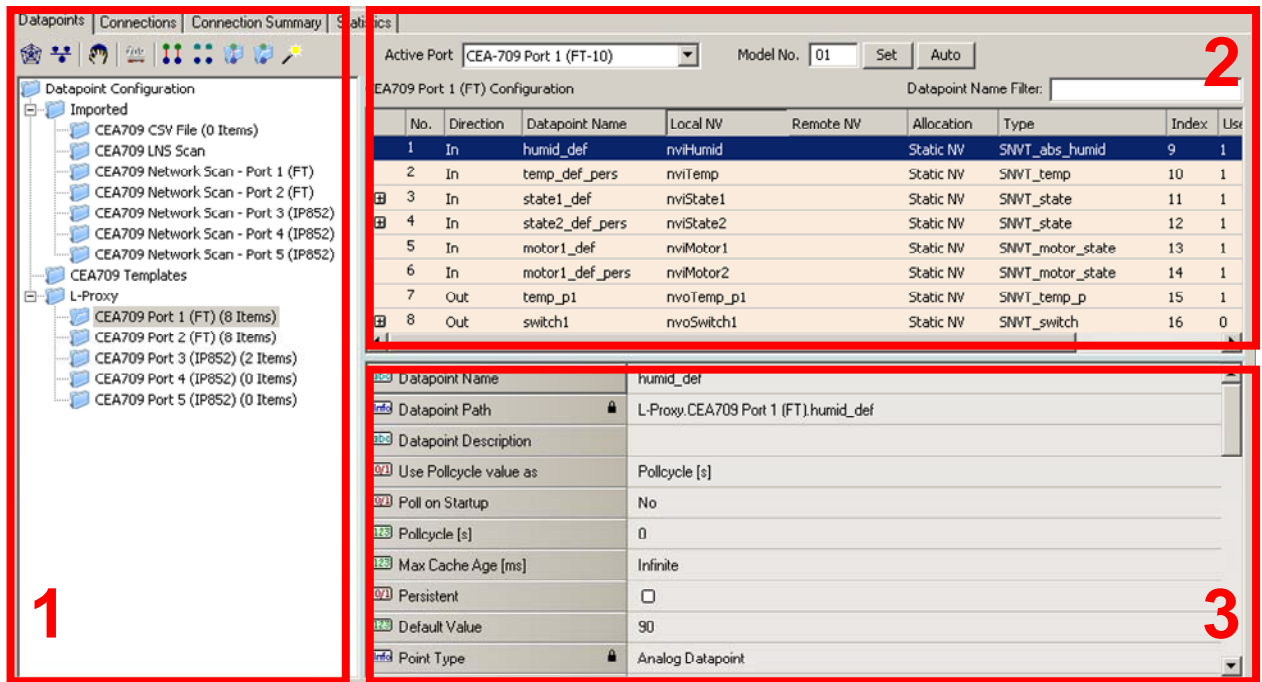
- And a property view (number 3 in Figure 59).

Figure 59: Data Point Manager Dialog

7.2.1 Folder List

At the left is a list of folders which is used to sort the available data objects by their category. There are a number of predefined folders available:

- **Imported**: This folder has a number of sub-folders for different import methods:

  o **CEA709 CSV Import:** This folder is used to display data points imported from CSV files.

  o **CEA709 LNS Database Scan**: This folder is used to hold data retrieved from a network database scan.

  o **CEA709 Network Scan**: This folder holds NVs scanned online from an attached CEA-709 network. For each CEA709 port of the device, there is a separate scan folder.

  Data objects in the import folder are not stored on the device when the project is downloaded. They represent data objects which are available on remote devices and are shown here as templates to create suitable data objects for use on the device by selecting the **Use on Device** option.

- **CEA709 Templates**: This folder contains the created data point templates. They contain a set of properties, which are applied to CEA-709 data points, when they are created on the L-Proxy.

- **L-Proxy**: This is the device folder of the L-Proxy. It contains all the necessary data points which constitute to the L-Proxy's port interface definition. These data points are created on the L-Proxy when the configuration is downloaded. The three subfolders represent

  o **System Registers**: This folder contains system registers, which provide information on the device itself.

  o **User Registers**: This folder holds user-definable registers. These registers are not visible on the underlying network and are intended for internal usage.

  o **CEA-709 Port**: This folder contains local data points, and remote data points of the CEA-709 network technology. For each CEA709 port of the device, there is a separate scan folder.

Using the context menu on a folder, sub-folders may be created to organize the available objects. If new objects are created automatically, they are usually placed in the base folder and can then be moved by the user to any of his sub-folders. Note, that the folder structure described above cannot be changed by adding or deleting folders at that level.

7.2.2 Data Point List

At the top right, a list of all data objects which are available in the selected folder is shown. From this list, objects may be selected (including multi-select) in order to modify some of their properties.

The list can be sorted by clicking on one of the column headers. For example, clicking on the **Direction** column header will sort the list by direction. Other columns display data point name, NV name, and SNVT.

New objects may be created in the selected folder by pressing the **New** button to the right of the list or via the **New** command in the context menu. A plus ⊞ sign in the list indicates that the data point contains sub-points. These can be structure members for structured SNVTs. Clicking on the plus ⊞ sign expands the view.

7.2.3 Property View

When one or multiple data points are selected, the available properties are displayed in the property view. Properties which are read-only are marked with a lock 🔒 sign. When applying multi-select, only those properties common to all selected data points are displayed. Depending on the network technology and data point class, different properties may exist.

Data point properties common to all technologies:

- **Datapoint Name**: This is the technology-independent data point name. This name may be longer than and different to the name of the native communication object (i.e., network variable). Data point names must be unique within a given folder. The maximum length is limited to 64 ASCII characters.

- **Datapoint Path**: This informational property specifies the entire path of the data point within the data point hierarchy. The maximum length is limited to 64 ASCII characters.

- **Datapoint Description**: This is a human-readable description of the data point. There are no special restrictions for a description.

- **Use Pollcycle value as**: For input data points, this property defines whether the input shall use a receive timeout or be constantly polling. See Section 6.3.2.

- **Poll on Startup**: For input data points this property defines, whether the data point shall be polled once at start-up. Poll-on-startup can be enabled independently of the pollcycle. See Section 6.3.2.

- **Pollcycle**: For input data points, this property defines the pollcycle in seconds. Set this property to 0 to disable polling. See Section 6.3.2.

- **Receive Timeout**: For input data points, this property defines the receive timeout in seconds. Set this property to 0 to disable polling. See Section 6.3.2.

- **Min Send**: For output data points, this property defines the min send time in seconds. See Section 6.3.2.

- **Max Send**: For output data points, this property defines the max send time in seconds. See Section 6.3.2.

- **Max Cache Age**: For output data points, this property defines the maximum cache age for poll requests. See Section 6.3.2.

- **Only notify on COV**: This property assists for binary and multi-state input data points. It defines, if a data point shall trigger an update only when the value changes or on every write. If this is enabled, consecutive writes with the same value do not trigger an update. If you want to convey every write, disable COV on the data point.

- **Persistent**: This property defines, if the last written value shall be stored as a persistent value. Persistent data points restore that value after a restart from the persistent storage. See Section 6.3.4.

- **Default Value**: This property defines a default value (see Section 6.3.3). Enter a default value to enable this feature in the data point. Delete the value entirely to remove the default value. If no default value is defined, this property reads "N/A". The default is no default value.

- **Send-on-delta**: For output data points this property defines, if value updates shall be sent only once they meet the COV condition of the data point. For analog data points the analog COV increment is used. If not checked, updates are always transmitted according to min and max send times. See Section 6.3.6.

- **Use Linear Scaling**: If this property is enabled, the analog values are pre-scaled from the technology to the data point. This scaling is in addition to any technology-specific scaling factors. If enabled, the properties **Custom Scaling Factor** and **Custom Scaling Offset** accept the scaling factors. See Section 6.3.6.

- **Custom Scaling Factor, Custom Scaling Offset**: These properties only exist, if linear scaling is enabled. They apply to analog data points only. See Section 6.3.6.

- **Point Type**: This is the base data point type, e.g., "Analog Datapoint".

- **Direction**: This is the data point direction. Use input or output as directions.

- **Unit Text**: For analog data points this property contains a human-readable text for the engineering units of the scalar value, e.g., "kilogram".

- **Analog Datapoint Max Value**: For analog data points this property contains the upper limit of the supported value range. Note that this does not define an alarm limit.

- **Analog Datapoint Min Value**: For analog data points this property contains the lower limit of the supported value range. Note that this does not define an alarm limit.

- **Analog Datapoint Precision**: For analog data points this property defines the number of decimals. '0' specifies an integer value. Display units may use this to format the floating point value accordingly.

- **Analog Datapoint Resolution**: For analog data points this property defines the smallest possible value increment.

- **Analog Point COV Increment**: This property is valid for analog input data points. It specifies by which amount the value needs to change, before an update is generated. If every write shall generate an update even when the value does not change, specify 0 as the COV increment.

- **Active Text**: For binary data points this property defines a human-readable text for the active state (true).

- **Inactive Text**: For binary data points this property defines a human-readable text for the inactive state (false).

- **State Count**: For multi-state data points this property defines the number of discrete states.

- **State Text**: For multi-state data points this property defines a human-readable state label for each state.

7.2.4 CEA-709 Properties

Apart from the common data point properties discussed in Section 7.2.3 the data points of the CEA-709 technology have additional properties. Depending on if a NV is local or external (remote), the properties may vary,

- **NV Allocation**: This property defines how a data point shall be allocated on the device. Choices are "Static NV", "Dynamic NV", and "External NV". If the allocation type cannot be changed, this property is locked.

- **SNVT**: This property defines the SNVT of the NV, e.g., "lux (79)".

- **Invalid Value**: This property defines the "invalid value" for the NV. If set, this specific value will be interpreted as "invalid" in the data point. If known by the SNVT, the invalid value is filled in. Otherwise, the user can specify an invalid value.

- **CEA-709 Mapping Information**: This information is derived from the SNVT. It defines how the NV contents are mapped to the data point.

- **NV Scaling A, B, C**: These are the scaling factors known from the SNVT table. The scaling factors are applied to translate a raw NV value into the scalar representation of the data point.

- **Data Type**: This is the basic NV data type. This is usually filled in from the SNVT definition.

- **Local NV Member Index**: This property specifies the NV member index within a given functional block. This must be a unique index in the functional block, which identifies the NV after other NVs have been added or removed from the interface.

- **Local/Remote NV Index**: This property specifies the NV index. For local, static NVs this is the NV index of the static NV. For external NVs, this is the NV index of the NV on the remote device.

- **Local/Remote NV Name**: This property specifies the programmatic name of the NV. For local, static NVs this is the programmatic name of the static NV. For external NVs, this is the programmatic name of the NV on the remote device.

- **Local/Remote Functional Block**: This property specifies the programmatic name of the NV. For local, static NVs, one of the reserved functional blocks can be selected.

- **Local/Remote NV Flags**: This property specifies the NV flags. For local (static or dynamic) NVs, the flags can be configured. For external NVs, these flags are only informational.

- **Remove NV Information**: For external NVs, this property contains the information on the remote device and the NV selector on that device.

- **Remote Device ID**: For external NVs, this property contains information on the remote device by listing the program ID and location string.

- **Remote Device Address**: For external NVs, this property contains the CEA-709 network addressing information to access the node, i.e., subnet, node, and NID.

- **Retry Count**: For external NVs, this property defines the retry count. The default is 3.

- **Repeat Timer**: For external NVs, this property defines the repeat timer in milliseconds. The default is 96 ms.

- **Transmit Timer**: For external NVs, this property defines the transmit timer in milliseconds. The default is 768 ms.

- **LNS Network Path**: If available from an LNS scan, this property specifies the LNS network path of the device where the given NV exists.

- **LNS Channel Name**: If available from an LNS scan, this property specifies the LNS channel name of the device where the given NV exists.

7.3 Project Settings

The project settings allow defining certain default behavior and default settings used throughout the project. To access the project settings go to the menu **Settings → Project Settings…**. This opens the project settings dialog, which provides several tabs as described in the following sections.

7.3.1 General

The general tab of the project settings as shown in Figure 60 contains settings independent of the technology port. The settings are:

- **Project Name**: This setting allows entering a descriptive name for the project.

- **Default FTP Connection Settings**: Enter a user name and password for the default FTP access. This access method is used implicitly when connected via LNS and the device is accessible over IP. For this implicit connection, there is no dialog to ask for a username and password and the username and the default password from the project settings are used.
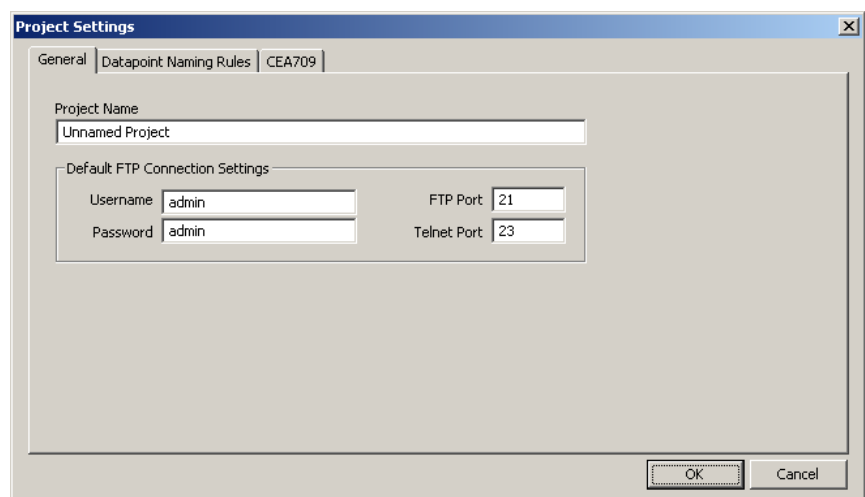
Figure 60: General Project Settings.

7.3.2 Data Point Naming Rules

The data point naming rules tab (see Figure 61) allows specifying how data point names are automatically derived from scanned network variables. The preview shows how names would look like, when the check marks are modified.
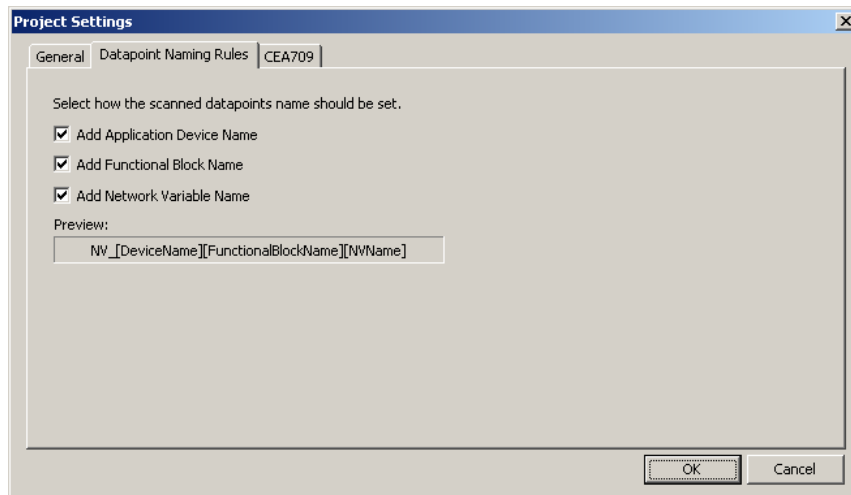
Figure 61: Data Point Naming Rules Project Settings.

7.3.3 CEA-709 Settings

The CEA-709 configuration tab as shown in Figure 62 allows configuring properties of the device's CEA-709 port. The options are:

- **Enable Legacy Network Management Mode**: This group box contains check boxes for each CEA-709 port of the device. Put a check mark on the port, if this port shall be operated in the legacy network management mode. In that mode, the port does not use the extended command set (ECS) of network management commands. This can be necessary to operate the device with some network management tools that do not support the ECS.

- **Default Pollcycle for External NVs**: When using external NVs, this pollcycle is set as a default for input data points. The pollcycle can be edited individually in the properties view of the data point manager.

- **Use state-member of SNVT_switch as**: This setting defines how the state member of the SNVT_switch shall be mapped to a data point. Depending on how the data point shall be used, it can be binary or multi-state. The multi-state setting allows setting the UNSET state explicitly. As a binary point the UNSET state is implicitly chosen, if the value is invalid.

- **L-Proxy Operating Mode**: The L-Proxy Configurator can be operated in one of two modes: Simple and advanced mode. In simple mode, the user can only use dynamic NVs created manually in LNS and create connections. The LNS database is never modified in this mode. In advanced mode, the user has full command over static, dynamic, and external NVs, automatic bindings and connections. The default mode is the simple mode.
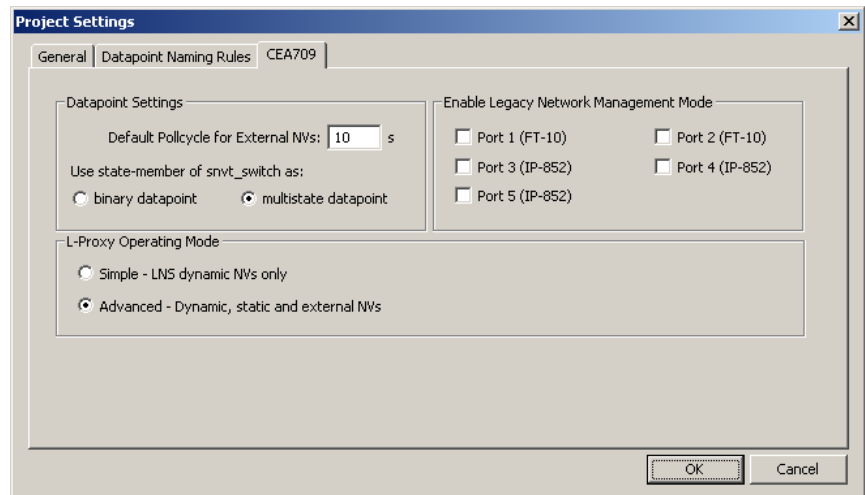
Figure 62: CEA-709 Project Settings.

7.4 Workflows for the L-Proxy

This section discusses a number of work flows for configuring the L-Proxy in different use cases in addition to the simple use case in the quick-start scenario (see Chapter 2). The description is intended to be high-level and is depicted in flow diagrams. The individual steps refer to later sections, which describe each step in more detail. In principle, the L-Proxy Configurator supports the following use cases:

- Network Management Tool based on LNS 3.x (see Section 7.4.2),

- network Management Tool based on LNS 3.x using a static NV interface (see Section 7.4.3),

- non-LNS 3.x network management tool (see Section 7.4.4).

7.4.1 Involved Configuration Files

In the configuration process, there are a number of files involved:

- Port interface definition file: This type of file contains all data points and their settings for one port of the L-Proxy. This file is exported from and imported into the Configurator software to exchange port interface definitions between the integrators. These files end with ".itf".

- XIF file: This is the standard file format to exchange the static interface of a device. This file can be used to create a device in the database without having the L-Proxy on-line. There exists a standard XIF file for the FT port (L-Proxy_V3_0_FT-10.xif) and one for the IP-852 port (L-Proxy_V3_0_IP-10L.xif).

- L-Proxy Configurator project file: This file contains all ports, data points, and connections of a project. These files end with ".lprxy". It stores all relevant configuration data and is intended to be saved on a PC to backup the L-Proxy's data point configuration. Alternatively to exchanging the port interface definition files, the integrators can also pass on the project file. In this case, however, integrators can only work incremental. As an advantage, the internal connections can already be created partly during the process instead of creating all connections in the end.

7.4.2 Configure with LNS and Dynamic NVs

The flow diagram in Figure 63 shows the steps that need to be followed in order to install L-Proxy in a network with LNS 3.x and using dynamic NVs. For this workflow the simple operation mode is sufficient and no LNS database changes occur.

First, a device of an L-Proxy port must be added to the LNS database (see Section 7.5). Then one or more functional blocks must be created (see Section 7.6). In those functional blocks the input and output network variables must be created dynamically (see Section 7.7). Then the binding with the other nodes in the network can be created.

Start the L-Proxy Configurator for the L-Proxy in LNS mode on the configured port (see Section 7.9.1). If working offline, one must start the L-Proxy Configurator software to extract the L-Proxy interface definition of the installed port for making it available to other engineers (see Section 7.9.12). If working online, the other installers can upload the configuration from the L-Proxy.

Close the L-Proxy Configurator and repeat this procedure for all other L-Proxy ports. Note, that the other L-Proxy ports may be added to different LNS databases (different domains) by different engineers. If the ports are used in different LNS databases you need to open the different LNS databases and extract the port interface definitions for the L-Proxy port in those LNS databases. If multiple engineers are working on a project they need to designate one engineer, who is responsible for creating the internal connections. In the end, a set of port definition files must be available to that engineer. If working online, the engineer can also upload all port definitions from the L-Proxy.

After all ports have been configured the engineer who is responsible for creating the internal connections opens the Configurator software on one of his L-Proxy ports. Then he must import the port interface definition files for all L-Proxy ports (see Section 7.9.12) or upload them from the device. When the interface configurations have been loaded the connections can be created (see Section 7.11).

After the connections have been created, one of the L-Proxy ports has to be designated as the *download port*. This is the port over which the configuration is downloaded. Before downloading the new L-Proxy configuration into L-Proxy, at least the download port must be commissioned. When the device corresponding to the download port of the L-Proxy is online the new configuration can now be downloaded using the configuration software (see Section 7.9.11). It is recommended to save the complete configuration to a disk file for being able to replace an L-Proxy in the network.

To add more NVs when all bindings are in place and the L-Proxy is being used, please refer to Section 7.4.5 on how to extend an existing configuration with LNS.

```
                           ┌─────────┐
                          (  START   )
                           └─────────┘
                                │
                                ▼
                    ┌───────────────────────┐
                    │   Add L-Proxy Port x   │
                    │      Section 7.5       │
                    └───────────────────────┘
                                │
                                ▼
                    ┌───────────────────────┐
                    │ Create Functional Block│
                    │   for Port x Section 7.6│
                    └───────────────────────┘
                                │
                                ▼
                    ┌───────────────────────┐
                    │ Create Network Variables│        yes
                    │  on Port x Section 7.7  │
                    └───────────────────────┘
                                │
                                ▼
                    ┌───────────────────────┐
                    │ Make Network Variable  │
                    │       Bindings         │
                    └───────────────────────┘
                                │
                                ▼
                ┌───────────────────────────────┐
                │ Start L-Proxy Configurator for │
                │   node "Port x" Section 7.9.1  │
                └───────────────────────────────┘
                                │
                                ▼
                ┌───────────────────────────────┐
                │ Extract and save the port      │
                │ interface definition Section 7.9.12│
                └───────────────────────────────┘
                                │
                                ▼
                          ◇ L-Proxy Ports
                            left to add? ◇
                                │
                               no
                                ▼
                    ┌───────────────────────┐
                    │ Upload/import port     │
                    │ definitions Section 7.9.12│
                    └───────────────────────┘
                                │
                                ▼
                    ┌───────────────────────┐
                    │ Make L-Proxy internal  │
                    │ connections Section 7.11│
                    └───────────────────────┘
                                │
                                ▼
                    ┌───────────────────────┐
                    │ Download configuration │
                    │ to L-Proxy Section 7.9.11│
                    └───────────────────────┘
                                │
                                ▼
                           ┌─────────┐
                          (  DONE    )
                           └─────────┘
```

Figure 63: Basic design-flow with LNS and dynamic NVs.

7.4.3 Configure with LNS and Static NVs

Configuration of the L-Proxy with static NVs in LNS can be beneficial if a basic configuration shall be pre-configured as a static interface. Later additions to the network variables can be done with dynamic NVs at run-time. Figure 64 depicts the basic work flow. This workflow requires the advanced operation mode and the LNS database is modified.
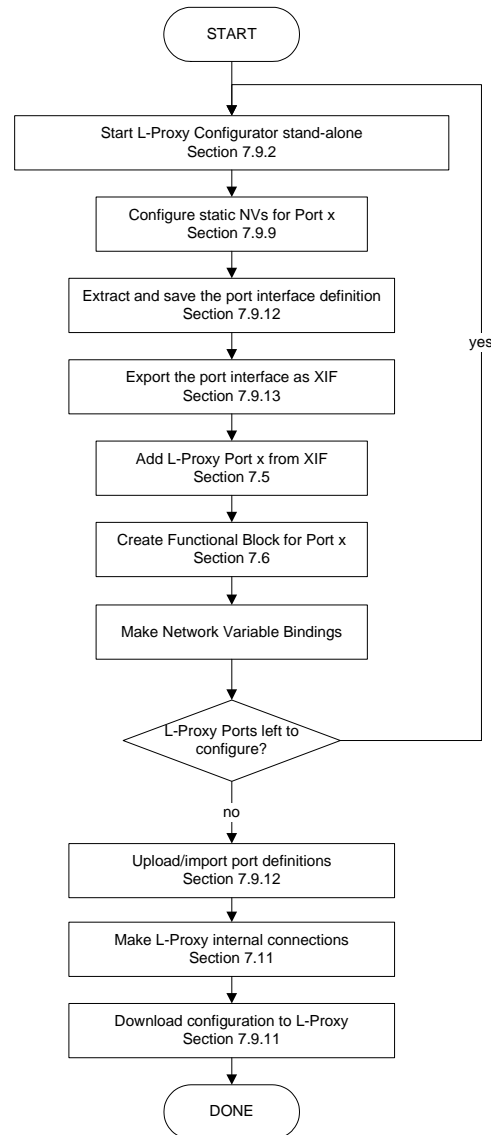
Figure 64: Basic design-flow with LNS and static NVs.

The L-Proxy Configurator software needs to be started in stand-alone mode (see Section 7.9.2). Then the user needs to configure the static NVs for the desired L-Proxy port (see Section 7.9.9). After all static network variables have been created, the port definition for the L-Proxy port needs to be exported (see Section 7.9.12). In addition, the static network variable interface of this L-Proxy port must be exported as a XIF file (see Section 7.9.13). Now an L-Proxy device can be added from this XIF file in the LNS database (see Section 7.5). Then one or more functional blocks must be created, which contain the static NVs (see Section 7.6). Having the static NVs visible, the bindings with the other nodes in the network can be created.

Close the Configurator software and repeat this procedure for all other L-Proxy ports. Note, that the other L-Proxy ports may be added to different LNS databases (different domains) by different engineers. If the ports are used in different LNS databases you need to open the different LNS databases and extract the port interface definitions for the L-Proxy port in those LNS databases. If multiple engineers are working on a project they need to designate one engineer, who is responsible for creating the internal connections. In the end, a set of port definition files must be available to that engineer.

After all ports have been configured the engineer who is responsible for creating the internal connections opens the Configurator software on one of his L-Proxy ports. Then he must load the port interface definition files (see Section 7.9.12). When the interface configurations have been loaded the connections can be created (see Section 7.11).

After the connections have been created, download the configuration when the L-Proxy is connected to the network using the configuration software (see Section 7.9.11). It is recommended to save the complete configuration to a disk file for being able to replace an L-Proxy in the network.

Note, that once the static NV interface is complete and all bindings are in place it is not recommended to change that interface. To add NVs to such a configuration it is recommended using dynamic NVs. Please refer to Section 7.4.5 on how to extend an existing configuration with LNS.

7.4.4 Configure without LNS using Static NVs

Without LNS the L-Proxy can be configured using static NVs. This is beneficial, if network variables shall use bindings, but the installer uses a network management tool, which is not based on LNS 3.x. The basic work flow is depicted in Figure 65. This workflow requires the advanced operation mode. To configure an L-Proxy without LNS, an IP connection must be available.

The L-Proxy Configurator software needs to be started in stand-alone mode (see Section 7.9.2). Then the user needs to configure the static NVs for the desired L-Proxy port (see Section 7.9.9). After all static NVs have been configured the port interface definition file for the L-Proxy port needs to be exported (see Section 7.9.12).

For network management tools, which do not support the ECS (enhanced command set) network management commands, the legacy network management mode must be configured (see Section 7.9.14). Please contact the tool's vendor for information whether ECS is supported or not.

Then also export the static NV interface as a XIF file (see Section 7.9.13). The XIF file has to be used in the non-LNS tool to create a device for the L-Proxy. Using that device, the integrator can create the bindings in that tool. Please refer to the documentation of the network management tool on how to create devices from a XIF file and bind network variables.

Close the Configurator software and repeat this procedure for all other L-Proxy ports. Note, that the other L-Proxy ports may be added to different domains by different engineers. If multiple engineers are working on a project they need to designate one engineer, who is responsible for creating the internal connections. In the end, a set of port definition files must be available to that engineer.

After all ports have been configured the engineer who is responsible for creating the internal connections opens the L-Proxy Configurator stand-alone. Then he must load the port interface definition files (see Section 7.9.12). When the interface configurations have been loaded the connections can be created (see Section 7.11).

After the connections have been created, the complete configuration can be saved. Before downloading the new L-Proxy configuration, the user must connect the configuration software to the L-Proxy via the FTP connection button (see Section 7.9.2). After the configuration has been downloaded to the L-Proxy the integrators need to commission the L-Proxy devices in their network management tools. It is recommended to save the entire configuration to a disk file for being able to replace an L-Proxy in the network.

Note, that once the static NV interface is complete and all bindings are in place it is not recommended to change that interface. Since the XIF files change the device may have to be deleted in the respective network management tool and created again from the new XIF

file. This means also that all existing bindings may be lost and have to be recreated. To add NVs to an existing configuration it is recommended using external NVs. Please refer to Section 7.4.6 on how to extend an existing configuration without LNS.

```
                    ┌─────────┐
                    │  START  │
                    └────┬────┘
                         │                                              yes
         ┌───────────────────────────────────┐                          │
         │  Start L-Proxy Configurator stand-alone │                     │
         │            Section 7.9.2          │                          │
         └───────────────┬───────────────────┘                          │
         ┌───────────────────────────────────┐                          │
         │   Configure static NVs for Port x  │                         │
         │            Section 7.9.9          │                          │
         └───────────────┬───────────────────┘                          │
         ┌───────────────────────────────────┐                          │
         │ Extract and save the port interface definition │             │
         │            Section 7.9.12         │                          │
         └───────────────┬───────────────────┘                          │
                    ╱         ╲                                          │
                   ╱  Tool supports ╲         no                         │
                   ╲    ECS ?     ╱────────┐                             │
                    ╲         ╱            │                             │
                         │ yes       ┌─────────────────────┐            │
                         │           │  Enable Legacy NM Mode │          │
                         │           │      Section 7.9.14   │          │
                         │           └──────────┬──────────┘            │
         ┌───────────────────────────────────┐                          │
         │     Export the port interface as XIF  │                      │
         │            Section 7.9.13         │                          │
         └───────────────┬───────────────────┘                          │
         ┌───────────────────────────────────┐                          │
         │ Add L-Proxy Port x from XIF in non-LNS tool and create │     │
         │              bindings             │                          │
         └───────────────┬───────────────────┘                          │
                    ╱         ╲                                          │
                   ╱ L-Proxy Ports left to ╲────────────────────────────┘
                   ╲    configure?  ╱
                    ╲         ╱
                         │ no
         ┌───────────────────────────────────┐
         │    Upload/import port definitions  │
         │            Section 7.9.12         │
         └───────────────┬───────────────────┘
         ┌───────────────────────────────────┐
         │   Make L-Proxy internal connections │
         │            Section 7.11          │
         └───────────────┬───────────────────┘
         ┌───────────────────────────────────┐
         │  Download configuration to L-Proxy │
         │            Section 7.9.11         │
         └───────────────┬───────────────────┘
                    ┌─────────┐
                    │  DONE   │
                    └─────────┘
```

Figure 65: Basic design-flow without LNS using static NVs.

7.4.5 Change an Existing Configuration with LNS

The recommended way to change an existing (probably static) port interface is to add/delete dynamic network variables. Dynamic network variables in the Proxy functional block or the virtual interface can be added and deleted without losing an existing binding in NL-220, LonMaker, or Alex. The L-Proxy Configurator software synchronizes with the added or deleted network variables. The work flow to change an existing configuration for a specific port is shown in Figure 66.
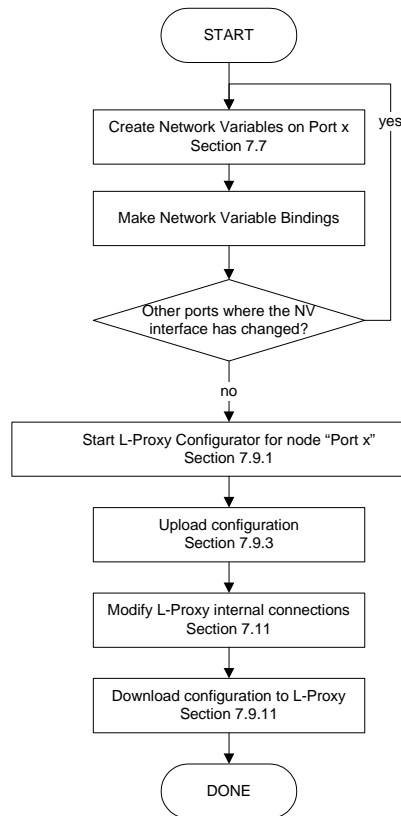
Figure 66: Work flow to modify an L-Proxy interface with LNS.

To change the network variable interface of Port x open the LNS network management tool and create, delete or modify the dynamic input and output network variables (see Section 7.7). Then create the bindings for the updated dynamic NVs with the other nodes in the network. This can be done independently by separate engineers in parallel.

At the end of all changes one engineer is designated to modify the internal connections in the L-Proxy to adapt to the updated NV interface. This engineer starts the Configurator as a plug-in on his designated *download port* (see Section 7.9.1) and uploads the current configuration (see Section 7.9.3). This upload also synchronizes the updated dynamic network variables. Then the connections can be modified (see Section 7.11). Finally, the updated configuration needs to be downloaded into the L-Proxy again (see Section 7.9.11).

7.4.6 Change an Existing Configuration without LNS

The recommended way to change an existing static port interface in systems without LNS is to add/delete external network variables. These network variables use polling to read data from the network and send explicit updates to write data to the network. Since the existing static NV interface is not changed by external NVs, no bindings are lost. Figure 67 shows the corresponding work flow.
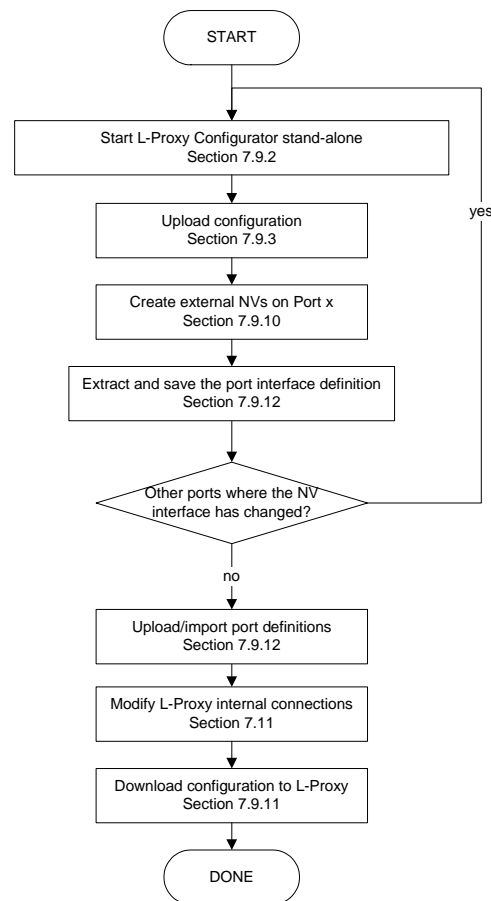
Figure 67: Work flow to modify an L-Proxy interface without LNS.

To change the network variable interface of Port x open the L-Proxy Configurator software stand-alone, connect to the L-Proxy using the FTP method (see Section 7.9.2) and upload the current configuration from the L-Proxy (see Section 7.9.3). Then create, delete or modify the external input and output network variables (see Section 7.9.10). Note, that there is no need to create bindings for external NVs. Finally, export the updated port interface definition for Port x (see Section 7.9.12). These steps can be done independently by separate engineers in parallel.

At the end of all changes one engineer is designated to modify the internal connections in the L-Proxy to adapt to the updated NV interface. This engineer starts the Configurator stand-alone and connects to the L-Proxy via the FTP method (see Section 7.9.2). Then he uploads the current configuration (see Section 7.9.12) and imports the updated port interface definitions (see Section 7.9.12). Then the connections can be modified (see Section 7.11). Finally, the updated configuration needs to be downloaded into the L-Proxy again (see Section 7.9.11).

7.4.7 Replace an L-Proxy

An L-Proxy can be replaced in the network by another unit. This might be necessary, if a hardware defect occurs. First of all, the replacement L-Proxy needs to be configured with the appropriate IP settings, including all relevant CEA-852 device settings. The remainder of this section focuses on the L-Proxy port interface configuration and internal connection configuration. The work flow is depicted in Figure 68.
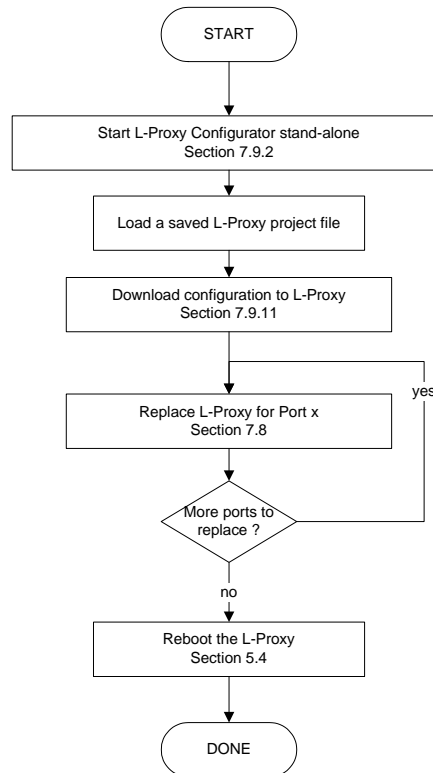
Figure 68: Basic work flow to configure a replacement device.

Start the L-Proxy Configurator software stand-alone and connect via the FTP method (see Section 7.9.2). Then load the L-Proxy configuration project file from disk, which has been saved when the original L-Proxy has been configured or modified. Double-check, if all connections and port configurations are sensible. Then download the configuration to the L-Proxy (see Section 7.9.11).

For each L-Proxy port open the network management tool. If using an LNS-based tool, the L-Proxy device needs to be replaced (see Section 7.8). If you are not using LNS, then refer to your network management tool's reference manual on how to replace a device. The replacement step needs to be repeated for each port of the L-Proxy. After replacing the device in the network management tools, reboot the L-Proxy (see Section 5.4).

7.5 Adding L-Proxy

This Section shows the basic steps that need to be followed in order to add the L-Proxy in a network management tool. Before you continue please make sure that you have installed the LOYTEC L-Proxy Configurator software as explained in Section 7.1.

When the L-Proxy port is not configured with a static NV interface, adding the L-Proxy uses the device templates, which have been created by the L-Proxy Configurator software: "L-Proxy_V3_0_FT-10" for an FT port, and "L-Proxy_V3_0_IP-10L" for an IP-852 port. If the L-Proxy port is configured with a static NV interface, use the XIF file, which has been exported for that port (see Section 7.9.13).

To configure an L-Proxy in your LNS-based network management tool, the device needs to be added to the LNS database and commissioned. This Section refers to NL220, LonMaker TE, and Alex and describes how to add an L-Proxy to your database. In the examples, port 2 of the L-Proxy is added.

To Add an Device in NL-220

1. Make sure you are in the **All subsystems** tree. For this, the button ⊞ in **Trees toolbar** must be pressed (if not click on it).

2. Right click on the subsystem you want to add the device in and select the option **New node in <…>**

3. In the dialog from Figure 69 specify a device name for the new device.

4. Check the option **Create node from a device template**.

5. Select the proper device template for the L-Proxy Port. An FT port (Port 1, 2) uses the "L-Proxy_V3_0_FT-10" template and the IP-852 port (Port 3, 4, 5) the "L-Proxy_V3_0_IP-10L" template.

6. Click **OK**.
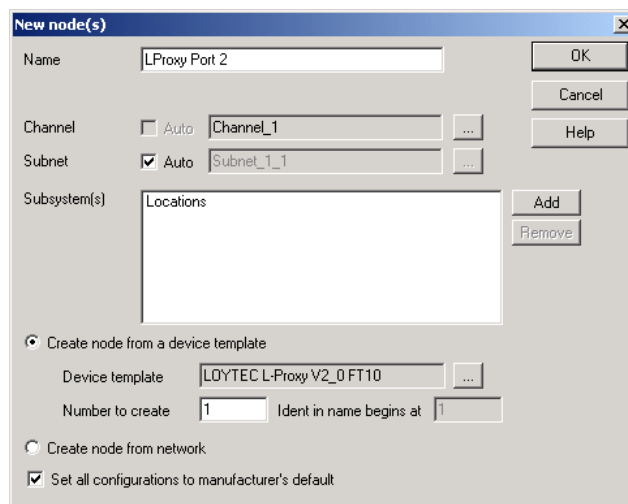
Figure 69 Adding a new L-Proxy port (Port 2) to the network.

Note: *You may select the channel manually by un-checking **Auto** and clicking on ⋯ . You will be able to select the channel you want to create the device in. If **Auto** is checked then **NL220** will try to automatically determine the channel of the device from the network.*

7. Your L-Proxy node should now appear in the NL220 tree as shown in Figure 70. Its icon must be ⊞.
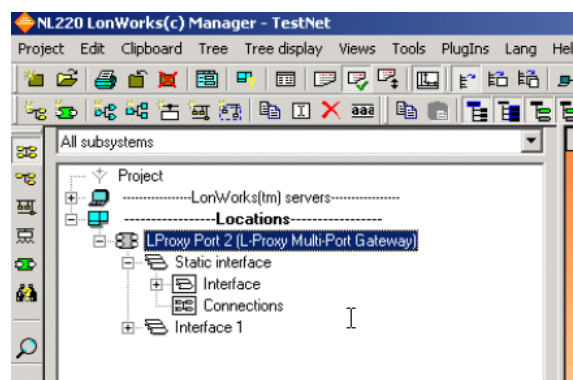
Figure 70: L-Proxy Interface.

To Add a Device to LonMaker TE

1. In your LonMaker drawing, drag a device stencil into the drawing. Enter an appropriate name as shown in Figure 71.
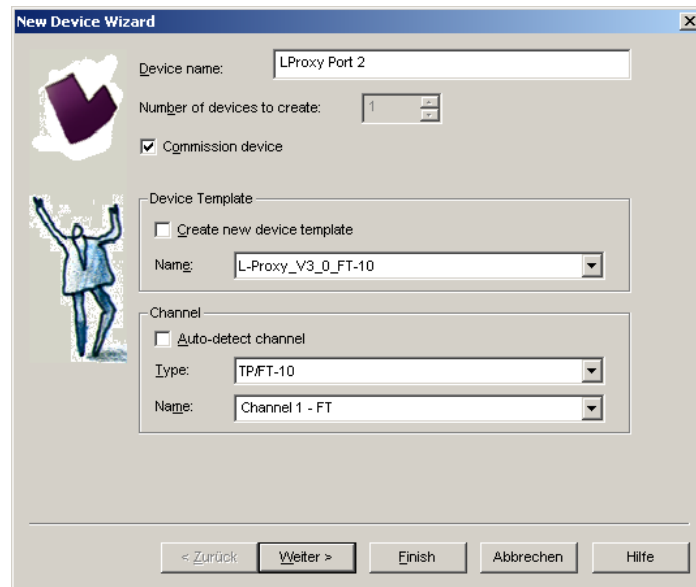
Figure 71: Create a new device in the drawing.

2. Select **Commission Device** if the L-Proxy is already connected to the network.

3. In the **Device Template** group box select the existing device template of the L-Proxy. Select "L-Proxy_V3_0_FT-10", if the L-Proxy is configured to use the FT-10 interface, or "L-Proxy_V3_0_IP-10L", if the L-Proxy is configured to be on the IP channel. For information on how to configure which port to use, refer to Section 4.5 for the console UI or Section 5.2.4 for the Web UI.

4. Select the channel, which the L-Proxy is connected to and click **Next**.

5. The following dialog shown in Figure 72 appears, click **Next**.
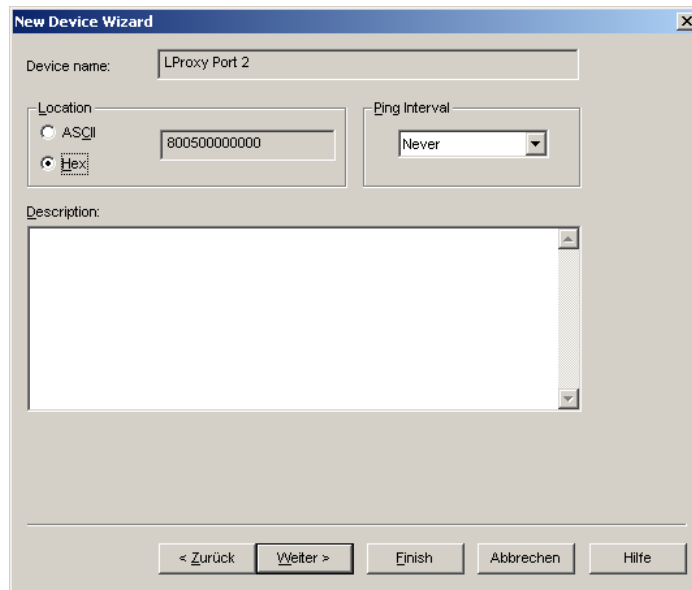
Figure 72: Leave defaults for Location.

6. Check Service Pin as the device identification method as shown in Figure 73 and click **Next**.
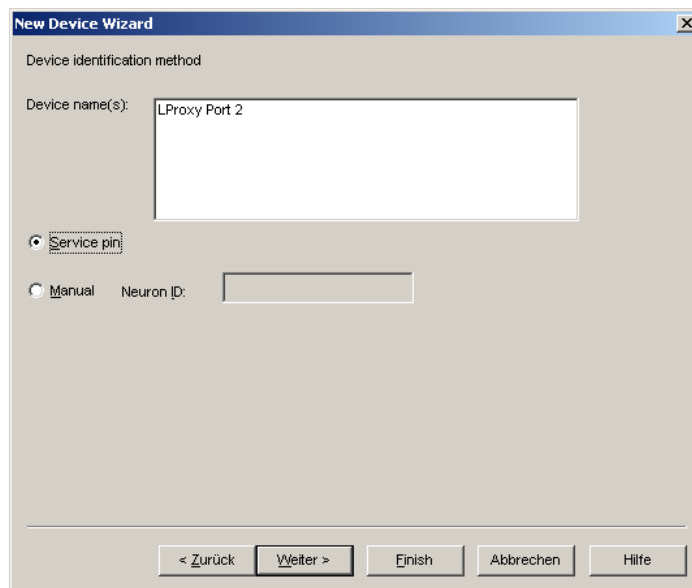
Figure 73: Use Service Pin.

7. Click **Next** in the following screens until you get to the final dialog shown in Figure 74.

8. If the device is already on-net, select **Online**.
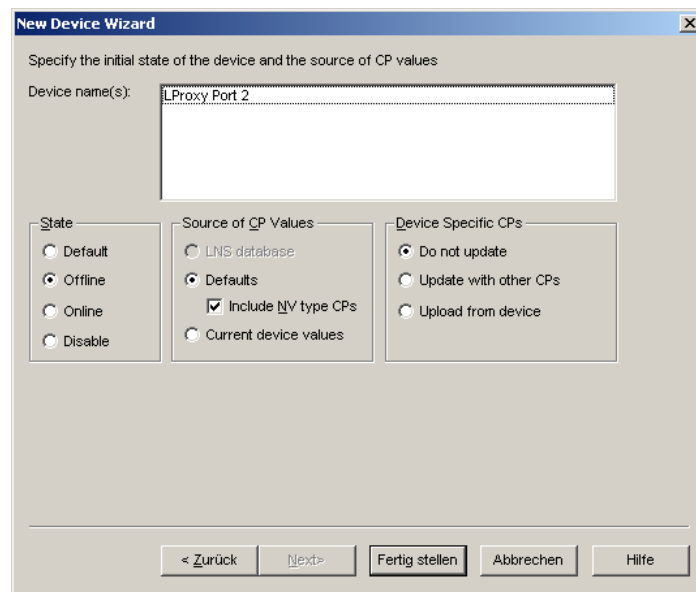
Figure 74: Final dialog.

9. Click **Finish**. A dialog will prompt to press the service pin.
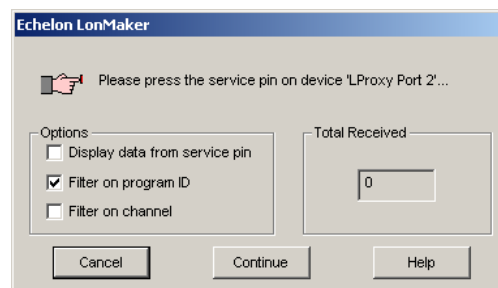
10. Finally, you should get the device added to your drawing as depicted in Figure 75.
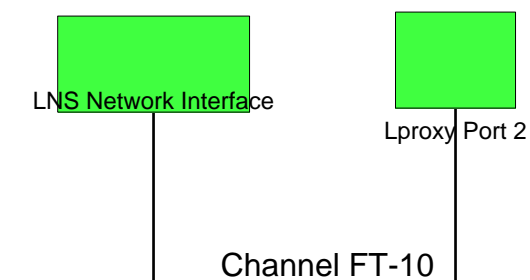
Figure 75: The L-Proxy has been added to the drawing.

To Add a Device in Alex

1. In the tree view, go to the subsystem to which the L-Proxy port should be added.

2. Select **Geräte** and choose **Neues Gerät**. The Dialog in Figure 69 is shown.

3. Enter the device name (e.g., L-Proxy Port 1) and choose the correct device template for the L-Proxy. Make sure to select the device template according to the L-Proxy port you are adding (FT10 version for port 1, 2, and the IP10-L version for ports 3, 4, 5).

4. If required, enter the Neuron ID or press the Service Pin and select **OK** to close the dialog and add the L-Proxy port to the project.
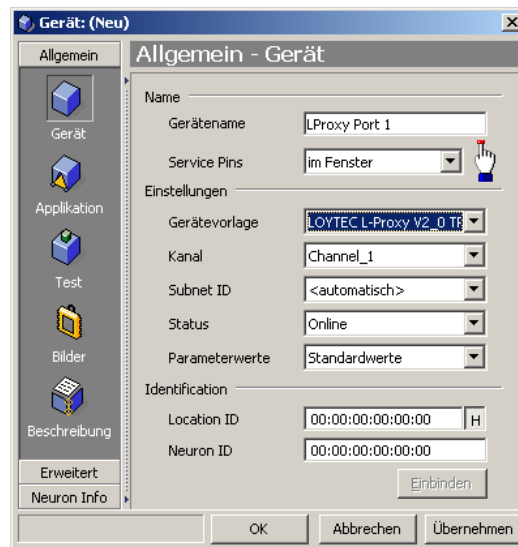
Figure 76: Adding a new L-Proxy port (Port 1) to the network.

7.6 Creating Functional Blocks/Virtual Interfaces

After adding the L-Proxy node at least one but up to eight functional block/virtual interfaces must be created for the proxy object, if dynamic NVs are going to be used. This section describes how to create the functional blocks in NL220, LonMaker TE, and Alex. It is assumed that the steps are executed after adding the L-Proxy has been added to the LNS database.

To Create Virtual Interfaces in NL-220

1. Right click on the device and select the option **New interface …** in the **Virtual interfaces** sub menu.

2. In the next window enter the name of the interface, for example **Interface 1**. You may create as many interfaces as needed (for example to sort network variables by functions).
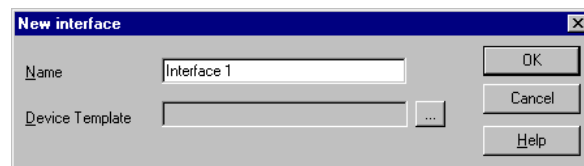
3. Click **OK**.

4. The virtual interface must now appear in the L-Proxy device in the tree (see Figure 77).

5. Open the **L-Proxy1 Port2** device in the tree (click on the ⊞). You must be able to see a **Static interface** (containing static network variables) and the virtual interface you created **Interface 1**.
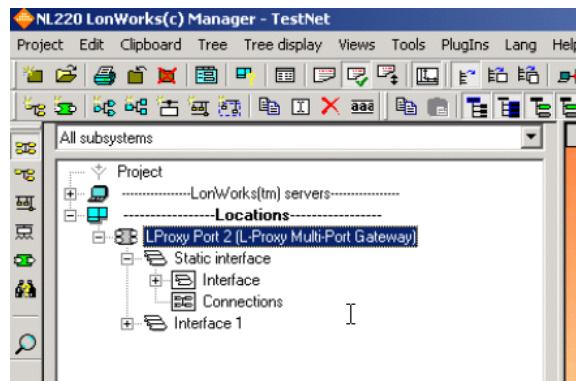
Figure 77: Interfaces of the L-Proxy device in tree.

6. You can repeat the above steps to create up to 8 virtual interfaces on every L-Proxy port. The different virtual interfaces for one L-Proxy port are only for logical grouping of the NVs.

7. You must repeat these steps for all L-Proxy ports that are connected to the network.

To Create Functional Blocks in LonMaker TE

1. Drag the Functional Block shape onto the drawing area. A dialog like the one in Figure 78 appears.

2. Under **Device** select the L-Proxy device, which has been added to the LonMaker drawing before.

3. Under **Functional Block** select the functional block, which shall be created in the drawing (**Gateway[0]**, **Gateway[1]**, *etc.*).

4. Check **Create all network variables shapes** to get all existing NVs of the functional block.
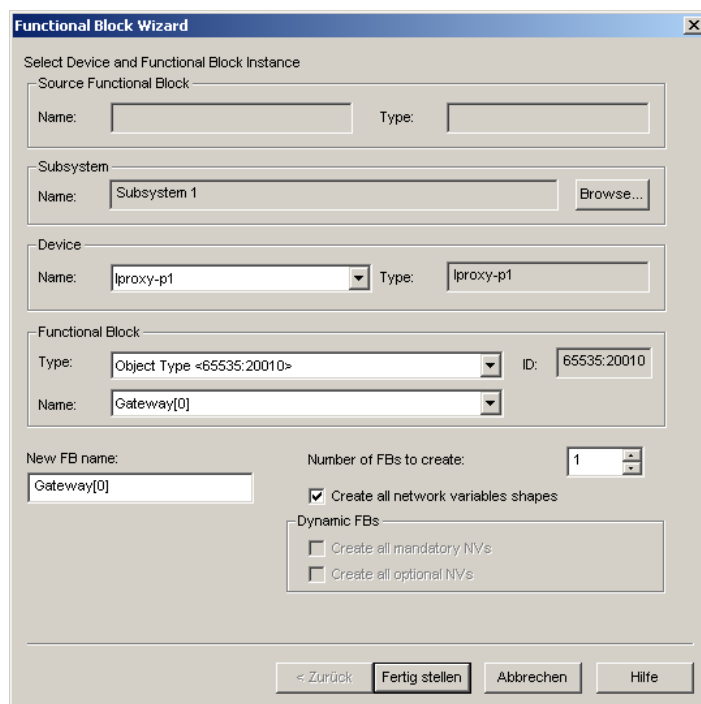
Figure 78: Functional Block Wizard in LonMaker TE.

5. Click **Finish**.

6. An empty functional block as shown in Figure 79 appears in the drawing area.

L-Proxy Port 2.Gateway[0]
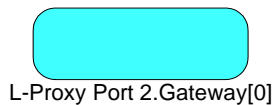
Figure 79: Empty functional block for L-Proxy Port 2.

7. You can repeat the above steps to create up to 8 functional blocks on every L-Proxy port. The different functional blocks for one L-Proxy port are only for logical grouping in the LonMaker drawing.

8. You must repeat these steps for all L-Proxy ports that are connected to the network.

To Create Virtual Interfaces in Alex

1. In the tree view, select **Virtuelle Funktionseinheiten** of the newly created device.

2. Click on **Neue virtuelle Funktionseinheit**.

3. In the dialog, enter the name of the interface, e.g., **Gateway[0]**. You may create as many interfaces as needed (for example to sort network variables by functions).
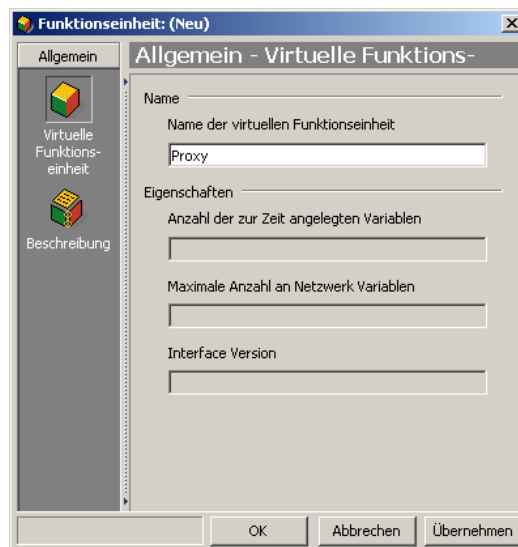
Figure 80: Creating a virtual interface in L-Proxy device

4. Click **OK**.

7.7 Dynamic Network Variables

After creating the functional block/virtual interface for the gateway object we need to create the input and output network variables for the gateway object. With LNS 3.x-based tools dynamic network variables can be used. Dynamic network variables are created during system configuration and can be added and deleted at any time whereas static network variables are created at system configuration time and are difficult to change afterwards.

Note: *Always close the L-Proxy Configurator when creating, adding, or deleting network variables in the gateway functional block.*

7.7.1 Creating a Dynamic Network Variable

Dynamic network variables are created by selecting the counterpart of the desired network variable binding. The dynamic network variable will inherit its properties from its counterpart, e.g., the SNVT. Figure 81 shows a simple network comprising 3 nodes and the newly created Proxy functional block.
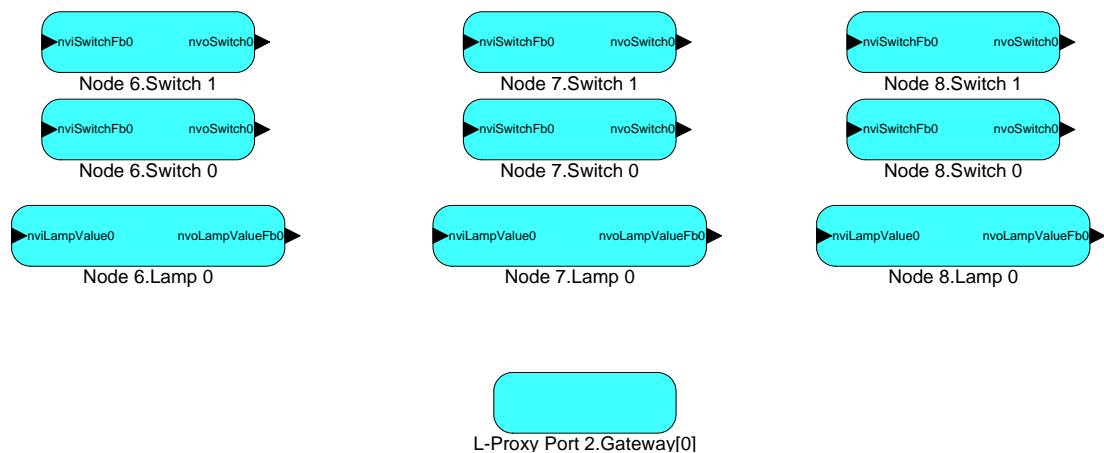
Figure 81: Simple network comprising 3 nodes and one L-Proxy Port.

Let's assume we want to connect network variable "nvoSwitch0" on Node 6 to L-Proxy. This means we need to create an input network variable in the gateway object with the same type as "nvoSwitch0". The remainder of this section describes how to create dynamic NVs in NL220, LonMaker TE, and Alex.

To Create Dynamic NVs in NL-220

1. Drag the counterpart (Node 6.nvoSwitch0) Network Variable in the tree onto the virtual interface **Interface 1** of the L-Proxy device.
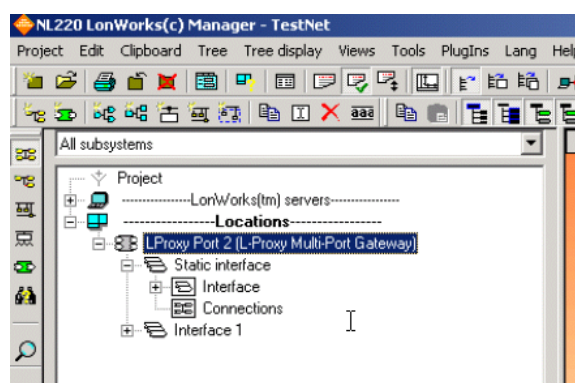
Figure 82 Dragging the counterpart network variable onto Virtual Interface 1.

2. This operation opens the connection window in working view (right view) and a new window pops up (see Figure 83).
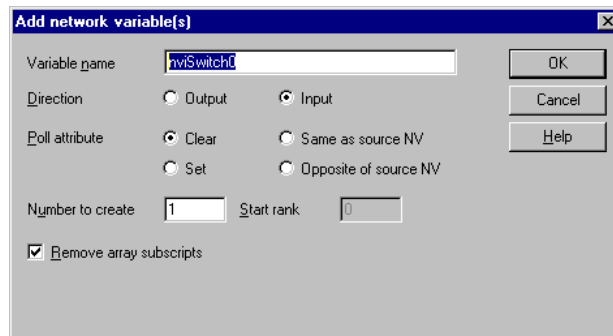
Figure 83: Add an input network variable to the L-Proxy virtual interface Interface 1.

3. This dialog is used to specify the properties of the new network variable. If you want to create multiple copies of the same network variable you can specify the number in the **Number to create** field. This feature is especially useful to create multiple copies of the same output network variable. When creating multiple identical NVs please make sure that the **Remove array subscripts** is checked. Otherwise these NVs are not properly displayed in the L-Proxy configuration plug-in utility.

4. A new name is already suggested for this newly created network variable. In our case we keep the *Variable Name: nviSwitch0*.

5. Make sure that the Poll Attribute of the new NV is set properly. Set it to **Clear** if the NV is updated and set it to **Set** if the NV is polled. If the NV is polled, both the source and the destination NV must be declared polled. Also if the NV is updated, both the source and the destination NV must have the Poll Attribute cleared.

6. Click on **OK**.

7. Now the tree shows the newly created input network variable in the virtual interface **Interface 1** (you must open the virtual interface in the tree to display the network variable).

8. As shown in Figure 84 the connection window in the work view (right view) includes now the nvoSwitch0 of Node 6 and the nviSwitch0 of the L-Proxy device. You can create or cancel the connection.
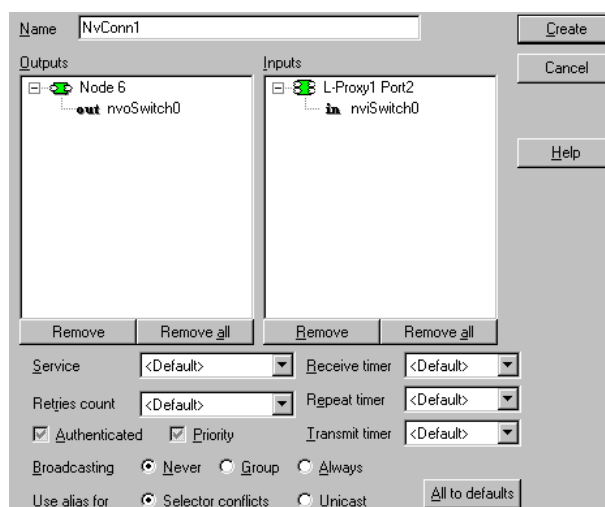
Figure 84: Connection window with the newly created L-Proxy variable and the Node 6 output variable.

To Create Dynamic NVs in LonMaker TE

1. Drag the **Input Network Variable** shape onto the gateway functional block. A new window appears (see Figure 85).
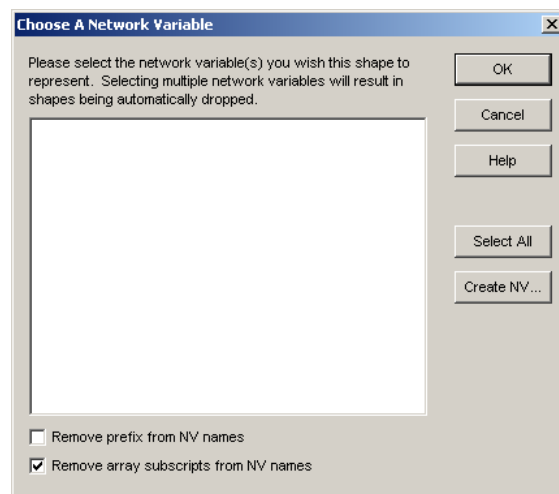
Figure 85: Add an input network variable to the Proxy functional block.

2. Click on **Create NV**. The dialog shown in Figure 86 appears.

3. Specify the properties of the new network variable. If you want to create multiple copies of the same network variable you can specify the number in the **How many?** field. This feature is especially useful to create multiple copies of the same output network variable.
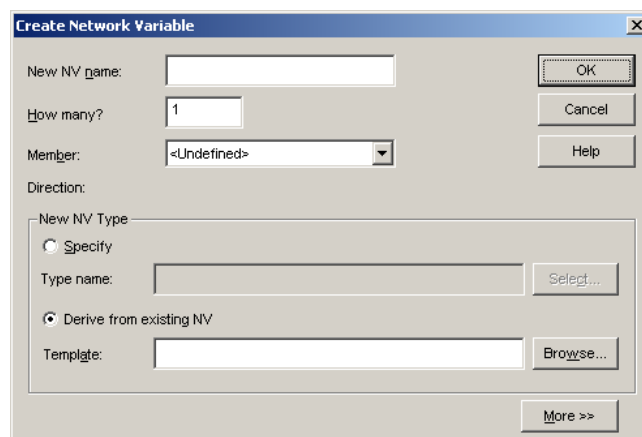
Figure 86: Create Network Variable dialog.

4. Click on **Browse…**

5. Select the counterpart network variable nvoSwitch0 on Node 6 for this connection.
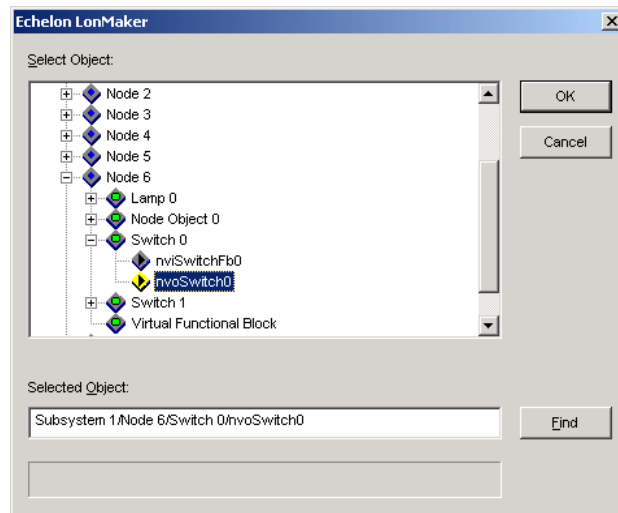
Figure 87: Select the counterpart NV on Node 6.

6. Click **OK**.

7. A new name is already suggested for this newly created network variable. In our case we keep the **New NV Name** of "nviSwitch0" as shown Figure 88.
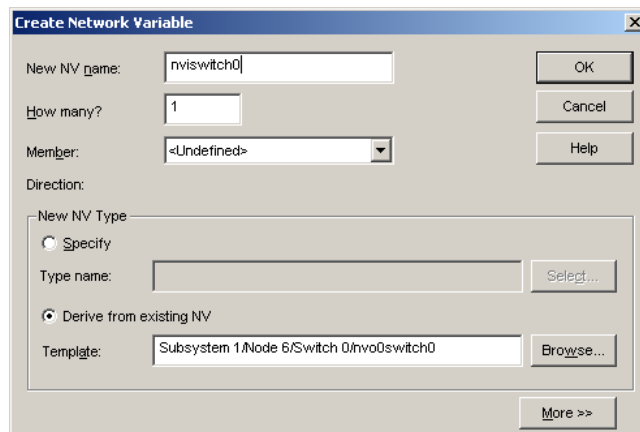
Figure 88: We keep the suggest name *nviSwitch0* for the new network variable.

8. Make sure that the Poll Attribute of the new NV is set properly. Set it to **Clear** if the NV is updated and set it to **Set** if the NV is polled. If the NV is polled both the source and the destination NV must be declared polled. Also if the NV is updated both the source and the destination NV must have the Poll Attribute cleared.

9. Click **OK**. The dialog shown in Figure 89 appears.
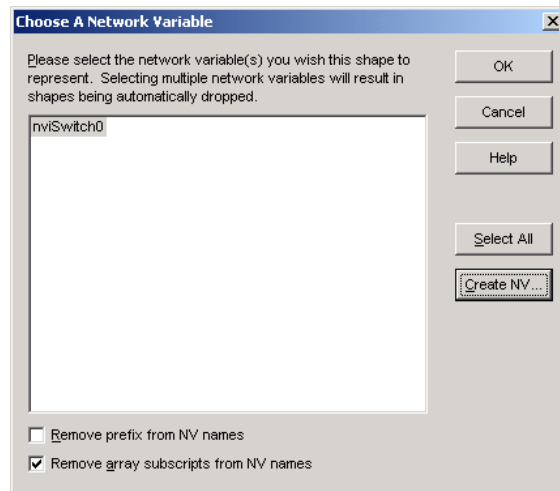
Figure 89: We have created a new input network variable in the Proxy functional block.

10. Click **OK**.

11. After the network drawing updates, it shows the newly created input network variable in the Proxy functional block.
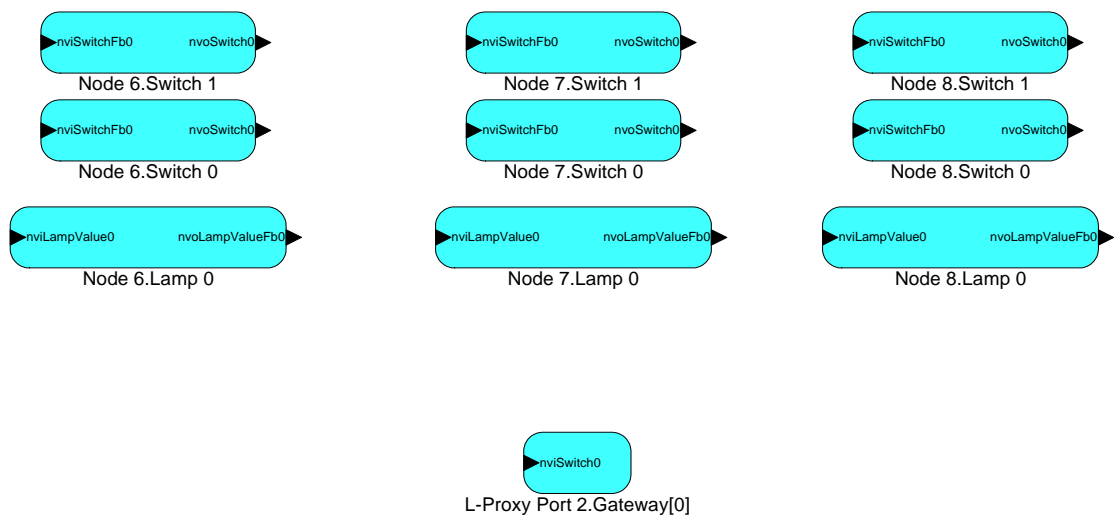
Figure 90: Updated network diagram that shows the new input network variable in the Proxy functional block.

To Create Dynamic NVs in Alex

1. Select **Netzwerkvariablen** in the tree view of one of the virtual interfaces of the L-Proxy device.

2. Click on **Neue Netzwerkvariable**.
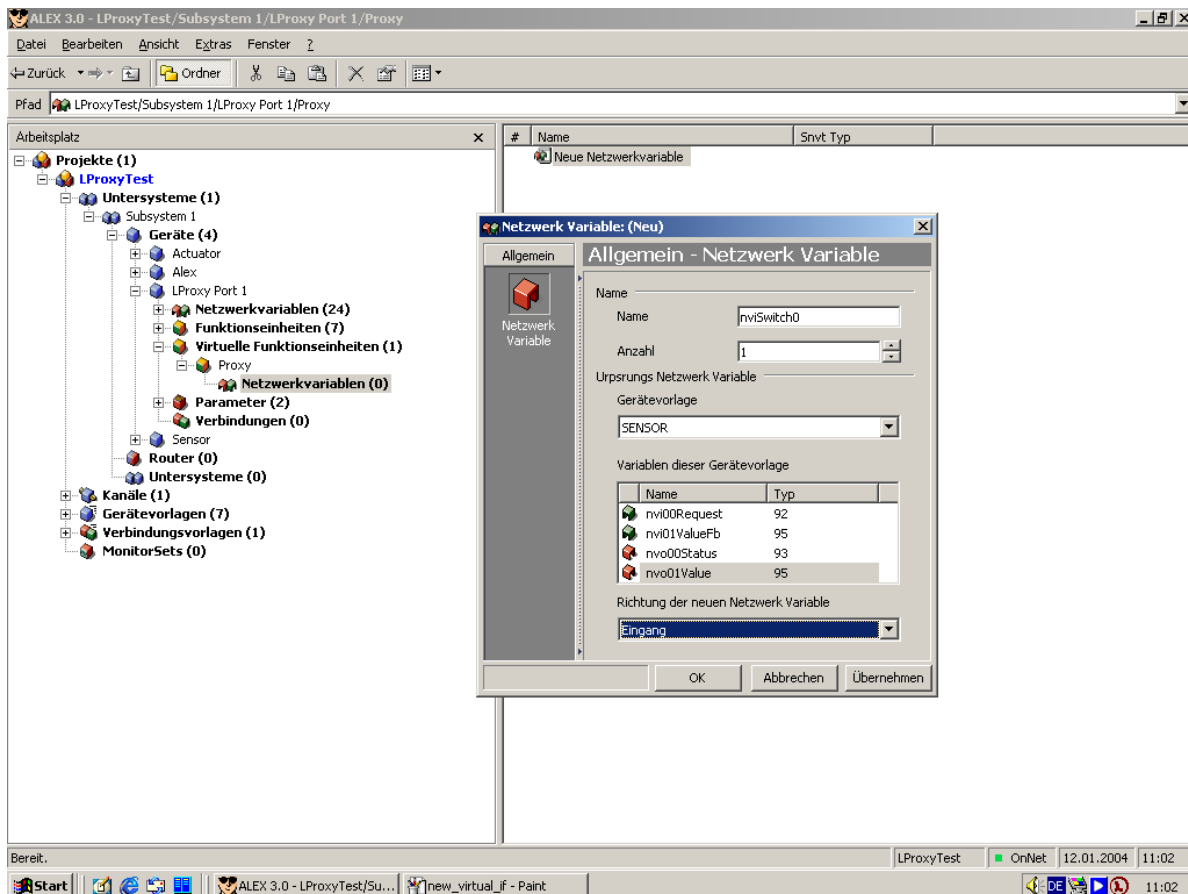
Figure 91: Add an input network variable to the L-Proxy virtual interface Proxy.

3. Enter the name for the network variable and the count how many network variables of this type should be created. In **Gerätevorlage**, select the device template of the node, which hosts the network variable to which the L-Proxy network variable will be bound later.

4. Select the counterpart network variable in the list and specify the correct direction (Eingang for an input network variable) and click **OK**.

5. Repeat this for all network variables which will be used on the L-Proxy.

7.8 Replace an L-Proxy

In the case of failure an L-Proxy might have to be replaced by another unit. Even if the configuration of the replacement unit is identical to the original one, the Node ID (NID) of the new unit is different. To account for that change, LNS provides the *replace* functionality.

When replacing a device in LNS, the association of the NID is transcribed to the new unit, given the new unit has an identical static NV interface. In the replace procedure LNS re-creates the dynamic variables and commissions the replacement unit.

This Section describes how to replace an L-Proxy in your LNS database. The description refers to NL220, LonMaker TE, and Alex. Let's assume there is a device 'L-Proxy' in the LNS database.

To Replace a Device in NL220

1. Right-click on the device in the device tree as shown in Figure 92 and select **Network → Replace**. Alternatively, the device can be selected and the device replacement can be started by pressing 'Ctrl+I'.
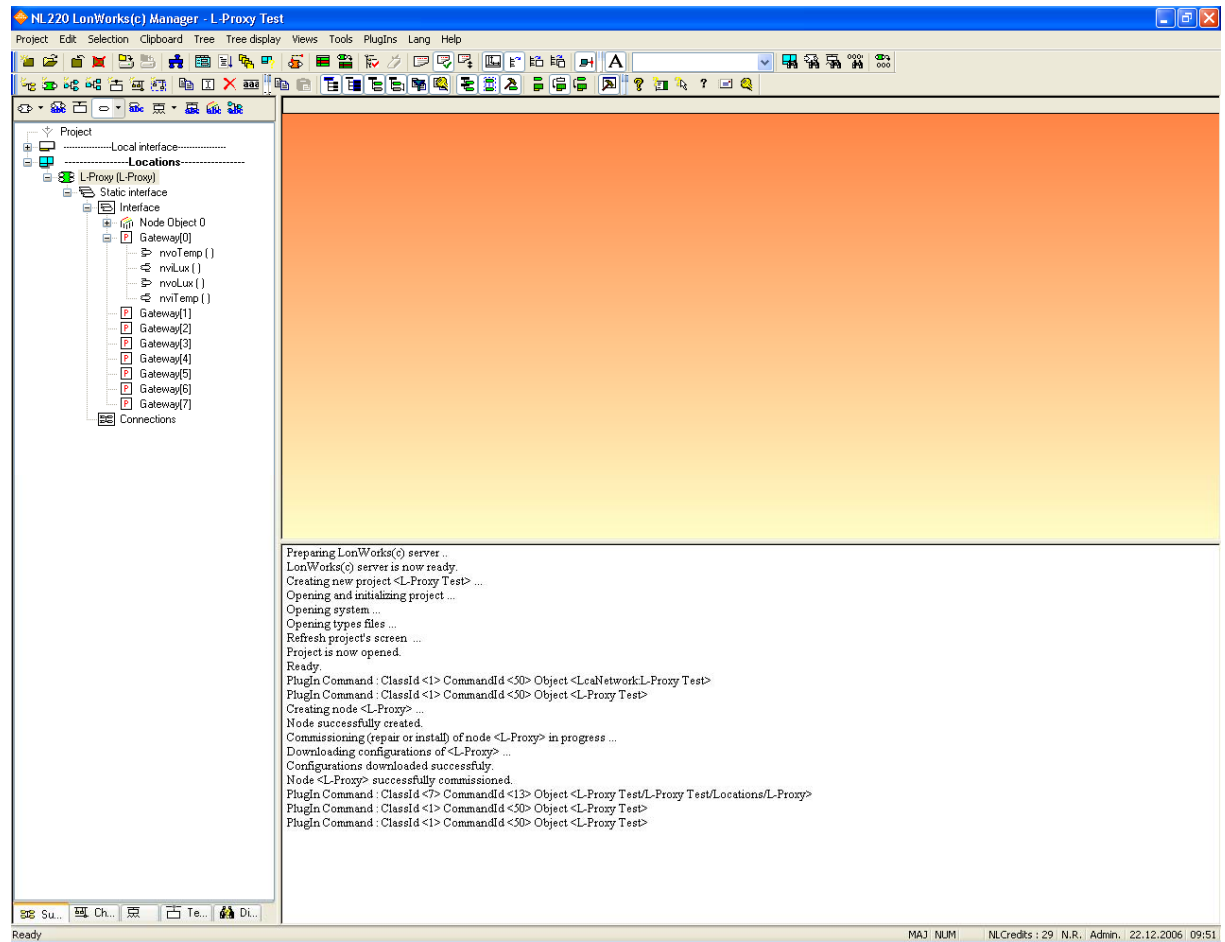
Figure 92: L-Proxy device in NL-220.

2. This opens the device replacement dialog box (see Figure 93).
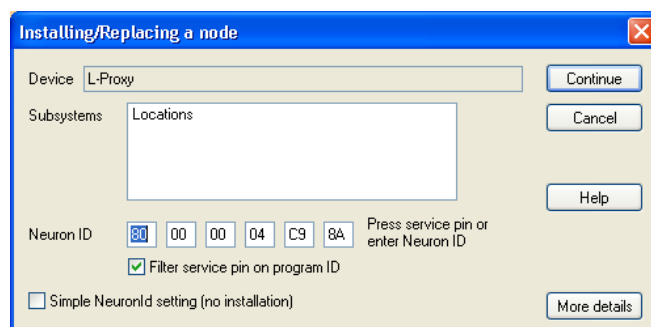
Figure 93: NL-220 node replacement dialog.

3. Press the service pin of the L-Proxy port to replace and press **Continue** to replace the device.

4. After the service pin has been received, NL-220 commissions the replacement unit's port, creates the dynamic NVs again (if any) and installs the bindings.

To Replace a Device in LonMaker TE

1. Select the device and right-click on the device shape as shown in Figure 94.
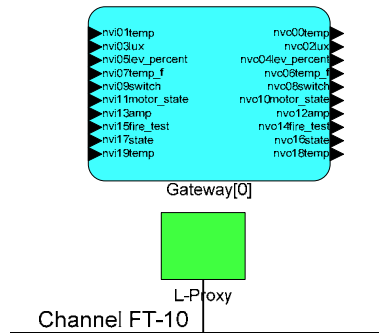
Figure 94: LonMaker drawing with one L-Proxy.

2. Select **Commissioning → Replace…**. This opens the LonMaker **Replace Device Wizard** as shown in Figure 95.
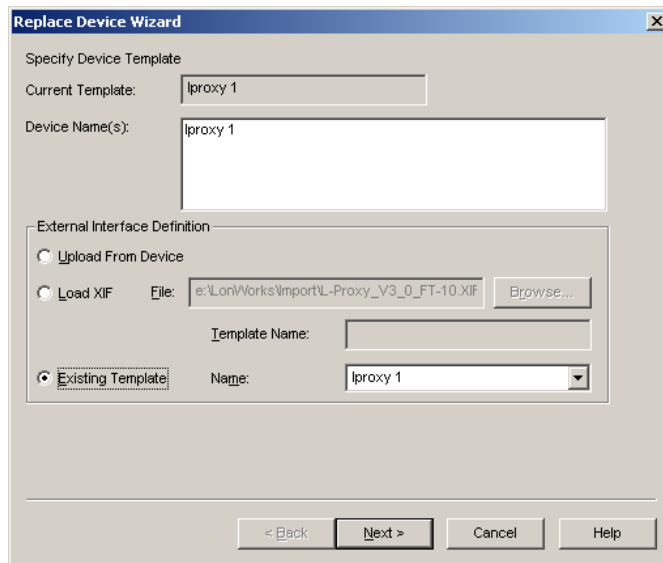
Figure 95: LonMaker replace device wizard.

3. Choose the existing device template and click **Next**.

4. In the following window shown in Figure 96 click **Next**.
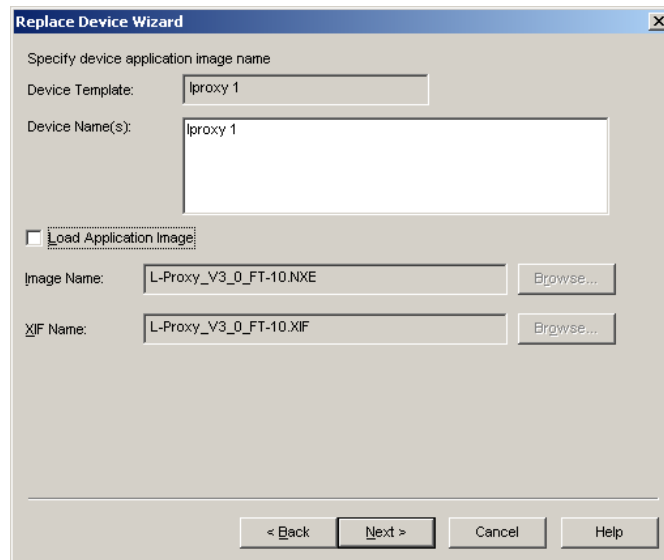
Figure 96: Click Next without loading an application image.

5. Then select **Online** as shown in Figure 97 and click **Next**.
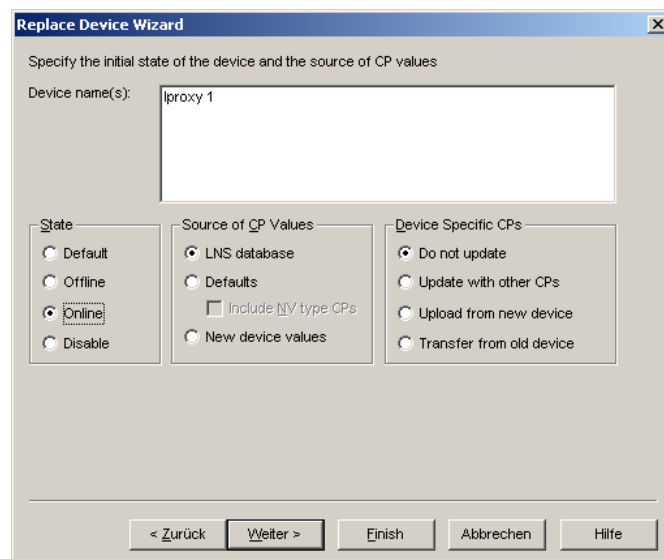
Figure 97: Select online state.

6. Select the **Service pin** method and click on **Finish** as shown in Figure 98.
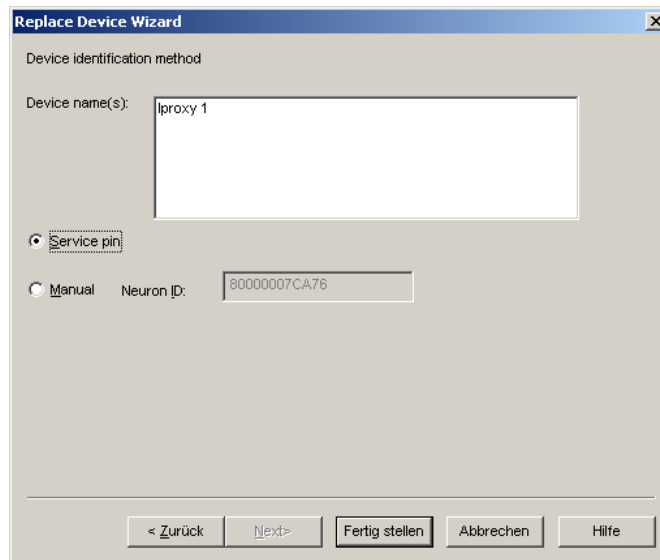
Figure 98: Select Service Pin and click Finish.

7. Then the service pin requestor opens. Press the service pin on the replacement L-Proxy on the correct port. You can also send the service pin using the Web interface (see Section 5.1).
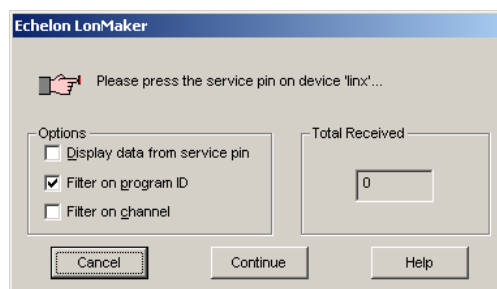
8. After the service pin has been received, LonMaker commissions the replacement device, creates the dynamic NVs again (if any), and installs the bindings.

Replace in Alex

1. Right-click on the device in the device tree as shown in Figure 99 and select **Ersetzen**.
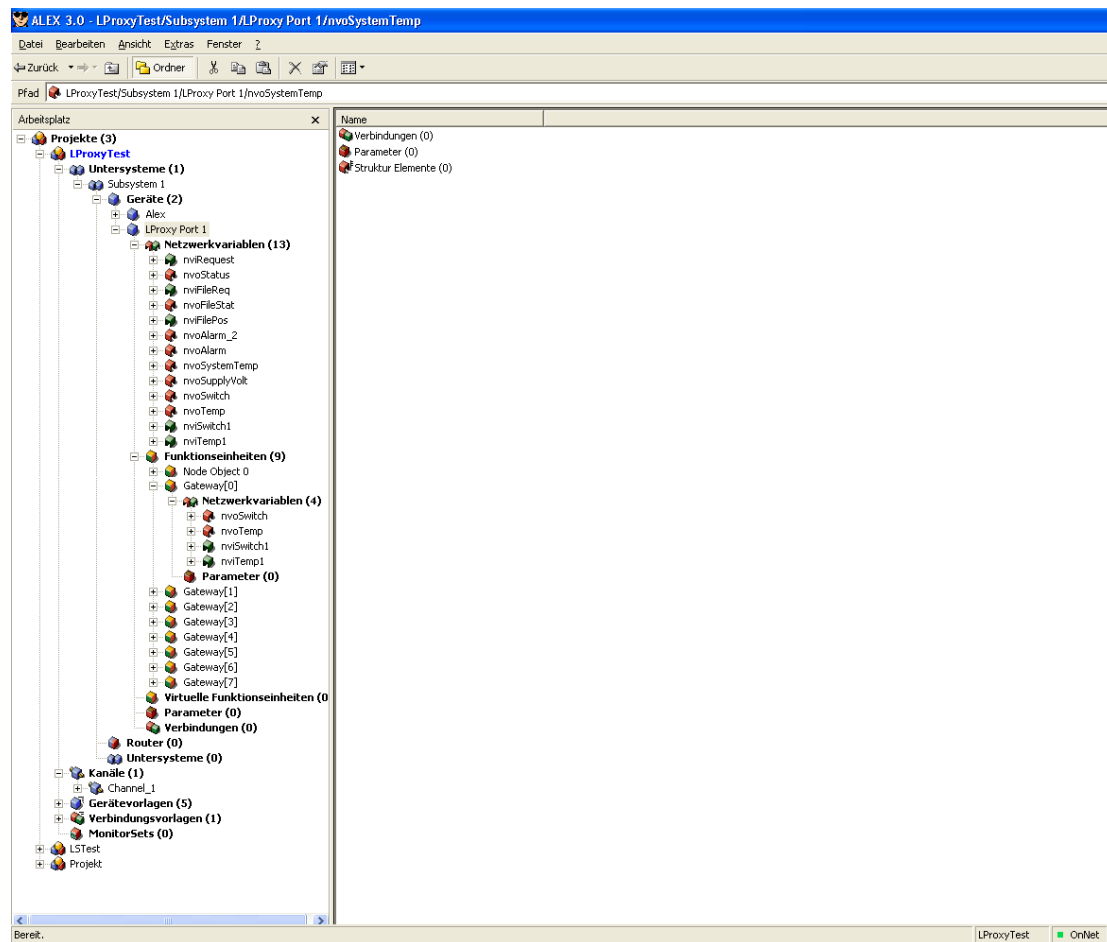
Figure 99: L-Proxy device in Alex.

2. This opens the device replacement dialog box (see Figure 100).
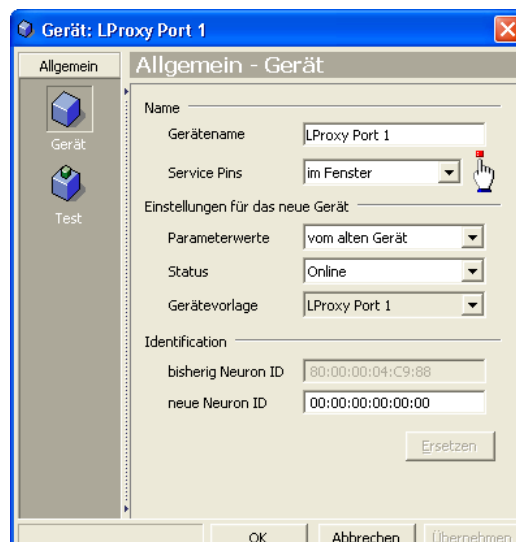
Figure 100: Device replacement dialog in Alex.

3. Press the service pin of the L-Proxy port to replace.

4. Click **OK** to replace the device.

5. After the service pin has been received, Alex commissions the replacement unit's port, creates the dynamic NVs again (if any) and installs the bindings.

7.9 Using the L-Proxy Configurator

7.9.1 Starting as an LNS Plug-In

In LonMaker the plug-in is started by right-clicking on the L-Proxy device shape or the Gateway functional block and selecting **Configure…** from the pop-up window.

In NL-220, the Plug-in is started by right clicking on the L-Proxy node, then selecting the Option **LOYTEC L-Proxy Configurator** in the **PlugIns** sub menu.

In Alex, the Plug-in is started by right clicking on the L-Proxy device and selecting the **LOYTEC L-Proxy Configurator** in the **Starte PlugIn** sub menu.

A window similar to what is shown in Figure 101 should appear.
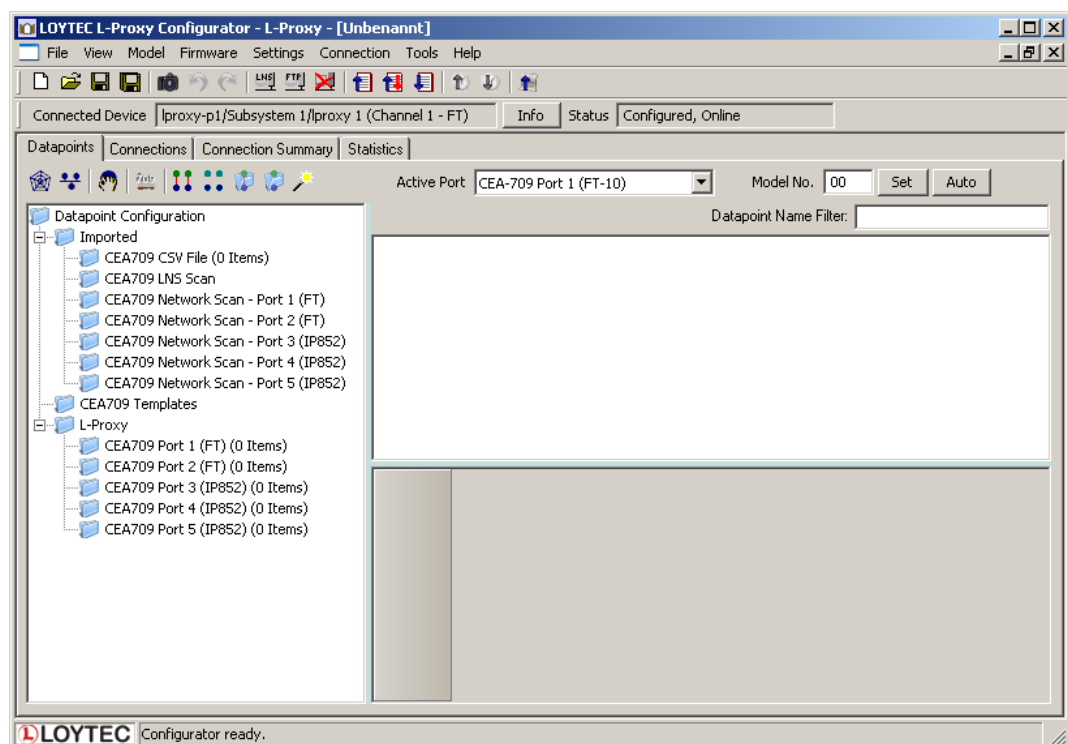
Figure 101: L-Proxy Configurator main window.

7.9.2 Starting Stand-Alone

The L-Proxy can also be used without LNS-based tools. In this case, the L-Proxy Configurator needs to be started as a stand-alone application. Go to the Windows **Start** menu, select **Programs**, **LOYTEC L-Proxy Configurator** and then click on **Configure L-Proxy**. This starts the L-Proxy Configurator and the main connections screen is displayed.

If the L-Proxy is not yet connected to the network, go to the **Firmware** menu and select the firmware version of the L-Proxy to be configured. If the L-Proxy is already connected to the network it is recommended to connect the configuration software to the L-Proxy.

To Connect to a L-Proxy Stand-Alone

1. Select the FTP connection method by clicking on the **FTP connect** button
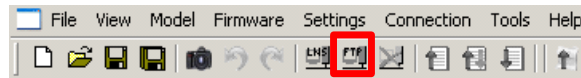
in the tool bar. The FTP connect dialog as shown in Figure 102 opens.
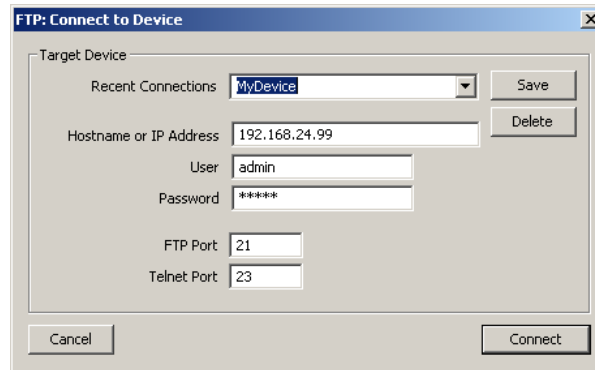
Figure 102: FTP connection dialog.

2. Enter the IP address of the device, the user name and password. The default user is 'admin' and the default password is 'admin'.

3. Optionally, click into the **Recent Connections** field and enter a user-defined name for this connection. That name can be selected later to connect. Click on **Save** to store that connection.

4. If your device is located behind a NAT router of firewall, you may change the FTP and Telnet ports to your needs for accessing the device. Clicking **Save** also stored these settings.

5. Click on **Connect**. This establishes the connection to the device.

7.9.3 Uploading the Configuration

To get the current network variable configuration of the L-Proxy, the port interface needs to be uploaded. This will upload the entire configuration from the L-Proxy, including data points, dynamic NVs, and schedules.

To Upload a Configuration

1. Click on the **Upload** button
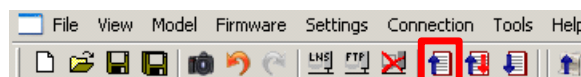
in the tool bar. The configuration upload dialog opens up as shown in Figure 103.
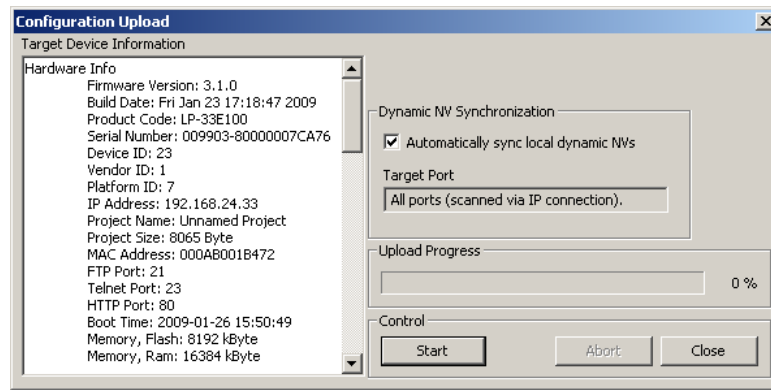
Figure 103: Configuration upload dialog.

2. If the check-box **Automatically sync local dynamic NVs** is marked, any manually created dynamic NVs will be uploaded and merged into the data point configuration.

3. Click on the button **Start** to start the transfer. This will upload the configuration of all ports, if the software is connected stand-alone via FTP or the network variable interface, for which the LNS plug-in was started for.

4. When asked, if schedules shall be uploaded also, click **Yes**, if you want the current schedule configuration be extracted from the device. Note, that when doing so, the original schedules in the project are replaced by the uploaded schedules.

5. If dynamic NVs were synchronized, click on **Finish**.

7.9.4 Scanning for Network Variables

When the L-Proxy Configurator is connected to an LNS database, network variables can be scanned from that data base.

To scan network variables from the LNS database

1. Click on the **Datapoints** tab.
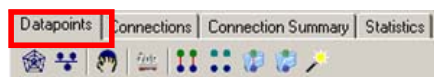
2. Click on the button 🔳 **Scan channel**. This scans in all NVs on all devices connected to the CEA-709 channel of the L-Proxy.

3. After the scan has completed, the folder **LNS Database Scan** is populated with the found NVs. Data point names for those NVs are automatically generated, following the data point naming rules defined in the project settings (see Section 7.3.2). By default the name is generated from node name, object name, and NV name. These names are ensured to be unique by adding a counter for multiple occurrences of the same name.
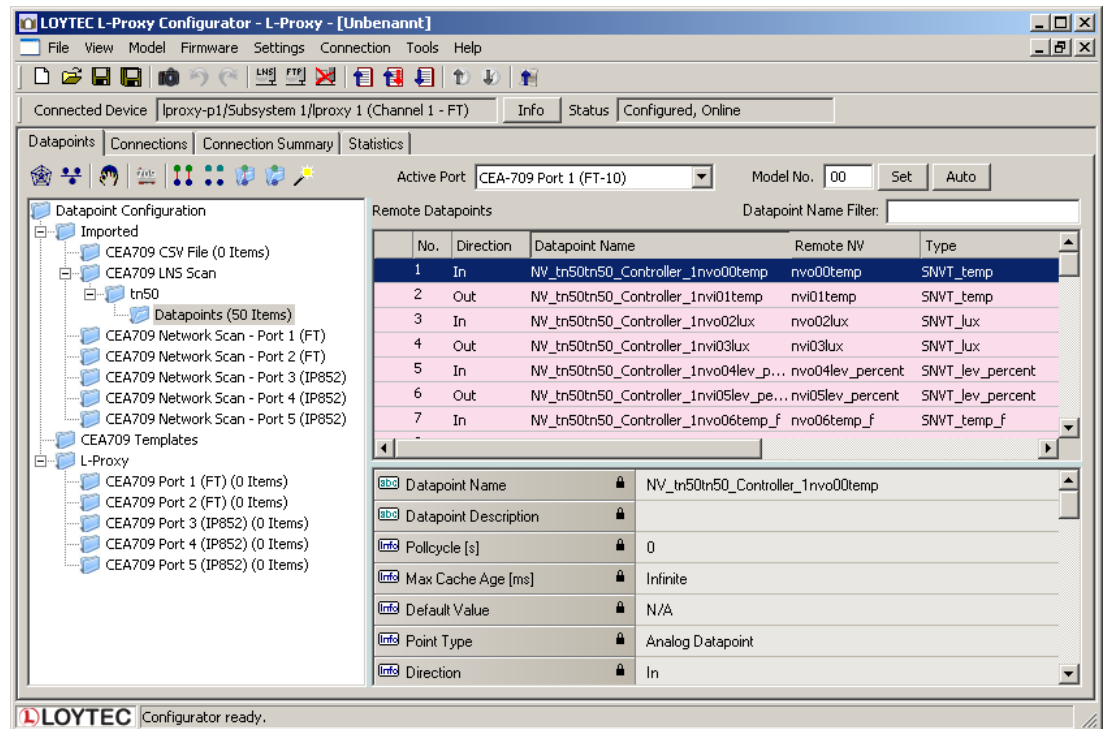
Figure 104: Scanned NVs in the LNS Database Scan Folder

Figure 104 shows an example result of the database scan. The list can be sorted by each column. Selecting a line will display a number of associated properties in the property view below. Multiple items can be selected by using the <Ctrl> key and clicking with the mouse. All items can be selected by pressing <Ctrl-A>.

7.9.5 Importing Network Variables

Without LNS, the tool cannot connect to an LNS database, where it scans for network variables (NVs). Therefore, the list of NVs to be used on L-Proxy has to be available in a CSV file. This file can be produced by external software or created by hand. The CSV format for importing NVs is defined in 9.1.1.

To Import NVs from a File

1. Click on the **Datapoints** tab.
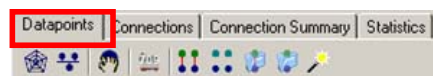
2. Select the folder **CEA709 CSV File**
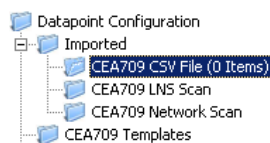
3. Right-click and select **Import File**. In the following file selector dialog, choose the CSV import file and click **OK**.
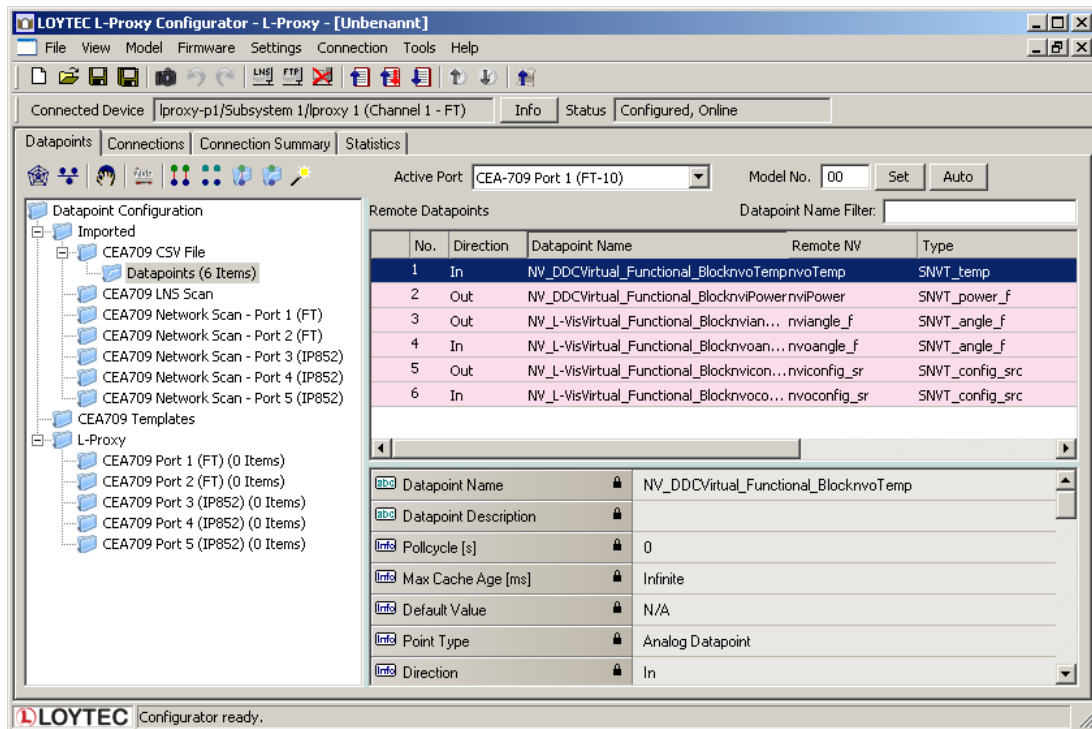
Figure 105: Imported NVs

4. Now the CSV File folder is populated with the imported NVs as shown in Figure 105.

The list can be sorted by each column. Selecting a line will display a number of associated properties in the property view below. Multiple items can be selected by using the <Ctrl> key and clicking with the mouse. All items can be selected by pressing <Ctrl-A>.

7.9.6 Scanning NVs Online From the Network

L-Proxy devices also support an online network scan on the CEA-709 network. In this scan, the device searches for other devices on the CEA-709 network and pulls in NV information of these devices. These NVs can then be used instead of importing them from a CSV file.

To Scan NVs Online Off the CEA-709 Network

1. Click on the **Datapoints** tab.

2. Select the folder **CEA709 Network Scan** of the appropriate port.
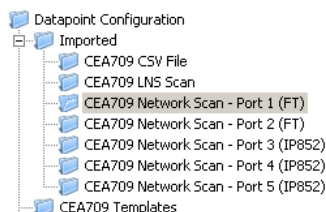
3. Right-click on that folder and select **Scan CEA709/852 Network…**. This opens the CEA709/852 Network Scan dialog as shown in Figure 106.
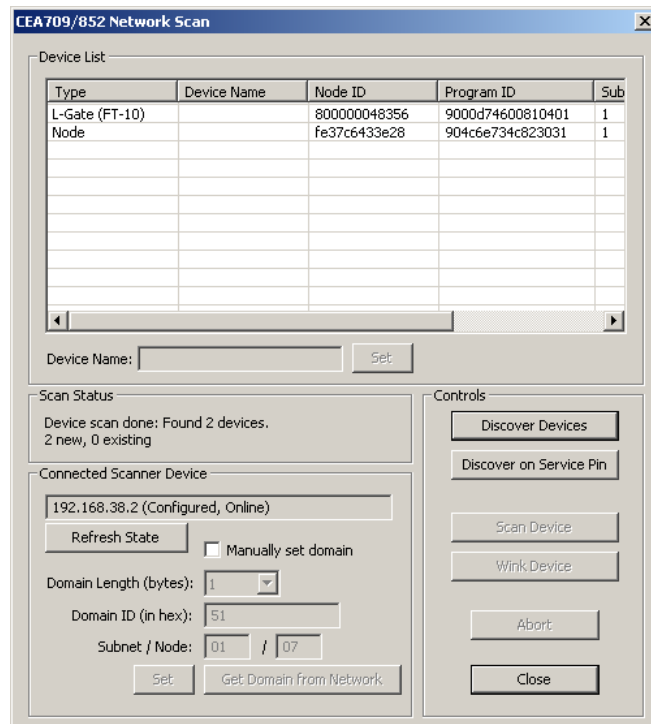
Figure 106: CEA-709 network scan dialog.

4. Click on the button **Discover Devices**. This starts a network scan. The results are put in the device list box.

5. Alternatively, click the button **Discover on Service Pin**. Then press the service pin of a particular device on the network. This device will be added to the device list.

6. Select a device in the device list and click the button **Scan Device**. This scans the NVs on the selected device and adds them to the CEA709/852 Network Scan folder as a separate sub-folder for the device as shown in Figure 107.

Tip!   *If you are not sure which device you have selected, click on **Wink Device**. The selected device will execute its wink sequence.*
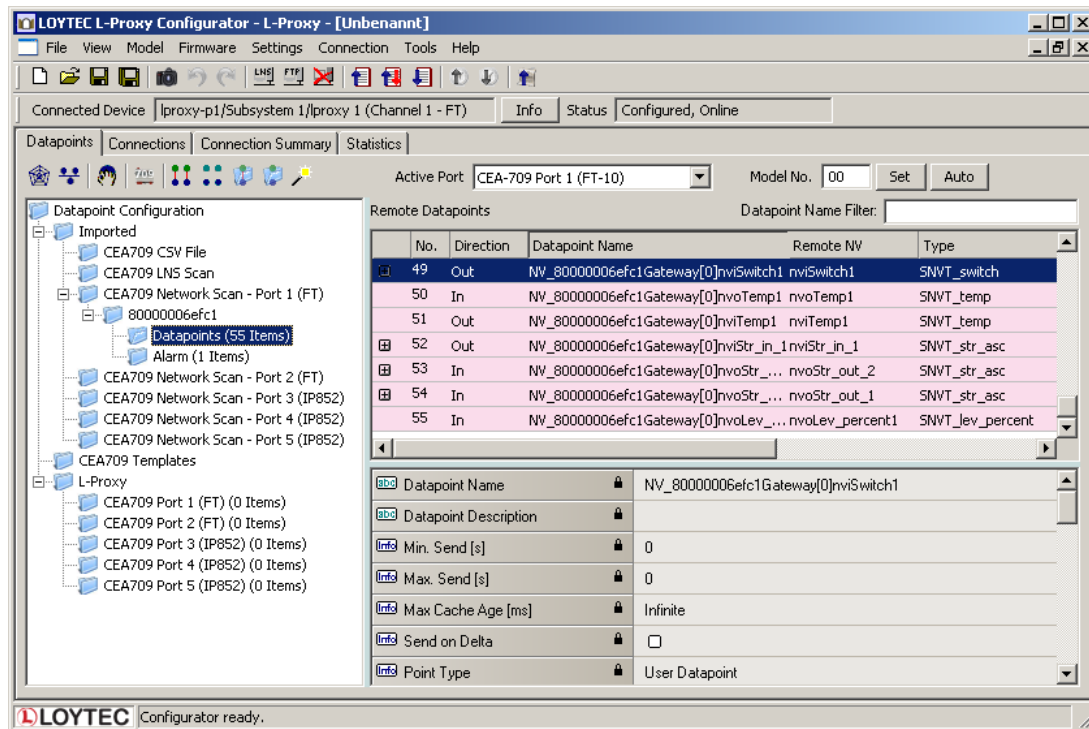
Figure 107: CEA-709 network scan results.

7. Click **Close** when all devices needed have been scanned.

7.9.7 Select and Use Network Variables

Data points in the **CEA709 LNS Scan** folder, the **CEA709 Network Scan** folder or in the **CEA709 CSV File** folder can be selected for use on the device. Select those NVs, which shall be used on the device.

To Use NVs on the Device

1. Go to any of the **CEA709 LNS Scan**, **CEA709 Network Scan** or the **CEA709 CSV File** folder.

2. Use the multi-select feature by holding the *Shift* or *Ctrl* keys pressed.

3. Click on the button 🖐 **Use on Device** in the tool bar.

4. This creates data points in the L-Proxy/CEA709 Port folder. All data points in that folder will actually be created on the L-Proxy device after downloading the configuration.

Tip!   *Data points can be edited by selecting a single point or using multi-select. The available properties to be edited are displayed in the property view below.*

7.9.8 Change the NV Allocation

After selecting the **Use on device** action on scanned or imported NVs, they are assigned a default NV allocation in the L-Proxy/CEA709 port folder. This default allocation can be changed, e.g., for imported NVs when they shall be allocated as static NVs on the L-Proxy.

To Change the NV Allocation Type

1. In the data point view, select the NVs in the L-Proxy/CEA709 port folder, for which the NV allocation shall be changed.

Tip!   *By using Ctrl-A all NVs can be selected.*

2. Select the **NV allocation** property as indicated by the red rectangle in Figure 108.

3. To make the data points static NVs on the L-Proxy, select **Static NV**.
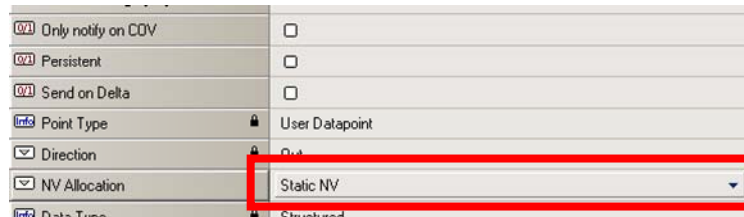
Figure 108: Change the NV allocation type.

7.9.9 Create Static NVs

The L-Proxy can be configured to change its static interface and boot with a new one. Apart from creating static NVs from scanned or imported data points, static NVs can also be created manually in the L-Proxy/CEA-709 folder.

To Create Static NVs Manually

1. Select the L-Proxy/CEA-709 Port/Datapoint folder
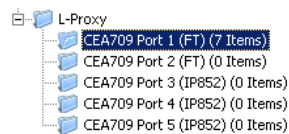
2. Right-click in the data point list and select **New Datapoint…** in the context menu. This opens the NV creation dialog as shown in Figure 109.

Figure 109: Create a static NV manually.

3. Enter a data point name and a programmatic name. The programmatic name is the name of the static NV which is being created.

4. Select a resource file. To create a SNVT, let the STANDARD resource file be selected.

5. Select a SNVT and a direction. If a non-standard resource file has been selected, choose from one of the UNVTs.

6. Choose a functional block, where this static NV shall be located in.

7. Click **Create Static NV**. The static NV is created and appears in the data point list.

8. Note, that the static interface of the L-Proxy will change as soon as static NVs are added or modified in the data point manager. This change is reflected in a new model number, which the L-Proxy will receive after the configuration download (see Section 6.5.2). Also note that the manually created static NVs are not bound automatically by the L-Proxy Configurator. They simply appear on the device and need to be bound in the network management tool.

7.9.10 Create External NVs

External NVs are not actually allocated NVs on the L-Proxy. Instead, the L-Proxy uses polling to read data from and explicit updates to write data to external NVs. Since external NVs do not affect the static NV interface of the L-Proxy, they can be used to extend an L-Proxy's interface configuration at run-time, where no LNS with dynamic NVs is available.

To Create an External NV manually

1. Select the L-Proxy/CEA-709 Port/Datapoints folder
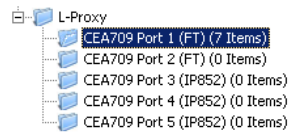
2. Right-click in the data point list and select **New Datapoint…** in the context menu. This opens the NV creation dialog.

3. Click on the tab **External** as shown in Figure 110.
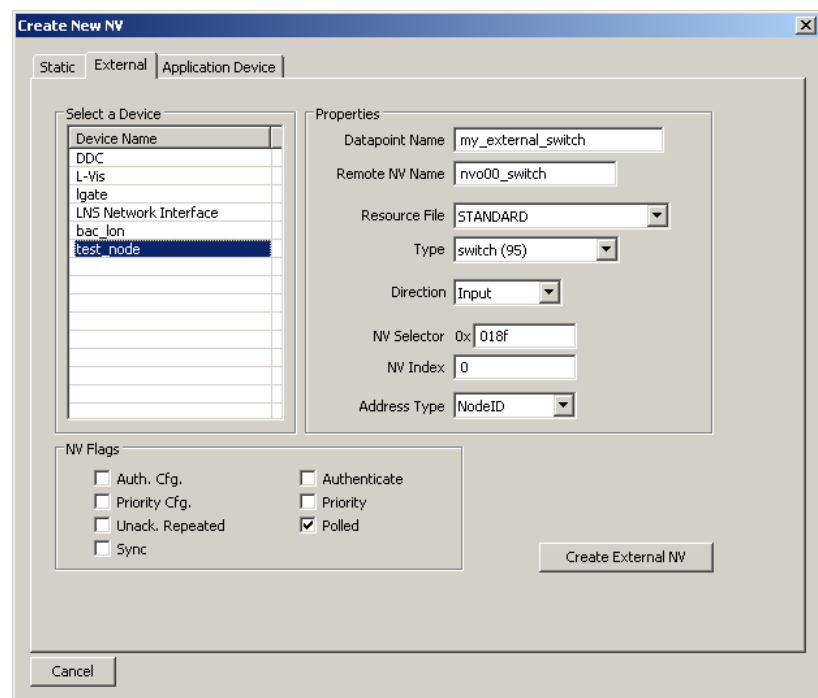
Figure 110: Create a new external NV.

4. Select the device in the box **Select a Device** on the left-hand side.

5. Enter the properties of the external NV on that device, starting with the local data point name, the remote programmatic NV name, the NV type (SNVT) and direction. Note, that the direction is the direction of the external NV on the L-Proxy. Therefore, the remote output NV nvo00_switch becomes an input on the L-Proxy. Also enter the NV selector in hexadecimal and the NV index in decimal notation. Choose the preferred addressing mode, e.g., Node ID.

6. Click **Create External NV** to add this NV to the data point list.

7. The external NV now appears in the data point list as shown in Figure 111. For external NVs which are inputs to the L-Proxy, adapt the poll cycle property to your needs.
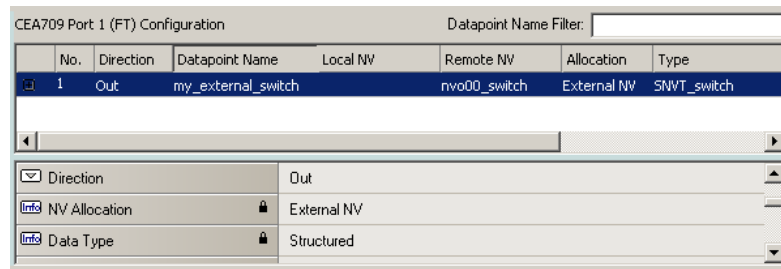
Figure 111: Manually created external NV in the port interface definition.

7.9.11 Configuration Download

After the data points have been configured, the configuration needs to be downloaded to the L-Proxy. For doing so, the L-Proxy must be online. If the L-Proxy is not yet connected to the network, the configuration can be saved to a project file on the local hard drive.

If connected via LNS, and the NVs on the L-Proxy are "Static NV" or "Dynamic NV", the L-Proxy Configurator can create the bindings automatically. This behavior can be influenced by the download dialog. When connected via LNS, the download procedure also manages the device template upgrade in the LNS database, if the static NV interface has been changed.

To Download a Configuration

1. In the main connections window, click on the **Download Configuration** speed button
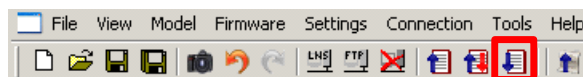
in the tool bar. This will open the configuration download dialog as shown in Figure 113.

2. If the static NV interface has been changed, a new model number for the L-Proxy needs to be selected. This is necessary, as the static network interface of the L-Proxy changes on the CEA-709 network. The L-Proxy Configurator opens a dialog to display the interfaces and needed updates as shown in Figure 112.
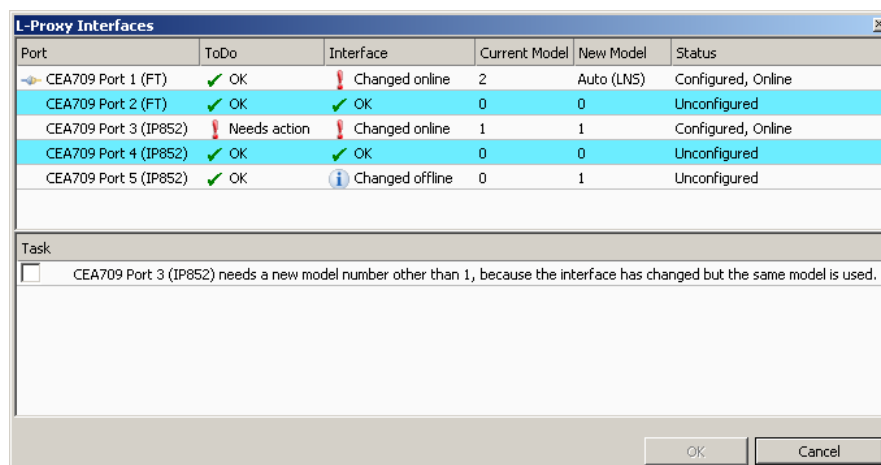
Figure 112: Model Number Dialog in the L-Proxy Configurator

3. When connected via LNS, the connected port is indicated by the 🔌 icon. On this port, the Configurator chooses an automatic model number to fit the LNS database and also upgrades the underlying device template. No further action is needed on that port.

4. Other ports, which are configured, online and the Configurator does not have an LNS connection for, any changed static interface appears with a red exclamation mark ❗ . The user needs to click in the **New Model** column and enter a new, unused model number for that port.

CEA709 Port 3 (IP852)	❗ Needs action	❗ Changed online	1	2	Configured, Online

---

Important!   ***Interfaces that are Configured, Online must be assigned a new, unique model number. Otherwise, the new static interface is not usable in the LNS database of that port.***

---

5. With the new model number the port gets a green check mark ✔ OK . The task item in the **Task** list below disappears.

6. Other ports, which have a changed static interface but are not configured in their LNS database appear with an information sign ℹ️. The Configurator increments the model number for that port. Still check, if that new model number will fit the needs.

7. Click **Ok**.

8. The download dialog as shown in Figure 113 appears.
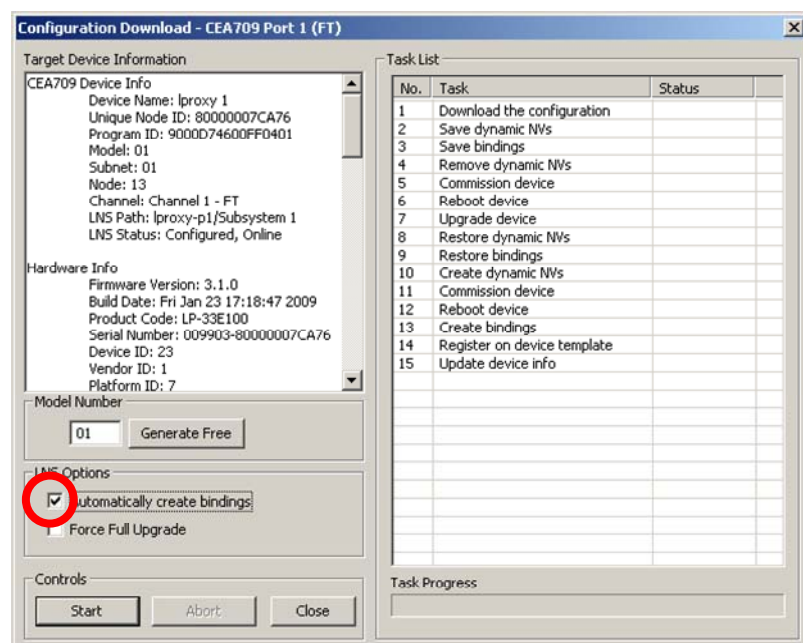
Figure 113: Configuration Download Dialog

9. If no bindings shall be generated, deselect the **Automatically create bindings** checkbox indicated by the red circle in Figure 113.

10. Click **Start** to start the download. Each of the actions is displayed in the **Task List** section of the dialog. The current progress is indicated by the progress bar below.

11. When the download process has finished, a notification window appears, which has to be acknowledged by clicking **OK**.

Note, that after the download is complete, the interface changes become active on the L-Proxy (i.e., the static NV interface has changed). Refresh the network management tool to synchronize the tool with the changes to the LNS database made by the L-Proxy Configurator (e.g., use the menu "LonMaker|Refresh" in LonMaker or hit *F5* in NL-220).

Normally, the Configurator software optimizes the download process by not executing certain LNS operations, if not necessary. For example, only those bindings and dynamic NVs are deleted and re-created, which correspond to real changes in the interface. The user can check the **Force Full Upgrade** option to clean and re-do all steps.

Note: *In the simple mode the L-Proxy Configurator never modifies the LNS database. In this mode, the configuration is only downloaded to modify connections.*

After the download has completed, the LNS databases for those ports on which the static interface has changed must be opened by the respective engineers and upgraded to the new interface. Refer to Section 7.9.16 on how to use the Configurator assisting this task.

7.9.12 Exchange the Port Interface Definition

To exchange the port interface definitions, engineers need to export and import the port interface definition files (.itf). Access to these functions is given through the Datapoint Manager dialog.

To Extract the Port Interface Definition

1. Select the **CEA-709 Port** folder
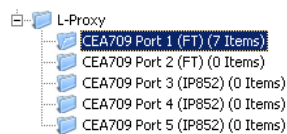
2. To upload dynamic NVs of the port to be exported, right-click on the port folder. In the context menu select **Sync Dynamic NVs**.

3. The Configurator then loads any new dynamic NVs, which have been created and are not yet part of the port. The process completes by reporting how many dynamic NVs have been synchronized.

4. Right-click on the port folder and select **Export Interface…** in the context menu. This opens a file requestor.

5. Save the port interface definition file giving it a useful name, e.g., as "myproxy-port2.itf".

To Import a Port Interface Definition

1. Right-click on the port folder and select **Import Interface…**. This opens a file requestor, where the corresponding .itf file can be chosen.

2. If the new port interface contains additional NVs they are created. If NVs have been removed in the new port interface, which is part of a current connection, the user is prompted whether these NVs shall really be deleted.

7.9.13 Build XIF for Port Interface

When using static NVs on the L-Proxy, the L-Proxy Configurator can export a new XIF file for the changed static interface. Before exporting the XIF for the interfaces it is recommended to download the configuration into the device. In this case, the Configurator can verify that the model number of the port is correct.

To Create a XIF File

1. Change the active port to the port the XIF shall be exported for.

    Active Port | CEA-709 Port 2 (FT-10) | ▼

2. Make sure the **Model No** will match the final model number on that port. If not, enter an appropriate model number and click **Set**.

    Model No. | 02 | Set | Auto

3. Select the **CEA-709 Port** folder

    ```
    ⊟ 📁 L-Proxy
         📁 CEA709 Port 1 (FT) (7 Items)
         📁 CEA709 Port 2 (FT) (0 Items)
         📁 CEA709 Port 3 (IP852) (0 Items)
         📁 CEA709 Port 4 (IP852) (0 Items)
         📁 CEA709 Port 5 (IP852) (0 Items)
    ```
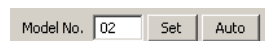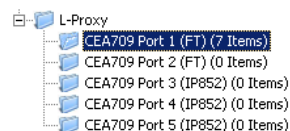
4. Right-click on that folder and in the context menu select **Build XIF …**.

5. This opens a file requestor where the XIF file name needs to be entered. Select a useful name to identify the L-Proxy, e.g., as "lproxy_p1_1.xif".

7.9.14 Enable Legacy NM Mode

For network management tools, which do not support the ECS (enhanced command set) network management commands, the legacy network management mode must be configured. Please contact the tool's vendor for information whether ECS is supported or not. Note, that changing to legacy network management mode changes the static interface of the device.

To Enable Legacy NM Mode

1. In the L-Proxy Configurator menu go to **Settings → Project settings …**

2. Click on the tab **CEA709**.

3. Put a check mark in **Enable Legacy Network Management Mode** of the appropriate port(s).

    Project Settings   ✕
    General | Datapoint Naming Rules | CEA709 |
    ┌ Datapoint Settings ─────────────┐   ┌ Enable Legacy Network Management Mode ─┐
    │ Default Pollcycle for External NVs: 10   s │   │ ☑ Port 1 (FT-10)   ☐ Port 2 (FT-10) │

4. Click **OK.**

5. Download the configuration to activate the change.

7.9.15 Upload Dynamic NVs from Device

In LNS-based tools it is possible to create dynamic NVs on the device manually. This is a possible workflow to engineer the NV interface of the device in the LNS database. To use those manually created dynamic NVs, the L-Proxy Configurator must synchronize its dynamic NV information with the port.

To Upload Dynamic NVs

1. Select the **CEA709 Port** folder.
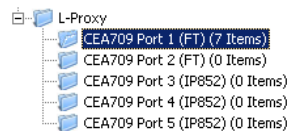
2. Right-click and select **Sync Dynamic NVs** in the context menu. The L-Proxy Configurator then loads any new dynamic NVs, which have been created and are not yet part of the port interface definition. The process completes when the dialog shown in Figure 114 appears.
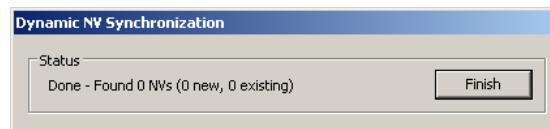
Figure 114: Synchronizing dynamic NVs from the device.

3. Click on **Finish**. The new dynamic NVs now appear in the data point list and can be edited and used on the device.

7.9.16 Repair LNS Database from Device

When working with static NVs in advanced mode, the static interface of any port can be changed by creating or modifying static NVs. If connected via LNS to port A, all changes to port A are upgraded into the LNS database when downloading the configuration. If another port (port B) that is not the port currently connected to the LNS database is modified, this can lead to problems. Because the static interface of port B is changed, it gets another model number and is no longer correctly recognized in port B's LNS database. The same problem can occur in advanced mode, when connected via FTP in stand-along mode. In this case, no static interface change can be upgraded into an LNS data base.

When this happens, the engineer of the changed port can no longer access his port in the LNS database. He would need to delete the old device and add a new device by uploading the device template from the network or by using the XIF file. In either case, the bindings and dynamic NVs are lost.

To fix the problem of a changed static interface, where the LNS database is out-of-sync, the L-Proxy Configurator provides a tool to update the database from the current device's interface without deleting the old device.

To Repair the LNS Database from the Device

1. Start the L-Proxy Configurator as LNS plug-in on the device to repair (see Section 7.9.1).

2. The Configurator will detect that the current static interface of the device's port is out-of-sync with the database and ask to repair.
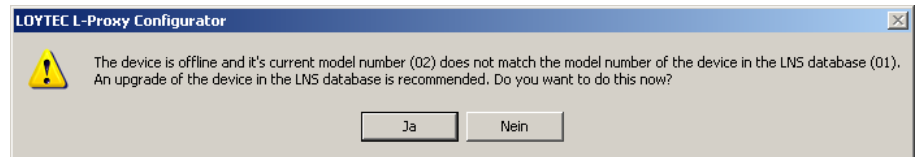
3. Click **Yes**.

4. To force the procedure you can alternatively click on the **Upload Configuration and Update LNS** button.
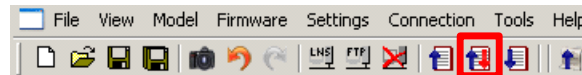
5. This uploads the current configuration from the device and opens the download dialog.

6. Click **Start** and follow the project download, which also upgrades the device in the LNS database according to the new static interface. For more information on the project download refer to Section 7.9.11.

7. Open your LNS-based or refresh (e.g., use the menu **LonMaker → Refresh** in LonMaker or hit **F5** in NL-220).

7.9.17 Deleting Connected Data Points

When deleting data points from the data points list these data points might be part of a connection. In principle, there are two options for the user. First, the data points are deleted and removed from any existing connections that they participated in. The connections are left untouched. Second, the connections and all connected data points are deleted altogether.

To Delete all Connected Data Points

1. Select the data points in the data point list, which shall be deleted. Use the multi-select features to select more than one data point.

2. Right-click and select **Delete** or hit the *Del* key.

3. A dialog as shown in appears listing the data point that re being deleted.
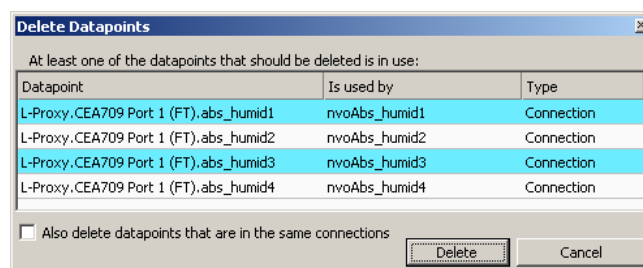
Figure 115: Report for Deleting Data Points and Connected Data Points.

4. Select the check mark at the bottom of the dialog.
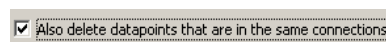
5. Click **Delete**.

7.10 Advanced CEA-709 Configuration

7.10.1 Working with Configuration Properties

Configuration properties (CPs) are supported by the LNS network scan and the online network scan. They can be selected and used on the device in a similar way as NVs. There is a notable difference to NVs: CPs are part of files on the remote nodes. Reading and writing CPs on the L-Proxy results in a file transfer.

The L-Proxy supports both, the LONMARK file transfer and the simpler direct memory read/write method. In both cases however, one has to keep in mind that a file transfer incurs more overhead than a simple NV read/write. Therefore, polling CPs should be done at a much slower rate than polling NVs.

Another aspect is how CPs are handled by network management tools. Formerly, those tools were the only instance that could modify CPs in devices. Therefore, most tools do not automatically read back CPs from the devices when browsing them. This can result in inconsistencies between the actual CP contents on the device and their copy in the network management tool. It is recommended to synchronize the CPs from the device into the LNS database before editing and writing them back.

To Synchronize CPs in NL220

1. Double-click on the device object in the device tree

2. Press the **Upload** button on the Configuration tab of the device properties (see Figure 116).
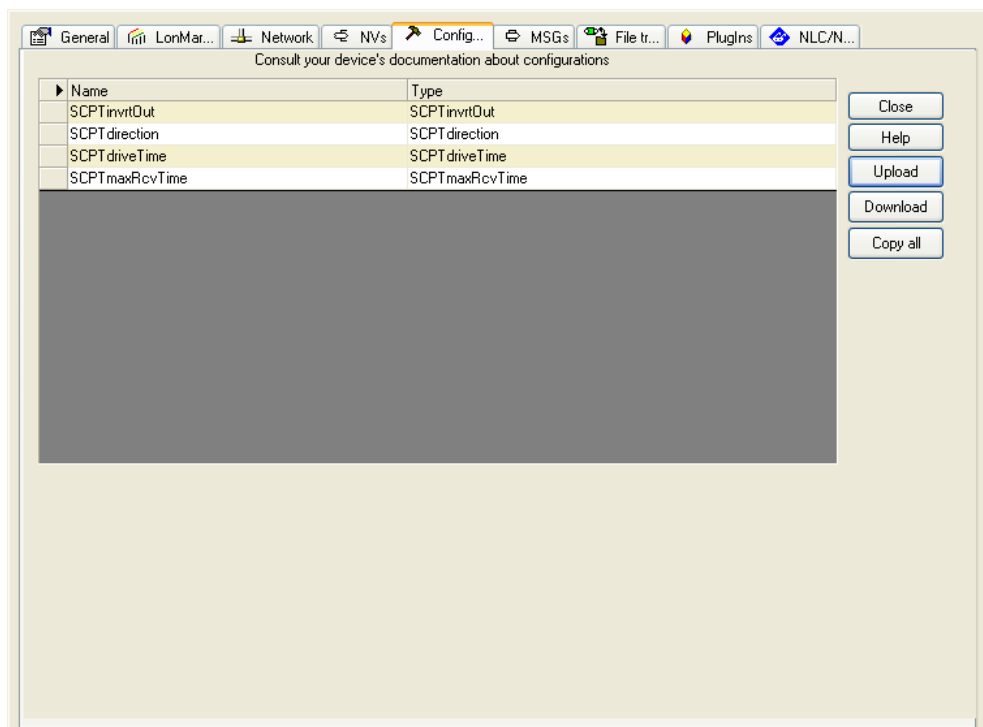
Figure 116: Configuration Tab for Configuration Properties in NL220.

To Synchronize CPs in LonMaker TE

1. Right-click on a device object and select **Commissioning → Resync CPs…** from the context menu.

2. This opens the dialog shown in Figure 117.
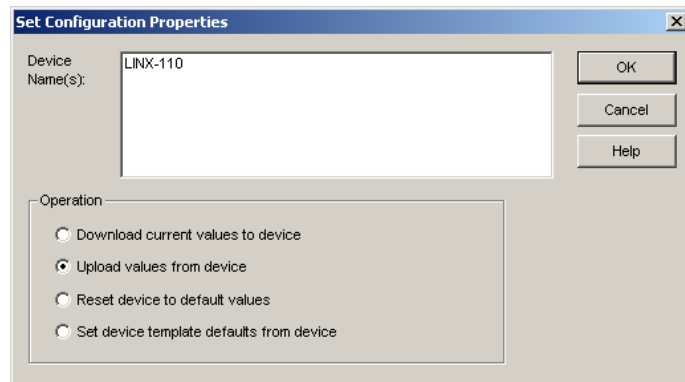
Figure 117: Set Configuration Properties in LonMaker TE.

3. In this dialog select the radio button **Upload values from device** in the **Operation** group box. To use the current settings of the device as default values for new devices, select **Set device template defaults from device**.

4. Execute the operation by clicking the **OK** button.

7.10.2 Upload the System Log

The system log on the device contains important log messages. Log messages are generated for important operational states (e.g., last boot time, last shutdown reason) or errors at run-time. This file is important for trouble-shooting and is available on the Web UI (see Section 5.3.5). The file can also be uploaded from the device with the L-Proxy Configurator.

To Upload the System Log

1. Connect to the L-Proxy via the FTP or LNS method (see Section 7.9.2).

2. Click on the **Upload system log** button
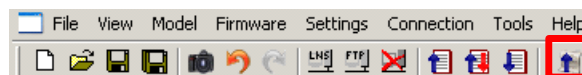
in the tool bar. The upload system log dialog as shown in Figure 118 opens showing the upload progress.
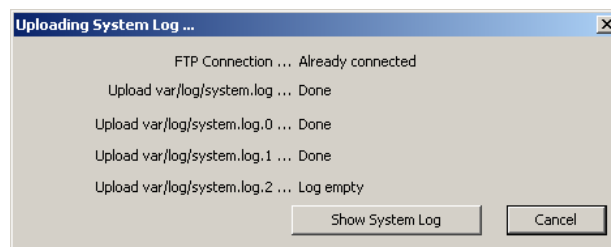
Figure 118: Upload system log dialog.

3. When the upload is finished, click on **Show System Log**. The system log window appears as shown in Figure 119.
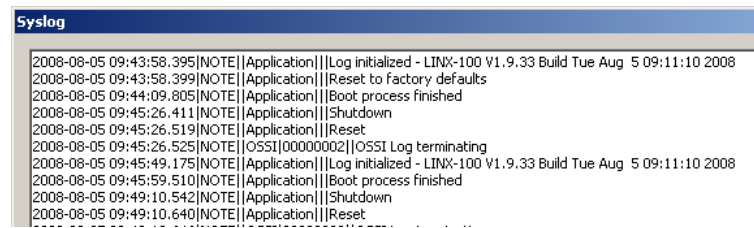
Figure 119: System log window.

4. Click on **Save** to store the system log into a file on your local hard drive.

7.11 Connections

7.11.1 Create a New Connection

After having configured the device's network ports with data points, internal connections between those data points can be created. Usually, the manual method to create a connection is used to create connections between different named data points.

A connection is an internal mapping in the device between input and output data points. A connection always consists of *one* hub data point and *one or multiple* target data points. Hub data points can be input or output. If the hub data point is an input, then the target data points must be output and vice-versa. All data points in the connection must be of a compatible type.

To Manually Create a New Connection

1. Click on the **Connections** tab.
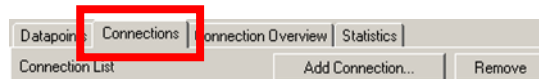
2. Click **Add Connection**. A new connection is added to the connection list. Rename the connection if you want to do so.

3. Click on **Select Hub Point …** to select the hub point. This opens a list of all available data points. Select one and click **OK**.

4. Then click on **Add Target…** Similar to 2) select all target data points. You may use multi-select to select more than one data point at a time.

Note: *By default only compatible data points are displayed. Sometimes compatible data points are available as member points (e.g., a SNVT structure member). Click on ⊞ to expand the data point and select the desired member point.*

5. Now the connection dialog contains a hub and two target data point as shown in Figure 120.
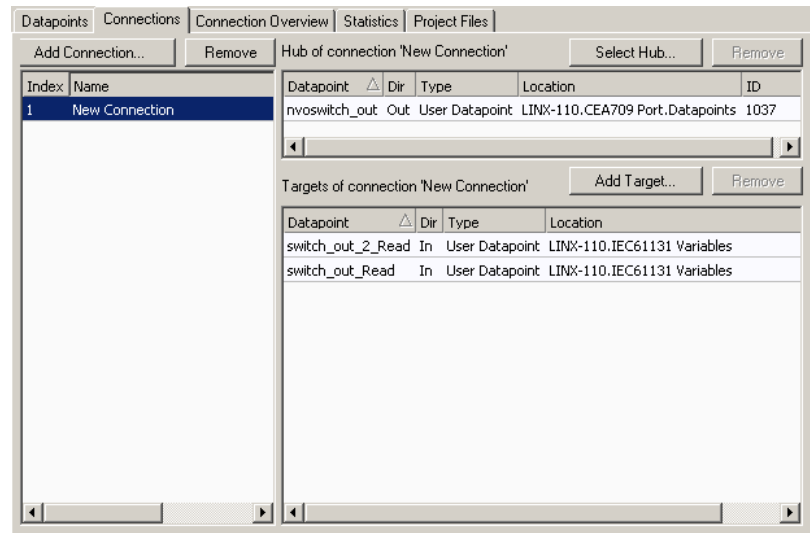
Figure 120: Connection dialog with hub and target points.

7.11.2 Auto-Create Connections for NVs

Creating internal connections in the L-Proxy manually is a slow process. The auto-connection feature provides a fast method to create connection for a large number of data points. To use this feature, one needs to take care when giving names to NVs. The auto-connect tool creates connections for all compatible input and output network variables that have the same name after the prefixes 'nvi' or 'nvo' have been removed from their names.

Here is an example: For "nviTemp0" on port1, "nvoTemp0" on port 2 and "nvoTemp0" on port 3 a connection called nviTemp0 is created containing those three data points.

Note, that NVs are not required to be on different L-Proxy ports in order to be added to connections. This means if an "nviHumid9" and an "nvoHumid9" are both on port 1, a connection for those two NVs will be created.

To Auto-Connect NVs

1.   Prepare NVs names as they shall take part in connections. Dynamic and static NVs can be created for this purpose.

2.   Click on the **Magic Wand** button
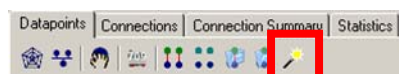
in the tool bar of the **Datapoints** tab.

3.   Once connections are generated, the auto-connect feature can be re-applied as soon as new NVs are added. If they are compatible and their names match, they are added to existing connections. Otherwise, new connections are created.

7.11.3 Generate and Connect from NVs

In advanced mode, there exists an alternative way to create data points and connections automatically. The *generate and auto-connect* feature allows selecting any number of data points on a port and generate the counterparts on another port. The counterparts are automatically added to a connection with their original data points. It shall be noted, that this method always changes the static interface of the port where the data points are created.

To Generate and Connect from NVs

1. Click on the **Datapoints** tab.
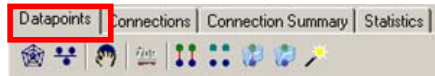
2. If the NVs shall be generated on another port than the currently connected one, select a different port in the drop-down list of the data point manager, e.g., Port 2.
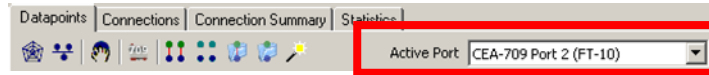
3. In the **CEA-709 Port** folder that contains the original data points, e.g., Port 1, select all the NVs, which shall be mapped. The multi-select feature or <Ctrl-A> may be used for doing this.

4. Click on the speed button **Generate Points and auto-connect** in the tool bar. This creates exact copies of the selected NVs as static NVs on Port 2 using the opposite direction.

5. Alternatively, you can select the **CEA-709 Port** folder (or any sub-folder) and click the speed button **Folder-wide Generate points and auto-connect** in the tool bar. This generates counter-part NVs and connections for all NVs in the selected folder.

6. When the generation is complete, a dialog reports how many connections have been created. To view a report click **Yes** in the dialog. Click **No** to proceed without a report.
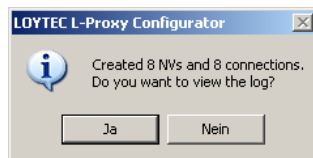
7. The generated NVs now appear as static NVs in the **CEA-709 Port** folder that has been selected as the configuration port.

Important!   *When generating static NVs on another port than the one connected to the LNS database, the static interface of that port will be changed and no longer be available in the LNS database for that port.*

If the static interface of another port has been changed, notify the engineer responsible for that port. Refer to Section 7.9.16 on how to repair such an interface in the LNS database.

7.11.4 Create Connections from a CSV File

A quick way to perform batch edit on connections is to export and import connections from the connections CSV file. Each line in the connections CSV file identifies a connection. The first column is the connection name. The second column specifies the hub data point. The full path to the data point must be specified using the dot '.' as the folder separator. The third and following columns specify the target data points.

To Create Connection from a CSV File

1. Select the menu **Tools → Export Connections …**

2. Select an appropriate file name and export.

3. Edit the connections CSV file. An example is shown in Figure 121.

```
#connection_csv_ver,1
#ConnectionName,HubDPName,TargetDPName
nvoAbs_humid1,L-Proxy.CEA709 Port 1 (FT).abs_humid1,L-Proxy.CEA709 Port 2
(FT).abs_humid1
nvoAbs_humid2,L-Proxy.CEA709 Port 1 (FT).abs_humid2,L-Proxy.CEA709 Port 2
(FT).abs_humid2
nvoAbs_humid3,L-Proxy.CEA709 Port 1 (FT).abs_humid3,L-Proxy.CEA709 Port 2
(FT).abs_humid3
nvoAbs_humid4,L-Proxy.CEA709 Port 1 (FT).abs_humid4,L-Proxy.CEA709 Port 2
(FT).abs_humid4
```

Figure 121: Example Connection CSV File.

4. Select the menu **Tools → Import Connections …**

5. If connections that are not part of the connection CSV file shall be deleted, click **Yes** when prompted. Click **No** if the other connections shall be left as is.
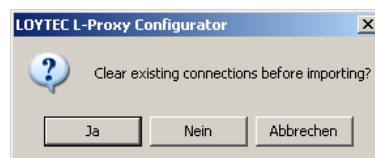
6. Choose the file to import and click **Ok**.

7. When the import has completed, optionally view the log to check, which connections have been added, modified, and deleted.

7.11.5 Modify Connections

Connections can be edited and deleted. This is also done in the **Connections** tab of the main window. Editing connections does not influence the data point configuration. This means, when deleting a connection or adding/removing data points to/from a connection, the data points are not deleted.

To Edit a Connection

1. Change to the **Connections** tab of the main window.

2. Select the connection to edit. Then follow the steps as applied when creating a connection.

3. To delete a target, select the target and click on **Remove Target(s)**.

To Delete a Connection

1. Change to the **Connections** tab of the main window.

2. Select the connection for removal. Use multi-select to select more than one connection.

3. Click **Remove**.

7.11.6 Connection Overview

Select the **Connection Summary** tab to get a graphical representation of all connections. It represents the two connected data points, their technology they are based on and the direction of the connection. An example for the overview is shown in Figure 122.

Figure 122: Connections Summary.

8 Application Scenarios

This chapter shows some networking scenarios that are typical applications for L-Proxy. Please note that only few scenarios are shown right now and this chapter will be continuously updated with new application areas.

8.1 Address Table Extension

L-Proxy can be used to expand the number of address table entries available in a standard node that uses a Neuron Chip. If more than 15 destination addresses are required by the application one can use L-Proxy to overcome this limitation. Also if the node is a member of more than 15 groups L-Proxy can help to remove this restriction.

8.1.1 Saving Entries in the Address Table

Figure 123 shows a simple network diagram comprising three Neuron Chip powered nodes. Each node contains four LONMARK objects: a node object, an actuator object and two sensor objects. The actuator object controls a lamp; the two sensor objects are connected to switches.

The two output network variables nvoSwitch0 on node 6 is bound to nviLampValue0 on node 7 and on node 8. The two bindings use up two entries in the address table.
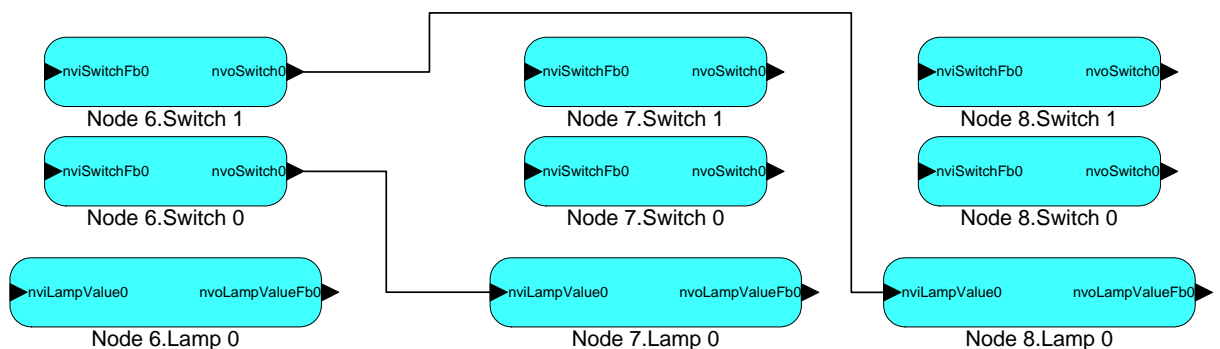
Figure 123: Two individual subnet/node addressed bindings use up two entries in the address table.

Figure 124: Protocol analyzer log file for the 2 subnet/node bindings shown in Figure 123. Node 6 first sends a packet to node 7 and then a packet to node 8.

L-Proxy can be used to make a single subnet/node addressed binding from the source node to L-Proxy. L-Proxy then completes the binding to the final destination nodes 7 and 8. In this case one entry in the address table was saved in the source node (node 6). Figure 125 shows the same network from above but now we added one port of L-Proxy (Port 2) to have a single destination address for node 6 thus saving an entry in the address table of node 6.
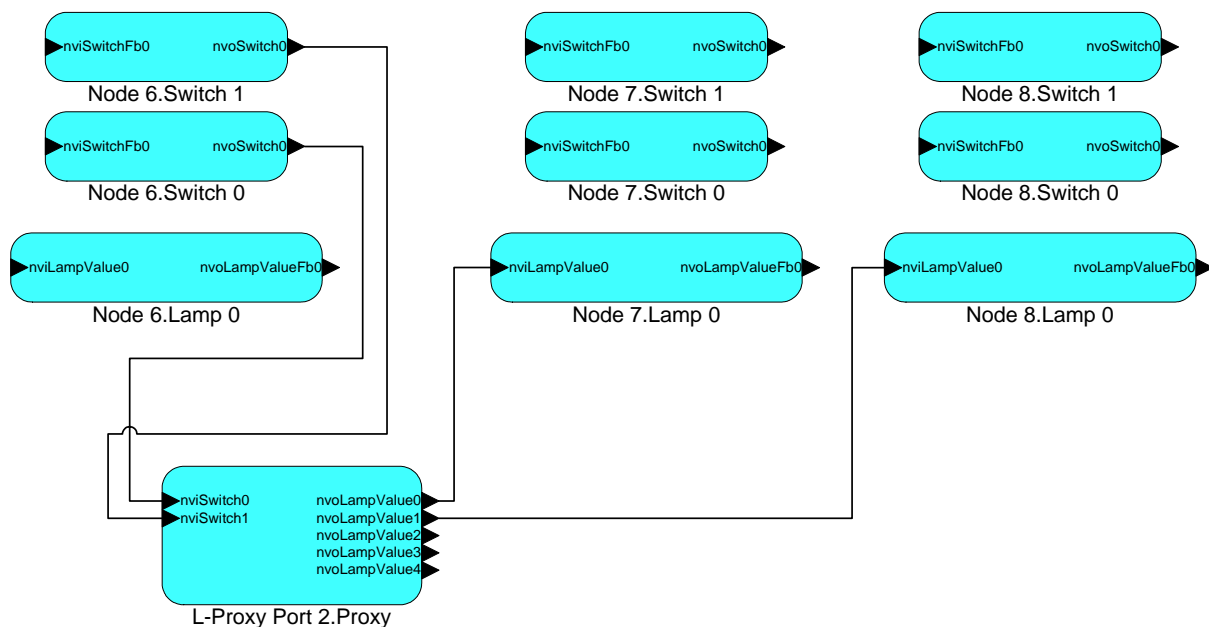
Figure 125: Node 6 only sends packet to L-Proxy Port 2 instead of sending message to nodes 7 and 8 directly. L-Proxy forwards the packet to the final destination nodes 7 and 8.

Figure 126: Protocol analyzer log file for the 2 subnet/node bindings shown in Figure 125. Node 6 first sends an update for nviSwitch0 to L-Proxy, which sends an update to node 7. Next node 6 sends an update for nviSwitch1 to L-Proxy, which send an update to node 8.

The following Figure 127 shows the L-Proxy internal bindings required to fulfill the application shown in Figure 125. The first entry connects the input network variable

nviSwitch0 on Port 2 to the output network variable nvoLampValue0 also in Port 2. The second entry connects the input network variable nviSwitch1 on Port 2 to the output network variable nvoLampValue1 also in Port 2. Note that these internal bindings are not visible within NL-220, LonMaker or Alex and cannot be seen with a protocol analyzer on the network.

Figure 127: L-Proxy internal binding for the network shown in Figure 125.

8.1.2 Saving a Group Address

Figure 128 shows a simple network diagram comprising three Neuron Chip powered nodes. Each node contains four LONMARK objects: a node object, an actuator object and two sensor objects. The actuator object controls a lamp, the two sensor objects are connected to switches.

The output network variable nvoSwitch0 on node 6 is bound to the input network variables nviLampValue0 on nodes 7 and 8. In this case NL-220 and LonMaker create a group with the 3 group members Node 6, Node 7, and Node 8. Figure 129 shows the log file from a protocol analyzer that clearly shows the acknowledged service using group addressing.
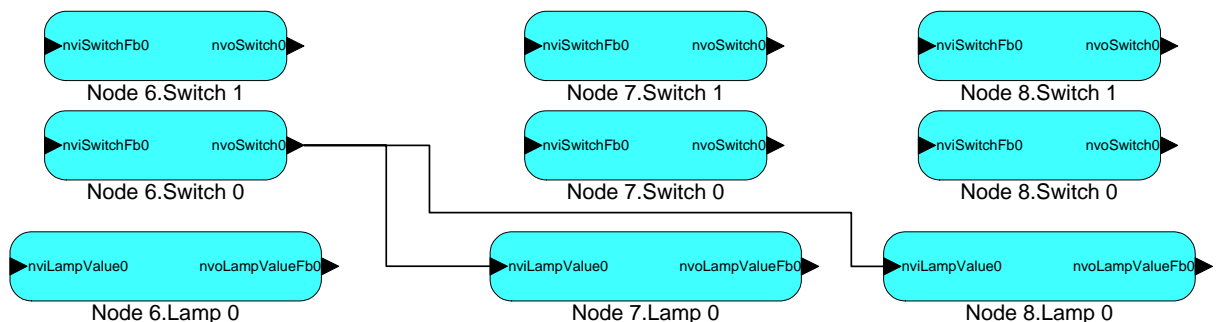
Figure 128: Acknowledged group binding between nodes 6, 7, and 8.

Figure 129: Protocol analyzer log file for the group binding shown in Figure 128. Node 6 uses acknowledged group binding to communicate with nodes 7 and 8.

L-Proxy can be used to break up the group into individual subnet/node addressed bindings, which saves valuable group addresses for group bindings with a higher member count. Figure 130 shows the same network from above but now we have added one port of L-Proxy (Port 2) to break up the group into individual subnet/node addressed messages.
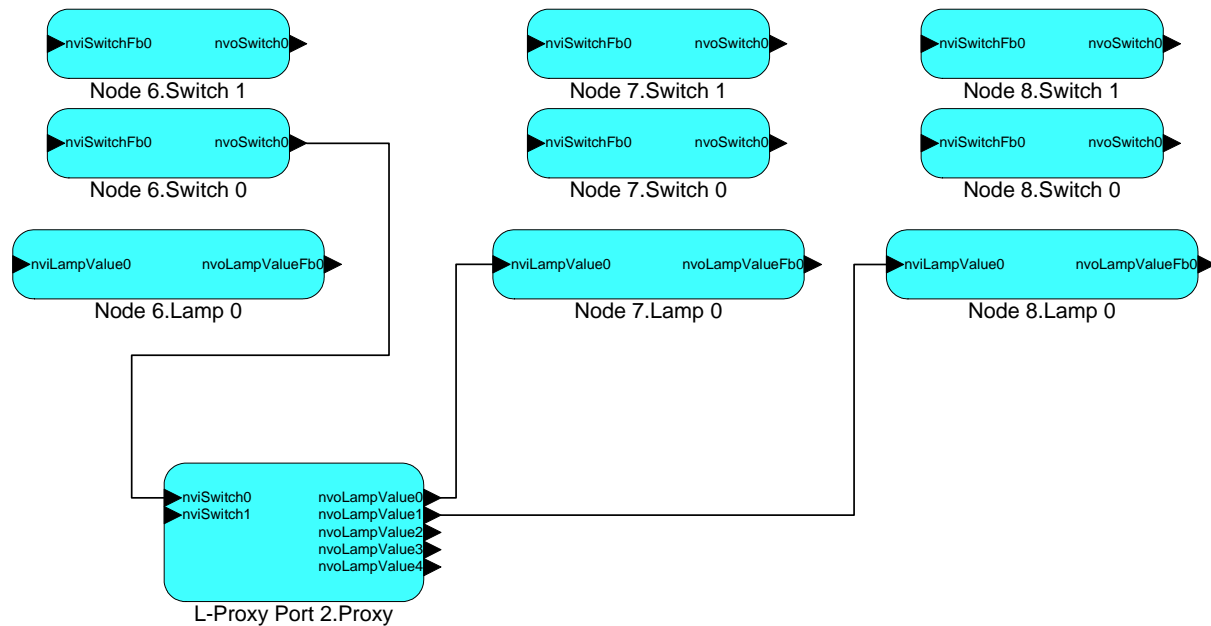
Figure 130: Acknowledged subnet/node addressed messages save a group address entry.

Figure 131: Protocol analyzer log file for the L-Proxy bindings shown in Figure 130. Node 6 uses acknowledged subnet/node binding to communicate with L-Proxy port 2. L-Proxy relays the information to nodes 7 and 8 using acknowledged subnet/node addressed messages.

The following Figure 132 shows the L-Proxy internal bindings required to fulfill the application shown in Figure 130. The entry connects the input network variable nviSwitch0 on Port 2 to the output network variables nvoLampValue0 through nvoLampValue4 on Port 2. One can see that in this configuration the input network variable nviSwitch0 is actually connected to 5 identical output network variables named nvoLampValue0-4. Therefore up to five destination nodes could be bound to the 5 output network variables on L-Proxy. Note that these internal bindings are not visible within NL220/LonMaker/Alex and cannot be seen with a protocol analyzer on the network.

Figure 132: L-Proxy internal binding for the network shown in Figure 130.

8.2 Binding across Domains

Let's assume the network configuration from Table 7. We have 3 nodes Node 6, Node 7, and Node 8, which reside in three different domains. Each of the three nodes has a switch and a lamp object. The switch object is controlled by a switch connected to the node and the lamp object turns on and off a lamp.

Node name	NV name	Domain	Comment
Node 6	NvoSwitch0	4C4F59544543	SNVT_switch output NV
Node 6	NviLampValue0	4C4F59544543	SNVT_switch input NV
Node 7	NvoSwitch0	03	SNVT_switch output NV
Node 7	NviLampValue0	03	SNVT_switch input NV
Node 8	NvoSwitch0	505859	SNVT_switch output NV
Node 8	NviLampValue0	505859	SNVT_switch input NV

Table 7 Network configuration that spans 3 domains.

Let's assume that Node 6 in Domain 4C4F59544543 ("LOYTEC") must turn on the lamp connected to Node 7 in Domain 03 and the lamp connected to Node 8 in Domain 505889 ("PXY"). Furthermore the switch connected to Node 8 must turn on the lamp connected to Node 6 in Domain 4C4F59544543.

This would require a binding across domains, which is not supported in state-of-the-art network installations tools. One can use L-Proxy to make the connections between the 3 domains as explained below.

Let's add L-Proxy1 Port 2 to the network with DomainID 4C4F59544543 as shown in Figure 133. Next we have to create the dynamic input and output network variables on L-Proxy Port 2. Now we can bind the output NV nvoSwitch0 on Node 6 to the corresponding input NV nviSwitch0 on L-Proxy Port 2. We also bind the input NV nviLampValue0 on Node 6 to the output NV nvoLampValue0 on L-Proxy Port 2.
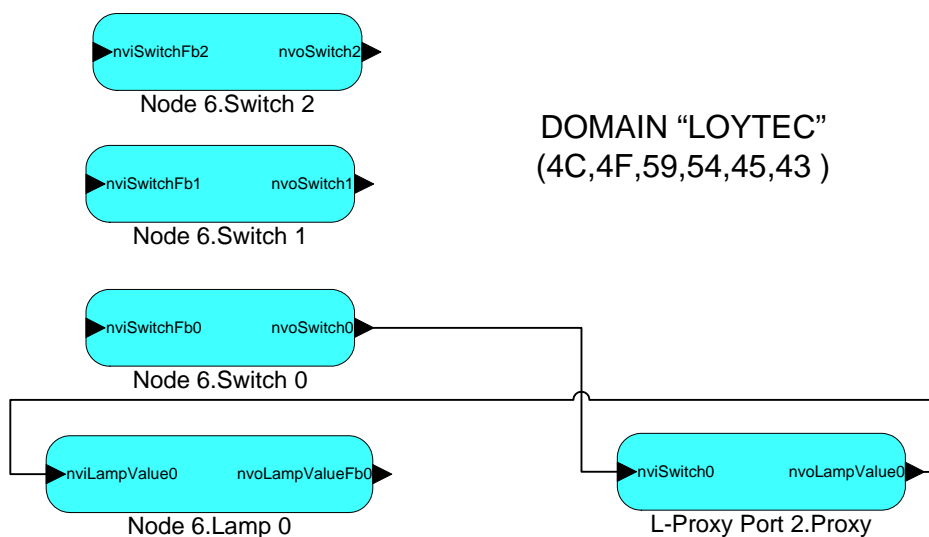
Figure 133: We bind the input and output NVs of Node 6 in domain 4C4F59544543 to the corresponding dynamically created NVs on L-Proxy Port 2.

Let's do similar bindings for the NVs on Node 7 and Node 8 as shown in Figure 134 and Figure 135 for L-Proxy Ports 3 and 4.
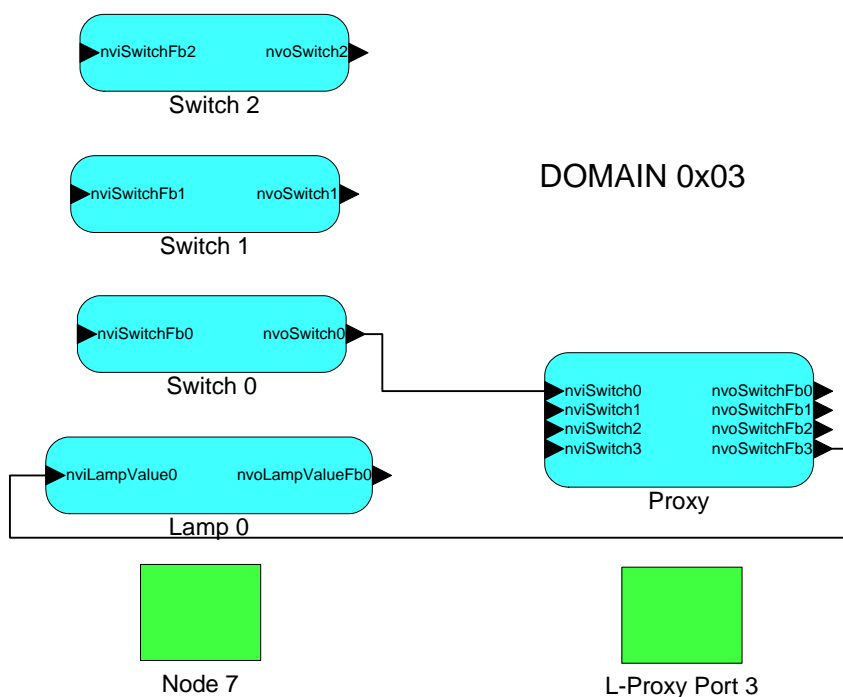

Figure 134: We bind the input and output NVs of Node 7 in domain 03 to the corresponding dynamically created NVs on L-Proxy Port 3.
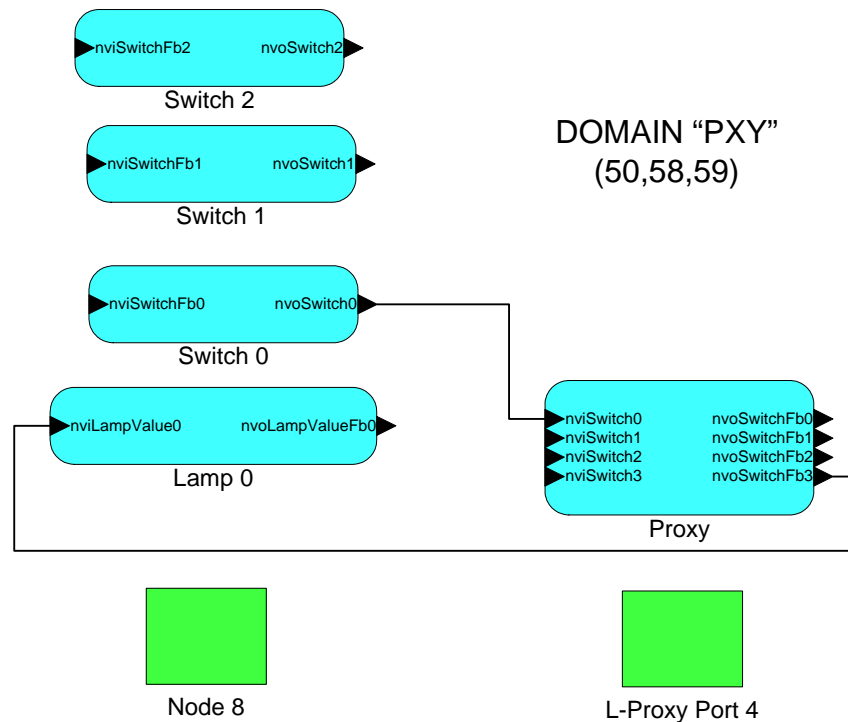
Figure 135: We bind the input and output NVs of Node 8 in domain 505859 to the corresponding dynamically created NVs on L-Proxy Port 4.

After extracting the port interface definitions for L-Proxy Ports 2-4 we can now create the Connections with the L-Proxy configuration utility. The results are shown in Figure 136. The first connection connects the switch on Node 6 (Port 2) with the lamp on Nodes 7 (Port 3) and 8 (Port 4). The second connection connects the switch on Node 8 (Port 4) with the lamp on Node 6 (Port 2).
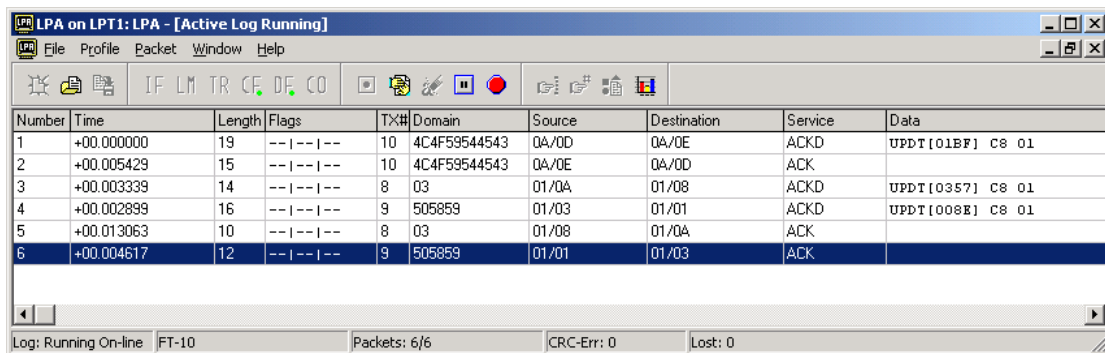

Figure 136: These 2 connections implement the desired functionality as specified:
Node 6 in Domain 4C4F59544543 ("LOYTEC") must turn on the lamp connected to Node 7 in Domain 03 and the lamp connected to Node 8 in Domain 505889 ("PXY"). Furthermore the switch connected to Node 8 must turn on the lamp connected to Node 6 in Domain 4C4F59544543.

If we now flip the switch on Node 6 the protocol analyzer log file will show the results from Figure 137:

- Packet #1: NV update sent from nvoSwitch0 on Node 6 to L-Proxy Port 2 nviSwitch0.

- Packet #2: L-Proxy Port 2 sends an acknowledgement back to Node 6 in domain 4C4F59544543.

- Packet #3: L-Proxy Port 3 forwards the NV update from "Node 6 nvoSwitch0" to Node 7 in domain 03.

- Packet #4: L-Proxy Port 4 forwards the NV update from "Node 6 nvoSwitch0" to Node 8 in domain 505859.

- Packet #5: Node 7 sends an acknowledgement back to L-Proxy Port 3.

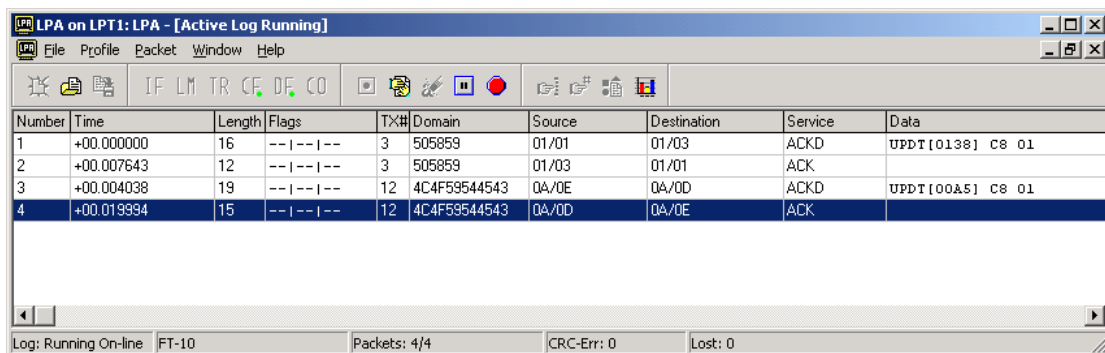- Packet #6: Node 8 sends an acknowledgement back to L-Proxy Port 4.

Figure 137: Turning on the switch on Node 6 creates the following packet stream in order to turn on the lamps on Node 7 and Node 8.

The second part of our desired network communication is shown in Figure 138. When we flip the switch on Node 8 the lamp on Node 6 should turn on. The following packet streams can be seen on a protocol analyzer log output:

- Packet #1: NV update sent from nvoSwitch0 on Node 8 to L-Proxy Port 4 nviSwitch0.

- Packet #2: L-Proxy Port 4 sends an acknowledgement back to Node 8 in domain 505859.

- Packet #3: L-Proxy Port 2 forwards the NV update from "Node 8 nvoSwitch0" to Node 6 in domain 4C4F59544543.

- Packet #4: Node 6 sends an acknowledgement back to L-Proxy Port 2.

Figure 138: Turning on the switch on Node 8 creates the following packet stream in order to turn on the lamp on Node 6.

Note, in this example the 3 L-Proxy ports can either be connected to the same network cable (as shown in the log file in Figure 137) or they can be connected to individual network cables.

8.3 Poll-Update Proxy

Let's assume a scenario with a node that cannot send updates by itself and must be polled instead. On the other hand the destination of the information e.g. a SCADA system or

OPC server cannot poll but must receive updates. The input NVs on the L-Proxy can then be configured to actively poll the source node at a defined poll cycle and the updates are sent to the destination node.
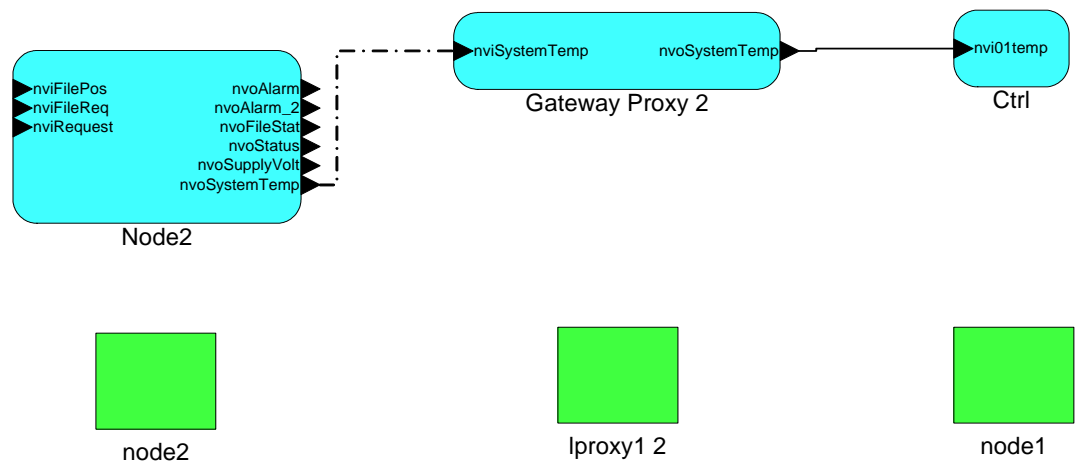
Figure 139: Active poll of nvoSystemTemp on node2 from nviSystemTemp on node lproxy1 2.

In our example the output network variable nvoSystemTemp on node 'node2' in Figure 139 cannot send updates by itself but must be polled. In our case the lproxy1 2 polls this output network variable with the input nviSystemTemp using a poll cycle of 30s as defined in the data point manager dialog (see Figure 140).
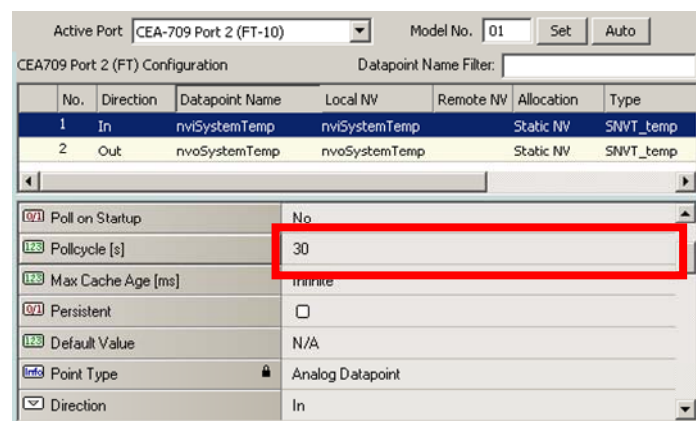
Figure 140: Poll cycle setting for input nviSystemTemp on node lproxy1 2

In this example lproxy1 2 sends an update out on nvoSystemTemp when the polled value changes. If the 30s are too long in some circumstances, a forward poll can be configured. Forward poll means that if poll requests are received from the destination node (node1) on the output side of L-Proxy, they are forwarded to the source node (node2) in addition to the periodic polls generated by the L-Proxy. To configure a forward poll set the Max Cache Age property to '0' as shown in Figure 141.

Figure 141: Max Cache Age setting for nvoSystemTemp on node lproxy1 2

8.4 Poll-On-Startup Proxy

Some scenarios require that at power-up or after a reset the network variable values from the source node should be polled once to obtain the current state of these network variables. In the Configurator software a poll-on-startup flag can be set for each individual input NV. An example is shown in Figure 142. The rate for sending poll-on-startup polls is automatically adjusted to not saturate the network channel.
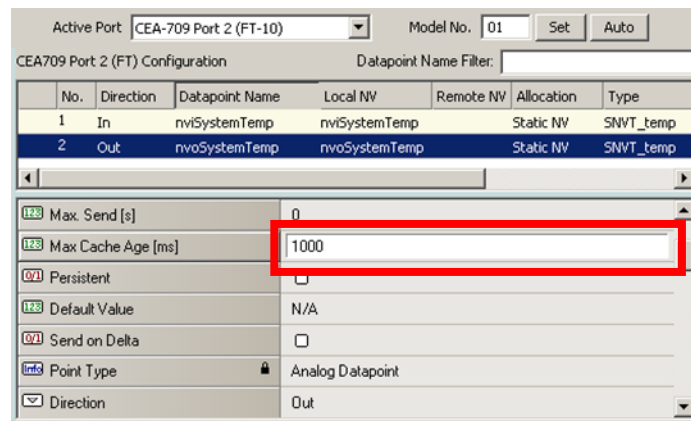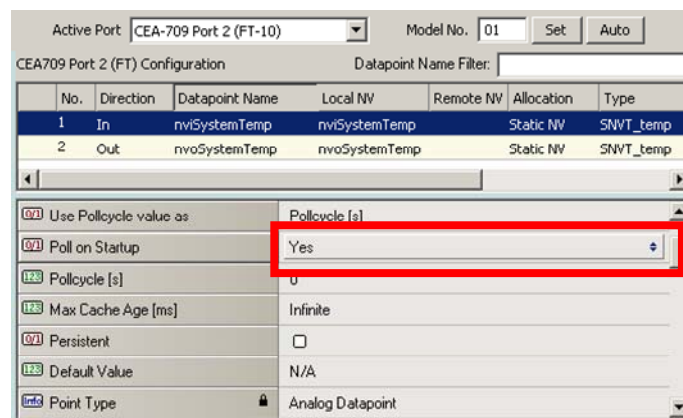

Figure 142: The poll-on-startup flag is set for this input NV.

8.5 SNVT Translation

The L-Proxy can generate connections containing data points of the same class (e.g., analog points). See also Section 6.4. This feature can be used to convert between different scalar SNVTs, which is often referred to as "SNVT translation".

The example in Figure 143 shows a node 1 that has network variables nvoAmpere of SNVT_amp and nvoTemperature of SNVT_temp. It also shows a node 2 with network variables nviAmpere_mil of SNVT_amp_mil and nviTemperature_f of SNVT_temp_f. Since the network variables are of different type on node 1 and on node2 these NVs cannot be bound directly. The L-Proxy can act as a translator between the different network variable types as shown in Figure 143.
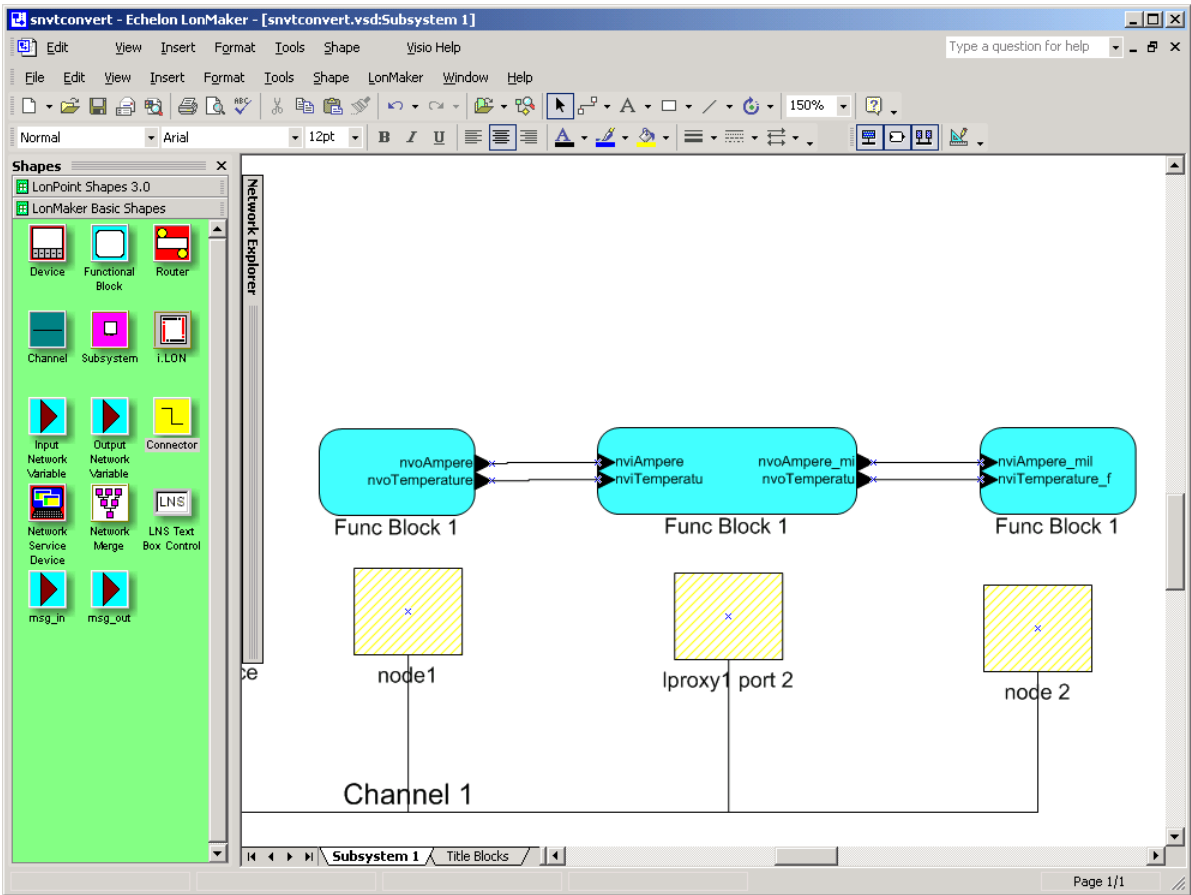
Figure 143: Example for scalar SNVT translation.

Create a manual connection for nviAmpere and nvoAmpere_mil on L-Proxy port 2 (see Section 7.11.1). An example connection dialog for this is shown in Figure 144.
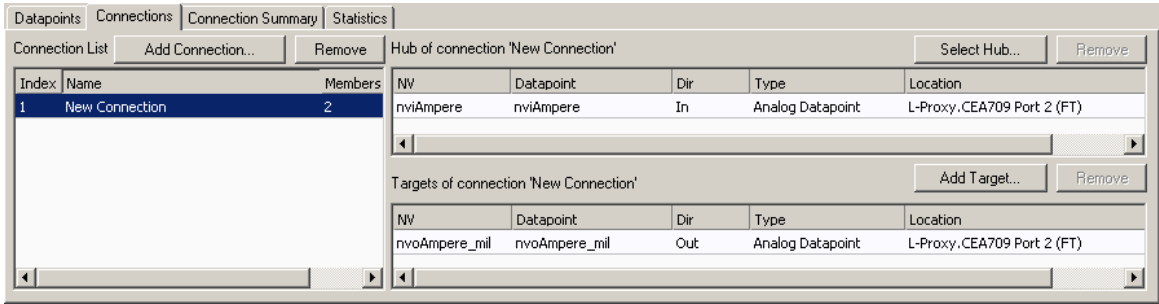
Figure 144: Manual Connection Setup for SNVT Translation.

Now repeat the same steps for the second network variable of type SNVT_temp and SNVT_temp_f. You will end up with two connections as depicted in Figure 145.

Figure 145 The two connections convert between the different network variable types used in the example in Figure 143.

9 Operating Interfaces

9.1 CEA-709 Interface

9.1.1 NV Import File

Network variables can be imported to the L-Proxy Configurator in a CSV file. The format of this file is described in this section.

The first line of the file must contain a comment, starting with a hash character '#' specifying the format version and import technology:

```
#dpal_csv_config;Version=1;Technology=CEA709
```

After that line any number of comment lines starting with the hash character '#' are allowed. Lines that are not comments specify one NV per line, using the column information as described in Table 8. The columns are separated by commas ',' or semi-colons ';'. Which separator is used can be configured in the Web UI (see Section 5.2.1).

Column	Field	Example	Description
A	SNVT	39	A numeric value of the SNVT (as defined in the SNVT master list). The example value 39 represents a SNVT_temp.
B	NV index	0	The NV index in decimal notation of the NV on the network node. Index starts at 0.
C	NV selector	1	The NV selector in decimal notation of the NV on the network node.
D	NV name	nvoTemp	The NV programmatic name of the NV on the network node.
E	is output	1	Defines if this NV is an output on the network node. '1' means the NV is an output on the network node.
F	flag auth cfg	1	'1' defines that authentication can be configured for this NV on the network node.
G	flag auth	0	'1' defines that the NV is authenticated.
H	flag priority cfg	1	'1' defines that the priority can be configured for this NV on the network node.
I	flag priority	0	'1' defines that the NV is using priority.
J	flag servicetype cfg	1	'1' defines that the service type can be configured for this NV on the network node.
K	flag service ack	1	'1' defines that the NV is using acknowledged service.
L	flag polled	0	'1' defines that the NV is using the polled attribute
M	flag sync	0	'1' defines that the NV is a synchronous NV.
N	Deviceref	1	This field is a numeric reference to a device description. If it is the first occurrence of this reference in the file, the columns defined below must be filled in. Otherwise, they can be left out.
O	programID	9000A44850060402	The program ID string of the network device.
P	neuronID	80000000C8C8	The NID of the network device.
Q	Subnet	2	The subnet address of the network device. Use '0' if the device has no subnet address information.
R	Node	3	The node address of the network device. Use '0' if the device has no node address information.
S	location str	0	The location string of the network device. Use '0' if no information is available.
T	Devicename	DDC	The device name of the network device. Leave this field blank if this information is not available.
U	node self-doc	&3.2@0,2	Self-documentation string of the device (special characters are escaped)
V	NV length	2	NV length in bytes
W	NV self-doc	@0|4	NV self-documentation string (special characters are escaped)
X	Allocation	1	Define, how this NV shall be allocated: external=1 (default) / static=2 / file=3

Table 8: CSV Columns of the NV Import File

9.1.2 Node Object

The L-Proxy provides a node object conforming to the LONMARK guidelines.

- The Node Object accepts the following commands via *nviRequest* and updating *nvoStatus*: RQ_NORMAL, RQ_UPDATE_STATUS, RQ_REPORT_MASK,

RQ_ENABLE, RQ_DISABLE, RQ_UPDATE_ALARM, RQ_CLEAR_ALARM, RQ_RESET, RQ_CLEAR_RESET

- LONMARK alarming is supported via *nvoAlarm* (SNVT_alarm) and *nvoAlarm_2* (SNVT_alarm_2). This allows devices supporting the LONMARK alarm notifier profile to receive alarms generated by the L-Proxy 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.

- LONMARK file transfer is supported via the network variables *nviFileReq*, *nvoFileStat*, and *nviFilePos*.

- nvoSystemTemp (*SNVT_temp*): This NV can be used to poll the system temperature of the L-Proxy. It does not send updates and must be polled.

- nvoSupplyVolt (*SNVT_volt*): This NV can be used to poll the supply voltage of the L-Proxy. It does not send updates and must be polled.

9.1.3 Gateway Objects

The L-Proxy contains eight proprietary Gateway objects. These are containers for all NVs which are configured on the L-Proxy's CEA-709 port. They are intended for grouping NVs. When static NVs are created, they can be assigned to any of the eight gateway blocks. When creating dynamic NVs in the LNS-based tool, the NVs should be added to the gateway blocks.

10 Network Media

10.1 FT

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

When using the Free Topology Segment feature of the FT, only one termination (Figure 146) is required and can be placed anywhere on the free topology segment. Instead of building the termination, one can order the L-Term module (LT-33) from LOYTEC, which can be used to properly terminate the bus.
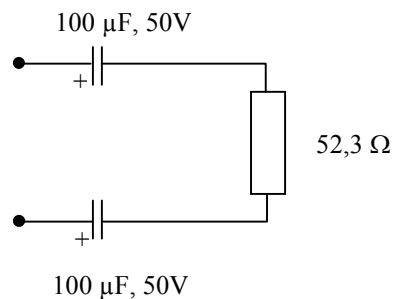

Figure 146: FT Free Topology Termination

In a proper bus topology, two terminations are required (Figure 147). These terminations need to be placed at each end of the bus. Here, also L-Term modules can be used at either end.
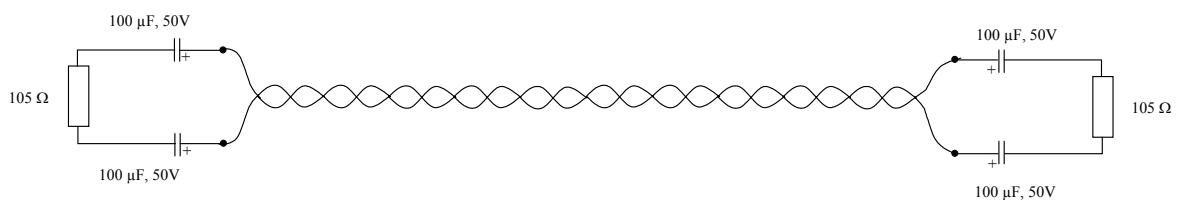

Figure 147: Termination in an FT Bus Topology

11 L-Proxy Firmware Update

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

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

- L-Proxy fallback image,

- L-Proxy primary image.

The L-Proxy fallback image cannot be changed. Thus, if the update of the primary image fails or the image is destroyed by some other means, the fallback image is booted and allows reinstalling a valid primary image.

When the L-Proxy boots up with the fallback image, the CEA-709 port LEDs and the CNIP LED are flashing red.

11.1 Firmware Update via the L-Proxy Configurator

The L-Proxy primary image can be updated using the L-Proxy Configurator. For this purpose, the L-Proxy must be connected to the Ethernet and must have a valid IP configuration (see Section 4.6 and 5.2.2). The L-Proxy Configurator must be installed (see Section 7.1).

To Update the Firmware using the L-Proxy Configurator

1. Start the L-Proxy Configurator from the Windows Start menu: **Start → Programs → LOYTEC L-Proxy Configuration → Configure L-Proxy**.

2. Select the menu: **Operations → Connect to L-Proxy → FTP**. This opens the FTP connection dialog as shown in Figure 148.
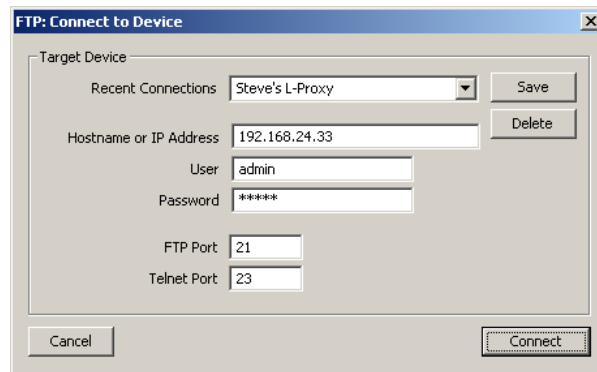
Figure 148: FTP connection dialog.

3. In the FTP connection dialog, enter the IP address of the L-Proxy as well as the FTP user name and password. The default user name and password are 'admin' and 'admin'. This can be changed via the Web interface (see Section 5.1) and reset via the console UI (see Section 4.8.2).

4. Click on **Connect**.

5. Select the menu: **Firmware → Update …**

6. This opens the Firmware Update dialog as shown in Figure 149. Click on the button "**…**" and select the firmware image ("lproxy_lc3k_3_1_0_primary.dl").

Figure 149: Firmware Update dialog of the L-Proxy Configurator.

7. Click on **Start Download**.

8. Observe the download progress. When the download is complete, the dialog shown in Figure 150 appears.

Figure 150: FTP download success dialog.

9. Click **OK**.

10. In the Firmware Update dialog, click **Close**.

11. The device's firmware has now been successfully upgraded.

11.2 Firmware Update via the Console

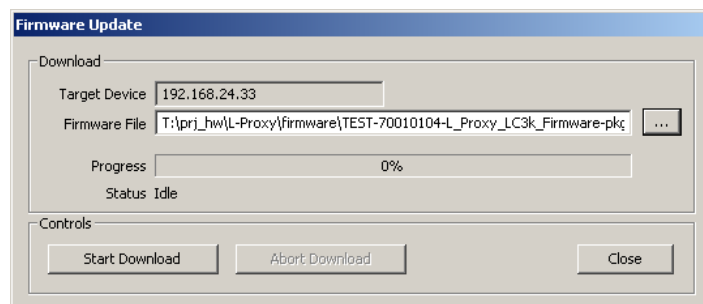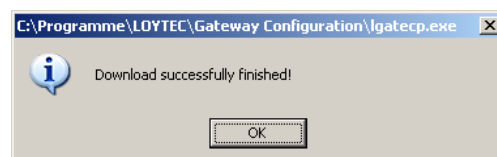To download the firmware via the console interface, the L-Proxy must be connected to the RS-232 port of a PC via its console interface as described in Section 4.1. You will need the LOYTEC serial upgrade tool (LSU Tool), which can be downloaded from our homepage at www.loytec.com.

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

To Upgrade via the Console

1. 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 151.
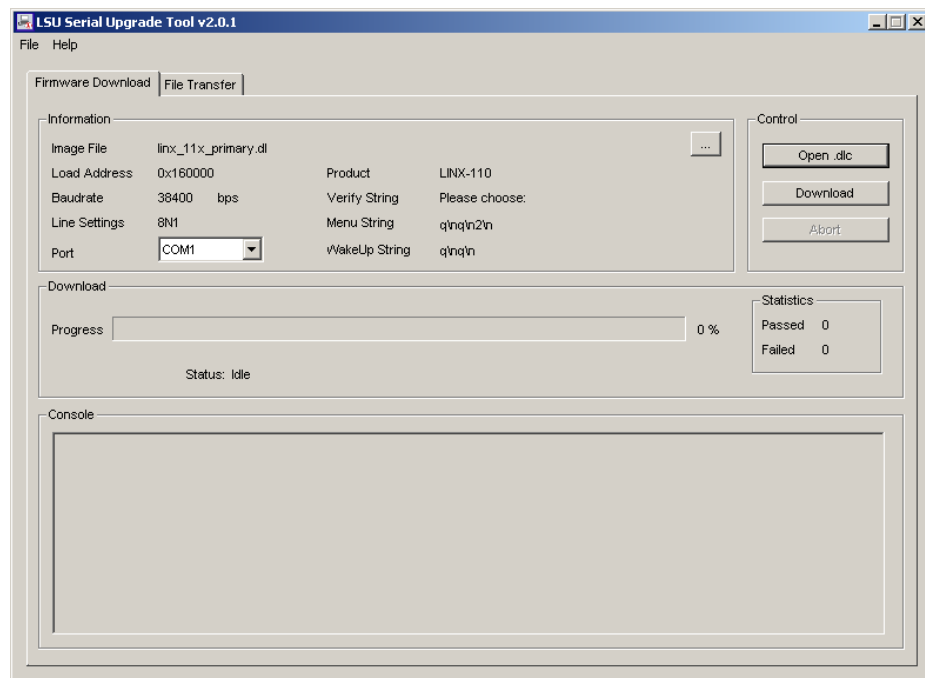
Figure 151: LSU Serial Upgrade Tool in Idle Mode

2. If the L-Proxy is not connected to COM1 you can change the port to COM2, COM3, or COM4. Make sure that the product shown under "Product" matches the device you are upgrading. Press **Download** to start the download. A progress bar as shown in Figure 152 can be seen.
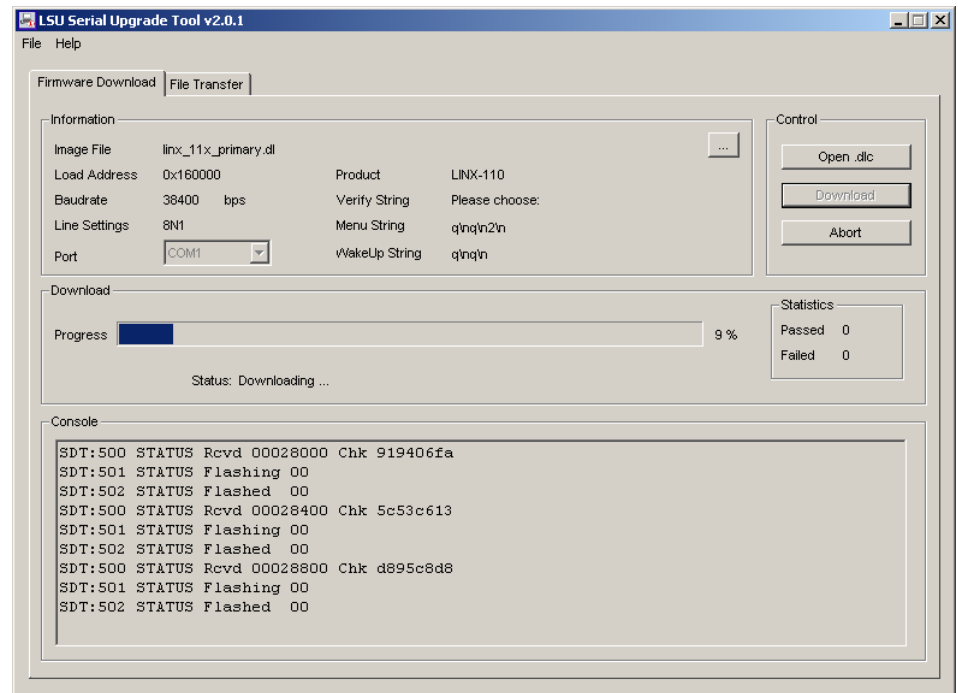
Figure 152: Progress Bar during Firmware Download.

3. If the upgrade is successful, the following window appears (Figure 153).
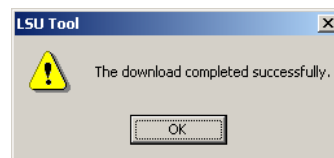
Figure 153: Successful Firmware Upgrade

4. 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.

11.3 Firmware Update via the CEA-709 Network

Basically, firmware downloads can be performed on every L-Proxy port. However, since the L-Proxy 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 13.1), must be used. See the LSD Tool documentation for details on how to download a new L-Proxy firmware via the CEA-709 network.

12 Troubleshooting

12.1 All port LEDs are flashing red

Problem

All port LEDs are flashing red at a rate of approximately once per second and the L-Proxy does not relay messages.

Explanation

Somehow the primary image was destroyed and the fall-back image was booted (see Section 9.1). This image does not support relaying 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 12.7).

12.2 LonMaker Warning appears during installation

Problem

When adding a new L-Proxy Port to the project the following warning messages might appear.
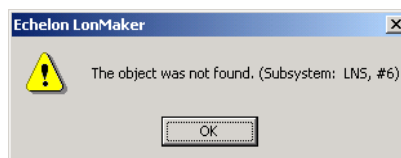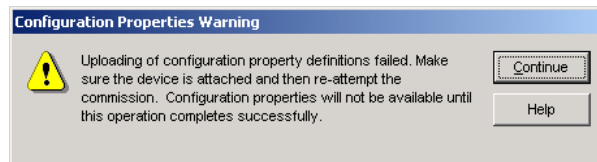
Figure 154 Click OK to continue.

Figure 155 Click on Continue.

Explanation

There are still some dynamically created NVs in L-Proxy. This can happen if the node has been used in a different project and it hasn't been de-commissioned in the old project before it was moved to the new network.

Solution

Click on Yes and Continue. In most cases this will be enough to use L-Proxy. If L-Proxy is behaving strange one should reset the L-Proxy to its default configuration via the console interface (see Section 4.8).

12.3 NL220 Warning appears during installation

Problem

When adding a new L-Proxy Port to the project the following warning messages might appear.

Figure 156 Warning when creating node

Explanation

There are still some dynamically created NVs in L-Proxy. This can happen if the node has been used in a different project and it hasn't been de-commissioned in the old project before it was moved to the new network.

Solution

Ignore the error. In most cases this will be enough to use L-Proxy. If L-Proxy is behaving strange one should reset the L-Proxy to its default configuration via the console interface (see Section 4.8).

12.4 Move L-Proxy into a new LNS project

Problem

When moving an L-Proxy device from one LonMaker/NL220/Alex project into a different LonMaker/NL220/Alex project one must delete the L-Proxy port in the old project before adding the L-Proxy device in a different project.

Explanation

> If L-Proxy is moved from one LonMaker/NL220/Alex project into a different project LonMaker/NL220 must release all captured resources in L-Proxy. Resources are released when the L-Proxy Port is deleted from the LonMaker/NL220/Alex project.

Solution

> Select the L-Proxy Port in the old LonMaker/NL220/Alex project and choose Delete/Remove from the context menue. Make sure that the device can be reached by LonMaker/NL220/Alex during the deletion process. Therefore LonMaker/NL220/Alex must be On-Net. This process must be followed for all L-Proxy ports that have been used.
>
> As a second alternative the L-Proxy can be set into its factory default state through the console interface, see Section 4.8.

12.5 Node does not respond to poll request

Problem

> The input NV on the L-Proxy is being polled by another node but L-Proxy does not respond to the poll message.

Explanation

> If the L-Proxy internal connection consists of only one input NV and one or more output NVs then this input NV cannot be polled by another node. If the internal connection has 2 or more input NVs and the poll is received on the first input NV the poll will be forwarded on the second input NV.
>
> If the internal connections uses active poll (active poll flag enabled) the input NV that outputs the active poll (first input NV if multiple input NVs exist) cannot be polled.

Solution

> Always poll the source of the information (output NV on source node) and not the input NV of the L-Proxy.

12.6 L-Proxy doesn't forward packets after commissioning

Problem

> No packets are forwarded by L-Proxy after one or more ports have been re-commissioned.

Explanation

> The L-Proxy configuration will be deleted when one or more ports are commissioned.

Solution

> Always download the L-Proxy configuration after commissioning one or more L-Proxy ports.

12.7 Technical Support

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

LOYTEC electronics GmbH
Blumengasse 35
A-1170 Vienna
Austria / Europe

e-mail :	*support@loytec.com*
Web :	*http://www.loytec.com*
tel :	*+43/1/4020805-100*
fax :	*+43/1/4020805-99*

or

LOYTEC Americas Inc.
11258 Goodnight Lane
Suite 101
Dallas, Texas 75229
USA

e-mail:	*support@loytec-americas.com*
Web:	*http://www.loytec-americas.com*
tel:	*+1/512/402 5319*
fax:	*+1/972/243 6886*

13 Application Notes

13.1 The LSD Tool

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

13.2 Use of Static, Dynamic, and External NVs on a Device

Please refer to application note "AN009E Changing Device Interface in LNS" for more information on the static NV interface, XIF files, device templates and the use of static, dynamic, and external NVs on LOYTEC gateway products.

14 Firmware Versions

Table 9 shows the most important features available only in certain firmware versions.

Firmware Version/ Features	1.0.0	2.0.0	2.1.0	3.0.0	3.1.0
Console Menu (configuration & firmware update)	√	√	√	√	√
Binding across domains	√	√	√	√	√
Address table extension	√	√	√	√	√
Firewall	√	√	√	√	√
Password protection	√	√	√	√	√
Statistics information	–	√	√	√	√
SNVT translation	–	√	√	√	√
Real time clock	–	√	√	√	√
TP-1250 backbone mode	√	√	√	n/a	n/a
RS-485 bit-rate detection	–	√	√	n/a	n/a
Active Polls	–	√	√	√	√
LSD 2.0 support	–	–	√	√	√
CEA-852 backbone	–	–	–	√	√
Web interface	–	–	–	√	√
Static and external (polled) NVs	–	–	–	√	√
UNVTs, SCPTs	–	–	–	–	√
Backup/Restore Configuration	–	–	–	–	√

Table 9: Available Features depending on Firmware Version

15 Specifications

15.1 L-Proxy

15.1.1 Physical Specifications

Operating Voltage	12 – 35 VDC or 12 – 24 VAC ±10 %
Power Consumption	typ. 3 W
In rush current	up to 950 mA @ 24 VAC
Operating Temperature (ambient)	0°C to +50°C
Storage Temperature	-10°C to +60°C
Humidity (non condensing) operating	10 to 90 % RH @ 50°C
Humidity (non condensing) storage	10 to 90 % RH @ 50°C
Enclosure	Installation enclosure 6 TE, DIN 43 880
Environmental Protection	IP 40 (enclosure); IP 20 (screw terminals)
Installation	DIN rail mounting (EN 50 022) or wall mounting

15.1.2 Resource Limits

Total number of data points	10000
NVs (static, dynamic)	512 (per port)
External NVs	512 (per port)
Alias NVs	512 (per port, both ECS and legacy mode)
Address table entries	512 (per port, 15 in legacy mode)
Configuration Properties (CPs)	512 (per port)

16 References

[1]   LONMARK Application Layer Interoperability Guidelines, Version 3.3, October 2002.

[2]   L-Proxy User Manual, Version 2.2, December 2004.

[3]   L-IP User Manual, LOYTEC electronics GmbH, Document № 88065909, June 2006.

17 Revision History

Date	Version	Author	Description
2002-09-30	1.0	DL	Initial revision V1.0
2002-07-11	1.1	DL	Released Version 1.1
2002-11-12	1.2	DL	Added support for NL220 network management tool
2003-02-18	2.0	DL	Release Version 2.0 of the user manual
2003-08-14	2.1	DL	Updated solutions section.
2004-01-14	2.2	NR	Add description how to use L-Proxy in Alex.
2007-01-07	3.0	STS	Changed for L-Proxy firmware 3.0 and LP-33E100.
2009-03-06	3.1	STS	Updated for firmware 3.1.0.