L-INX 10X™

LINX-10X Automation Server

User’s Manual

LOYTEC electronics GmbH

Contact

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

Version 3.0

Document No. 88073002

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

Contents

Abbreviations

100BaseT	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
AST	Alarming, Scheduling, Trending
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
CN/IP	Control Network over IP
CN/IP Channel	logical IP channels that tunnels CEA-709 packets according CEA-852
CN/IP packet	IP packet that tunnels one or multiple CEA-709 packet(s)
COV	change-of-value
CR	Channel Routing
CS	Configuration Server that manages CEA-852 IP devices
DA	Data Access
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
OPC	Open Process Control
RNI	Remote Network Interface
RTT	Round-Trip Time
SL	Send List
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
SNVT	Standard Network Variable Type
SSL	Secure Socket Layer
TLS	Transport Layer Security
XML	eXtensible Markup Language

1 Introduction

1.1 Overview

The LINX-10X is a high performance, reliable, and secure network infrastructure component that contains an embedded OPC server and exposes a defined set of data points as OPC tags. It implements the OPC XML-DA standard, which lets OPC clients access the data points via Web services. The LINX-10X can provide up to 1000 OPC tags. Which native data points are exposed to OPC can be configured by a configuration software, which provides a fast and easy way to configure the LINX-10X. Using the supplied L-Web designer, users can easily generate a Web-based visualization for the LINX-10X. Easy to understand diagnostic LEDs allow installers and system integrators to install and troubleshoot this device without expert knowledge and dedicated troubleshooting tools.

The CEA-709 OPC Server (LINX-100, LINX-101) is equipped with an FT port (CEA-709) and a 100-BaseT Ethernet port (CEA-852) and exposes CEA-709 network variables (NVs) and configuration properties (CPs) to the OPC world. The configuration software can be run as an LNS plug-in or stand-alone. The OPC server node is connected to the FT port. The LINX-101 also contains a router between the FT and the IP-852 channel, which can be configured like an L-IP. It also includes a configuration server (CS) to manage the IP-852 channel. The LINX-100 contains a remote network interface (RNI) instead of the router for remote network access. The device is fully compliant with ANSI/CEA-709, ANSI/CEA-852-A, ENV14908, and OPC XML-DA 1.01.

The OPC server’s NVs can be bound in the CEA-709 network or operated as “external NVs”. External NVs are polled or explicitly written to without allocating static or dynamic NVs on the LINX-10X. 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. All of those new CEA-709 data points can be exposed as OPC tags.

The LINX-10X also supports the LOYTEC Alarming, Trending, and Scheduling (AST) feature set. The device provides LonMark scheduler/calendar objects, which can directly schedule NVs or registers. For alarm conditions, the LINX-10X can be configured to send E-Mails to pre-defined addresses. Alarms can be also stored in a historical *alarm log*. There can be up to 100 trend log objects with an aggregated total log buffer size of 2MB. Finally, the LINX-10X provide mathematics objects, which can be used to combine data points using a mathematical formula. The AST objects are exposed to a set of OPC tags. Trend logs can be uploaded from the device in CSV format. In addition, a dedicated Web service can be used to access trend log information.

Like the L-Switch the LINX-10X permanently collects statistics information from the attached network channels (channel load, CRC errors, forwarding statistics, etc.). Using this data the LINX-10X software is able to detect problems on these channels (overload, connections problems, etc.) and warns the system operator via LEDs (see Section 3.4.10). An intuitive user interface allows fast and easy network troubleshooting without any additional analysis tools and deep system knowledge. The LSD Tool can be used for a more detailed view of the collected statistics data. See Section 14.1 for more information on this powerful system diagnostics tool. The LINX-10X also includes channel monitoring objects for the FT and the IP-852 channel, which make the channel statistics available through NVs. The channel statistics is also exposed to the OPC interface.

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.

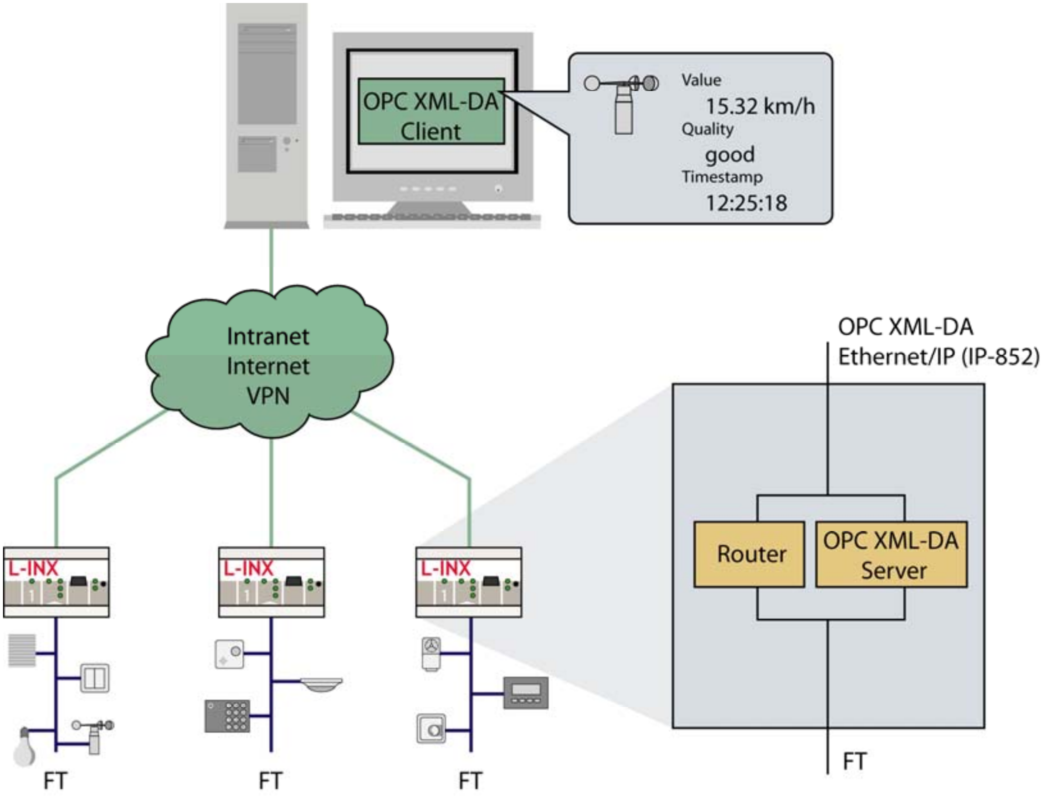


Figure 1: LINX-10X application example with an IP-852 channel.

The LINX-10X is used for:

- Exposing CEA-709 network variables (NVs) and configuration properties (CPs) as OPC tags,
- visualization of an CEA-709 network with the supplied LOYTEC L-Web software,
- visualization of an CEA-709 network in an OPC XML-DA SCADA package,
- reading, writing, and subscribing to CEA-709 NVs, CPs via Web services (.NET),
- building custom Web pages with active content,
- browsing data points on the Web interface,
- supporting standard (SNVT, SCPT) and user-defined (UNVT, UCPT) types,
- scheduling CEA-709 network variables,

- trending data points,
- generating alarms,
- logging alarms,
- sending E-Mails on alarms, trend logs, or scheduled events,
- network interface for LNS-based network management tools (LonMaker, NL-220),
- remote LPA functionality,
- communicating on CEA-709 with either FT-10 or CEA-852 (IP channel on the Intranet/Internet),
- connecting to a high-performance backbone using existing IP infrastructure,
- configuration server for IP-852 devices.

1.2 LINX-100 / LINX-101

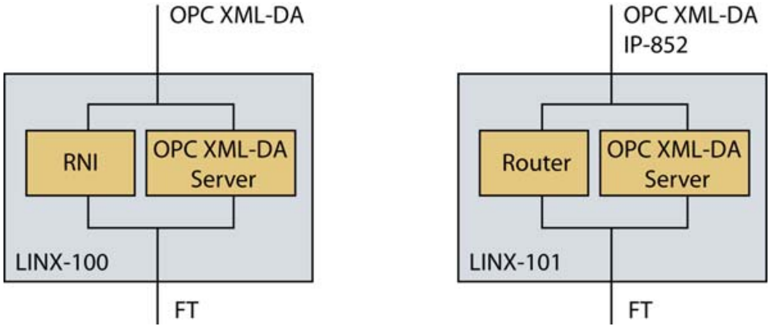


Figure 2: LINX-100 versus LINX-101.

The LINX-100 and the LINX-101 are both capable of exposing CEA-709 network variables and configuration properties to OPC XML-DA. Depending on additional features, there are flavors of the product. Figure 2 depicts the differences.

The LINX-101 possesses a router between the CEA-852 interface (IP-852) and the FT-10 interface. The built-in router can be used behind NAT routers and firewalls, which allows seamless integration in already existing Intranet networks. It supports DHCP even with changing IP addresses in an Intranet environment. The CEA-852 interface can be used to connect the LINX-101 to an IP-based high-speed backbone. The LINX-101's router can be used as a standard CEA-709 configured router or it can be used as a self-learning plug&play router based on the high-performance, well-proven routing core from our L-Switch plug&play multi-port router devices ("smart switch mode"). The self-learning router doesn't need a network management tool for configuration but is a true plug&play and easy to use IP infrastructure component.

The LINX-100 can be configured to run either on the CEA-852 interface (IP-852 mode) or on the FT-10 interface (FT mode). In the FT mode, the device provides a remote network interface (RNI), which can be used together with the LOYTEC NIC software. The RNI can be utilized for remote access and configuration as well as trouble-shooting with the remote LPA. Please consult our product literature for the LPA-IP to learn more about this IP protocol analyzer.

1.3 Scope

This document covers LINX-10X devices with firmware version 3.0 and the LINX-10X Configurator version 3.0. See Section 15 for differences between the different LINX-10X firmware versions.

2 Quick-Start Guide

This Chapter shows step-by-step instructions on how to configure the LINX-10X for a simple OPC server application.

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 3. More detailed instructions are shown in Chapter 3.

Important: ***Do not connect terminal 17 with Earth-ground! Terminal 16 may be connected to Earth-ground.***

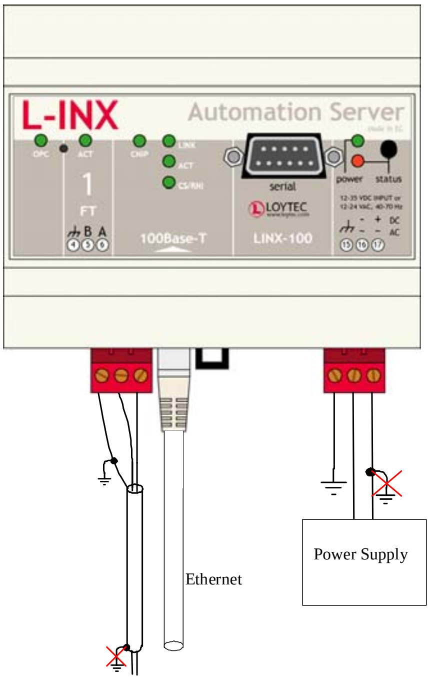


Figure 3: Basic Hardware Installation

2.2 Configuration of the LINX-10X

The LINX-10X can be configured via a console interface or via the Web interface. To configure the LINX-10X, the following steps have to be performed:

1. Setup IP configuration (see Sections 2.2.1 and 2.2.2).

2. Setup the OPC configuration (see Section 2.3).

Note: *This setup procedure assumes the use of the IP interface. Alternatively, a configuration via the console interface is possible. See Chapter 4 for details.*

2.2.1 IP Configuration on the Console

Use a PC terminal program with the communication settings set to 38,400 bps / 8 data bits / no parity / 1 stop bit / no handshake. To connect COM1 of the PC to the Console on the LINX-10X, use a standard null-modem-cable with full handshaking. Power up the LINX-10X or press Return if the LINX-10X is already running. The following menu should appear on the terminal:

```
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 4: LINX-101 Main Menu

Select 5 from the LINX-10X Configuration Menu and enter the IP address, netmask, and gateway address. Note that you must use different IP addresses if you are using multiple LINX-10X in your setup.

```
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-linx101
[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 5: Enter basic IP settings.

Press ‘x’ to save the IP settings and reset the LINX-10X with the main menu item ‘0’ in order to let the new IP settings take effect.

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.***

You should now be able to connect to the LINX-10X with an OPC XML-DA client and add the LINX-101’s router to an IP-852 channel in the configuration server member list. If the LINX-101 should also act as the configuration server please proceed to Section 4.9.

2.2.2 IP Configuration via the Web Interface

Optionally to using the console interface one can also use the Web interface to configure the client device. In a Web browser enter the default IP address 192.168.1.254 of the LINX-10X. Note that if your PC has an IP address in a subnet other than 192.168.1.xxx please open a command tool and enter the following route command to add a route to the LINX-10X.

To Add a Route to the Device

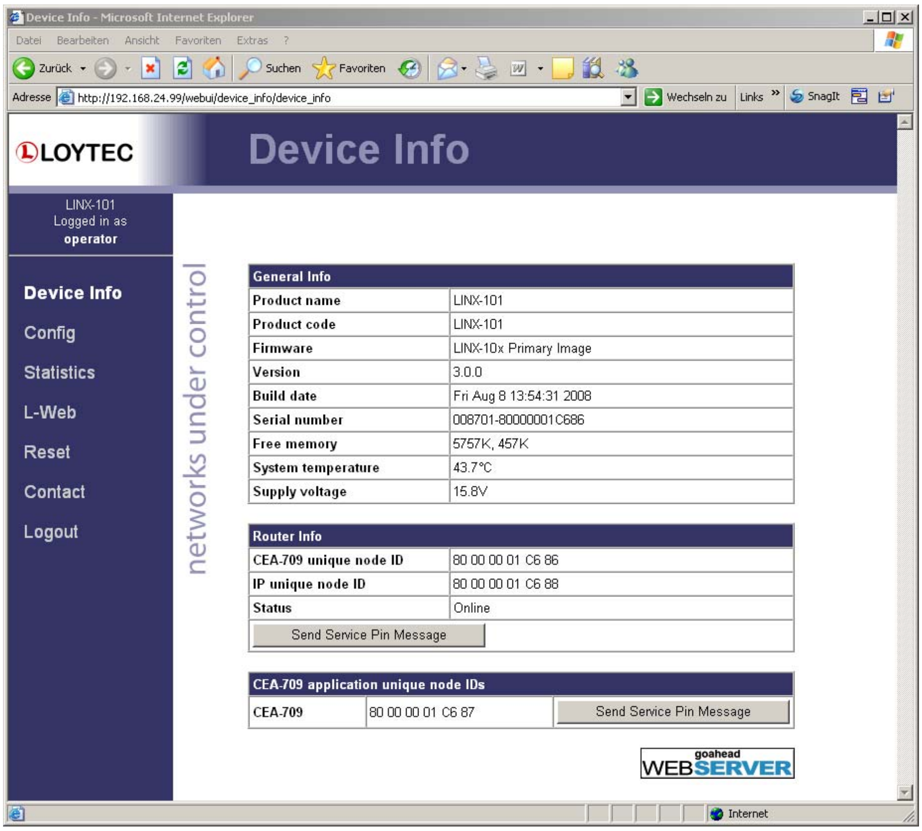
1. Windows START → Run

2. Enter ‘cmd’ an 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.



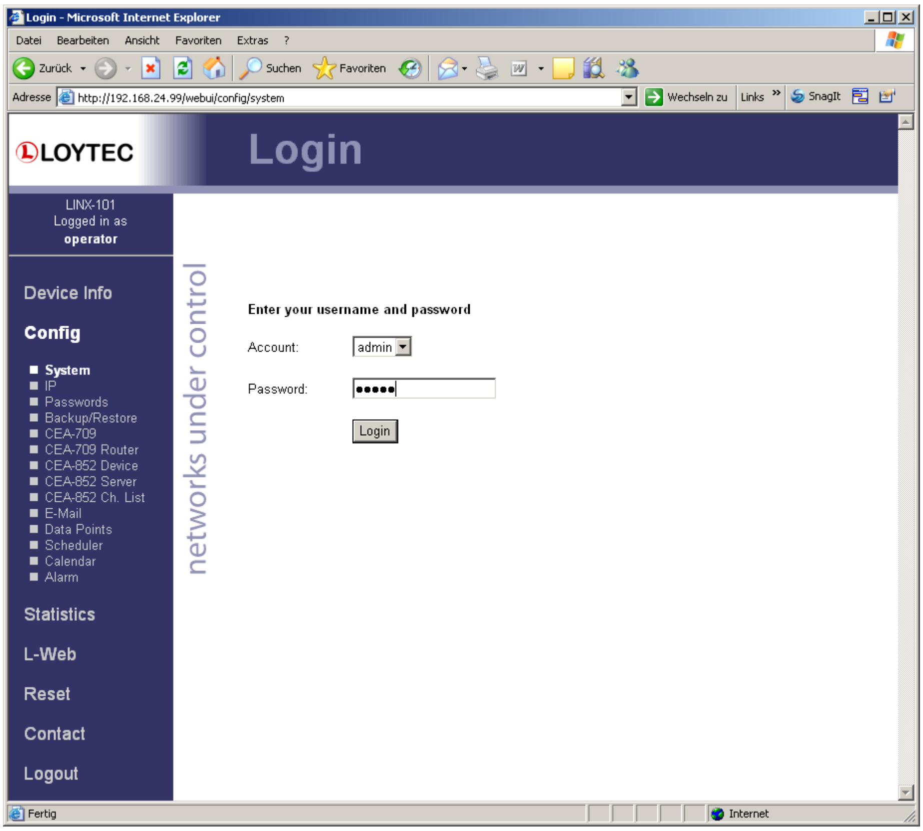
General Info	
Product name	LINX-101
Product code	LINX-101
Firmware	LINX-10x Primary Image
Version	3.0.0
Build date	Fri Aug 8 13:54:31 2008
Serial number	008701-80000001C686
Free memory	5757K, 457K
System temperature	43.7°C
Supply voltage	15.8V

Router Info	
CEA-709 unique node ID	80 00 00 01 C6 86
IP unique node ID	80 00 00 01 C6 88
Status	Online

CEA-709 application unique node IDs		
CEA-709	80 00 00 01 C6 87	Send Service Pin Message

Figure 6: Example Start Screen

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



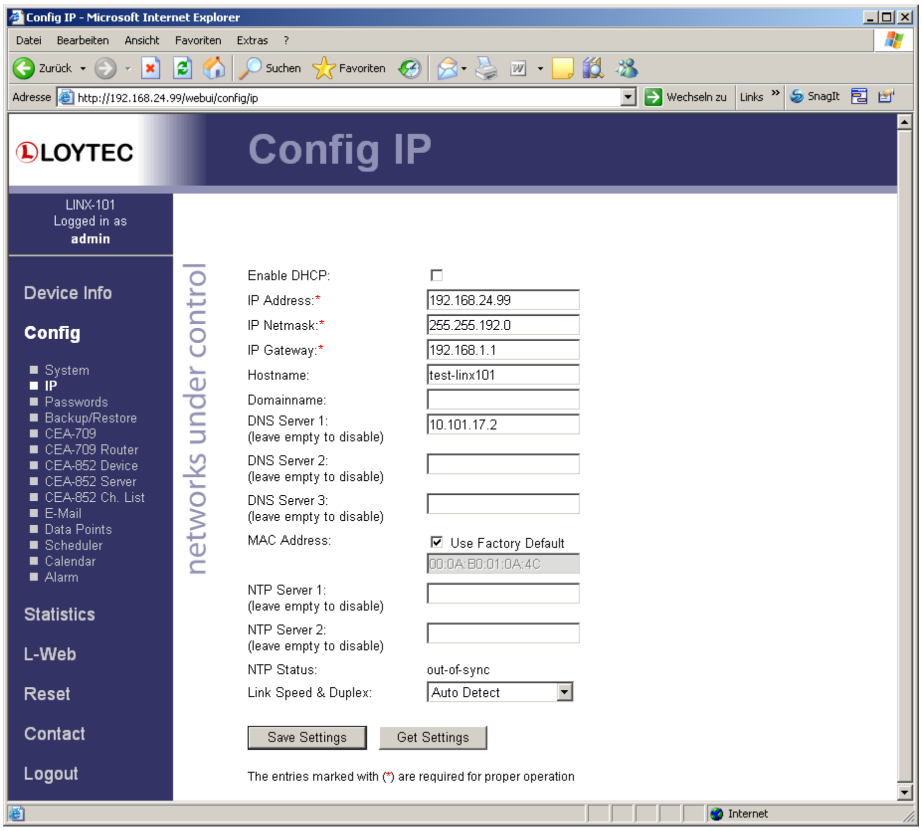
Enter your username and password

Account: admin

Password: ●●●●●

Figure 7: Enter admin as the default administrator password.

6. The Config menu opens. Click on IP in the Config menu and enter the IP address, the IP netmask, and IP gateway for this LINX-10X as shown in Figure 8.



Enable DHCP: □

IP Address:* 192.168.24.99

IP Netmask:* 255.255.192.0

IP Gateway:* 192.168.1.1

Hostname: test-linx101

Domainname:

DNS Server 1: (leave empty to disable) 10.101.17.2

DNS Server 2: (leave empty to disable)

DNS Server 3: (leave empty to disable)

MAC Address: ☑ Use Factory Default 00:0A:B0:01:0A:4C

NTP Server 1: (leave empty to disable)

NTP Server 2: (leave empty to disable)

NTP Status: out-of-sync

Link Speed & Duplex: Auto Detect

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

Figure 8: Enter IP address and gateway.

7. Press **Save Settings** and then reset the device by selecting **Reset** in the highlighted text. This changes the IP settings of the LINX-10X.

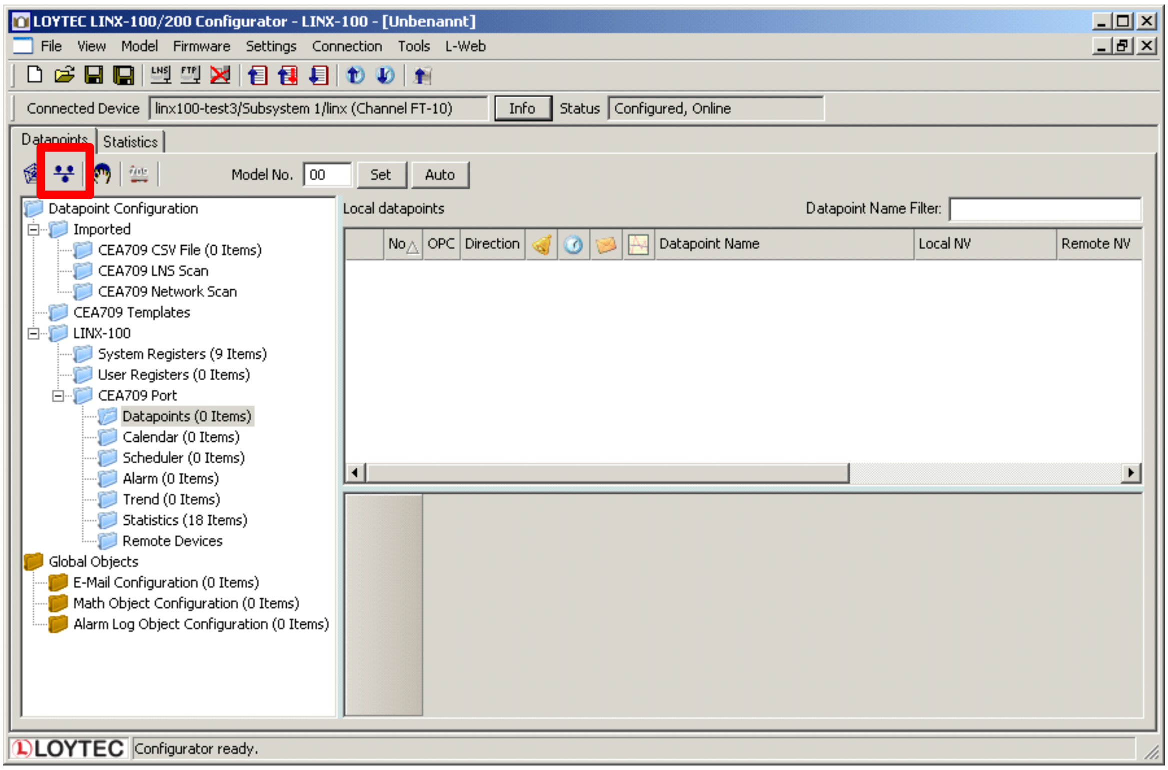
2.3 Configuration with LNS-based Tools

This section describes a quick start scenario for the LINX-10X. In this scenario network variables of nodes connected to the FT port shall be exposed as OPC tags. As a network management tool an LNS-based tool is used.

First, install the LINX-10X Configurator Software from the setup.exe. This file can be downloaded from www.loytec.com. In your LNS-based tool register the LINX-10X Configurator as an LNS plug-in.

Then open an LNS database and add an LINX-10X device using the device template, which has been created for the LINX-10X (LINX-10x_FT-10). Configure the added device with the LINX-10X Configurator plug-in. This opens the data point manager screen of the software as shown in Figure 9. Note that the device status is displayed as “Configured” on the right-hand side below the speed button bar.

Click on the “Scan Channel” speed button marked by the red rectangle in Figure 9 to scan all NVs found on nodes connected to the LINX-10X’s FT-10 channel. Figure 10 shows an example result of the scan. Now select the NVs, which shall be exposed as OPC tags and click on the “Use on Device” speed button as marked by the red rectangle in Figure 10.



Connected Device: linx100-test3/Subsystem 1/linx (Channel FT-10)

Status: Configured, Online

Model No.: 00

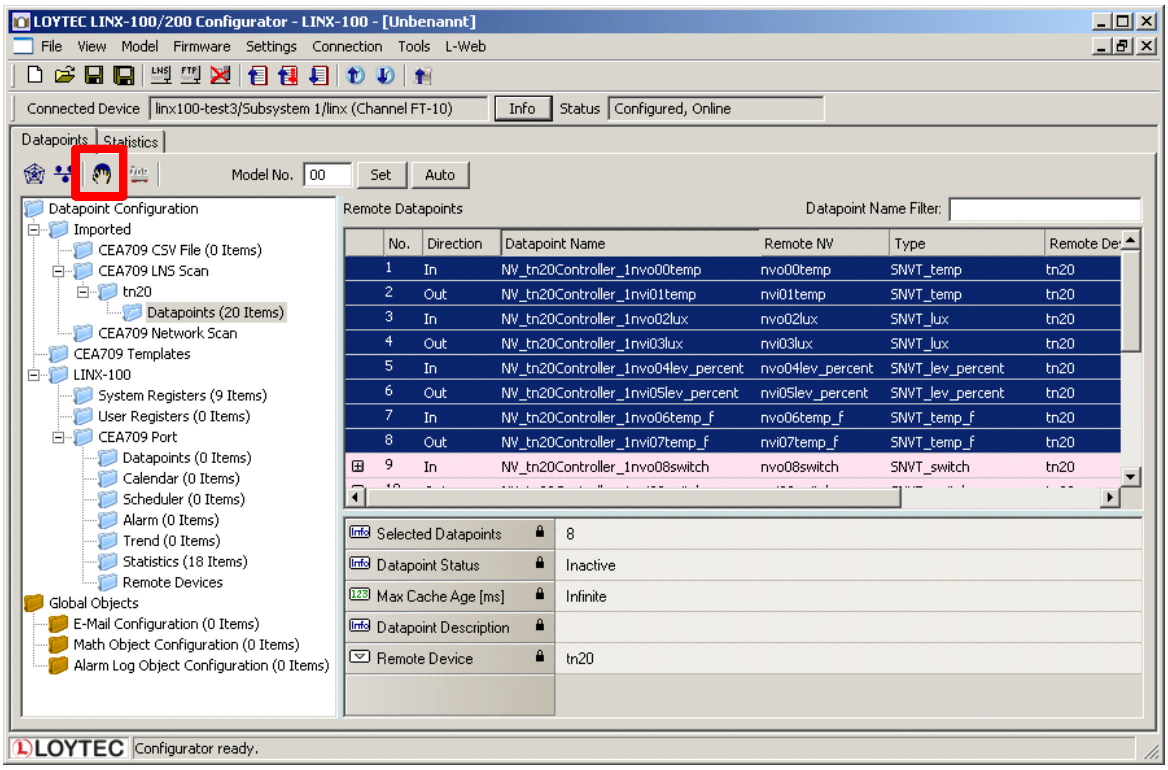
Local datapoints

Datapoint Name Filter:

No	OPC	Direction					Datapoint Name	Local NV	Remote NV

Configurator ready.

Figure 9: LINX-10X plug-in main screen.



Connected Device: linx100-test3/Subsystem 1/linx (Channel FT-10)

Status: Configured, Online

Model No.: 00

Remote Datapoints

Datapoint Name Filter:

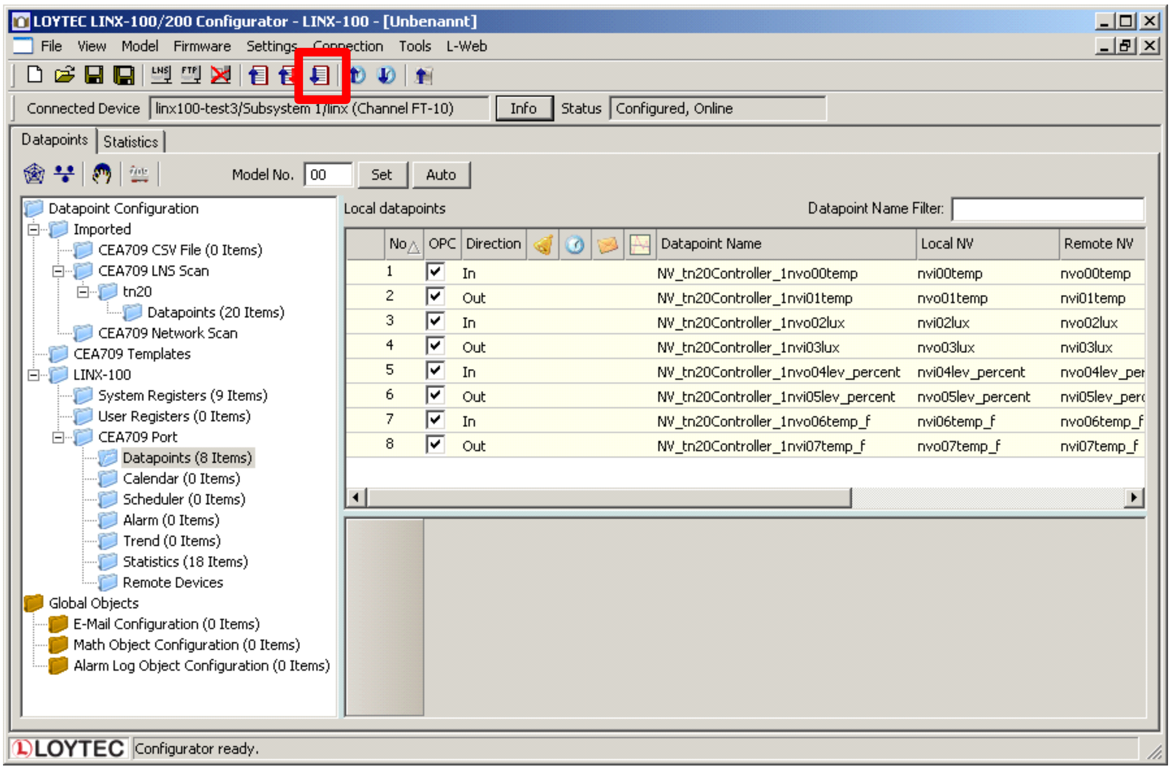
	No.	Direction	Datapoint Name	Remote NV	Type	Remote De
	1	In	NV_tn20Controller_1nvo00temp	nvo00temp	SNVT_temp	tn20
	2	Out	NV_tn20Controller_1nvi01temp	nvi01temp	SNVT_temp	tn20
	3	In	NV_tn20Controller_1nvo02lux	nvo02lux	SNVT_lux	tn20
	4	Out	NV_tn20Controller_1nvi03lux	nvi03lux	SNVT_lux	tn20
	5	In	NV_tn20Controller_1nvo04lev_percent	nvo04lev_percent	SNVT_lev_percent	tn20
	6	Out	NV_tn20Controller_1nvi05lev_percent	nvi05lev_percent	SNVT_lev_percent	tn20
	7	In	NV_tn20Controller_1nvo06temp_f	nvo06temp_f	SNVT_temp_f	tn20
	8	Out	NV_tn20Controller_1nvi07temp_f	nvi07temp_f	SNVT_temp_f	tn20
⊞	9	In	NV_tn20Controller_1nvo08switch	nvo08switch	SNVT_switch	tn20

Selected Datapoints	8
Datapoint Status	Inactive
Max Cache Age [ms]	Infinite
Datapoint Description	
Remote Device	tn20

Configurator ready.

Figure 10: Example result of scanned NVs from LNS channel.

The data points now appear in the LINX-10X device folder as shown in Figure 11. The data point name will be the name of the OPC tag. Now click on the “Download Configuration” speed button as indicated by the red rectangle in Figure 11.


LOYTEC LINX-100/200 Configurator - LINX-100 - [Unbenannt]
File View Model Firmware Settings Connection Tools L-Web
Datapoints Statistics
Set
Auto
Info
LOYTEC

Connected Device: linx100-test3/Subsystem 1/linx (Channel FT-10)

Status: Configured, Online

Model No.: 00

Datapoint Configuration
- Imported
  - CEA709 CSV File (0 Items)
  - CEA709 LNS Scan
    - tn20
      - Datapoints (20 Items)
  - CEA709 Network Scan
- CEA709 Templates
- LINX-100
  - System Registers (9 Items)
  - User Registers (0 Items)
  - CEA709 Port
    - Datapoints (8 Items)
    - Calendar (0 Items)
    - Scheduler (0 Items)
    - Alarm (0 Items)
    - Trend (0 Items)
    - Statistics (18 Items)
    - Remote Devices

Global Objects
- E-Mail Configuration (0 Items)
- Math Object Configuration (0 Items)
- Alarm Log Object Configuration (0 Items)

Local datapoints

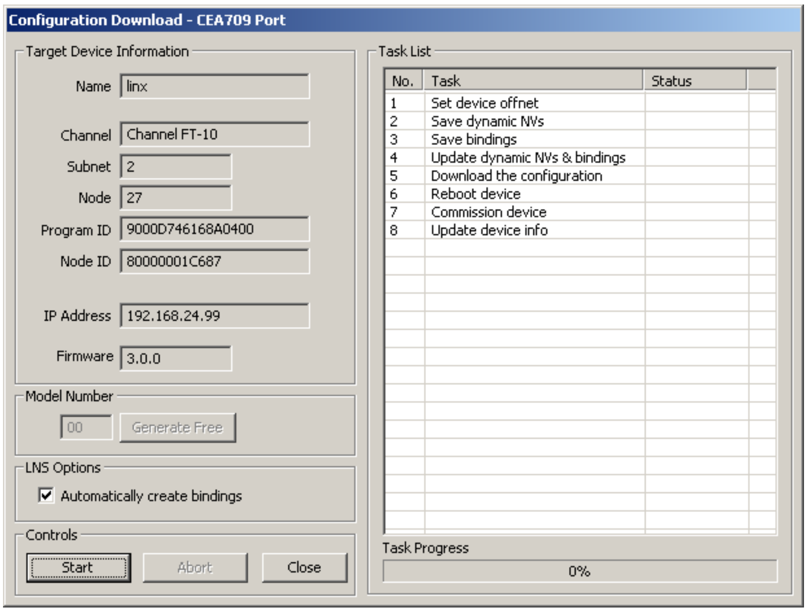
Datapoint Name Filter:

No	OPC	Direction	Datapoint Name	Local NV	Remote NV
1	☑	In	NV_tn20Controller_1nvo00temp	nvi00temp	nvo00temp
2	☑	Out	NV_tn20Controller_1nvi01temp	nvo01temp	nvi01temp
3	☑	In	NV_tn20Controller_1nvo02lux	nvi02lux	nvo02lux
4	☑	Out	NV_tn20Controller_1nvi03lux	nvo03lux	nvi03lux
5	☑	In	NV_tn20Controller_1nvo04lev_percent	nvi04lev_percent	nvo04lev_per
6	☑	Out	NV_tn20Controller_1nvi05lev_percent	nvo05lev_percent	nvi05lev_perc
7	☑	In	NV_tn20Controller_1nvo06temp_f	nvi06temp_f	nvo06temp_f
8	☑	Out	NV_tn20Controller_1nvi07temp_f	nvo07temp_f	nvi07temp_f

Configurator ready.

Figure 11: NVs used for OPC tags on the LINX-10X.

This opens the Configuration Download dialog as depicted in Figure 12. Then press “Start”. The tasks executed are displayed and their progress is visualized by the progress bar below.



Target Device Information

Name: linx

Channel: Channel FT-10

Subnet: 2

Node: 27

Program ID: 9000D746168A0400

Node ID: 80000001C687

IP Address: 192.168.24.99

Firmware: 3.0.0

Model Number: 00

LNS Options

☑ Automatically create bindings

Controls

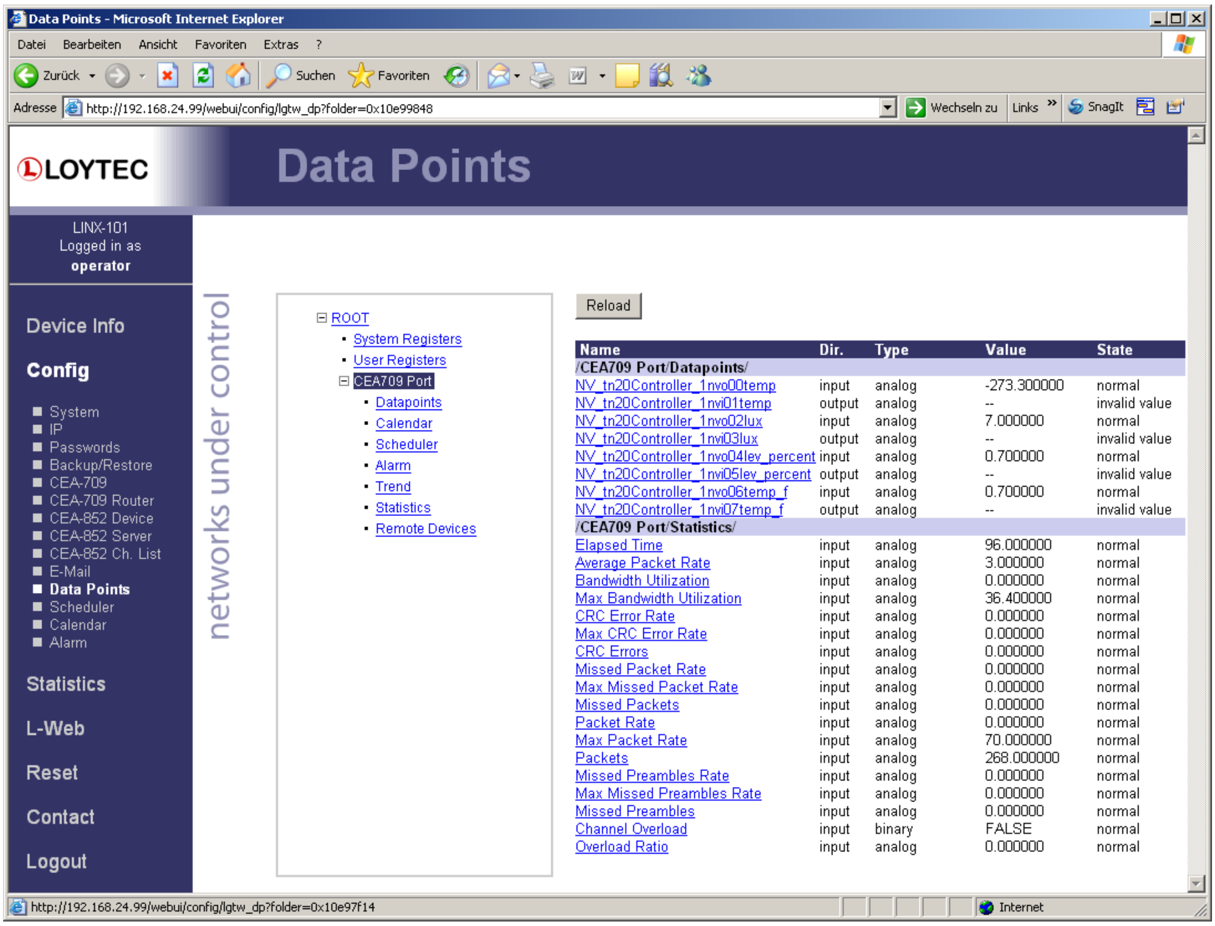
Task List

No.	Task	Status
1	Set device offset	
2	Save dynamic NVs	
3	Save bindings	
4	Update dynamic NVs & bindings	
5	Download the configuration	
6	Reboot device	
7	Commission device	
8	Update device info	

Task Progress: 0%

Figure 12: Configuration Download Dialog

When the configuration process is complete, a dialog box is shown, which must be acknowledged by clicking “Ok”. Then the LINX-10X is up and running with the new configuration. To verify the configuration go to the LINX-10X’s Web interface and click on “Config” and “OPC Data Points”, which brings up the Web page as shown in Figure 13. The list displays current data point values and status.



Name	Dir.	Type	Value	State
/CEA709 Port/Datapoints/				
NV_tn20Controller_1nvo00temp	input	analog	-273.300000	normal
NV_tn20Controller_1nvi01temp	output	analog	--	invalid value
NV_tn20Controller_1nvo02lux	input	analog	7.000000	normal
NV_tn20Controller_1nvi03lux	output	analog	--	invalid value
NV_tn20Controller_1nvo04lev_percent	input	analog	0.700000	normal
NV_tn20Controller_1nvi05lev_percent	output	analog	--	invalid value
NV_tn20Controller_1nvo06temp_f	input	analog	0.700000	normal
NV_tn20Controller_1nvi07temp_f	output	analog	--	invalid value
/CEA709 Port/Statistics/				
Elapsed Time	input	analog	96.000000	normal
Average Packet Rate	input	analog	3.000000	normal
Bandwidth Utilization	input	analog	0.000000	normal
Max Bandwidth Utilization	input	analog	36.400000	normal
CRC Error Rate	input	analog	0.000000	normal
Max CRC Error Rate	input	analog	0.000000	normal
CRC Errors	input	analog	0.000000	normal
Missed Packet Rate	input	analog	0.000000	normal
Max Missed Packet Rate	input	analog	0.000000	normal
Missed Packets	input	analog	0.000000	normal
Packet Rate	input	analog	0.000000	normal
Max Packet Rate	input	analog	70.000000	normal
Packets	input	analog	268.000000	normal
Missed Preambles Rate	input	analog	0.000000	normal
Max Missed Preambles Rate	input	analog	0.000000	normal
Missed Preambles	input	analog	0.000000	normal
Channel Overload	input	binary	FALSE	normal
Overload Ratio	input	analog	0.000000	normal

Figure 13: Verify the data point configuration on the Web interface

Note that the auto-generation has created dynamic NVs as counterparts to the scanned NVs on the CEA-709 network and also created bindings for those NVs. If static NVs or external NVs (with polling) shall be used on the CEA-709 network, or more advanced NV selection schemes shall be employed, please refer to Chapter 6 to learn more about the Configurator software.

2.4 Connect with an OPC XML-DA Client

After the configuration has been downloaded to the LINX-10X it is ready to serve OPC XML-DA clients. Connect to the LINX-10X using the URL

http://192.168.24.99/DA,

given that 192.168.24.99 is the IP address of the LINX-10X. Note, that by default writing to OPC tags needs basic HTTP authentication using the password for the "operator" user. This is by default "operator".

3 Hardware Installation

3.1 Enclosure

3.1.1 LINX-10X

The LINX-10X enclosure is 6 TE (1 TE = 17.5 mm) wide for DIN rail mounting, following DIN 43 880 (see Figure 14).

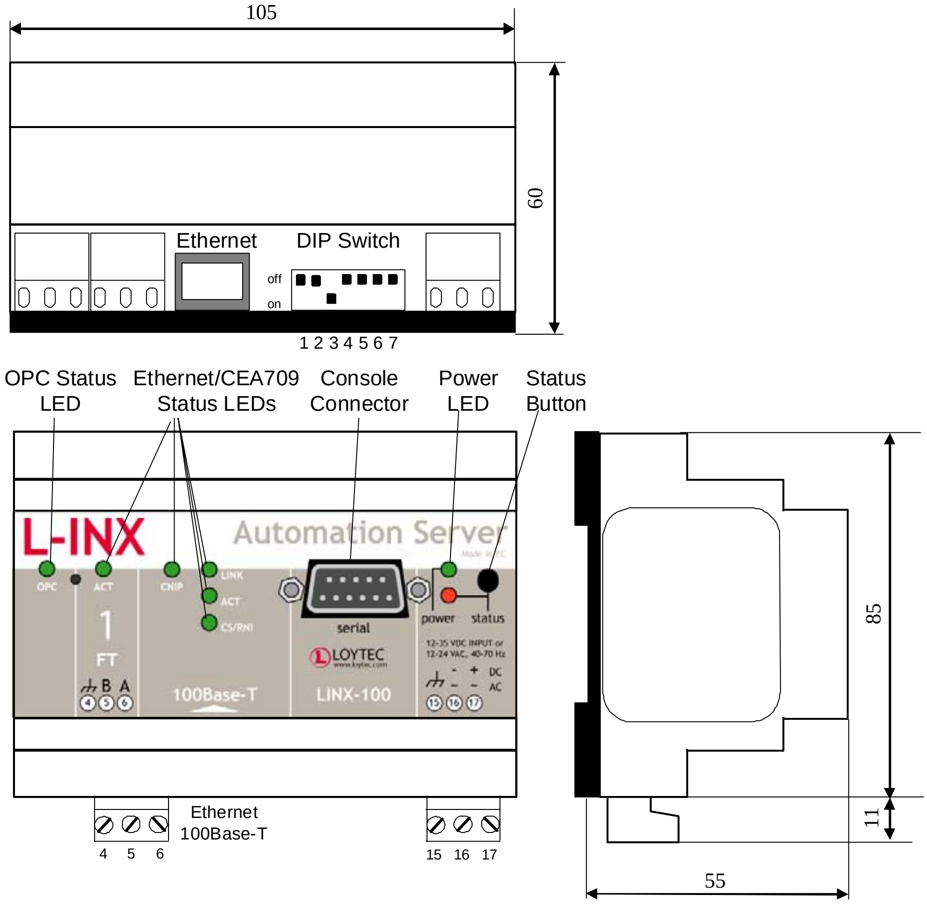


Figure 14: LINX-10X Enclosure (dimensions in mm)

3.2 Product Label

The product label on the side of the LINX-10X contains the following information (see Figure 14):

- LINX-10X order number with bar-code (e.g., LINX-100, LINX-101),
- 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).

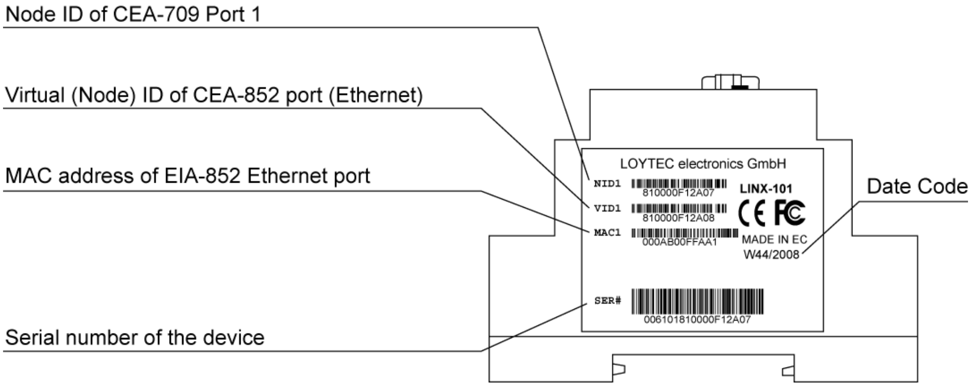


Figure 15: LINX-10X product label.

Unless stated otherwise, all bar codes are encoded using “Code 128”. An additional label is also supplied with the LINX-10X 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 LINX-10X’s temperature does not exceed the specified range (see Chapter 16).

3.4 LED signals

3.4.1 Power LED

The LINX-10X power LED lights up green when power is supplied to terminals 16 and 17.

3.4.2 Status LED

The LINX-10X is equipped with a red status LED (see Figure 14). This LED is normally off. During boot-up the status LED is used to signal error conditions (red). If the fall-back image is executed the status LED flashes red once every second.

3.4.3 OPC LED

The OPC Server LED illuminates green when at least one OPC client is connected to the OPC server. The LED flickers on OPC XML-DA traffic activity.

3.4.4 FT Activity LED

The FT port on the LINX-10X has a three-color LED (green, red, and orange, see Figure 14). Table 1 shows different LED patterns of the port and their meaning.

Behavior	Description	Comment
GREEN flashing fast	Traffic	
GREEN flashing at 1Hz	The OPC node or LINX-101's router port is unconfigured	On the LINX-101 this LED is only permanent on if both, node and router, are commissioned.
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

3.4.5 Ethernet Link LED

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

3.4.6 Ethernet Activity LED

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

3.4.7 CNIP LED

The CNIP LED is a three color LED that indicates different operating states of the LINX-10X'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 LINX-10X can be seen. Stale packets or packets not addressed to the LINX-10X 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 LINX-10X 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 LINX-10X's CEA-709 side of the gateway has not been commissioned yet. The color indicates the CEA-852 IP channel status as described above.

3.4.8 CS/RNI LED

On the LINX-101 this LED indicates the status of the CEA-852 configuration server. If illuminated green, the configuration server is enabled.

On the LINX-100 this LED indicates the remote network interface (RNI) status. The LED is dark, if RNI is not supported by this device or the interface is not enabled. The LED is green, if the RNI is currently in use.

3.4.9 Wink Action

If the LINX-10X 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 LINX-10X LEDs resume their normal behavior.

3.4.10 Network Diagnostics

The LINX-10X provides simple network diagnostics via its CEA-709 activity LED:

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

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

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

A port overload condition occurs if

- the average bandwidth utilization of this port was higher than 70% or
- the collision rate was higher than 5% or
- more than 15% CRC errors have occurred on a port with a power-line transceiver or more than 5% on a port with a transceiver other than power-line or
- the LINX-10X was not able to process all available messages.

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

3.5 Status Button

The LINX-10X is equipped with a status button (see Figure 14). When pressing the status button shortly during normal operation of the LINX-10X, it sends a "Service Pin Message" on the active CEA-709 network port (FT-10 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 4.3.8).

3.5.1 Resetting Forwarding Tables

In order to reset the forwarding tables of the LINX-10X's router, the status button needs to be pressed for at least 20 seconds during normal operation of the LINX-10X. Resetting forwarding tables means:

- Resetting the CEA-709 transceiver to the standard values.
- Setting all ports to unconfigured.
- Clearing the group forwarding, the subnet/node forwarding and the router domain table when used in smart switch mode.
- Clearing the LINX-10X status and statistic data.
- But **does not** clear the IP address, the CEA-852 configuration settings, and the data point configuration.

All this is done when the button is released. Afterwards a reset is performed to let the changes take effect.

Important: ***If the LINX-10X is moved from one location to another or if major changes to the configuration of the network are made, it is recommended to reset the LINX-10X configuration to factory defaults.***

Important: ***Wait at least 30 seconds after power-up of the LINX-10X before pressing the Status Button to ensure that the LINX-10X has booted properly!***

3.6 DIP Switch Settings

The LINX-10X has seven switches to select the mode of operation. The DIP switch assignment for the LINX-10X is shown in Table 2.

DIP Switch #	Function	Factory Default
1	Reserved/LINX-101	OFF
2	Reserved/LINX-101	OFF
3	Reserved	OFF
4	Must be OFF	OFF
5	Reserved	OFF
6	Reserved	OFF
7	Reserved	OFF

Table 2: DIP Switch Settings for LINX-10X

3.7 Power Supply

The LINX-10X can either be DC or AC powered. The LINX-10X power terminals are listed in Table 3.

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

Table 3: Power Terminals on LINX-10X

Important: ***Do not connect the power supply wire on terminal 17 to earth ground as shown in Figure 16! Terminal 16 may be connected to earth ground.***

3.8 Terminal Layout

The LINX-10X 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.

Terminal	Function
4	Earth Ground
5, 6	CEA-709 A, B of TP/FT-10 Channel Port
8	Ethernet 100BaseT
15	Earth Ground
16, 17	Power Supply (do not connect 17 to Earth Ground)

Table 4: LINX-10X Terminals LINX-10X.

3.9 Wiring

The CEA-709 network segment connected to the LINX-10X needs to be terminated according to the rules found in the specification of the transceiver (see Section 11.1).

Important: ***All Earth ground terminals are internally connected to the Earth Ground terminal 15. 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 LINX-10X terminals or somewhere else in the network, but never at more than one place (see Figure 16)!***

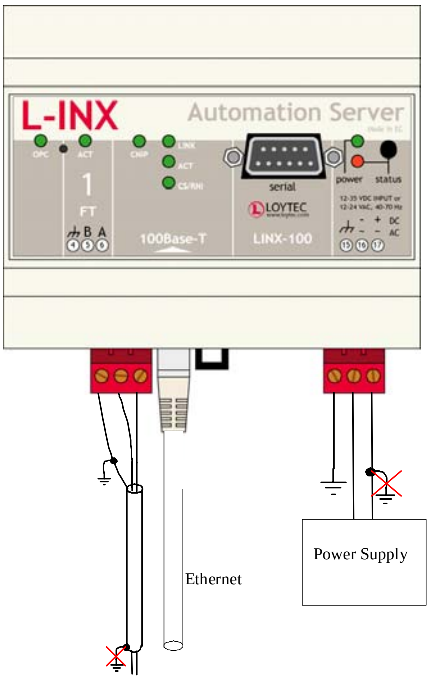


Figure 16: Connecting the Earth Ground to the LINX-10X

4 Console Interface

4.1 Console Connection

The LINX-10X is equipped with a serial interface to

- display the results of the self test,
- allow configuration via a console menu,
- upgrade the LINX-10X firmware.

To use the serial interface, the console connector (see Figure 14) of the LINX-10X can be connected to the RS-232 port of a PC. The PC can communicate with the LINX-10X 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 LINX-10X serial console interface to your PC.

4.2 Self Test

Whenever the LINX-10X comes out of reset it performs a self-test. The console output of a successful boot sequence on an LINX-10X reads as depicted in Figure 17. The duration of a successful boot sequence of an LINX-10X is typically 30 seconds.

```
LOYTEC electronics GmbH
www.loytec.com


Testing Board ID (0)                                       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
LINX-10x Primary Image loading...
Firmware version 3.0.0

Type bootshell to enter the boot shell...

Mounting file system                                       Passed
Starting TCP/IP networking                                 Passed
Starting FTP server                                        Passed
Starting Telnet server                                     Passed
Starting CEA-852 config. server                            Passed
Starting CEA-852 device                                    Passed
Detecting CEA-709 port 1 (FT-10)                           Passed
Starting remote LPA                                        Passed
Starting CEA-709 scanner                                   Passed
Starting CEA-709 networking                                Passed
Starting OPC server                                        Passed
Starting Web server                                        Passed

LINX-101(c)
LOYTEC electronics GmbH
Fri Aug  8 13:54:31 2008 - V3.0.0
```

Figure 17: Console messages during the boot phase.

4.3 LINX-10X Device Main Menu

After booting has completed, the LINX-10X displays the console menu as shown in Figure 18.

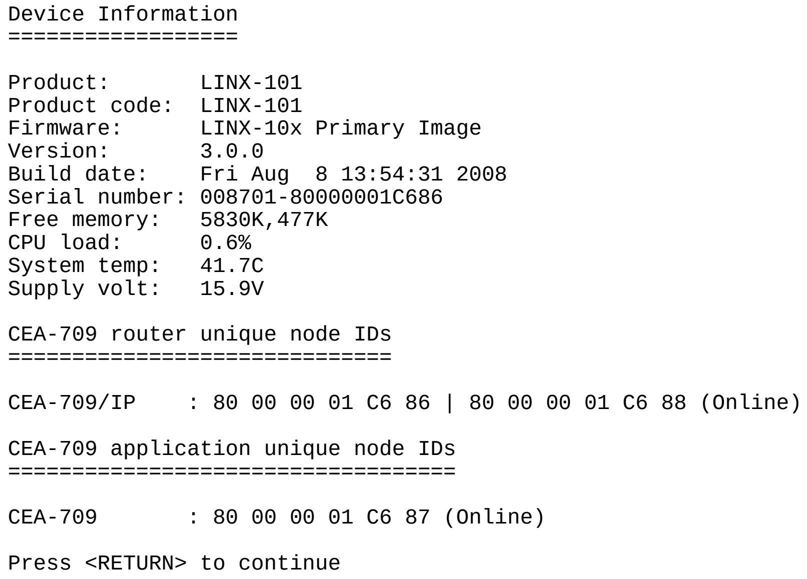
```
Device Main Menu
================

[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 18: LINX-10X 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 LINX-10X and the current firmware version. The output should look like what is shown in Figure 19.



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

Product:       LINX-101
Product code:  LINX-101
Firmware:      LINX-10x Primary Image
Version:       3.0.0
Build date:    Fri Aug  8 13:54:31 2008
Serial number: 008701-80000001C686
Free memory:   5830K,477K
CPU load:      0.6%
System temp:   41.7C
Supply volt:   15.9V

CEA-709 router unique node IDs
==============================

CEA-709/IP    : 80 00 00 01 C6 86 | 80 00 00 01 C6 88 (Online)

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

CEA-709       : 80 00 00 01 C6 87 (Online)

Press <RETURN> to continue
```

Figure 19: Device Information

4.3.2 Option 2 – Serial firmware upgrade

This menu item allows updating the LINX-10X firmware via the serial interface (console). See Section 12.2 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 client configuration / RNI configuration

Depending on the CEA-709 configuration this menu item is used to set the CEA-852 client configuration or to set the RNI configuration. The LINX-100 can be switched between FT mode (RNI configuration is available) or IP-852 mode (CEA-852 client configuration is available). The LINX-101 always provides the CEA-852 client configuration for the built-in router.

In case of CEA-852 client configuration select this menu item to change settings like configuration server IP address, device name, SNTP server, escrow timeout, aggregation timeout, MD5 authentication secret.

In case of RNI select this menu item to change settings like the communication port, the device name, the location string or settings concerning the MD5 authentication.

See Section 4.7 or Section 4.8 for details.

4.3.7 Option 7 – CEA-852 server configuration

The LINX-101 provides the CEA-852 server configuration menu. Select this menu item to change the CEA-852 configuration server configuration settings like the channel name, channel membership list, the SNTP time server, channel timeout, MD5 authentication. See Section 4.9 for details. The CEA-852 server can also be configured over the Web UI (see Section 5.2.7).

4.3.8 Option 8 - Reset configuration (factory defaults)

This menu item resets the LINX-10X to factory defaults. See Section 3.5 for details on how to load factory defaults by pressing the status button and Section 4.10 on how to load factory defaults through the console menu.

4.3.9 Option 9 – Device statistics

Select this menu item to display advanced IP, CEA-852 device, and statistics information like number of packets sent and received, number of channel members, etc. See Section 4.11 for details.

4.3.10 Option 0 – Reset Device

Select this menu item to reboot the LINX-10X. Some configuration changes require to reboot the device. Note, that this option does not reset the configuration.

4.3.11 Option a – Data Points

This menu option takes the user to the data point menu. In this menu the configured data points in the LINX-10X can be viewed and set with values. See Section 4.12 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 20.

```
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)
[c]  E-mail account configuration

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

Please choose:
```

Figure 20: System Configuration Menu

4.4.1 Option 1 - Configure Date/Time

This menu item allows to configure the LINX-10X’s system time. It provides several sub-items as shown in Figure 21. 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 21: Configure Date/Time Menu

The timezone 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/U.S.A. is –06:00). Start and end of daylight savings time (DST) is defined in menu option '5'. Pre-defined choices are offered for Europe and U.S.A./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 to configure the LINX-10X's earth position. This setting defines the longitude, latitude and elevation of the device on the planet. 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 22). For moving locations, this setting can be updated over the network using the network variable nciEarthPos (see Section 10.2.2).

```
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 22: Configure Earth Position

The latitude and longitude are entered through menu items '2' and '3' as degrees, minutes, and seconds. The altitude (or elevation) is entered in menu item '3' in meters from 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 12.1).

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 LINX-10X. You can disable the Web server if you do not want to provide access to the LINX-10X 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 c – E-Mail Account Configuration

This menu item allows configuring the LINX-10X's E-Mail account for your E-Mail provider. The content and time when E-Mails are sent is configured elsewhere. The E-Mail configuration menu is shown in Figure 23.

Enter <1> to specify the outgoing e-mail server. This is the SMTP server of your provider. Typically the SMTP server port is 25. If not, enter <2> and specify another port. Enter <3> to set your source e-mail address and <4 to enter the name displayed for this source e-mail address. Optionally, enter <5> to specify a reply-to address, if replies shall not be sent to the specified source e-mail address.

If the provider's SMTP server requires authentication, enter the required user name and password in menu item '6'. Note, that only username/password is supported. SSL/TLS authentication is not supported by the LINX-10X (e.g., Hotmail, gmail cannot be used).

```
E-Mail Account Configuration Menu
=================================

[1]  Outgoing e-mail server (SMTP) : <unset>
[2]  Outgoing e-mail server port   : 25 (default)
[3]  Source e-mail address         : <unset>
[4]  Source e-mail sender name     : <unset>
[5]  Reply e-mail address (opt.)   : <unset>
[6]  E-Mail server user name       : <no authentication>
     E-Mail server password        : <unset>
[9]  SMTP debug output             : off
[0]  Send test e-mail

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

Please choose:
```

Figure 23: E-Mail Account Configuration Menu

For testing the e-mail setup, enter <0> to send a test e-mail. For debugging delivery problems, turn on logging information by selecting <9>. The e-mail transmission log is then output to the console.

4.5 CEA-709 Configuration Menu

This menu allows changing the settings of the CEA-709 port of the LINX-10X. The menus differ between the LINX-100 and the LINX-101. On the LINX-100 the menu looks like shown in Figure 24.

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

[0]  Port configuration    : CEA-709

     CEA-709               : FT-10
     IP                    : IP-852 (inactive)

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

Please choose:
```

Figure 24: CEA-709 Configuration Menu on the LINX-100.

The menu in the LINX-101 contains also the router and has both ports always active. See the depicted example in Figure 25.

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

     CEA-709               : FT-10
     IP                    : IP-852

[r]  Router configuration  : Configured Router

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

Please choose:
```

Figure 25: CEA-709 Configuration Menu on the LINX-101.

4.5.1 Option 0 – Port configuration

This menu item allows configuring which CEA-709 port is active in the LINX-10X. Choose <1> for CEA-709 (e.g., FT-10) or <2> for CEA-852 (IP channel).

4.5.2 Option r – Router configuration

This menu is only available on the LINX-101. The router configuration as shown in allows setting the principal operating mode of the LINX-101 routing core. The default is “configured router”. Choose <1> to change the router mode.

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

[1]  Router mode              : Configured Router

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

Please choose:
```

Figure 26: Router Configuration Menu.

Figure 27 depicts the router mode menu. Choose <1> for configured router or select <2> for the Smart Switch mode.

```
Set router mode
===============

[1]  Enable Configured Router Mode
[2]  Enable Smart Switch Mode

Please choose:
```

Figure 27: Router Mode Configuration Menu.

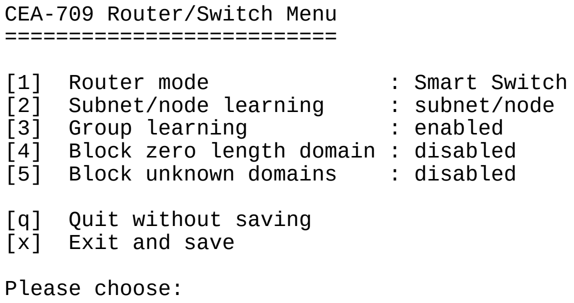
4.5.2.1 Option 1 – Enable Configured Router Mode (Default)

Select this menu item if you want to use the LINX-101 as a standard configured CEA-709 router that can be configured in a network management tool such as NL-200 or LonMaker. This operating mode is also the factory default mode. The LINX-101 must be rebooted to let the change take effect.

4.5.2.2 Option 2 – Enable Smart Switch Mode

Select this menu item if you want to use the LINX-101’s router as a self-learning router like the L-Switch (“smart switch mode”). In this configuration the LINX-101’s router doesn’t need to be configured with a network management tool but is completely transparent in the network. Use this operating mode in a plug&play networking environment. If Smart Switch Mode is enabled the system configuration menu has 3 additional entries as shown in Figure 28. The switch mode should only be used in LAN networks.

Note: *If you change the router mode of the LINX-101’s router you must reset the device with the main menu item 0 or by pressing the reset button in order to have the changes take effect.*



```
CEA-709 Router/Switch Menu
==========================

[1]  Router mode              : Smart Switch
[2]  Subnet/node learning     : subnet/node
[3]  Group learning           : enabled
[4]  Block zero length domain : disabled
[5]  Block unknown domains    : disabled

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

Please choose:
```

Figure 28: CEA-709 Router/Switch Menu

Entry 2 allows setting the mode for learning of subnet/node addresses. The selection can be Subnet/node learning, Subnet learning, or Disable. If subnet/node learning is selected, the LINX-10X's router will learn based on subnet/node addresses (see Section 8.1.2). Subnet broadcasts are flooded. This mode is plug&play.

If subnet learning is disabled, all subnet-wide broadcasts are forwarded by the LINX-10X's router from one side to the other side. If subnet learning is enabled the LINX-10X's router will learn the subnet addresses on both network ports and will only flood subnet broadcasts if the destination subnet address doesn't exist on the local channel. Subnet learning should be enabled, if group overloading is used in the case that more than 256 group addresses are needed. Subnet learning is not plug&play. Please use NL-200, LonMaker, or other network management tools to ensure that one subnet address is only used behind one LINX-10X device. This can be achieved by using our LINX-10X LonMaker shapes or by placing phantom routers in e.g. NL-220. Please contact LOYTEC support if you think you need this feature!

Entry 3 allows enabling or disabling learning of group addresses.

Entry 4 should be left at the default. Please contact LOYTEC support if you think you might need to block zero length domain!

Entry 5: The LINX-10X in Smart Switch Mode will learn up to four domains. If your network contains more than four domains please contact LOYTEC support for advice!

4.6 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 29.

```
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-linx101
[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 29: IP Configuration Menu when DHCP is disabled

The IP configuration menu, when DHCP is enabled, is shown in Figure 30.

```
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-linx101
     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 30: 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 for the LINX-10X, the netmask (e.g., 255.255.255.0), and the default gateway address.

4.6.3 Option 5 – Hostname, 6 – Domainname

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

4.6.4 Option 7 – DNS Servers

You can configure up to 3 Domain Name Servers. You need to enter at least one IP address of a DNS server, if you need DNS name resolution, e.g., for sending E-Mails (see Section 5.2.13).

4.6.5 Option 9 – MAC Address

The LINX-10X 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.

4.6.6 Option 0 – NTP Servers

You can configure up to 2 NTP server. 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).

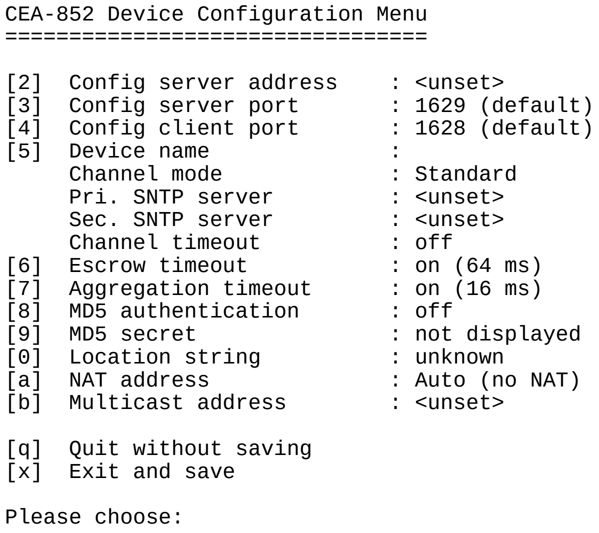
4.6.7 Option b – Link Speed & Duplex

If the LINX-10X is operated with an old 10Mbit/s-only hub, the link speed should be switched from "Auto Detect" to "10Mbps/Half-Duplex". With modern 100/10Mbit/s switches this setting can be left at its default (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 LINX-10X to an IP channel. The recommended method is to enter the information at the configuration server. The configuration server will then contact the LINX-10X and configure the relevant information. If for some reason the LINX-10X 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. Then LINX-10X tries to register with the configuration server. The device configuration menu is shown in Figure 31.



```
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 31: CEA-852 Device Configuration Menu

In case that the configuration server contacts the LINX-10X, 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 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 LINX-10X 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 LINX-10X 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 LINX-10X behind one NAT router), the channel switches to “Extended NAT mode”. Please refer to the L-IP User’s Manual 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 LINX-10X 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 LINX-10X.

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 *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 LINX-10X 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 LINX-10X behind a NAT router or firewall, which has a dynamic public IP address, and determines the correct NAT address from an L-IP CS. This is the default setting.

```
Enable automatic NAT router discovery (y/n):
```

Figure 32: Enable/Disable automatic NAT Router Discovery

To enable/disable automatic NAT router discovery select this menu option. The question in Figure 32 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 LINX-10X uses automatic NAT router discovery and the NAT address is known beforehand, the LINX-10X 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 LINX-10X to a CEA-852 IP channel in the configuration server:

1. On the LINX-10X 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 LINX-10X 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 LINX-10X 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's Manual to learn when it is beneficial to use multi-cast addresses in your channel.

4.8 RNI Configuration

This menu item allows setting up the remote network interface configuration of the LINX-10X. The RNI sub menu is shown here:

```
RNI Configuration Menu
======================

[2]  RNI port                : 1628 (default)
[3]  Device name             :
[4]  MD5 authentication      : off
[5]  MD5 secret              : not displayed
[6]  Location string         : unknown

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

Please choose:
```

Figure 33: RNI Configuration Menu

4.8.1 Option 2 - RNI port

This is the port for PC-to-LINX-10X communication. If the LINX-10X resides behind a NAT router, UDP and TCP port forwarding to the NIC-IP must be enabled in the NAT router for the specified port (default 1628). If several LINX-10Xs are located behind the NAT router, each LINX-10X must be configured with a different port and all ports must be forwarded accordingly in the NAT router. To switch back to the default port, simply enter 0 (or 1628).

4.8.2 Option 3 - Device Name and Option 6 - Location String

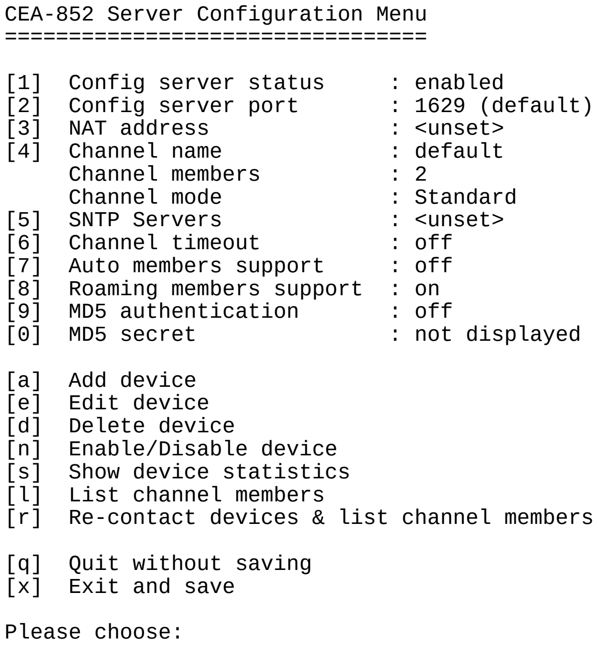
These settings specify the name and location of LINX-10X device. These strings can be used to identify the LINX-10X in the L-Config tool.

4.8.3 Option 4 - MD5 authentication and Option 5 - MD5 secret

If MD5 authentication is enabled, only PCs that have the correct 'MD5 secret' configured can access the LINX-10X. Using MD5 authentication is highly recommended when using a LINX-10X remotely over the Internet. Observe that the MD5 secret is never shown in the console menu for security reasons.

4.9 CEA-852 Server Configuration

This menu holds relevant information regarding the configuration of the CEA-852 server. If the built-in configuration server is used to manage the devices on the IP-852 channel, all CEA-852 devices on the IP-852 channel must be entered in the device list of the server. The CEA-852 devices themselves then only need to have a unique IP address, device name, and if operated behind a NAT router the NAT address assigned. The configuration server will contact all devices in the device list and update the relevant information in the client devices. The server configuration menu is shown in Figure 34. The device name can also be set by the configuration server.



```
CEA-852 Server Configuration Menu
=================================

[1]  Config server status     : enabled
[2]  Config server port       : 1629 (default)
[3]  NAT address              : <unset>
[4]  Channel name             : default
     Channel members          : 2
     Channel mode             : Standard
[5]  SNTP Servers             : <unset>
[6]  Channel timeout          : off
[7]  Auto members support     : off
[8]  Roaming members support  : on
[9]  MD5 authentication       : off
[0]  MD5 secret               : not displayed

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

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

Please choose:
```

Figure 34: Configuration Server Menu.

4.9.1 Option 1 – Config server status

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

4.9.2 Option 2 – Config server port

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

4.9.3 Option 3 – Channel name

The menu item allows setting a channel name that can consist of up to 15 characters. The number of channel members is shown below the channel name.

4.9.4 Item Channel Mode

This field reflects the current channel mode. The LINX-101 configuration server automatically determines this mode depending if there are any two devices in the channel which use the same IP address but different ports (e.g. multiple LINX-101s behind one NAT router). If all IP addresses are unique the mode is "Standard", if some are not unique the mode is "Extended NAT mode". Please refer to Section 8.4.2 to learn more about the implications of this mode.

4.9.5 Option 4 – Primary SNTP server, 5 – Secondary SNTP server

The two menu items allow setting the IP address of the primary and secondary SNTP time server. Please specify one or better two SNTP servers if CEA-852 devices are communicating over the Internet rather than an Intranet. A list of available timeservers can be found at www.ntp.org. A subset of this list is shown in Table 6 on page 67. More SNTP servers can be found at http://www.eecis.udel.edu/~mills/ntp/clock1.html.

4.9.6 Option 6 – Channel Timeout

This menu item allows setting the channel timeout. The channel timeout is an IP-852 channel property and indicates how old a packet can be before it is discarded. The channel timeout is set in ms. To disable the channel timeout enter a value of 0. To select the proper value please consult Section 8.7. Setting a channel timeout other than 0 requires a valid SNTP server entry on the configuration server (see Section 4.9.5).

4.9.7 Option 7 – Auto members support

This menu item allows members to be automatically added to the channel. If turned on, CEA-852 devices can register on the IP-852 channel without the device being explicitly added on the configuration server. This special feature is useful in combination with the LPA-IP since it can add itself to the configuration server during the debug session. Non-responding auto members are automatically removed from the channel. This feature is turned off by default and must be explicitly turned on.

Use this option with care because new CEA-852 devices can add themselves to the channel without knowledge of the system operator. This could cause a potential security hole.

4.9.8 Option 8 – Roaming members support

This menu item allows tracking CEA-852 devices when their IP address changes. This feature must be turned on, if DHCP is used and the DHCP server can assign different IP addresses to the same device (same Neuron-ID). In combination with Auto-NAT LINX-101s can also be operated behind NAT routers, which change their IP address between connection setups. For more information on this topic refer to Section 8.4.1.

The roaming member feature is turned on by default. It is recommended to turn off this feature if DHCP is not used or if the DHCP server always assigns the same IP address to a given MAC address.

4.9.9 Option 9 – MD5 authentication

This menu item allows enabling and disabling MD5 authentication. If MD5 authentication is enabled all devices on the IP-852 channel must have MD5 enabled and must use the same secret.

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

4.9.10 Option 0 - MD5 secret

Enter the 16-byte MD5 secret. Note that for security purposes the currently set 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.

4.9.11 Option a – Add device

Select this menu item to add a CEA-852 device to the IP-852 channel. A new menu appears as shown in Figure 35.

```
CEA-852 Member Menu
===================

[1] IP Address          : <unset>
[2] Port                : <unset>
[3] NAT Address         : <unset>
[4] Device name         :

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

Figure 35: Add CEA-852 device.

Please enter the IP address and device name of the new CEA-852 device that should join the IP-852 channel. If the port is different from the default port 1628 you must also enter the port address otherwise the default port address will be entered automatically. If the device is behind a NAT router enter the local address in item 1 and the NAT routers address in item 4. Do not forget to set up a port forwarding rule in the NAT router for the port specified in item 2.

4.9.12 Option e – Edit device

Select this menu item to edit a CEA-852 device on the IP-852 channel. The LINX-10X prompts the device number which shall be edited. A list of available CEA-852 devices is displayed with the menu item '1'. A new menu appears as shown in Figure 36.

```
CEA-852 Member Menu
===================

[1] IP Address          : 192.168.2.170
[2] Port                : 1628
[3] NAT Address         : <unset>
[4] Device name         : pc-sts

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

Figure 36: Edit CEA-852 device in channel member list.

You can now change the IP address, port, NAT address or device name of the CEA-852 device.

4.9.13 Option d – Delete device

Select this menu item to delete a CEA-852 device on the IP-852 channel. The LINX-101 prompts the device number which shall be deleted. A list of available CEA-852 devices is displayed with the menu item '1'.

4.9.14 Option n – Enable/Disable device

Select this menu option to enable or disable a CEA-852 device on the IP-852 channel. An enabled device can be disabled and a disabled device can be enabled. The LINX-101 prompts the device number which shall be enabled/disabled. A list of available CEA-852 devices with their current status is displayed with the menu item '1'. Disabled members are temporarily removed from the IP-852 channel and do not receive messages.

4.9.15 Option s – Show device statistics

Select this menu item to display statistics information for the client devices. The LINX-101 prompts the device number which shall be examined. This number can be found in the Channel Member List (see Section 4.9.16). Please note that this feature allows extracting the statistics information from remote client devices over the IP-852 channel.

4.9.16 Option l – List channel members

Select this menu item to list all IP-852 channel members.

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

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

Press <RETURN> to continue
```

Figure 37: List all IP-852 channel members.

The list shows the list entry number, the device name, the IP address and the current status of this device. Note that the first entry is always the local device, which the CEA-852 device is built into the configuration server. Devices behind a NAT router are listed in a tree view style. The A-flag indicates that this device is an auto member. The X-flag indicates that the device got disabled because it does not support the extended NAT mode (e.g. pre 3.0 L-IP or *i*.LON 1000). If the channel mode falls back to standard, these devices are enabled again.

4.9.17 Option r – Recontact devices & list channel members

Select this menu item to contact all CEA-852 devices on the IP-852 channel and watch the state of the individual CEA-852 devices.

This menu item can also be used when a CEA-852 device (e.g. LINX-101) is replaced and the CEA-852 configuration must be propagated to the new device without deleting the device in the configuration server and adding the device again.

This menu item can also be used to remove all auto members from the configuration server that are no longer responding (see 4.9.7).

4.10 Reset configuration (load factory defaults)

This menu item allows resetting the device into its factory default state. The menu appears as shown in Figure 38.

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

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

[q]  Quit

Please choose:
```

Figure 38: Reset to Factory Defaults Menu

4.10.1 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.).

4.10.2 Option 3 – Reset all passwords

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

4.10.3 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 LINX-10X must be rebooted to let the changes take effect.

Note: *This option does not reset the configuration of the built-in router of the LINX-101. The nodes connected by the router are still reachable after clearing the data point configuration.*

4.11 Device Statistics Menu

This menu holds relevant information regarding the device statistics of the LINX-10X. The device statistics menu is shown in Figure 39. 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 39: Device Statistics Menu

4.11.1 Option 1a – CEA-852 device statistics

A sample console output is shown in Figure 40. The first part displays CEA-852 device statistics, which are part of the standard and are comparable to e.g. the *i*.LON 600. Press <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 40: CEA-852 Device Statistics

A sample console output of the extended CEA-852 device statistics is shown in Figure 41. At the end the user is prompted if the statistics shall be cleared. Press <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 41: Extended CEA-852 Device Statistics

4.11.2 Option 1b – RNI Device Statistics

A sample console output is shown in Figure 42. The first part displays RNI device statistics, which are part of the standard and are comparable to e.g. the *i*.LON 600. Press <y> to go on to extended statistics.

```
RNI Device Statistics
=====================

Seconds since cleared               : 21
Date/Time of clear (GMT)            : Tue Jun 17 11:01:13 2008
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 RNI device statistics (y/n)? y
```

Figure 42 RNI Device Statistics

A sample console output of the extended RNI device statistics is shown in Figure 43. At the end the user is prompted if the statistics shall be cleared. Press <y> to reset all counters to 0.

```
Extended RNI Device Statistics
==============================

Session ID                            : 0x7c5f71b6
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 RNI device 1 statistics (y/n)?
```

Figure 43: Extended RNI Device Statistics

4.11.3 Option 2 – CEA-709 Application Statistics

A sample console output is shown in Figure 44.

```
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 44: CEA-709 Application Statistics

4.11.4 Option 4 – IP statistics

A sample console output is shown in Figure 45.

```
*********** 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 45: IP Statistics

The IP statistics menu has the additional feature of displaying any IP address conflicts. If the LINX-10X's IP address conflicts with another host on the network, the banner shown in Figure 46 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 46: IP Address Conflict

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

4.11.5 Option 6 – Enhanced Communications Test

This menu item allows testing the communication path between the CEA-852 device of the LINX-10X 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 47.

```
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 47: 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 LINX-10X. 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 5.

A warning “Incorrect NAT configuration detected!” is displayed if the enhanced communications test determines that the CEA-852 device of the LINX-10X 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 LINX-10X 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 5: Possible Communication Problems

4.12 Data Point Menu

The LINX-10X data point menu as shown in Figure 48 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 5.2.9).

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

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

[q]  Quit without saving

Please choose:
```

Figure 48: LINX-10X Data Point Menu.

4.12.1 Option 1 – List Data Points

Select this option to list all data points on the LINX-10X. The list is flat and displays the values and status of each data point. An example is shown in Figure 49.

```
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 49: Example data point listing.

4.12.2 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".

4.12.3 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 LINX-10X comes with a built-in Web server and a Web interface to configure the LINX-10X and extract statistics information. The Web interface allows configuring the IP settings, CEA-852 and CEA-709 settings. This interface is very simple to use and has an intuitive, self-explanatory user interface.

5.1 Device Information and Account Management

In a Web browser enter the default IP address 192.168.1.254 of the LINX-10X. 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 LINX-10X.

To Add a Route to the Device

1. Windows START → Run

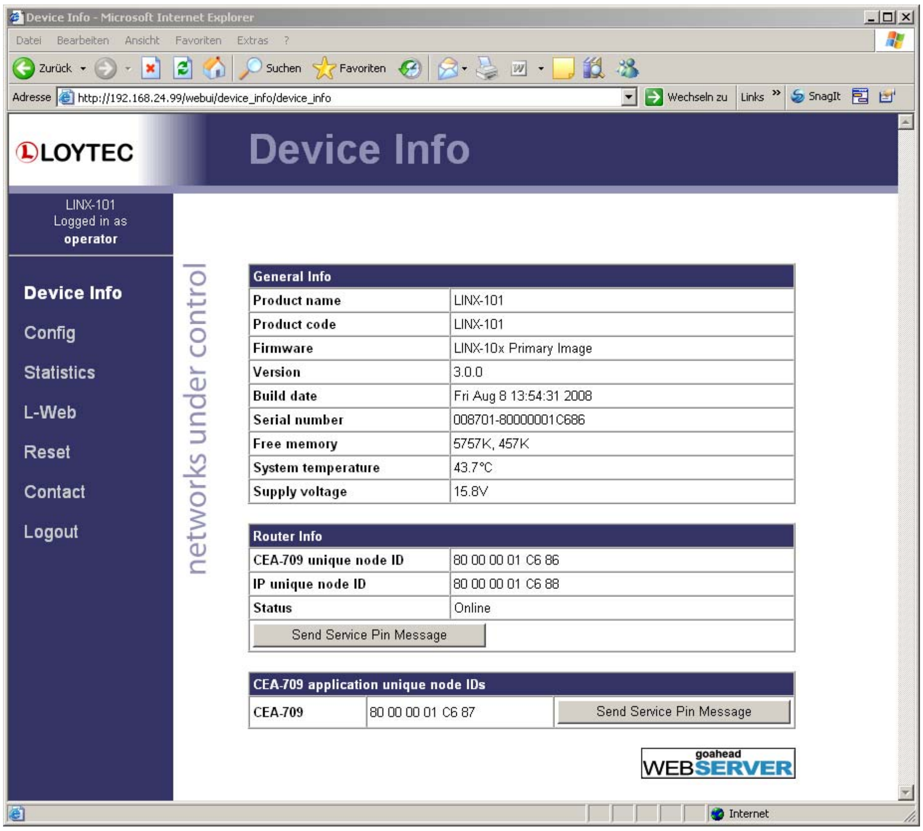
2. Enter ‘cmd’ an click **Ok**.

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 50.



General Info	
Product name	LINX-101
Product code	LINX-101
Firmware	LINX-10x Primary Image
Version	3.0.0
Build date	Fri Aug 8 13:54:31 2008
Serial number	008701-80000001C686
Free memory	5757K, 457K
System temperature	43.7°C
Supply voltage	15.8V

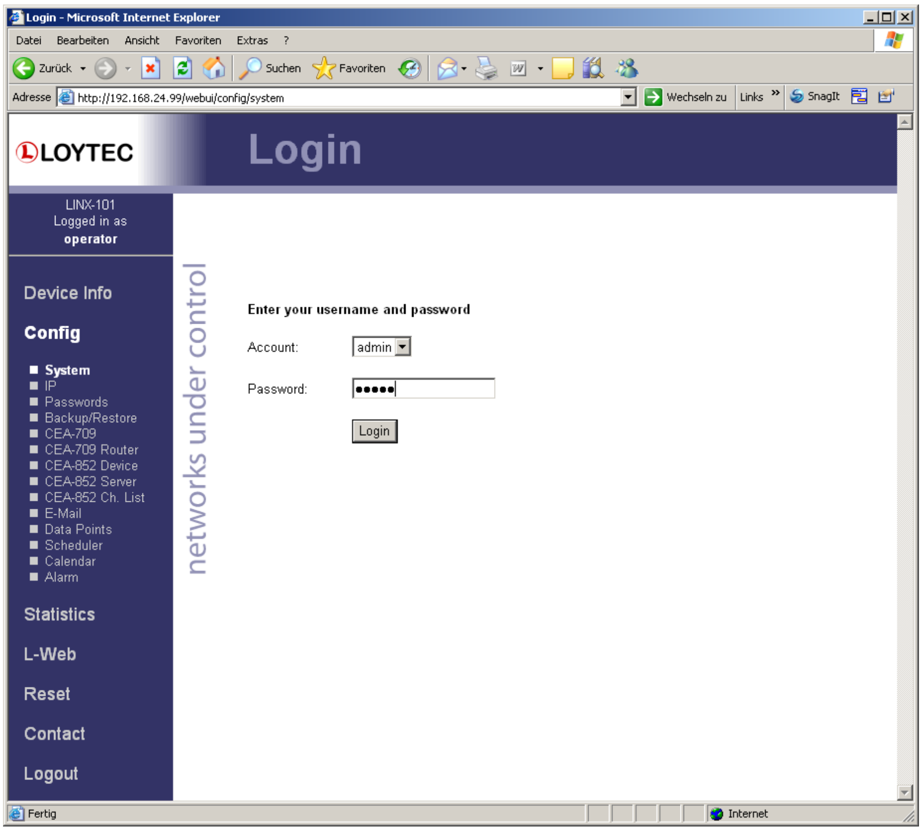
Router Info	
CEA-709 unique node ID	80 00 00 01 C6 86
IP unique node ID	80 00 00 01 C6 88
Status	Online
Send Service Pin Message	

CEA-709 application unique node IDs		
CEA-709	80 00 00 01 C6 87	Send Service Pin Message

Figure 50: Device Information Page

The device information page shows information about the LINX-10X 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 LINX-10X, 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 51. Enter the default administrator password “admin” and select “Login”.



http://192.168.24.99/webui/config/system

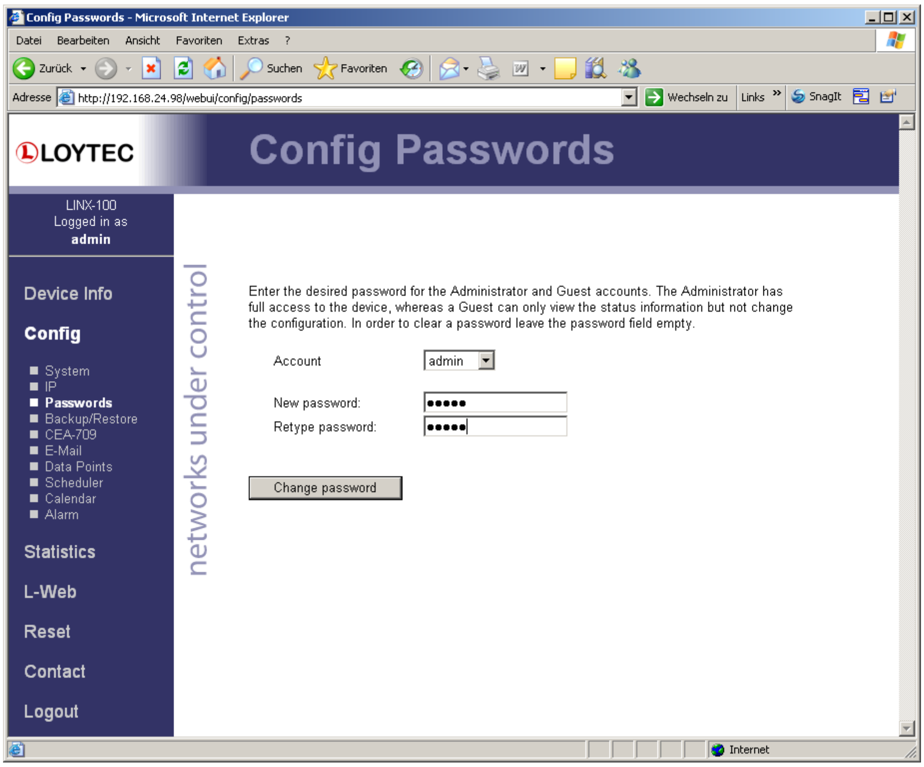
Enter your username and password

Account: admin

Password: ●●●●●

Figure 51: 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 52. The LINX-10X 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” in opposite to the guest the operator is able to read more sensible information such as calendar data. (3) “admin” has full access to the LINX-10X and can make changes to its configuration. Note that the user accounts are also used to log on to the FTP and Telnet server.



Enter the desired password for the Administrator and Guest accounts. The Administrator has full access to the device, whereas a Guest can only view the status information but not change the configuration. In order to clear a password leave the password field empty.

Account: admin

New password: •••••

Retype password: •••••

Figure 52: 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 LINX-10X without entering a password. Click on **Change password** to activate the change.

5.2 Device Configuration

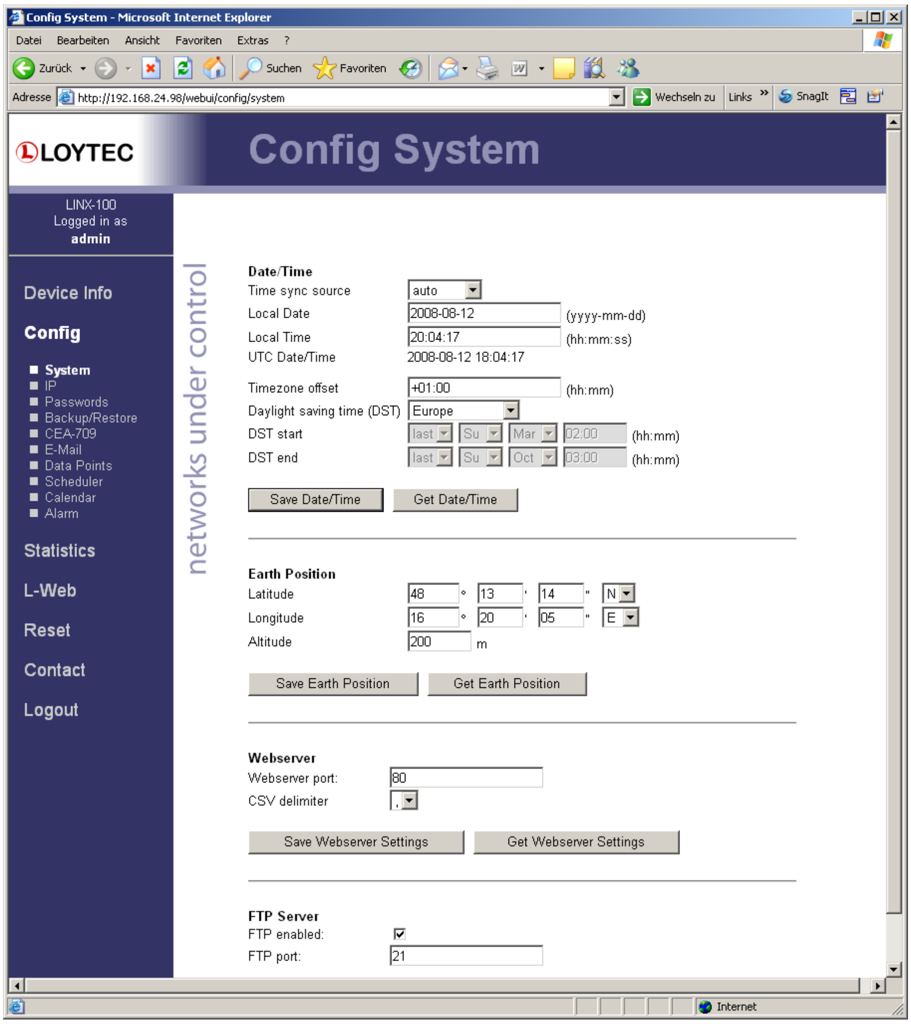
The device configuration pages allow viewing and changing the device settings of the LINX-10X. Here are some general rules for setting IP addresses, port numbers, and time values:

- 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 53. This page allows to configure the LINX-10X’s system time. The time sync source can be set to ‘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 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 timezone 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/U.S.A. is -06:00). For setting the daylight saving time (DST) pre-defined choices are offered for Europe and U.S.A./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.



Date/Time

Time sync source: auto

Local Date: 2008-08-12 (yyyy-mm-dd)

Local Time: 20:04:17 (hh:mm:ss)

UTC Date/Time: 2008-08-12 18:04:17

Timezone offset: +01:00 (hh:mm)

Daylight saving time (DST): Europe

DST start: last Su Mar 02:00 (hh:mm)

DST end: last Su Oct 03:00 (hh:mm)

Save Date/Time | Get Date/Time

Earth Position

Latitude: 48 ° 13 ' 14 " N

Longitude: 16 ° 20 ' 05 " E

Altitude: 200 m

Save Earth Position | Get Earth Position

Webserver

Webserver port: 80

CSV delimiter: ,

Save Webserver Settings | Get Webserver Settings

FTP Server

FTP enabled: ☑

FTP port: 21

Figure 53: System Configuration Page

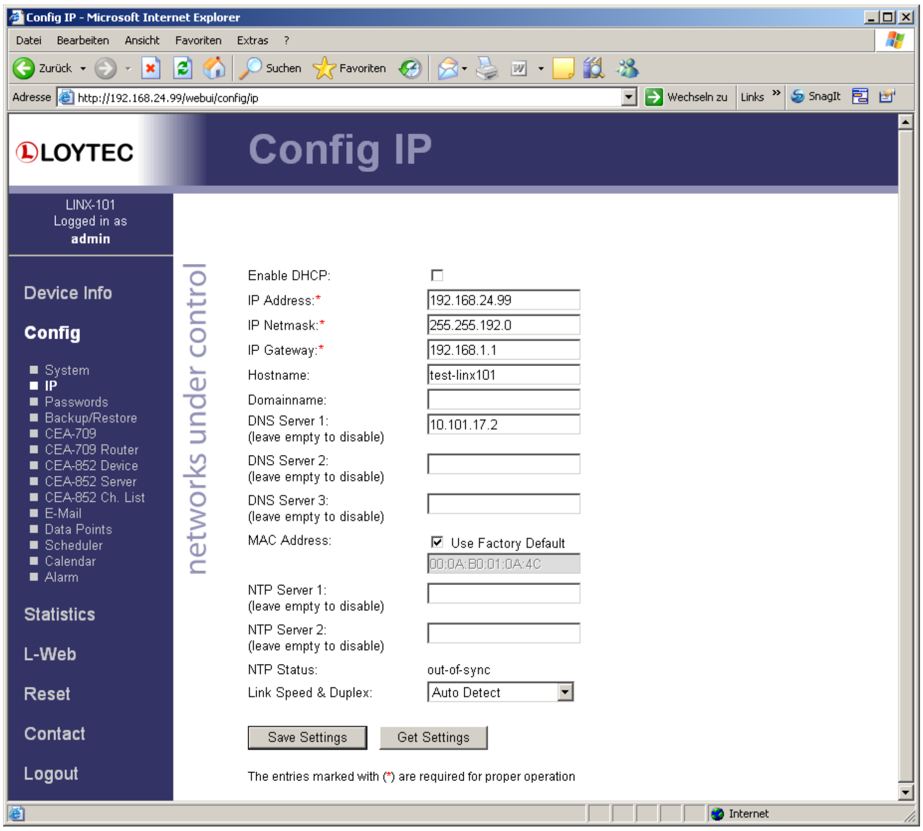
The next section on the page allows to configure the LINX-10X's earth position. This setting defines the longitude, latitude and elevation of the device on the planet. The latitude and longitude are entered as degrees, minutes, and seconds. The altitude (or elevation) is entered in meters from sea level. This setting is used for an astronomical clock. For fixed locations such as a building, the position can be entered on this page. For moving locations, this setting can be updated over the network using the network variable nciEarthPos (see Section 10.2.2).

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 12.1) or download 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 54 shows the IP configuration page with DHCP disabled, while Figure 55 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.

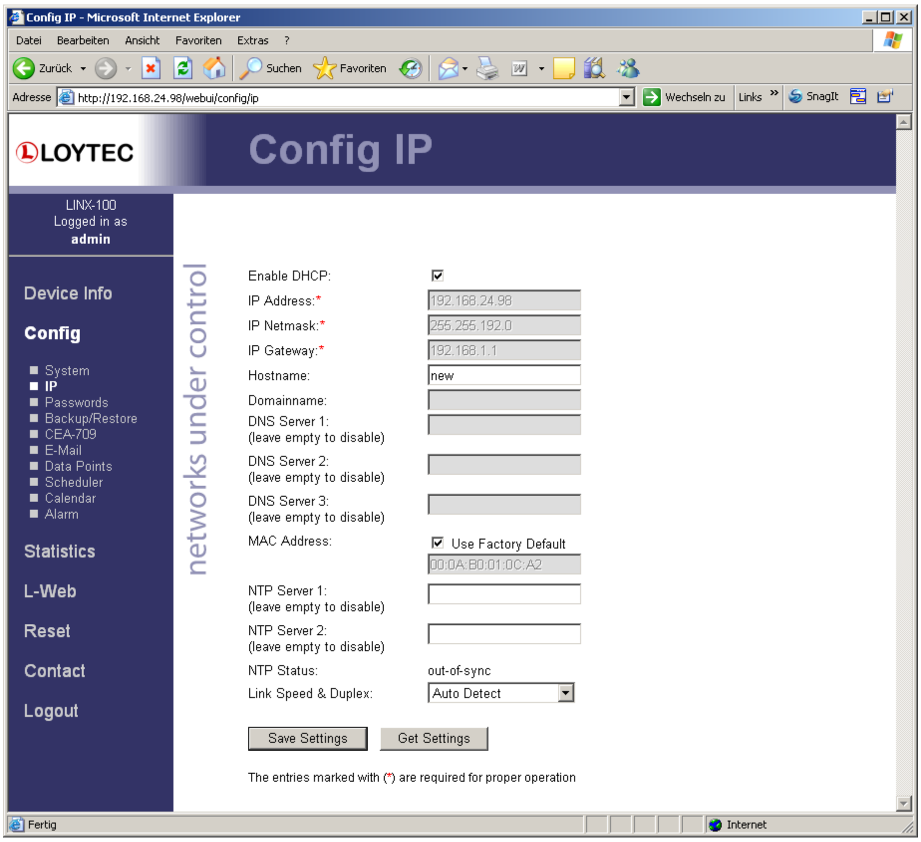


Enable DHCP: □
IP Address:* 192.168.24.99
IP Netmask:* 255.255.192.0
IP Gateway:* 192.168.1.1
Hostname: test-linx101
Domainname:
DNS Server 1: (leave empty to disable) 10.101.17.2
DNS Server 2: (leave empty to disable)
DNS Server 3: (leave empty to disable)
MAC Address: ☑ Use Factory Default 00:0A:B0:01:0A:4C
NTP Server 1: (leave empty to disable)
NTP Server 2: (leave empty to disable)
NTP Status: out-of-sync
Link Speed & Duplex: Auto Detect

Save Settings Get Settings

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

Figure 54: IP Configuration Page with DHCP disabled



Enable DHCP: ☑
IP Address:* 192.168.24.98
IP Netmask:* 255.255.192.0
IP Gateway:* 192.168.1.1
Hostname: new
Domainname:
DNS Server 1: (leave empty to disable)
DNS Server 2: (leave empty to disable)
DNS Server 3: (leave empty to disable)
MAC Address: ☑ Use Factory Default
00:0A:B0:01:0C:A2
NTP Server 1: (leave empty to disable)
NTP Server 2: (leave empty to disable)
NTP Status: out-of-sync
Link Speed & Duplex: Auto Detect

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

Figure 55: IP Configuration Page with DHCP enabled

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

5.2.3 Backup and Restore

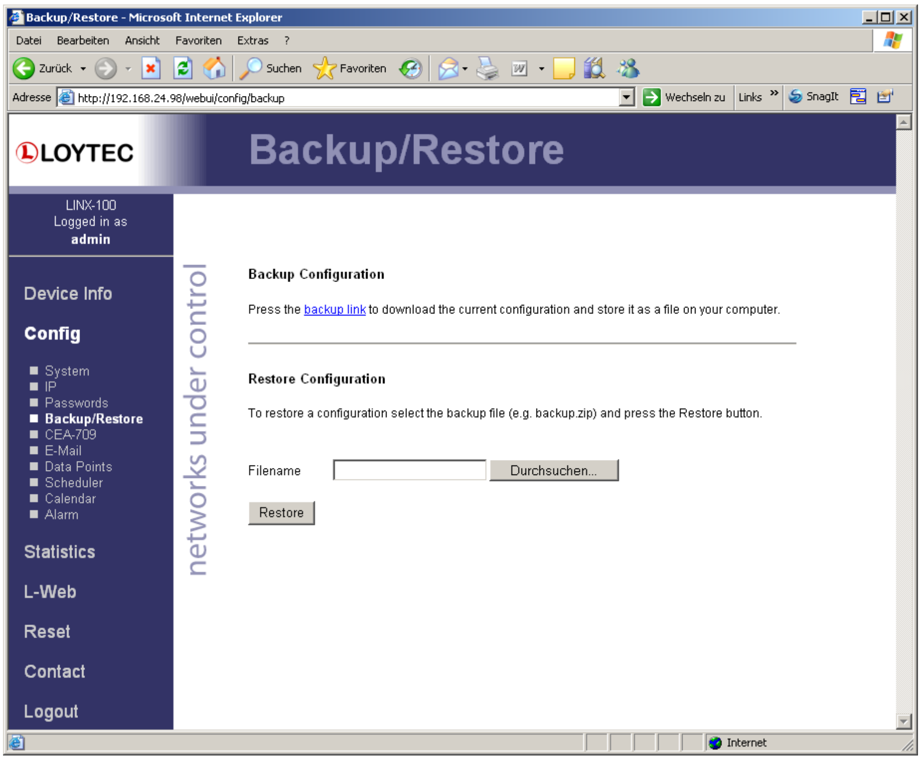
A configuration backup of the LINX-10X device can be downloaded via the Web interface. Press the backup link as shown in Figure 56 to start the download. Then the LINX-10X device assembles a single file including all required files. A file requestor dialog allows specifying the location where the backup 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
- AST settings
- L-Web configuration and custom Web pages



Backup Configuration

Press the backup link to download the current configuration and store it as a file on your computer.

Restore Configuration

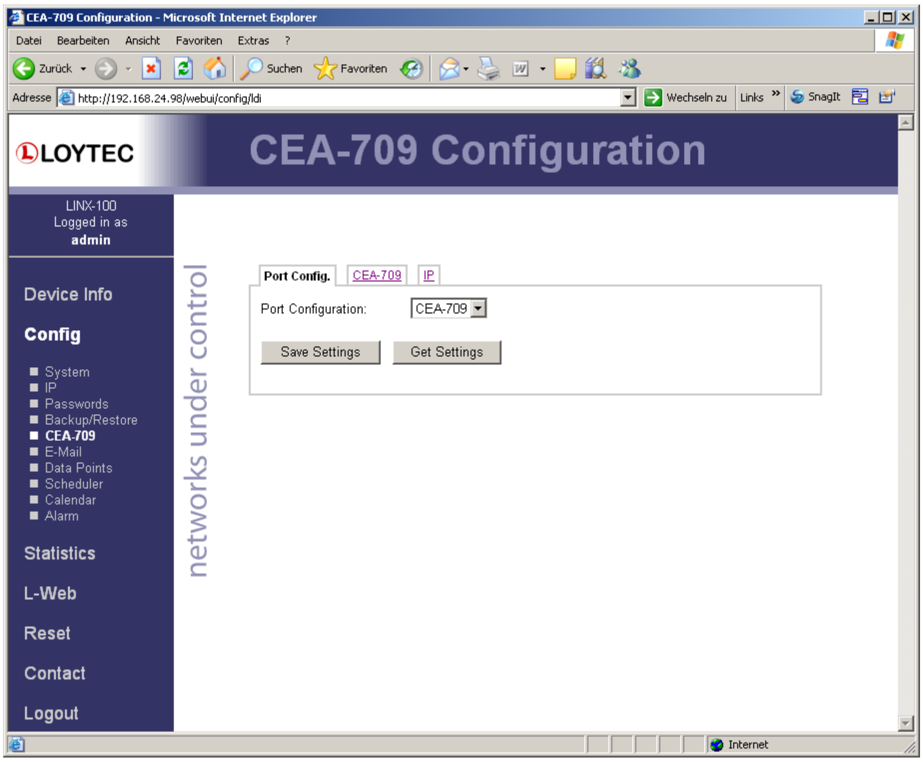
To restore a configuration select the backup file (e.g. backup.zip) and press the Restore button.

Filename

Figure 56: Backup/Restore page.

5.2.4 CEA-709 Configuration

On the CEA-709 configuration page (shown in Figure 57) the user can configure, which of the available CEA-709 ports of the LINX-10X shall be active. Select "CEA-709" from the drop-down box to use the LINX-10X on a FT-10 channel, or "CEA-852" to use the LINX-10X on an IP channel. Click on the tables "CEA-709" and "IP" to learn more about the current transceiver settings.



Port Configuration: CEA-709

Figure 57: CEA-709 Configuration Page.

5.2.5 CEA-709 Router Configuration

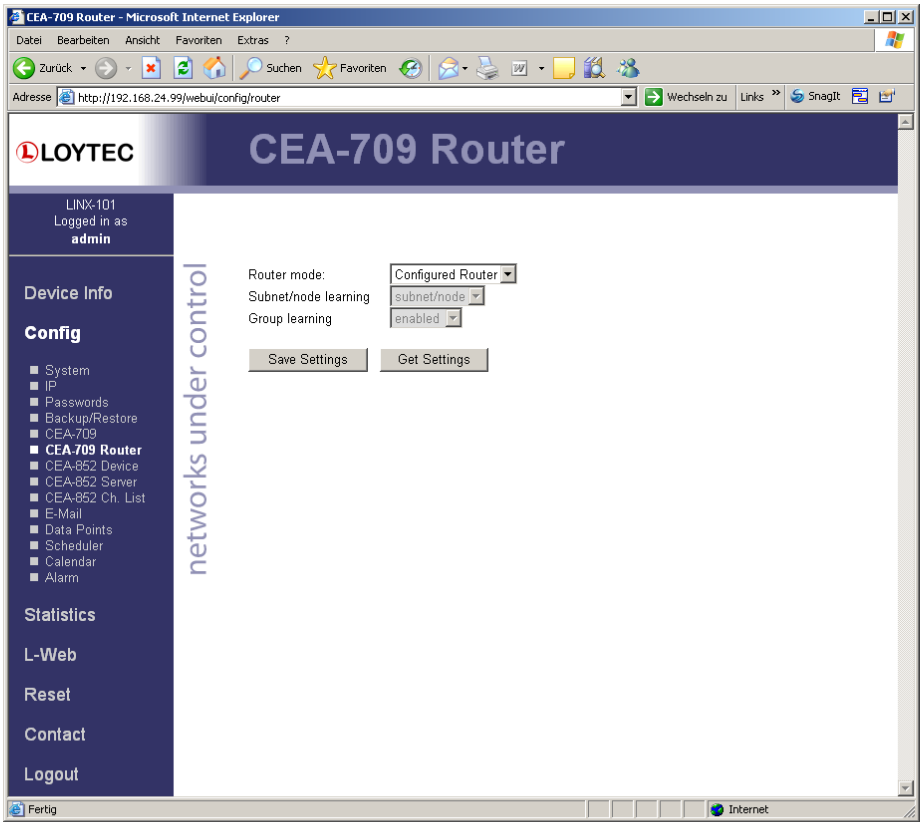
This page is only available on the LINX-101. The CEA-709 router configuration page allows configuring the built-in router mode. Available modes are "Configured Router" and "Smart Switch". The LINX-101 must be rebooted to let the changes on this page take effect.

The configured router mode is the default setting. Choose this setting if you want to use the LINX-101 as a standard configured CEA-709 router that can be configured in a network management tool such as NL-200 or LonMaker.

The Smart Switch mode lets the device act as a self-learning router like the L-Switch. In this configuration the LINX-101's router doesn't need to be configured with a network management tool but is completely transparent in the network. Use this operating mode in a plug&play networking environment. The switch mode should only be used in LAN networks. In Smart Switch mode, this page has two more configuration fields: Subnet/node learning and Group learning.

The field "Subnet/node learning" allows setting the mode for learning of subnet/node addresses. The selection can be "subnet/node", "subnet", or "disabled". If subnet/node learning is selected, the LINX-10X's router will learn based on subnet/node addresses (see Section 8.1.2). Subnet broadcasts are flooded. This mode is plug&play.

If subnet learning is disabled, all subnet-wide broadcasts are forwarded by the LINX-10X's router from one side to the other side. If subnet learning is enabled the LINX-10X's router will learn the subnet addresses on both network ports and will only flood subnet broadcasts if the destination subnet address doesn't exist on the local channel. Subnet learning should be enabled, if group overloading is used in the case that more than 256 group addresses are needed. Subnet learning is not plug&play. Please use NL-200, LonMaker, or other network management tools to ensure that one subnet address is only used behind one LINX-10X device. This can be achieved by using our LINX-10X LonMaker shapes or by placing phantom routers in e.g. NL-220. Please contact LOYTEC support if you think you need this feature!



Router mode: Configured Router

Subnet/node learning: subnet/node

Group learning: enabled

Figure 58: CEA-709 Router Configuration Page.

5.2.6 CEA-852 Device Configuration

The CEA-852 device of the LINX-10X can be configured in the CEA-852 device configuration page, which is depicted in Figure 59. Typically, the LINX-10X 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 LINX-10X 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 LINX-10X and the IP channel. The field "Config client port" represents the IP port of the LINX-10X's CEA-852 device. This setting should be left at its default (1628) unless there are more than one CEA-852 device operated behind a single NAT router. Please refer to the L-IP User's Manual to learn more about NAT configuration.

In the field "Device name" the user can enter a descriptive name for the LINX-10X, 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 LINX-10X behind one NAT router) the channel switches to "Extended NAT mode". Please refer to the L-IP User's Manual 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 LINX-10X waits for out-of-sequence CEA-852 data packets before they are discarded. Please enter the time in ms or 0 to disable escrowing. The maximum time is 255 ms.

The field “Aggregation timeout” defines the time interval in which multiple CEA-709 packets are combined into a single CEA-852 data packet. Please enter the time in ms or 0 to disable aggregation. The maximum time is 255 ms. Note that disabling aggregation will negatively affect the performance of the CEA-852 device of the LINX-10X.

The field “MD5 authentication” enables or disables MD5 authentication. Note that MD5 authentication cannot be used together with the *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.

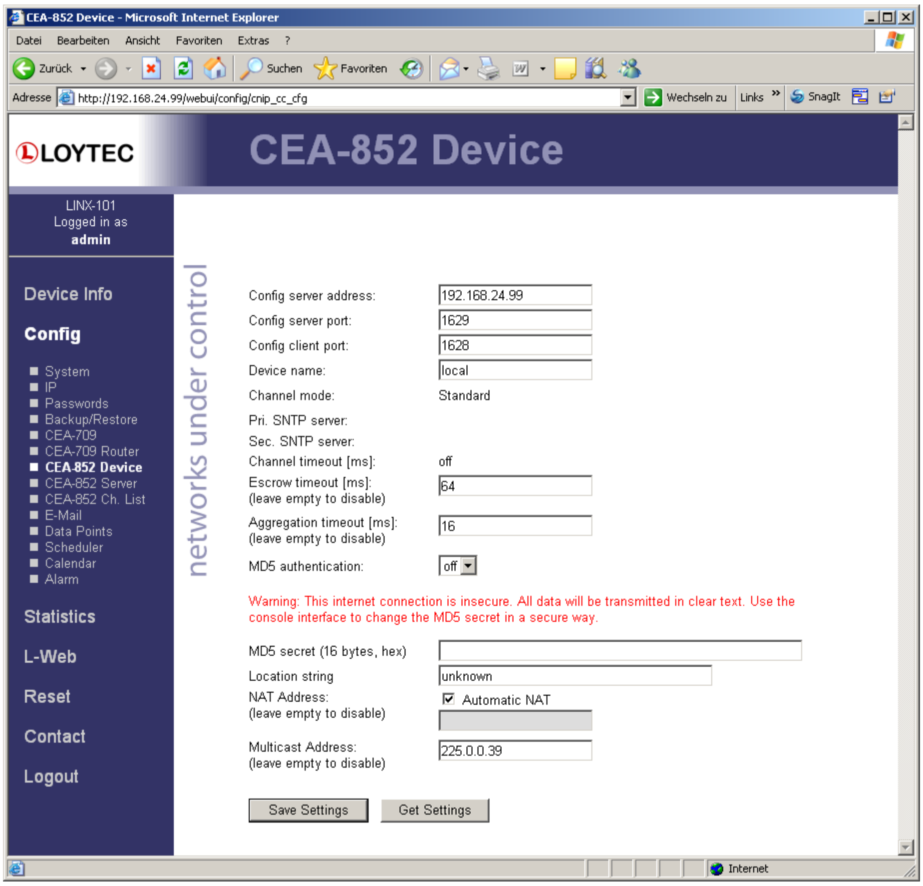
Also note that entering the MD5 secret on the Web interface may pose a security risk. Since the information is transmitted over the network it can be subject for eavesdroppers on the line. It is recommended to either use a cross-over cable or enter the secret on the console UI (see Section 4.7).

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

In the field “Location string” the user can enter a descriptive test which identifies the physical location of the LINX-10X. 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 LINX-10X 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 LINX-10X into a multi-cast group for the CEA-852 IP channel. Enter the channel’s IP multi-cast address here. On how to obtain a valid multi-cast address please contact your system administrator. To learn when it is beneficial to use multi-cast addresses in your channel please refer to the L-IP User’s Manual.



Config server address: 192.168.24.99
Config server port: 1629
Config client port: 1628
Device name: local
Channel mode: Standard
Pri. SNTP server:
Sec. SNTP server:
Channel timeout [ms]: off
Escrow timeout [ms]: (leave empty to disable) 64
Aggregation timeout [ms]: (leave empty to disable) 16
MD5 authentication: off

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

MD5 secret (16 bytes, hex)
Location string unknown
NAT Address: (leave empty to disable) ☑ Automatic NAT
Multicast Address: (leave empty to disable) 225.0.0.39

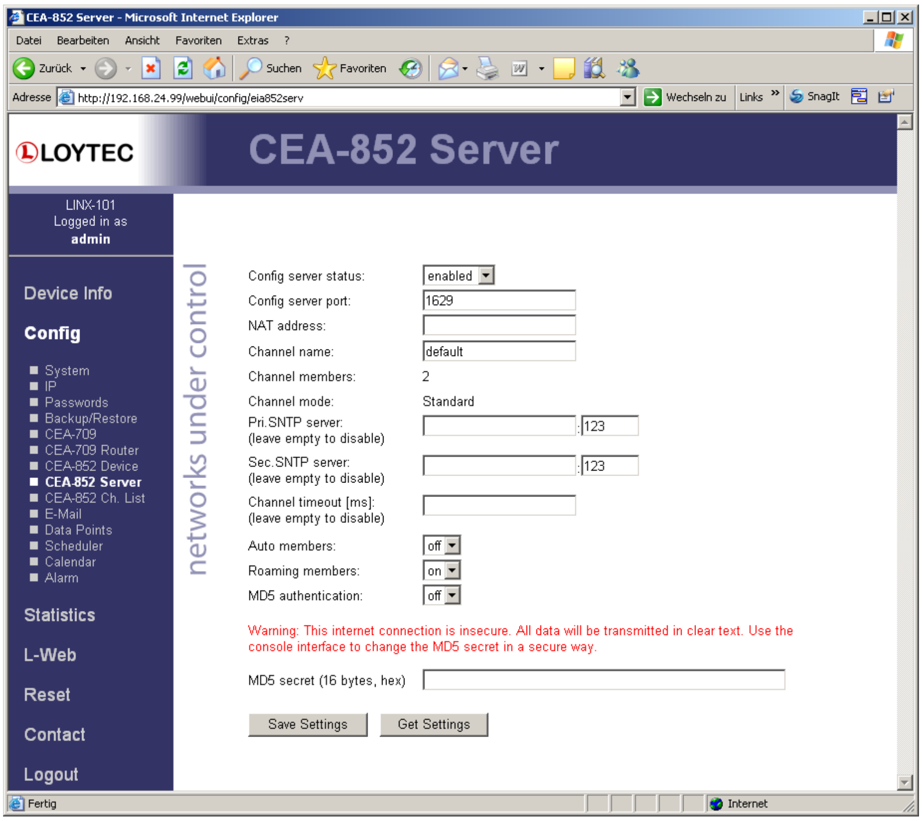
Figure 59: CEA-852 Device Configuration Page.

5.2.7 CEA-852 Server Configuration

This page is only available on the LINX-101. On this configuration page the configuration server on the LINX-101 can be enabled or disabled. In the drop-down box "Config server status" select "enabled" and click on "Save Settings" to activate the configuration server. Then the configuration server settings page appears as shown in Figure 60. If the configuration server is enabled the green configuration server LED labeled "server" will be on, otherwise it will be off.

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

The field "Channel members" displays the current number of members on the IP-852 channel. The field "Channel mode" reflects the current channel mode. The LINX-101 configuration server automatically determines this mode depending if there are any two devices in the channel which use the same IP address but different ports (e.g., multiple L-IPs behind one NAT router). If all IP addresses are unique the mode is "Standard", if some are not unique the mode is "Extended NAT mode". Please refer to Section 8.4.2 to learn more about the implications of this mode.



Config server status: enabled

Config server port: 1629

NAT address:

Channel name: default

Channel members: 2

Channel mode: Standard

Pri.SNTP server: (leave empty to disable) 123

Sec.SNTP server: (leave empty to disable) 123

Channel timeout [ms]: (leave empty to disable)

Auto members: off

Roaming members: on

MD5 authentication: off

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

MD5 secret (16 bytes, hex)

Figure 60: Configuration server settings.

Enter NTP timer server address and ports in the fields “Primary SNTP” and “Secondary SNTP”. The LINX-101 will synchronize to NTP time if primary or primary and secondary NTP servers are specified. For possible NTP servers please refer to Table 6. More SNTP servers can be found at http://www.eecis.udel.edu/~mills/ntp/clock1.html.

Country	Service Area	Hostname	IP Address
AT	Austria/Europe		130.149.17.21
CH	Swiss/Europe	swisstime.ethz.ch	129.132.2.21
DE	Germany/Europe	ntp0.fau.de	131.188.3.220
DK	Denmark	GPS.dix.dk	192.38.7.240
FR	France	canon.inria.fr	192.93.2.20
IT	Italy/Europe	ntp1.ien.it	193.204.114.232
JP	Japan/Pacific Area	clock.nc.fukuoka-u.ac.jp	133.100.9.2
NL	Netherlands/Europe	ntp0.nl.net	193.67.79.202
NO	NordUnet	time.service.uit.no	
SE	Sweden	ntp1.gbg.netnod.se	192.36.133.130
SG	Singapore/Asia	jamtepat.singnet.com.sg	165.21.110.7
UK	United Kingdom, Western Europe	chronos.csr.net	194.35.252.7
US	BARRnet, Alternet-west, CIX-west	clock.isc.org	192.5.5.250

Table 6: NTP timer server locations.

The channel timeout is an IP-852 channel property and indicates how old a packet can be before it is discarded. The channel timeout is set in ms. To disable the channel timeout enter a value of 0. To select the proper value please consult Section 8.7.1. Setting a channel timeout other than 0 requires a valid SNTP server entry on the configuration server.

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

The "Roaming members" option allows tracking CEA-852 devices when their IP address changes. This feature must be turned on if DHCP is used and the DHCP server can assign different IP addresses to the same device (same Neuron-ID). In combination with Auto-NAT the LINX-101's router can also be operated behind NAT routers, which change their IP address between connection setups. For more information on this topic refer to Section 8.4.1. The roaming member feature is turned on by default. It is recommended to turn off this feature if DHCP is not used or if the DHCP server always assigns the same IP address to a given MAC address.

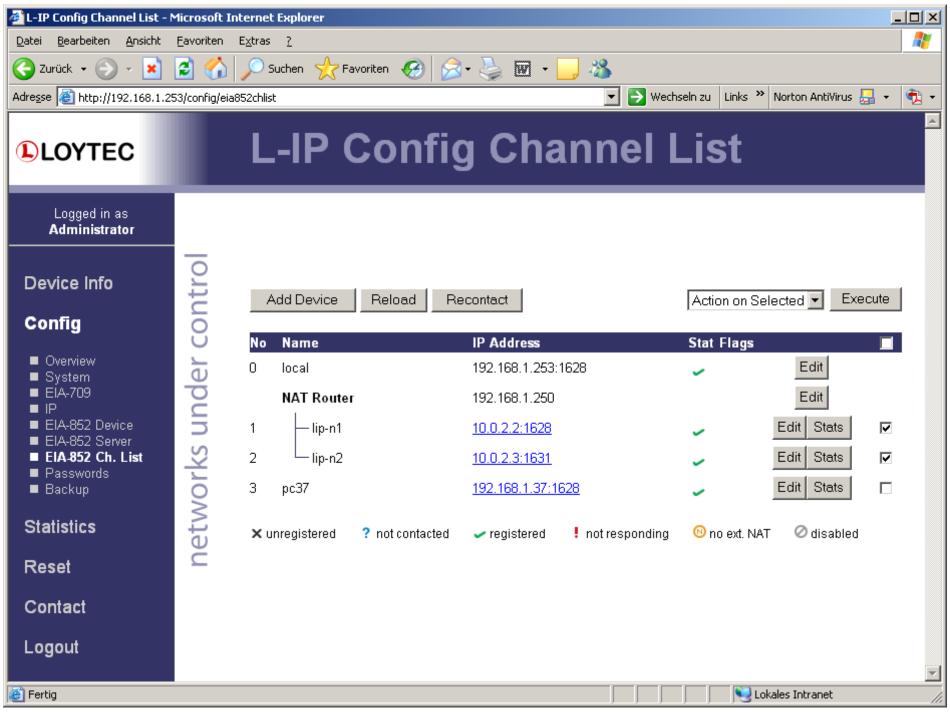
Use the drop-down box "MD5 authentication" to enable and disabe MD5 authentication. If MD5 authentication is enabled, all devices on the IP-852 channel must have MD5 enabled and must use the same MD5 secret. Note, that MD5 authentication cannot be used together with the *i*.LON 1000 since the *i*.LON 1000 is not fully compliant with the CEA-852 authentication method. MD5 can be used with the *i*.LON 600. The MD5 secret can be entered over the Web interface. You may enter the 16 bytes as one string or with spaces between each byte. E.g., 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.

It is recommended, however, to enter the secret on the console UI as the Web connection is not secure. See Section 4.9.10 for entering the MD5 secret on the console UI.

5.2.8 CEA-852 Channel List

This page is only available on the LINX-101. If the configuration server is enabled on the LINX-101, the CEA-852 device list can be seen in the CEA-852 channel list menu. An example is given in Figure 57.

The **Add Device** button is used to add another CEA-852 device to the IP-852 channel. The **Reload** button updates the Web page and the **Recontact** button contacts all devices to update their status. The Execute button executes the option selected in the adjacent drop-down box on the checked members. Each member can be checked for that action in an individual check-box in the **Sel** column. Actions available are: disable, enable, delete, assign to NAT and remove from NAT. For more information on the actions on NAT routers refer to Section 8.4.2.



L-IP Config Channel List - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten
Adresse http://192.168.1.253/config/eia852chlist
Wechseln zu Links Norton AntiVirus
LOYTEC
networks under control
Logged in as Administrator
Device Info
Config
Overview
System
EIA-709
IP
EIA-852 Device
EIA-852 Server
EIA-852 Ch. List
Passwords
Backup
Statistics
Reset
Contact
Logout
Fertig
Lokales Intranet

L-IP Config Channel List

Add Device | Reload | Recontact | Action on Selected | Execute

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

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

Figure 61: CEA-852 channel membership list.

The device status information is indicated with descriptive icons of different colors. The description for the different status indicators is shown in Table 7. The Flags column indicates with an **A** that the device is an auto member.

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

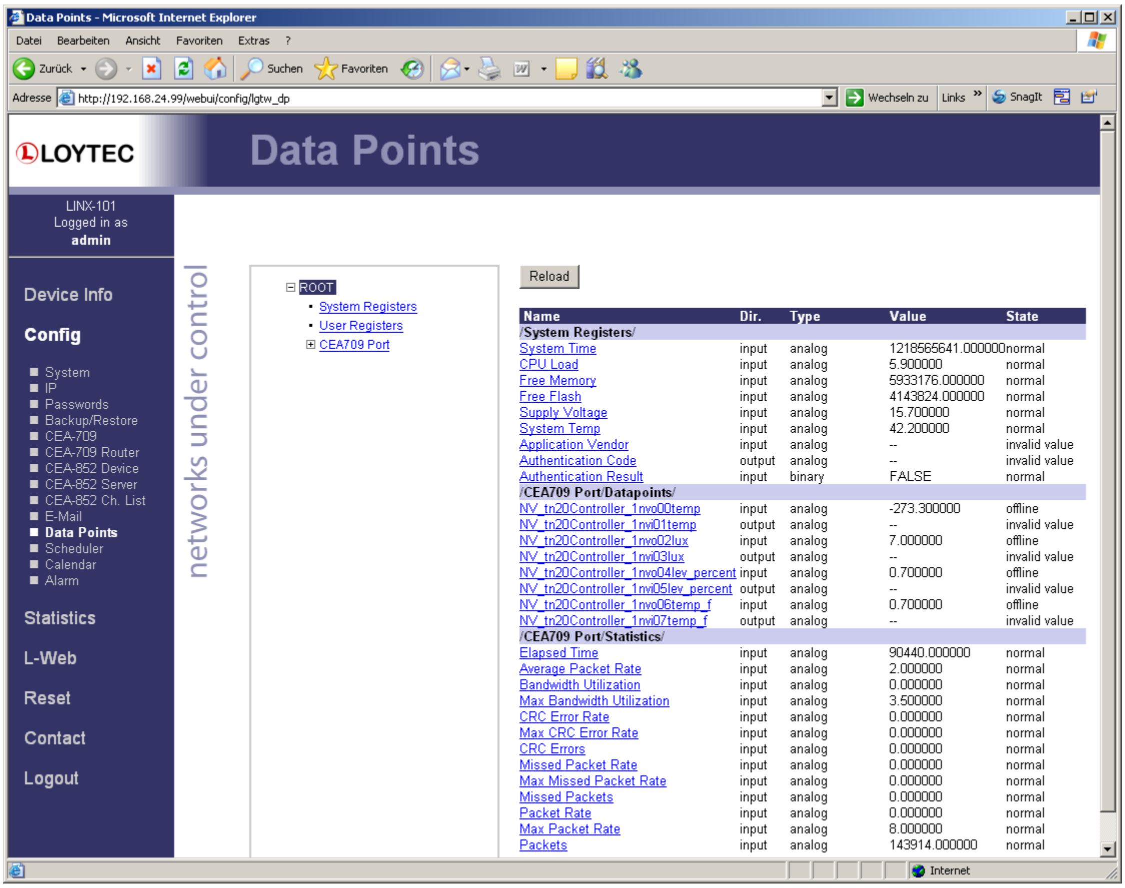
Icon	Status	Description
✓	registered	The CEA-852 device has been successfully registered with the IP-852 channel and is fully functional.
✗	unregistered	The CEA-852 device has never been registered with the IP-852 channel.
?	not contacted	The CEA-852 device has not been contacted since the configuration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

Table 7: Possible Communication Problems in the Configuration Server.

5.2.9 Data Points

The LINX-10X’s Web interface provides a data point page, which lists all configured data points on the LINX-10X. An example is shown in Figure 62. 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.

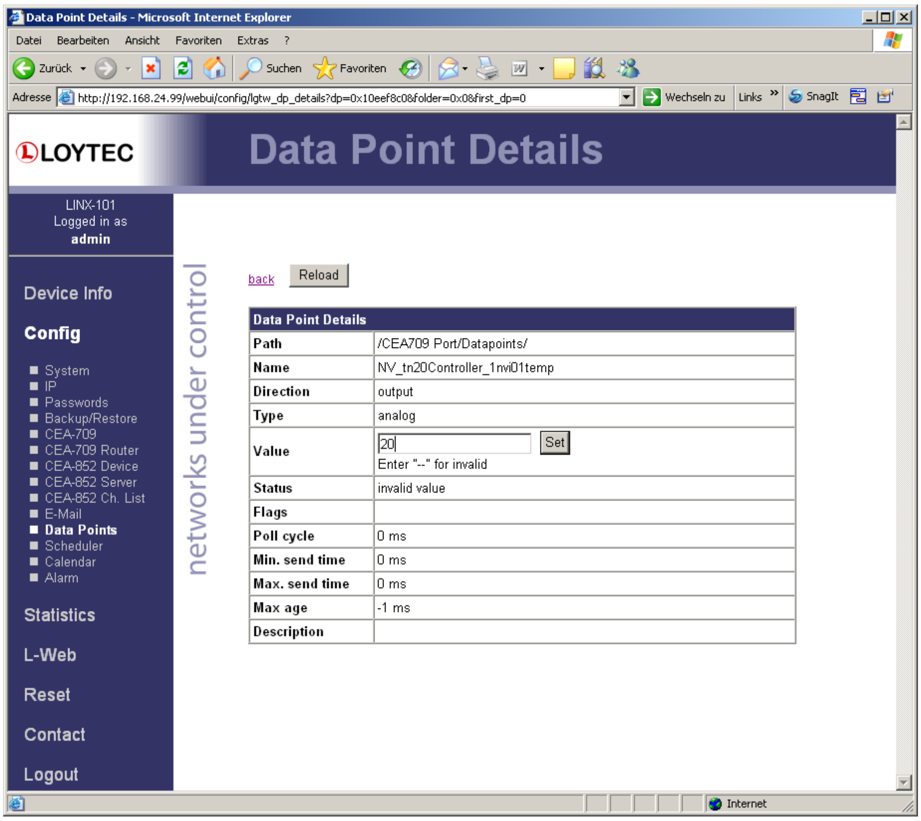
The data point list displays the data point name, direction, type, current value and data point state. Inactive points are displayed in gray. If the data point list does not fit on one page, there are page enumerator links at the bottom.



Name	Dir.	Type	Value	State
/System Registers/				
System Time	input	analog	1218565641.000000	normal
CPU Load	input	analog	5.900000	normal
Free Memory	input	analog	5933176.000000	normal
Free Flash	input	analog	4143824.000000	normal
Supply Voltage	input	analog	15.700000	normal
System Temp	input	analog	42.200000	normal
Application Vendor	input	analog	--	invalid value
Authentication Code	output	analog	--	invalid value
Authentication Result	input	binary	FALSE	normal
/CEA709 Port/Datapoints/				
NV_tn20Controller_1nvo00temp	input	analog	-273.300000	offline
NV_tn20Controller_1nvi01temp	output	analog	--	invalid value
NV_tn20Controller_1nvo02lux	input	analog	7.000000	offline
NV_tn20Controller_1nvi03lux	output	analog	--	invalid value
NV_tn20Controller_1nvo04lev_percent	input	analog	0.700000	offline
NV_tn20Controller_1nvi05lev_percent	output	analog	--	invalid value
NV_tn20Controller_1nvo06temp_f	input	analog	0.700000	offline
NV_tn20Controller_1nvi07temp_f	output	analog	--	invalid value
/CEA709 Port/Statistics/				
Elapsed Time	input	analog	90440.000000	normal
Average Packet Rate	input	analog	2.000000	normal
Bandwidth Utilization	input	analog	0.000000	normal
Max Bandwidth Utilization	input	analog	3.500000	normal
CRC Error Rate	input	analog	0.000000	normal
Max CRC Error Rate	input	analog	0.000000	normal
CRC Errors	input	analog	0.000000	normal
Missed Packet Rate	input	analog	0.000000	normal
Max Missed Packet Rate	input	analog	0.000000	normal
Missed Packets	input	analog	0.000000	normal
Packet Rate	input	analog	0.000000	normal
Max Packet Rate	input	analog	8.000000	normal
Packets	input	analog	143914.000000	normal

Figure 62: Data point page

The data point names are links. Clicking on such a link opens a details page on that data point. For output data points, the user can also enter a new data point value as depicted in Figure 63. Clicking on the “Set” button writes the new value to the LINX-10X’s data server.



Data Point Details	
Path	/CEA709 Port/Datapoints/
Name	NV_tn20Controller_1nvi01temp
Direction	output
Type	analog
Value	20 Enter "--" for invalid
Status	invalid value
Flags	
Poll cycle	0 ms
Min. send time	0 ms
Max. send time	0 ms
Max age	-1 ms
Description	

Figure 63: Data point details page.

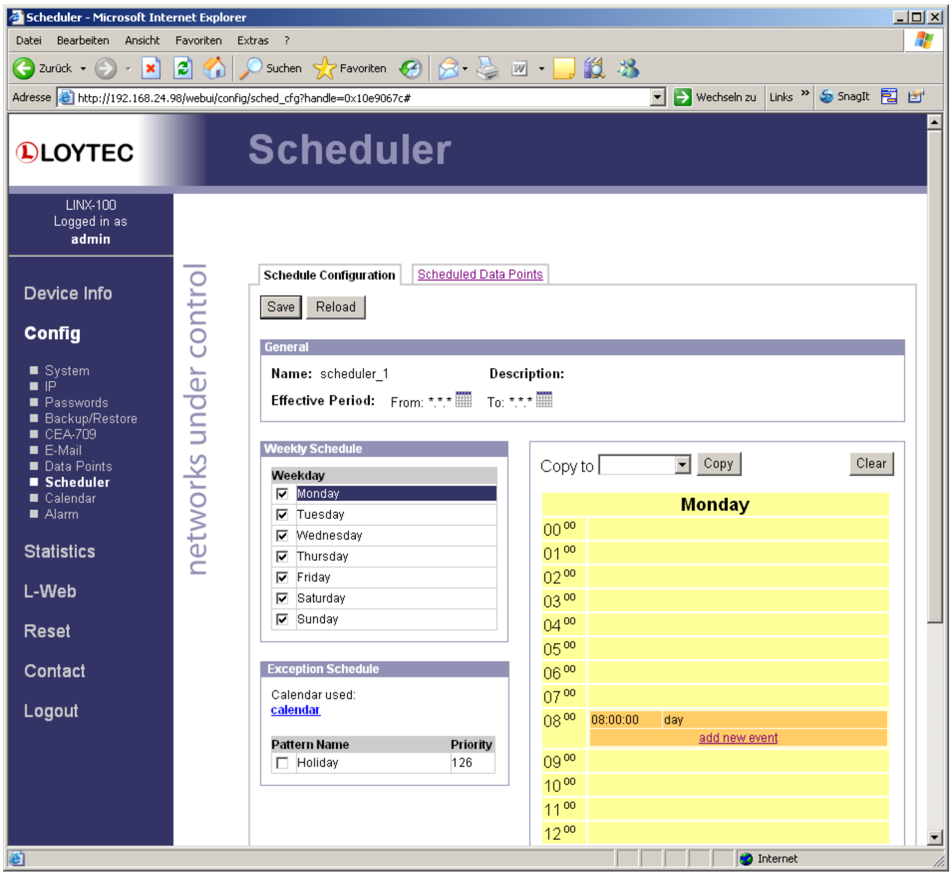
5.2.10 Scheduler

The Web interface provides the scheduler page to edit its schedules at run-time, i.e., change the times and values that shall be scheduled. Allocating new schedules and attaching data points to those schedules can only be done in the configuration software (see Section 7.9). The scheduler main page displays all available schedules. Click on the schedule to be edited. This opens the scheduler page. An example is shown in Figure 64.

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

Schedules are defined per day. On the left-hand side, the weekdays Monday through Sunday can be selected, or exception days from the calendar, e.g. Holidays. Once a day is selected, the times and values can be defined in the daily planner on the right-hand side. In the example shown in Figure 64, on Monday the value “day” is scheduled at 8:00am. The same principle applies to exception days. Exception days override the settings of the normal weekday. Put a check mark on those exception days from the calendar, which shall be used in the schedule. For more information on how to set up schedules and calendars refer to Section 7.9.

To define actual values for the names such as “day” click on the tab “Scheduled Data Points” as shown in Figure 65. Which data points are scheduled is determined by the configuration software. On this page, only the actual values can be changed. To define a new value, click on the button “Add Preset”. This adds a new column. Enter a new preset name (e.g., “day”). Then enter values for the data points in the preset column. The data point name column displays the short-hand name defined in the configuration software.



Schedule Configuration | Scheduled Data Points

Save | Reload

General

Name: scheduler_1 Description:

Effective Period: From: *.*.* To: *.*.*

Weekly Schedule

Weekday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Copy to Copy Clear

Monday

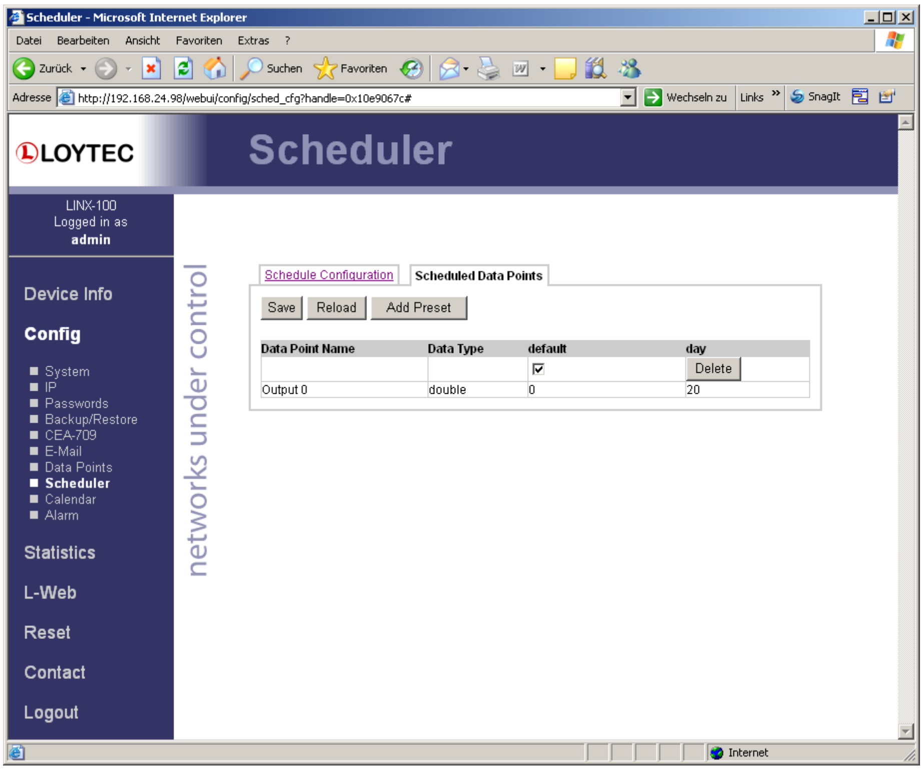
00^{00}
01^{00}
02^{00}
03^{00}
04^{00}
05^{00}
06^{00}
07^{00}
08^{00} 08:00:00 day
add new event
09^{00}
10^{00}
11^{00}
12^{00}

Exception Schedule

Calendar used:
calendar

Pattern Name	Priority
□ Holiday	126

Figure 64: Schedule Configuration Page



Schedule Configuration | Scheduled Data Points

Save | Reload | Add Preset

Data Point Name	Data Type	default	day
		☑	Delete
Output 0	double	0	20

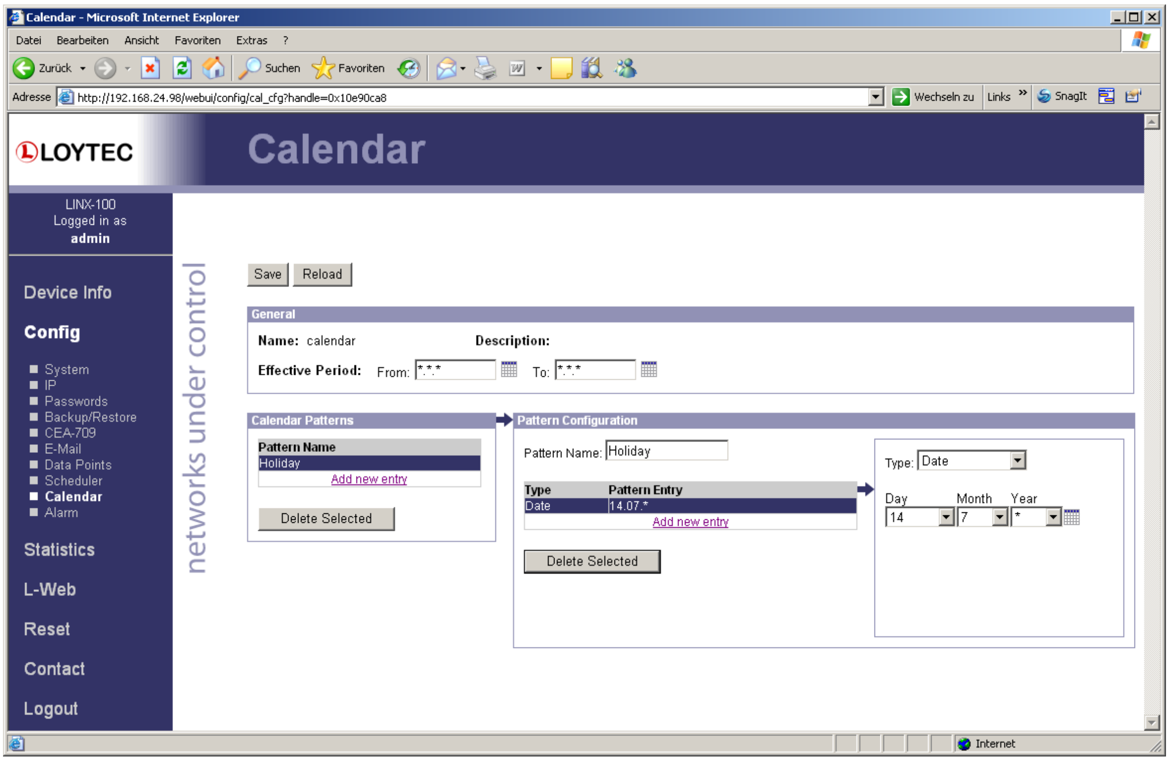
Figure 65: Scheduled Data Point Value Configuration Page

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

5.2.11 Calendar

The Web interface provides the calendar page to edit its calendars at run-time, i.e., change the exception days. The calendar main page displays all available calendars. Click on the calendar to be edited. This opens the calendar configuration page. An example is shown in Figure 66.

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



Name: calendar
Description:
Effective Period: From: *.*.* To: *.*.*

Pattern Name
Holiday

Pattern Name: Holiday

Type	Pattern Entry
Date	14.07.*

Type: Date

Day	Month	Year
14	7	*

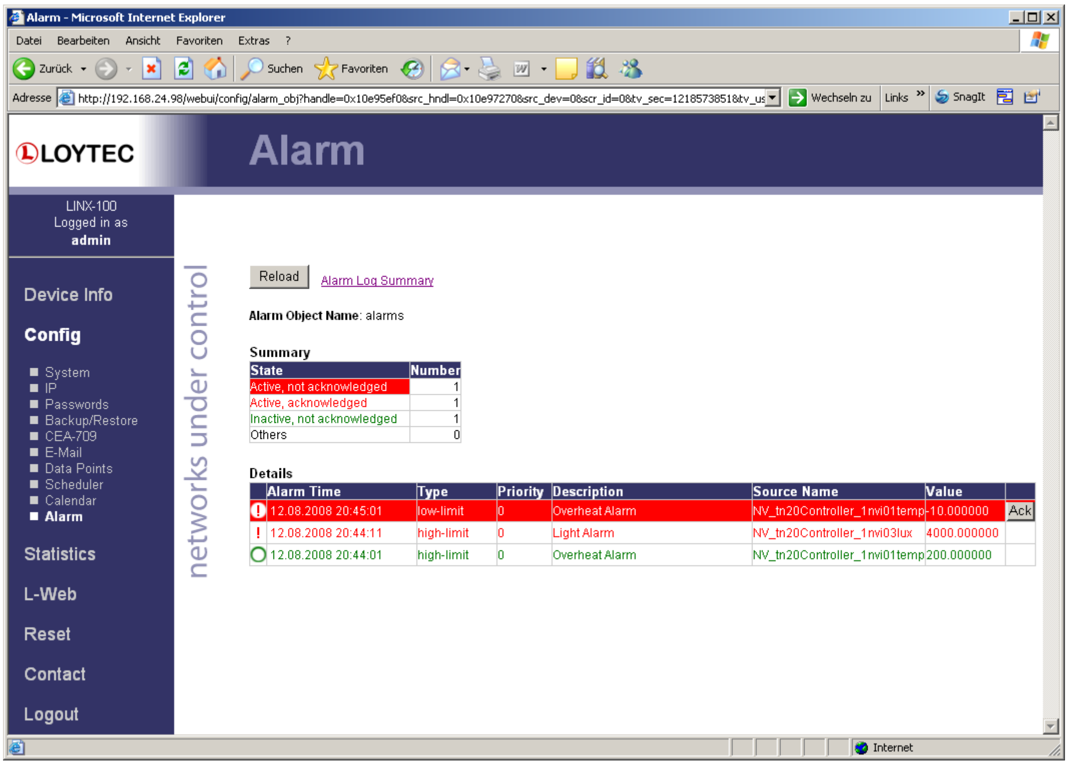
Figure 66: Calendar Configuration Page

On the remainder of this page work from left to right. Click on a calendar pattern or create a new calendar pattern by clicking “Add new entry”. A calendar pattern defines a set of pattern entries, which defines the actual dates or date ranges. In the example in Figure 66 the calendar pattern “Holidays” is selected.

In the “Pattern Configuration” box, the calendar pattern’s name can be edited. It also lists the entries. New entries can be added by clicking “Add new entry”. Existing entries can be selected and edited in the box on the right-hand side. In the example in Figure 66 the date “14.7.*” is selected, which means “The 14.7. of every year”. Other entry types such as “Date Range” and “Week-and-Day” can be selected. See Section 6.3.3 for more information about defining exception dates.

5.2.12 Alarm

The Web interface provides the alarm page to view the currently pending alarms of its alarm data points. The alarm main page displays all available alarm data points. Alarm objects, which have active alarms are displayed in red. Click on the alarm object to be viewed. This opens the alarm summary page. An example is shown in Figure 66.



Alarm Object Name: alarms

Summary

State	Number
Active, not acknowledged	1
Active, acknowledged	1
Inactive, not acknowledged	1
Others	0

Details

	Alarm Time	Type	Priority	Description	Source Name	Value	
!	12.08.2008 20:45:01	low-limit	0	Overheat Alarm	NV_tn20Controller_1nvi01temp	-10.000000	Ack
!	12.08.2008 20:44:11	high-limit	0	Light Alarm	NV_tn20Controller_1nvi03lux	4000.000000	
○	12.08.2008 20:44:01	high-limit	0	Overheat Alarm	NV_tn20Controller_1nvi01temp	200.000000	

Figure 67: Alarm Summary Page

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

Inactive alarms that have been acknowledged disappear from the list. To record historical information about those alarms, the alarm log must be used. See Section 5.3.7 for the alarm log Web interface.

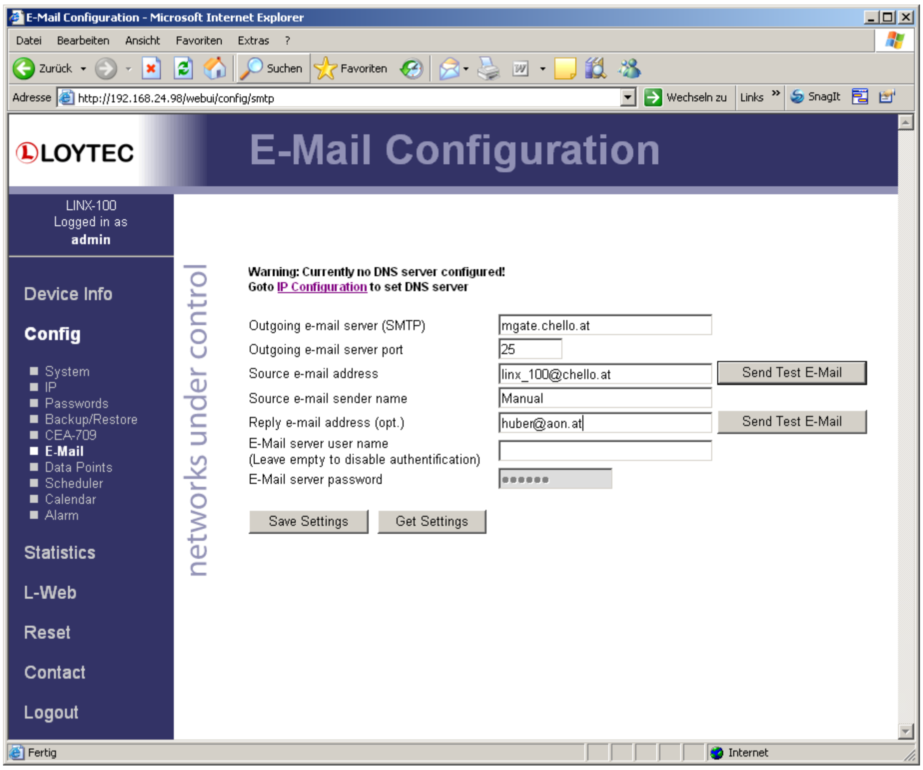
5.2.13 E-Mail Configuration

The Web interface provides the E-Mail configuration page to set up an E-Mail account, which is used to send E-Mails. The content and time when E-Mails are sent is configured elsewhere. The E-Mail configuration page is shown in Figure 68.

In the field for the outgoing e-mail server enter the SMTP server of your Internet provider. Typically, the SMTP server port can be left at 25. In the field "Source E-Mail Address", enter the E-Mail address of the LINX-10X's E-Mail account. In the field "Source E-Mail Sender Name" enter a name that the E-Mail will display as the source name. Note, that only ASCII characters are allowed in the name. If replies shall be sent to another E-Mail address, specify this in the "Reply E-Mail Address".

If the provider's SMTP server requires authentication, enter the required user name and password. Note, that only username/password is supported. SSL/TLS authentication is not supported by the LINX-10X (e.g., Hotmail, gmail cannot be used).

To verify the E-Mail configuration, reboot the device to let the changes take effect and return to the E-Mail configuration page. Then press one of the "Send Test E-Mail" buttons. Note, that a DNS server must be configured in the IP settings (see Section 5.2.2) to resolve the E-Mail server host name. The Web UI displays a warning message at the top of the page, if the DNS configuration is missing.



Warning: Currently no DNS server configured!
Goto IP Configuration to set DNS server

Outgoing e-mail server (SMTP)	mgate.chello.at
Outgoing e-mail server port	25
Source e-mail address	linx_100@chello.at
Source e-mail sender name	Manual
Reply e-mail address (opt.)	huber@aon.at
E-Mail server user name (Leave empty to disable authentification)	
E-Mail server password	••••••

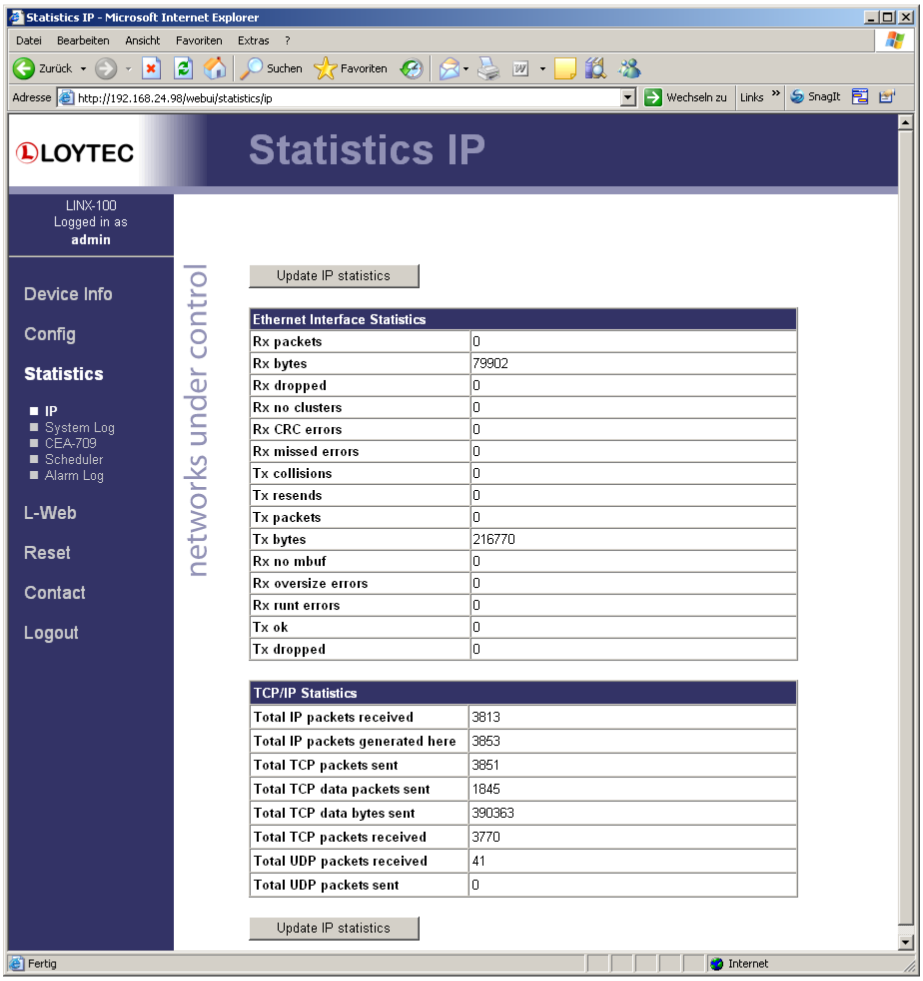
Figure 68: E-Mail Configuration Page

5.3 Device Statistics

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

5.3.1 IP Statistics

Figure 69 shows the IP statistics page. It allows to find possible problems related to the IP communication. Specifically any detected IP address conflicts are displayed (if the LINX-10X’s IP address conflicts with a different host on the network).



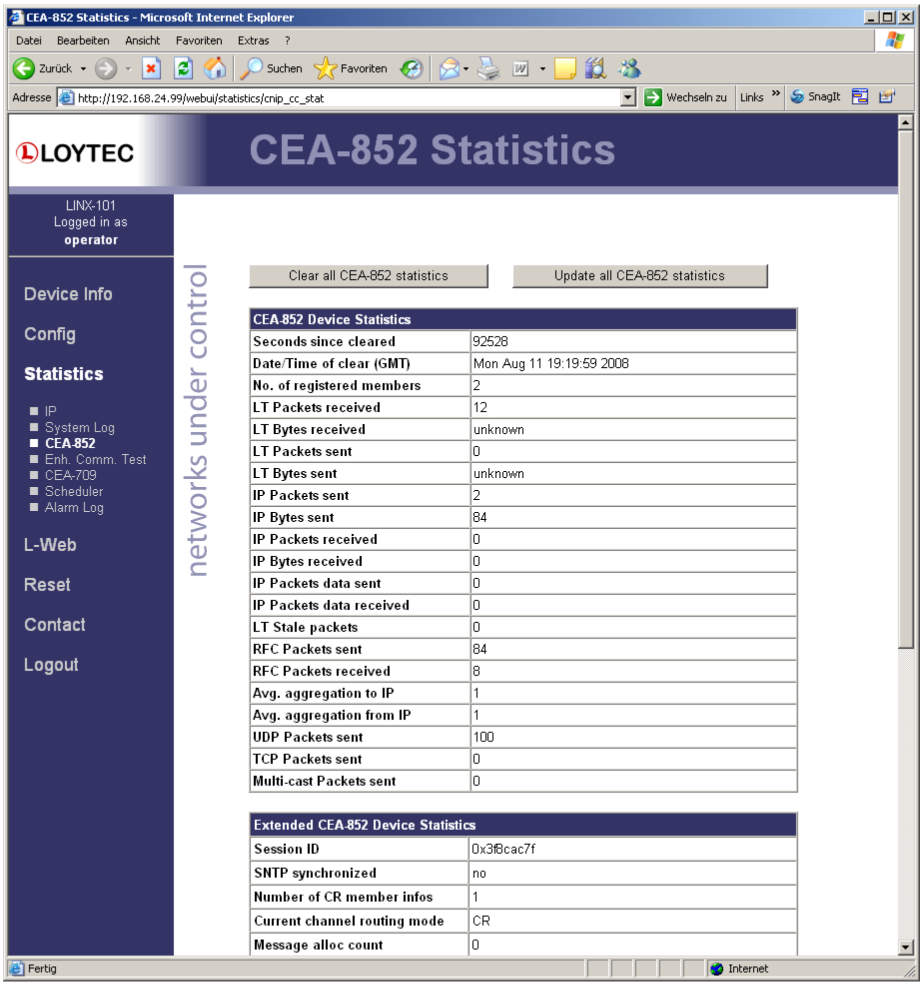
Ethernet Interface Statistics	
Rx packets	0
Rx bytes	79902
Rx dropped	0
Rx no clusters	0
Rx CRC errors	0
Rx missed errors	0
Tx collisions	0
Tx resends	0
Tx packets	0
Tx bytes	216770
Rx no mbuf	0
Rx oversize errors	0
Rx runt errors	0
Tx ok	0
Tx dropped	0

TCP/IP Statistics	
Total IP packets received	3813
Total IP packets generated here	3853
Total TCP packets sent	3851
Total TCP data packets sent	1845
Total TCP data bytes sent	390363
Total TCP packets received	3770
Total UDP packets received	41
Total UDP packets sent	0

Figure 69: 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 LINX-10X. It is only displayed if the CEA-852 interface is enabled. The contents are the same as available through the console UI (see Section 4.11.1). The upper part of the CEA-852 statistics page is depicted in Figure 70. To update the statistics data press the button “Update all CEA-852 statistics”. To reset all statistics counters to zero click on the button “Clear all CEA-852 statistics”. The field “Date/Time of clear” will reflect the time of the last counter reset.



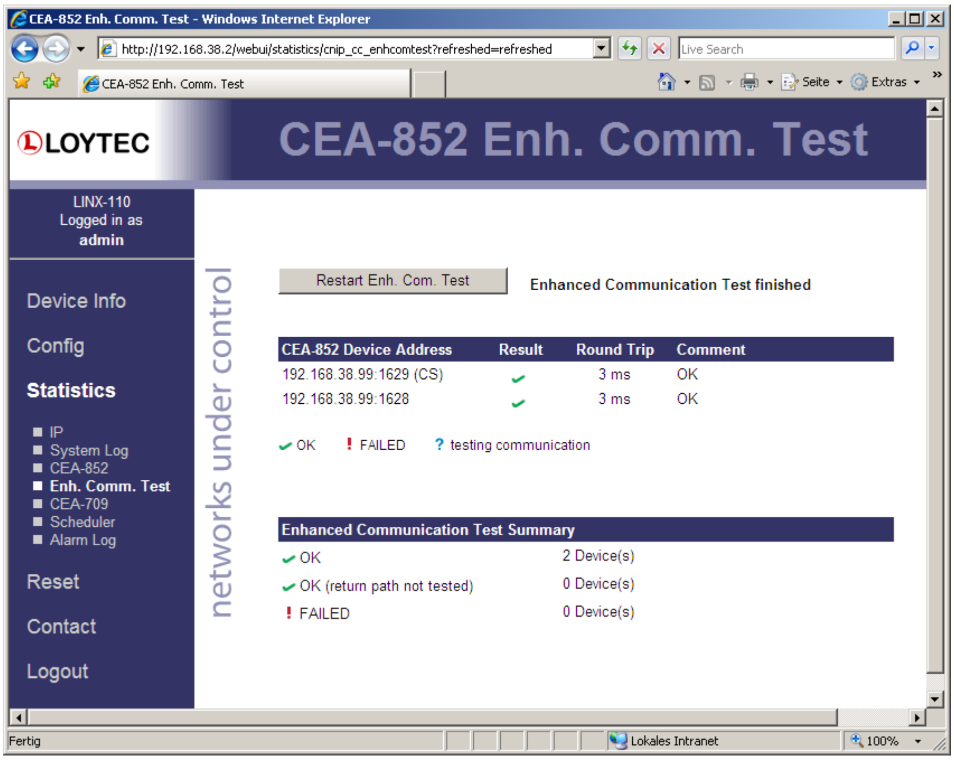
CEA-852 Device Statistics	
Seconds since cleared	92528
Date/Time of clear (GMT)	Mon Aug 11 19:19:59 2008
No. of registered members	2
LT Packets received	12
LT Bytes received	unknown
LT Packets sent	0
LT Bytes sent	unknown
IP Packets sent	2
IP Bytes sent	84
IP Packets received	0
IP Bytes received	0
IP Packets data sent	0
IP Packets data received	0
LT Stale packets	0
RFC Packets sent	84
RFC Packets received	8
Avg. aggregation to IP	1
Avg. aggregation from IP	1
UDP Packets sent	100
TCP Packets sent	0
Multi-cast Packets sent	0

Extended CEA-852 Device Statistics	
Session ID	0x3f8cac7f
SNTP synchronized	no
Number of CR member infos	1
Current channel routing mode	CR
Message alloc count	0

Figure 70: 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 LINX-10X 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 71.



Enhanced Communication Test finished

CEA-852 Device Address	Result	Round Trip	Comment
192.168.38.99:1629 (CS)	✓	3 ms	OK
192.168.38.99:1628	✓	3 ms	OK

✓ OK ! FAILED ? testing communication

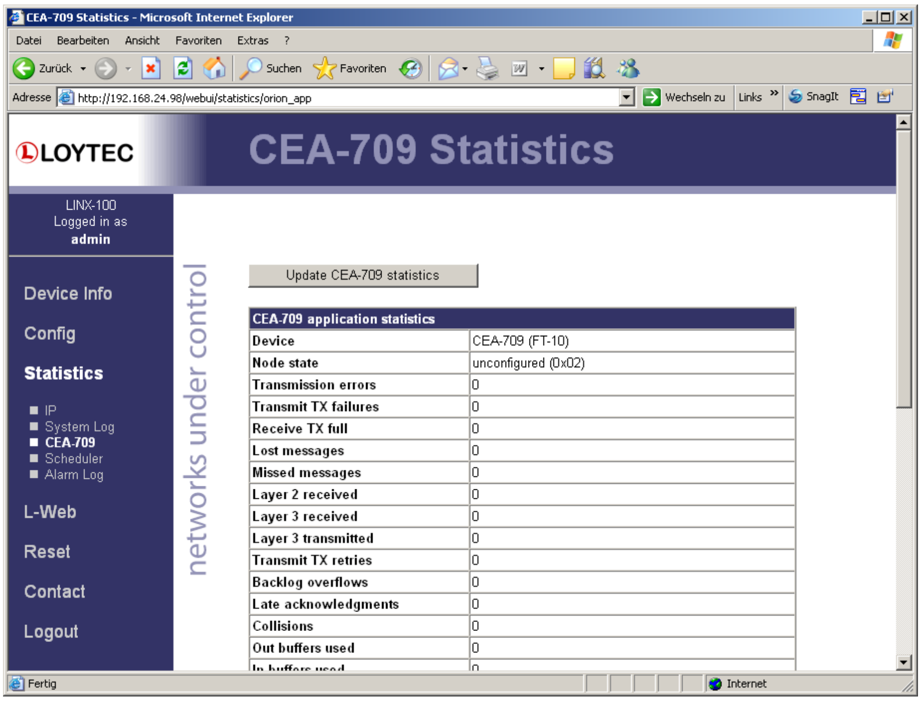
Enhanced Communication Test Summary	
✓ OK	2 Device(s)
✓ OK (return path not tested)	0 Device(s)
! FAILED	0 Device(s)

Figure 71: Enhanced Communication Test Output

The round-trip value (RTT) is measured as the time a packet sent to the peer device needs to be routed back to the LINX-10X. 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 5.

5.3.4 CEA-709 Statistics

The CEA-709 statistics page displays statistics data of the CEA-709 port on the LINX-10X as shown in Figure 72. This data can be used to troubleshoot networking problems. To update the data, click on the button “Update CEA-709 statistics”.

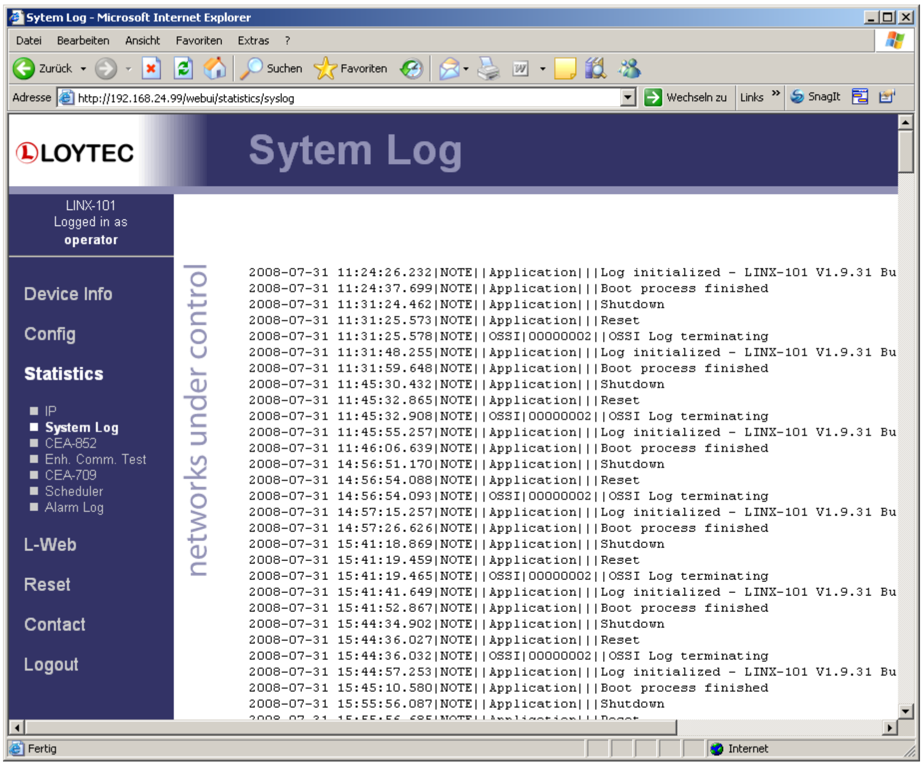


CEA-709 application statistics	
Device	CEA-709 (FT-10)
Node state	unconfigured (0x02)
Transmission errors	0
Transmit TX failures	0
Receive TX full	0
Lost messages	0
Missed messages	0
Layer 2 received	0
Layer 3 received	0
Layer 3 transmitted	0
Transmit TX retries	0
Backlog overflows	0
Late acknowledgments	0
Collisions	0
Out buffers used	0
In buffers used	0

Figure 72: CEA-709 Statistics Page

5.3.5 System Log

The System Log page prints all messages stored in the system log of the LINX-10X. An example is shown in Figure 73. 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.

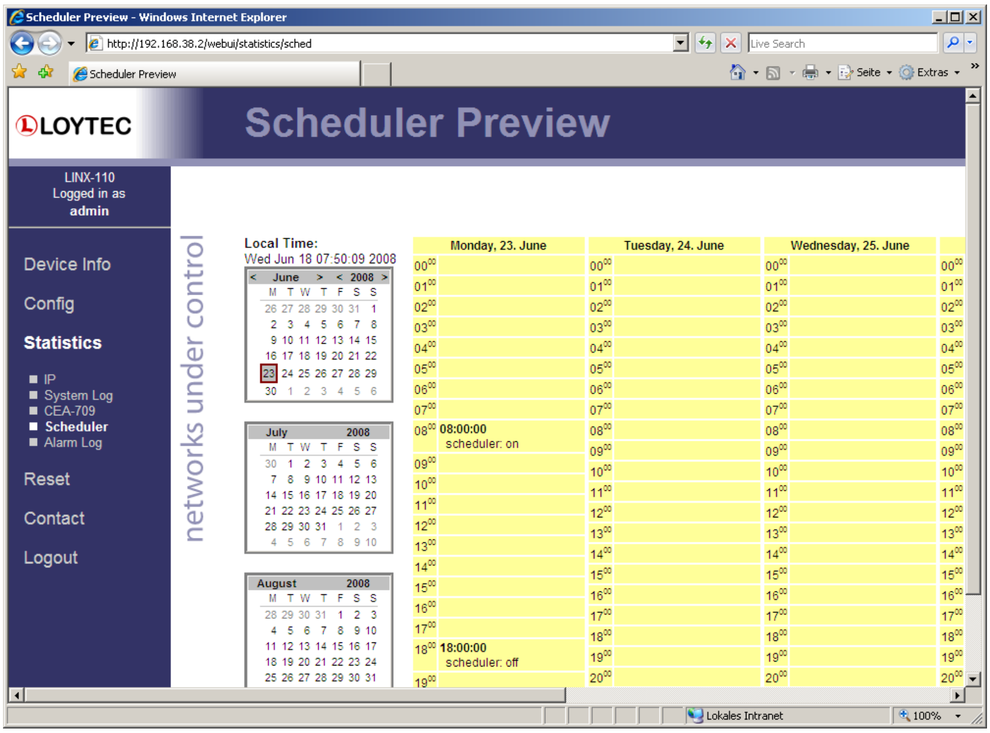


```
2008-07-31 11:24:26.232|NOTE||Application|||Log initialized - LINX-101 V1.9.31 Bu
2008-07-31 11:24:37.699|NOTE||Application|||Boot process finished
2008-07-31 11:31:24.462|NOTE||Application|||Shutdown
2008-07-31 11:31:25.573|NOTE||Application|||Reset
2008-07-31 11:31:25.578|NOTE||OSSI|00000002||OSSI Log terminating
2008-07-31 11:31:48.255|NOTE||Application|||Log initialized - LINX-101 V1.9.31 Bu
2008-07-31 11:31:59.648|NOTE||Application|||Boot process finished
2008-07-31 11:45:30.432|NOTE||Application|||Shutdown
2008-07-31 11:45:32.865|NOTE||Application|||Reset
2008-07-31 11:45:32.908|NOTE||OSSI|00000002||OSSI Log terminating
2008-07-31 11:45:55.257|NOTE||Application|||Log initialized - LINX-101 V1.9.31 Bu
2008-07-31 11:46:06.639|NOTE||Application|||Boot process finished
2008-07-31 14:56:51.170|NOTE||Application|||Shutdown
2008-07-31 14:56:54.088|NOTE||Application|||Reset
2008-07-31 14:56:54.093|NOTE||OSSI|00000002||OSSI Log terminating
2008-07-31 14:57:15.257|NOTE||Application|||Log initialized - LINX-101 V1.9.31 Bu
2008-07-31 14:57:26.626|NOTE||Application|||Boot process finished
2008-07-31 15:41:18.869|NOTE||Application|||Shutdown
2008-07-31 15:41:19.459|NOTE||Application|||Reset
2008-07-31 15:41:19.465|NOTE||OSSI|00000002||OSSI Log terminating
2008-07-31 15:41:41.649|NOTE||Application|||Log initialized - LINX-101 V1.9.31 Bu
2008-07-31 15:41:52.867|NOTE||Application|||Boot process finished
2008-07-31 15:44:34.902|NOTE||Application|||Shutdown
2008-07-31 15:44:36.027|NOTE||Application|||Reset
2008-07-31 15:44:36.032|NOTE||OSSI|00000002||OSSI Log terminating
2008-07-31 15:44:57.253|NOTE||Application|||Log initialized - LINX-101 V1.9.31 Bu
2008-07-31 15:45:10.580|NOTE||Application|||Boot process finished
2008-07-31 15:55:56.087|NOTE||Application|||Shutdown
2008-07-31 15:55:56.685|NOTE||Application|||Reset
```

Figure 73: System Log Page

5.3.6 Scheduler Statistics Page

The scheduler statistics page provides an overview of what is scheduled at which day and which time. In the “Display Schedules” list select a single schedule to view its scheduled values and times. Use the multi-select feature to get the overview of more schedules. An example is shown in Figure 74.



Local Time:
Wed Jun 18 07:50:09 2008

Monday, 23. June	Tuesday, 24. June	Wednesday, 25. June
08:00:00 scheduler: on		
18:00:00 scheduler: off		

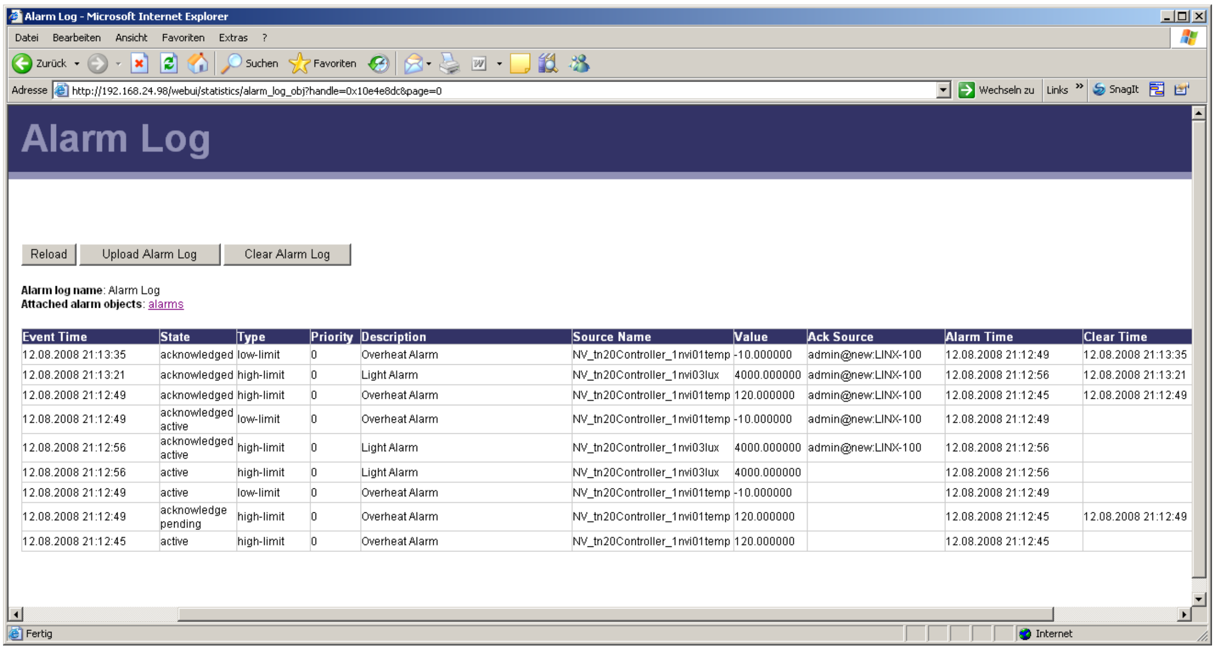
Figure 74: Scheduler Statistics Page

5.3.7 Alarm Log Page

The alarm log page provides an overview of all alarm logs on the system. Click on one of the links to view a specific alarm log. Each alarm log contains a historical log of alarm transitions. When an inactive and acknowledged alarm disappears from the alarm summary page (live list), the alarm log contains this last transition and maintains this over a reboot. An example is shown in Figure 75.

To refresh the alarm log contents click on the “Reload” button. Currently active alarms cannot be acknowledged in this historical view. Follow the link to the attached alarm objects to get to the respective live lists, where alarms can be acknowledged on the Web interface (see Section 5.2.12).

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



Alarm Log - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten
Adresse http://192.168.24.98/webui/statistics/alarm_log_obj?handle=0x10e4e8dc&page=0
Wechseln zu Links SnagIt
Alarm Log
Reload
Upload Alarm Log
Clear Alarm Log
Fertig
Internet

Alarm log name: Alarm Log
Attached alarm objects: alarms

Event Time	State	Type	Priority	Description	Source Name	Value	Ack Source	Alarm Time	Clear Time
12.08.2008 21:13:35	acknowledged	low-limit	0	Overheat Alarm	NV_tn20Controller_1nvi01temp	-10.000000	admin@new:LINX-100	12.08.2008 21:12:49	12.08.2008 21:13:35
12.08.2008 21:13:21	acknowledged	high-limit	0	Light Alarm	NV_tn20Controller_1nvi03lux	4000.000000	admin@new:LINX-100	12.08.2008 21:12:56	12.08.2008 21:13:21
12.08.2008 21:12:49	acknowledged	high-limit	0	Overheat Alarm	NV_tn20Controller_1nvi01temp	120.000000	admin@new:LINX-100	12.08.2008 21:12:45	12.08.2008 21:12:49
12.08.2008 21:12:49	acknowledged active	low-limit	0	Overheat Alarm	NV_tn20Controller_1nvi01temp	-10.000000	admin@new:LINX-100	12.08.2008 21:12:49	
12.08.2008 21:12:56	acknowledged active	high-limit	0	Light Alarm	NV_tn20Controller_1nvi03lux	4000.000000	admin@new:LINX-100	12.08.2008 21:12:56	
12.08.2008 21:12:56	active	high-limit	0	Light Alarm	NV_tn20Controller_1nvi03lux	4000.000000		12.08.2008 21:12:56	
12.08.2008 21:12:49	active	low-limit	0	Overheat Alarm	NV_tn20Controller_1nvi01temp	-10.000000		12.08.2008 21:12:49	
12.08.2008 21:12:49	acknowledge pending	high-limit	0	Overheat Alarm	NV_tn20Controller_1nvi01temp	120.000000		12.08.2008 21:12:45	12.08.2008 21:12:49
12.08.2008 21:12:45	active	high-limit	0	Overheat Alarm	NV_tn20Controller_1nvi01temp	120.000000		12.08.2008 21:12:45	

Figure 75: Alarm Log Page.

5.4 L-Web

This configuration page provides a download link to the L-Web application installer. Clicking on **Install** will download the installer for L-Web and start the installation process. See Section 9.2 for more information on working with the L-Web visualization.

5.5 Reset, Contact, Logout

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

- Rebooting the LINX-10X from a remote location, and
- Resetting the data point configuration from a remote location (see also Section 4.10.3). 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 CEA-709 OPC Server

The LINX-10X implements an embedded OPC server, which exposes network variables (NVs) and configuration properties (CPs) from the CEA-709 network to OPC. The OPC server is based on OPC XML-DA Web service.

The LINX-10X has one physical FT port and one IP-852 port, which is accessible over Ethernet. On the LINX-100 the OPC server node is internally connected either to the FT port or to the IP-852 port. Which one is used can be configured in the CEA-709 configuration (see Section 5.2.4). The schematic is shown in Figure 76 (a). If configured for the FT channel, the LINX-100 provides an RNI for remote access to the FT channel. The RNI can be used to commission nodes and trouble-shoot communications on the FT channel.

The LINX-101 possesses a CEA-709 router, which connects the FT port and the IP-852 port. On the LINX-101 the OPC server node is always internally connected to the FT port. The schematic is shown in Figure 76 (b).

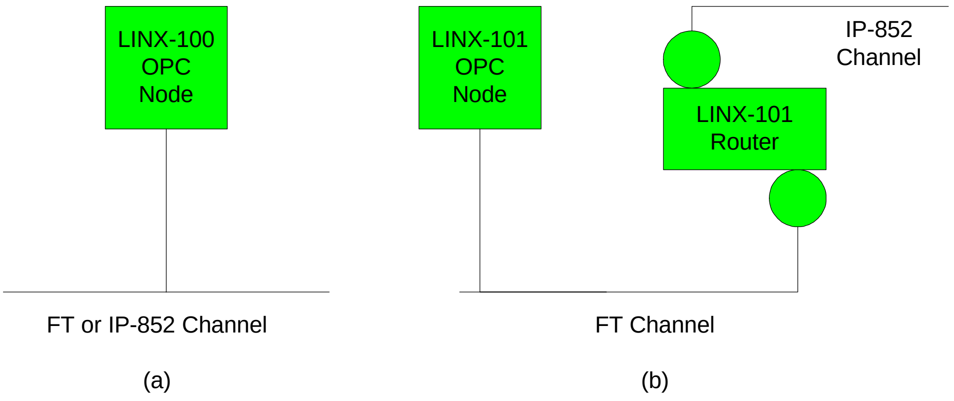


Figure 76: (a) OPC server node on LINX-100, (b) OPC server node and and router on the LINX-101

If the OPC server shall only expose network variables from the local FT channel and there is no IP-852 backbone, then the router is not needed. In this case, the user needs to commission only the OPC node. To attach the FT channel to an IP-852 backbone, the router in the LINX-101 needs to be commissioned. See Chapter 8 for more information on the built-in router and configuration server.

6.2 Data Points

6.2.1 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 are 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.

6.2.2 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.

6.2.3 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.

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.

6.2.4 System Registers

The LINX-10X provides a number of built-in system registers. They are present without a data point configuration. The system registers, such as the System time or the CPU load, can be exposed to the OPC server. By default, all system registers are checked for being exposed to OPC. To reduce the number of needed OPC tags, you may deselect certain system registers, which are not useful in a specific project.

System register can also serve as a testing setup for the OPC XML-DA communication without a CEA-709 network configuration. The *System Time* register is updated every second and may serve for testing subscriptions. The *Authentication Code* register can be used to verify writing to OPC tags.

6.2.5 User Registers

The LINX-10X can be configured to contain user registers. In contrast to system registers, these are only available as a part of the data point configuration. User registers are data points on the device that do not have a specific, technological representation on the control network. Thus, they are not accessible over a specific control network technology.

A register merely serves as a container for intermediate data (e.g., results of math objects). The register can have the following, basic data types:

- **Double**: A register of base type *double* is represented by an *analog* data point. It can hold any scalar value. No specific scaling factors apply.
- **Signed Integer**: A register of base type *signed integer* is represented by a *multi-state* data point. This register can hold a set of discrete states, each identified by a signed stats ID.

- **Boolean**: A register of base type *boolean* is represented by a *binary* data point. This register can hold a Boolean value.

Since a register has not network direction, it can be written and read. Therefore, two data points are generated for each register, one for writing the register (output) and one for reading the register (input). A suffix is added to the register name to identify the respective data point. For example, the register *MyValue* will have two data points generated for: *MyValue_Read* and *MyValue_Write*.

6.2.6 Math Objects

Math objects are advanced application objects that can execute mathematical operations on data points. A math object takes a number of input data points (variables v_1, v_2, …, v_n) and calculates a result value according to a specified formula. The result is written to a set of output data points. The formula is calculated each time one of the input data points updated its value. The formula is only evaluated if all of the input data points have a valid value (i.e., don't show the *invalid value* status).

6.3 AST Features

6.3.1 Alarming

The alarming architecture comprises a number of entities. Objects that monitor values of data points and generate alarms depending on an *alarm condition* are called *alarm sources*. The alarms are reported to an *alarm server* on the same device. The alarm server maintains a list of alarm records, called the *alarm summary*. The alarm server is the interface to access the local alarms. This can be done over the network or the Web UI.

An alarm record contains the information about the alarm. This includes information about the alarm time, the source of the alarm, an alarm text, an alarm value, an alarm type, an alarm priority, and an alarm state. An alarm record undergoes a number of state changes during its life-cycle. When the alarm appears it is *active*. When the alarm condition subsides, the alarm becomes *inactive*. Active alarms can be acknowledged by an operator. Then they become *active acknowledged*. Active alarms can also become inactive, but an acknowledgement is still required. Then they become *ack-pending*. When an alarm is inactive and was acknowledged it disappears from the alarm summary.

Other devices can access the alarm information of an alarm server. These devices are *alarm clients*. They register with the alarm server and get notified about changes to the alarm summary. Alarm clients can be used to display the current alarm summary and acknowledge alarms.

Depending on the underlying technology, some restrictions to the available alarm information and acknowledgement behavior may exist.

6.3.2 Historical Alarm Log

The alarm summary of the alarm objects contains a live list of currently active and acknowledge-pending alarms. As soon as an alarm becomes inactive and has been acknowledged, it disappears from the alarm summary. To store a historical log of alarm transitions an *alarm log* is utilized. An alarm log can log transitions of one or more alarm objects.

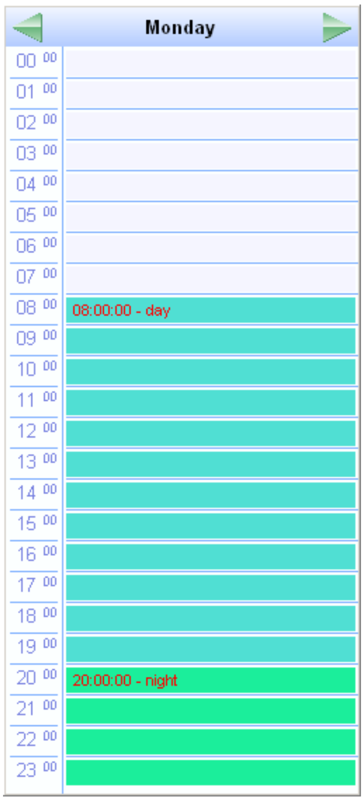
The alarm log is always local and stored as a file on the device. The size of an alarm log is configurable. The alarm log operates as a ring buffer. As soon as its size limit is reached, the oldest alarm log records are overwritten by newer alarm transitions. The alarm log is available on the Web UI or can be uploaded from the device as a CSV file. The CSV file can also be used as an E-Mail attachment.

6.3.3 Scheduling

Schedulers are objects that schedule values of data points on a timely basis. A scheduler object is configured by which data points it shall schedule. This configuration is done by the system engineer once when the system is designed. The configuration of the times and values that shall be scheduled is not part of that initial configuration and may be changed later. This distinction has to be kept in mind.

A scheduler object sets its data points to pre-defined values at specified times. The function of the scheduler is state-based. This means, that after a given time, the scheduler maintains this state. It can re-transmit the scheduled values as appropriate (e.g., when rebooting). The pre-defined values are called *value presets*. A value preset contains one or more values under a single label (e.g., "day" schedules the values { 20.0, TRUE, 400 }).

Which value preset is scheduled at what time is defined through a *daily schedule*. The daily schedule defines the times and value presets in a 24-hour period. A schedule typically contains daily schedules for the weekdays Monday through Sunday. See Figure 77 for an example of a daily schedule.



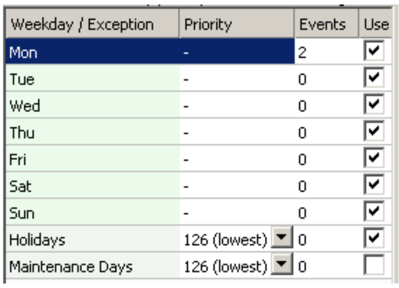
08:00:00 - day

20:00:00 - night

Figure 77: Example of a Daily Schedule.

For some tasks the daily schedules on weekdays is sufficient. However, on some specific dates, there may be exceptions to the regular week. This can be implemented by using defining daily schedules for *exception days*. For instance, there may be a separate daily schedule for *Holidays*. The exception days are defined through a *calendar*. The calendar contains a number of *calendar patterns*. Each calendar pattern describes a pattern of dates that define the class of an exception, e.g., *Holidays*.

When a calendar is defined on a system, the exception days are available in all schedules. When a schedule wants to define daily schedules for some of the available exception days, they need to be enabled in the schedule. See Figure 78 for an example where *Holidays* is used.



Weekday / Exception	Priority	Events	Use
Mon	-	2	☑
Tue	-	0	☑
Wed	-	0	☑
Thu	-	0	☑
Fri	-	0	☑
Sat	-	0	☑
Sun	-	0	☑
Holidays	126 (lowest)	0	☑
Maintenance Days	126 (lowest)	0	□

Figure 78: Example of on used Exception Day.

The function of the exception is simple. The daily schedule of a regular weekday is overridden by the daily schedule of the exception, when one of the specified date patterns is in effect (e.g., July 14th in Holidays overrides the regular weekday). If more than one exception days are in use, there may be conflicts on specific dates. These conflicts are resolved by defining *priorities* for the different exceptions. The daily schedule of the exception with the higher priority is eventually in effect. If two exceptions with the same priority exist, it is not defined, which one is in effect. Therefore, always use distinct priorities.

The configuration of exceptions is done by calendar patterns in the calendar. Each calendar pattern contains a number of pattern entries. These entries can define the following:

- A single date: This defines a singe date. Wildcards may be used in the year to specify July 14th of every year.
- A date range: This defines a range. Starting with a start date and ending with the end date. No wildcards should be used.
- A Week-and-Day definition: This defines dates based on a week, such as every 1st Friday in a month, every Monday, every last Wednesday of a month.

When a scheduler is executing the schedule on the local device, it is called a *local scheduler*. Such a scheduler is configured to schedule data points and later its daily schedules can be modified. When accessing the daily schedules of a scheduler, which executes on a remote device, the object is called a *remote scheduler*. A remote scheduler has the same interface to the user to modify daily schedules. A remote scheduler object can be used as a user-interface for schedulers that execute on different devices.

6.3.4 Trending

Trending refers to the ability to log values of data points over time. A trend log object is responsible for this task. It is configured, which data points shall be trended. Log records are generated either in fixed time intervals, or on change-of-value conditions. Trend log objects can trend either local or remote data points.

The trend data is stored in a binary format on the device. The capacity of a given trend log is configured. The trend log can be operated in one of two modes: (1) In linear mode the trend file fills up until it reaches its capacity. It then stops logging. (2) In ring buffer mode. In this mode the oldest log records are overwritten when the capacity is reached.

How many data points can be trended in one trend log is limited by the underlying technology. So are some of the log modes. Refer to the technology sections for more information.

6.3.5 E-Mail

The E-Mail function can be combined with the other AST features. The format of an E-Mail is defined through *E-Mail templates*. An E-Mail template defines the recipients, the E-Mail text, value parameters inserted into the text and triggers, which invoke the transmission of an E-Mail. An E-Mail template can also specify one or more files to be sent along as an attachment.

A prerequisite to sending E-Mails is the configuration of an E-Mail account on the LINX-10X. This can be done on the Web UI (see Section 5.2.13). It is recommended to use the E-Mail server of your Internet provider. For public mailers enable the required authentication. Please note that the LINX-10X does currently not support the SS/TLS E-Mail authentication mechanism. Therefore, Hotmail and gmail cannot be used.

The amount of generated E-Mails can be limited using a rate limit algorithm. The transmission of E-Mails can be disabled altogether by using a special data point. That data point can be scheduled or driven over the network.

6.4 CEA-709 Technology

6.4.1 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 LINX-10X consists of the following steps:

1. Select the data points of the network to be used on the LINX-10X (e.g., select the NVs in the CEA-709 network nodes)

2. Create necessary registers, math objects

3. Select those data points on the LINX-10X, which shall be exposed as OPC tags

The CEA-709 NVs on the LINX-10X can be created in three different ways:

- **Static NV**: For each selected NV on the network there is a static NV created on the LINX-10X. This NV can be bound to the NV on the network. Note that adding static NVs to the LINX-10X results in a change to the default XIF file. The LINX-10X is assigned a new “model number” to reflect this change (see Section 6.4.2). 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 LINX-10X. Compared to static NVs, dynamic NVs do not change the XIF interface of the LINX-10X. 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 LINX-10X. The LINX-10X doesn’t create any NVs on the device and instead uses polling to read from those NVs and explicit updates to send values. 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, 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, scaling factors are already 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 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 14.2. For CPs the allocation type "File" is used.

6.4.2 Static Interface Changes

The LINX-10X 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 LINX-10X changes its static interface and boots with a new one.

Each time the static interface of the LINX-10X 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 LINX-10X Configurator 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 LINX-10X device in the LNS database and restores the previous bindings and dynamic NVs. If the LINX-10X 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 14.2.

7 The LINX-10X Configurator

This Chapter gives step-by-step instructions on how to commission LINX-10X, create a data point configuration with input and output network variables, and how to expose those data points to the OPC server. We show the configuration steps using NL-220, LonMaker 3.1, and Alex 3 but other LNS-based network management tools can be used as well to install and configure the LINX-10X. We also show how to configure the LINX-10X without LNS.

7.1 Installation

7.1.1 Software Installation

The LINX-10X Configurator must be used to setup the data point configuration of the LINX-10X. 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 XP, Windows 2000, Windows 2003 Server, and Windows Vista.

The LINX-10X Configurator can be downloaded from the LOYTEC website http://www.loytec.com. To install the Configurator, double click on Setup and follow the installation steps. When asking 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.

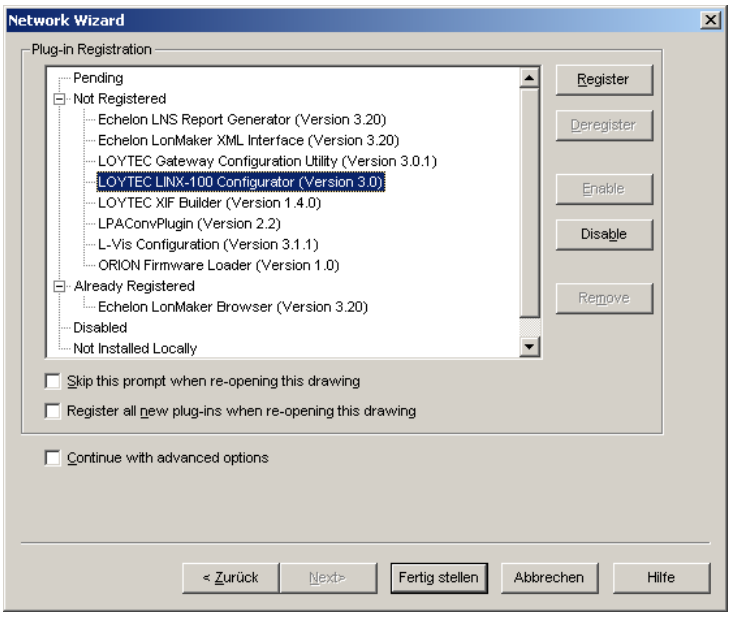
7.1.2 Registration as a Plug-In

If the LINX-10X shall be configured using LNS-based tools (e.g. NL200 or LonMaker), the LINX-10X Configurator needs to be registered as an LNS plug-in. In the following, the process is described for LonMaker for Windows 3.1. 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 LINX-100 Configurator 3.0** from the list of “Not Registered” (see Figure 79).



Pending
Not Registered
Echelon LNS Report Generator (Version 3.20)
Echelon LonMaker XML Interface (Version 3.20)
LOYTEC Gateway Configuration Utility (Version 3.0.1)
LOYTEC LINX-100 Configurator (Version 3.0)
LOYTEC XIF Builder (Version 1.4.0)
LPAConvPlugin (Version 2.2)
L-Vis Configuration (Version 3.1.1)
ORION Firmware Loader (Version 1.0)
Already Registered
Echelon LonMaker Browser (Version 3.20)
Disabled
Not Installed Locally

☐ Skip this prompt when re-opening this drawing

☐ Register all new plug-ins when re-opening this drawing

☐ Continue with advanced options

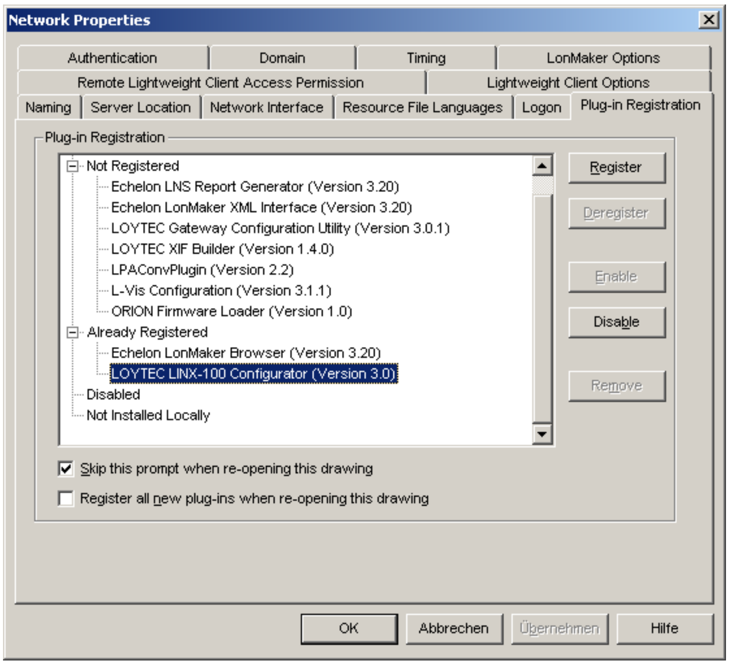
Figure 79: Select the Plug-in to be registered.

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

4. Click **Finish** to complete the registration. Device templates for the LINX-10X 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 LINX-100 Configurator (Version 3.0)** shows up under "Already Registered".



Not Registered
Echelon LNS Report Generator (Version 3.20)
Echelon LonMaker XML Interface (Version 3.20)
LOYTEC Gateway Configuration Utility (Version 3.0.1)
LOYTEC XIF Builder (Version 1.4.0)
LPAConvPlugin (Version 2.2)
L-Vis Configuration (Version 3.1.1)
ORION Firmware Loader (Version 1.0)
Already Registered
Echelon LonMaker Browser (Version 3.20)
LOYTEC LINX-100 Configurator (Version 3.0)
Disabled
Not Installed Locally

☑ Skip this prompt when re-opening this drawing

☐ Register all new plug-ins when re-opening this drawing

Figure 80: Double check that the LINX-10X Configurator is properly registered.

7.1.3 Operating Modes

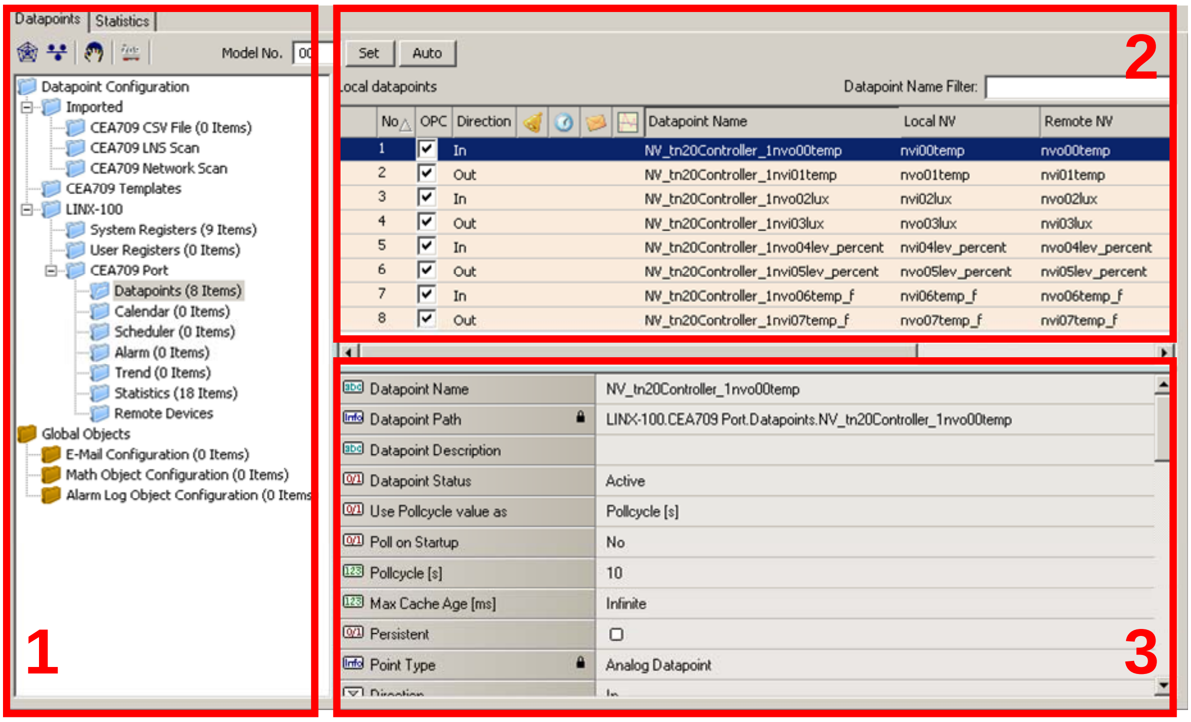
The Configurator can be used in on-line, off-line, and stand-alone mode. On-line and off-line mode refers to the 2 operating modes of your configuration tool.

- **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 to download the configuration into the device.
- **Off-line Mode**: In off-line mode the network management tool 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 a network management tool (e.g., NL-220, LonMaker or Alex). Instead the engineer can work directly with the device when online or engineer it offline.

7.2 Data Point Manager

The Configurator uses a central concept to manage data points. The data point manager as shown in Figure 81 is used to select, create, edit and delete data points. The dialog is divided into three sections:

- The folder list (number 1 in Figure 81),
- The data point list (number 2 in Figure 81),
- And a property view (number 3 in Figure 81).



No	OPC	Direction	Datapoint Name	Local NV	Remote NV
1	☑	In	NV_tn20Controller_1nvo00temp	nvi00temp	nvo00temp
2	☑	Out	NV_tn20Controller_1nvi01temp	nvo01temp	nvi01temp
3	☑	In	NV_tn20Controller_1nvo02lux	nvi02lux	nvo02lux
4	☑	Out	NV_tn20Controller_1nvi03lux	nvo03lux	nvi03lux
5	☑	In	NV_tn20Controller_1nvo04lev_percent	nvi04lev_percent	nvo04lev_percent
6	☑	Out	NV_tn20Controller_1nvi05lev_percent	nvo05lev_percent	nvi05lev_percent
7	☑	In	NV_tn20Controller_1nvo06temp_f	nvi06temp_f	nvo06temp_f
8	☑	Out	NV_tn20Controller_1nvi07temp_f	nvo07temp_f	nvi07temp_f

Datapoint Name	NV_tn20Controller_1nvo00temp
Datapoint Path	LINX-100.CEA709 Port.Datapoints.NV_tn20Controller_1nvo00temp
Datapoint Description	
Datapoint Status	Active
Use Pollcycle value as	Pollcycle [s]
Poll on Startup	No
Pollcycle [s]	10
Max Cache Age [ms]	Infinite
Persistent	☐
Point Type	Analog Datapoint
Direction	In

Figure 81: Datapoint 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:

- **Import**: This folder has three sub-folders. The LNS Database Scan folder is used to hold data retrieved from a network database scan. The CEA709 Network Scan folder holds NVs scanned online from an attached CEA-709 network. The CSV Import folder is used to display data points imported from CSV files. 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 CEA709 data points, when they are created on the LINX-10X.
- **LINX-10X**: This is the device folder of the LINX-10X. It contains all the necessary data points which constitute to the LINX-10X's port interface definition. These data points are created on the LINX-10X when the configuration is downloaded. The three subfolders represent the CEA-709 port, the System Registers and IEC61131 variables on the LINX-10X.
- **Datapoints**: The CEA-709 port folder contains a data points sub-folder. This folder holds all data points, which are allocated on the port. To create a data point, select the folder and use the context menu.
- **Calendar**: This folder is used to hold a locally available calendar object with its calendar patterns (definitions of day classes like holiday, maintenance day, and so on). Current devices allow one local calendar object. To create a calendar, select the folder and use the context menu.
- **Scheduler**: This folder is used for local scheduler objects. Each of these objects will connect to a local scheduler on the device and will be configurable through this data object, that is, the data objects transfers *schedule configuration data* between the actual scheduler present on the device and the user interface. To create a scheduler, select the folder and use the context menu.
- **Trend**: This folder is used for local trend log objects. Each of these objects will be able to trend a data point over time and store a local trend log file. To create a trend log object, select the folder and use the context menu.
- **Alarm**: This folder is used for local alarm server objects. Each of these alarm server objects represent an alarm class, which other objects can report alarms to. Other devices can use the alarm server object to get notified about alarms. To create an alarm server object, select the folder and use the context menu.
- **Remote Devices**: This folder is used to collect all remote calendars, schedulers, trend logs and alarm client objects, which were created from network scan data. For each remote device, a subfolder will be created where the objects referencing this device are collected.
- **Global Objects**: This top-level folder contains sub-folders that organize specific application objects that operate on data points.
- **E-Mail Configuration**: This folder contains E-Mail templates. An E-Mail template defines the destination address and text body of an E-Mail, which is triggered by data points and may contain data point values or file attachments. To create an E-Mail template, select the folder and use the context menu.
- **Alarm Log Configuration**: This folder contains the alarm log objects. Each alarm log object creates a historical log of alarm transitions of one or more alarm objects (alarm server or client). To create an alarm log, select the folder and use the context menu.

- **Math Objects Configuration**: This folder contains math objects. Math objects are used to perform a pre-defined calculation on a number of input data points are write the result to a defined set of output data points. Each math object contains one formula. To create a math object, select the folder and use the context menu.

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. A double-click will select the data point, if the dialog is opened for selecting data points.

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.

The **OPC** column provides check boxes for each data point. If checked, the respective data point is exposed to OPC on the device. Deselect the check box, if a data points shall not be exposed to OPC. Note, that deselected data points do not add to the OPC tag limit.

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.

For the alarming, scheduling, trending (AST) features, there are columns, which display icons for data points that are attached to an AST function. See Table 8 for details.

Icon	Data Point Usage
🕐	Data point is scheduled
🔔	Data point has an active alarm condition
🔕	Data point has an inactive alarm condition.
✉	Data point is a trigger for E-Mails
📈	Data point used for trending

Table 8: Icons for used data points in the data point list 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 used for the native communication object (i.e., network variable), but can be different (e.g. longer). 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 as**: For input data points this property defines whether the input shall use a receive timeout or be constantly polling. See Section 6.2.2.
- **Pollcycle**: For input data points this property defines the pollcycle/receive-timeout in seconds. Set this property to '0' to disable polling. See Section 6.2.2.
- **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 6.2.2.
- **Min Send**: For output data points, this property defines the min send time in seconds. See Section 6.2.2.
- **Max Send**: For output data points, this property defines the max send time in seconds. See Section 6.2.2.
- **Max Cache Age**: For output data points, this property defines the maximum cache age in milliseconds. See Section 6.2.2.
- **Only notify on COV**: This property is valid 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 6.2.3.
- **Datapoint Type**: This is the base data point type, e.g., analog.
- **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., "kilograms".
- **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.
- **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 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 this property defines the retry count. The default is 3.
- **Repeat Timer**: For external this property defines the repeat timer in milliseconds. The default is 96 ms.
- **Transmit Timer**: For external 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.

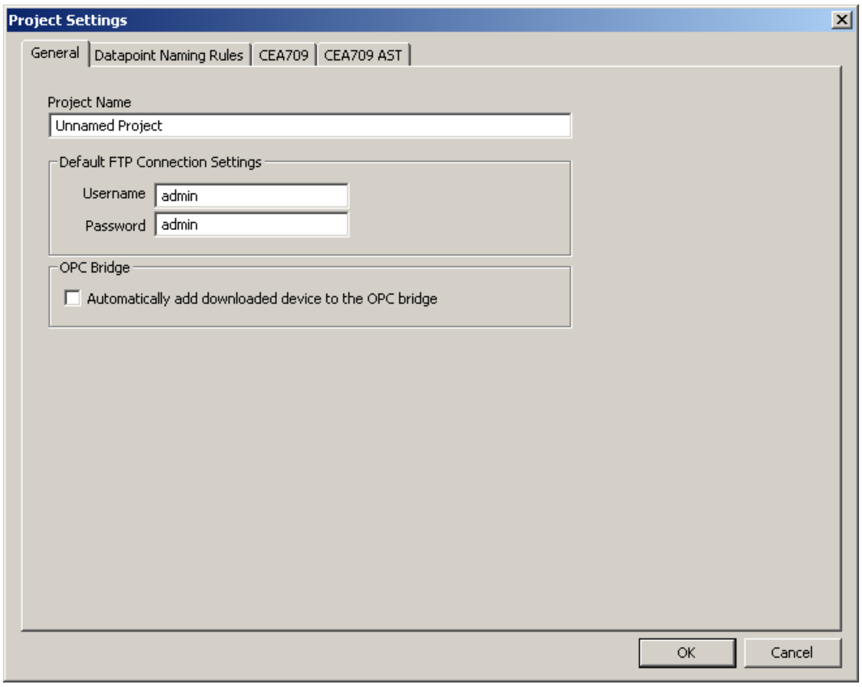
7.3 Project Settings

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 82 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.
- **Automatically add downloaded device to the OPC Bridge**: This option is only available, if the LOYTEC OPC bridge software is installed on the same PC. If enabled, The LINX-10X device a configuration is downloaded to is automatically added to the OPC server list in the bridge. For more information on using the bridge refer to Section 9.3.



Project Name: Unnamed Project

Default FTP Connection Settings

Username: admin

Password: admin

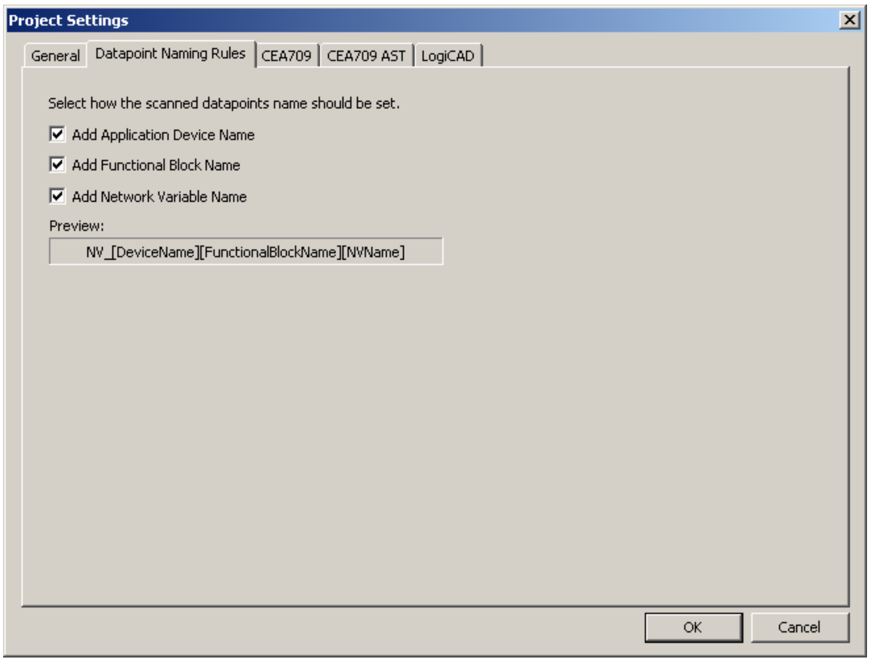
OPC Bridge

□ Automatically add downloaded device to the OPC bridge

Figure 82: General Project Settings.

7.3.2 Data Point Naming Rules

The data point naming rules tab (see Figure 83) 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.



Select how the scanned datapoints name should be set.

☑ Add Application Device Name

☑ Add Functional Block Name

☑ Add Network Variable Name

Preview:

NV_[DeviceName][FunctionalBlockName][NVName]

Figure 83: Data Point Naming Rules Project Settings.

7.3.3 CEA-709 Settings

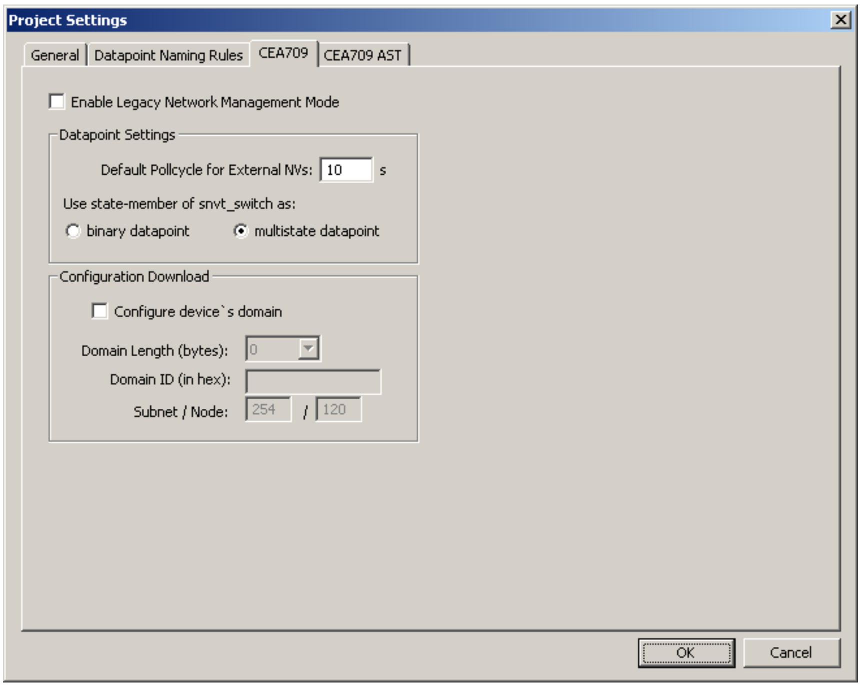
The CEA-709 configuration tab as shown in Figure 84 allows configuring properties of the device's CEA-709 port. The options are:

- **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 when the invalid value is written.

- **Configuration Download**: This group box contains self-configuration settings for the CEA-709 ports. This is necessary, when the device shall be used without being commissioned by a network management tool. Set the check mark and enter the CEA-709 domain and subnet/node information. If operated in self-configured mode, the CEA-709 network can be scanned using the network scan (see Section 7.7.6) and external NVs can be used on the device. Note, that the domain must match the nodes' domain on the network and the subnet/node address must not be used by another device.



☐ Enable Legacy Network Management Mode

Datapoint Settings

Default Pollcycle for External NVs: 10 s

Use state-member of snvt_switch as:

○ binary datapoint ● multistate datapoint

Configuration Download

☐ Configure device`s domain

Domain Length (bytes): 0

Domain ID (in hex):

Subnet / Node: 254 / 120

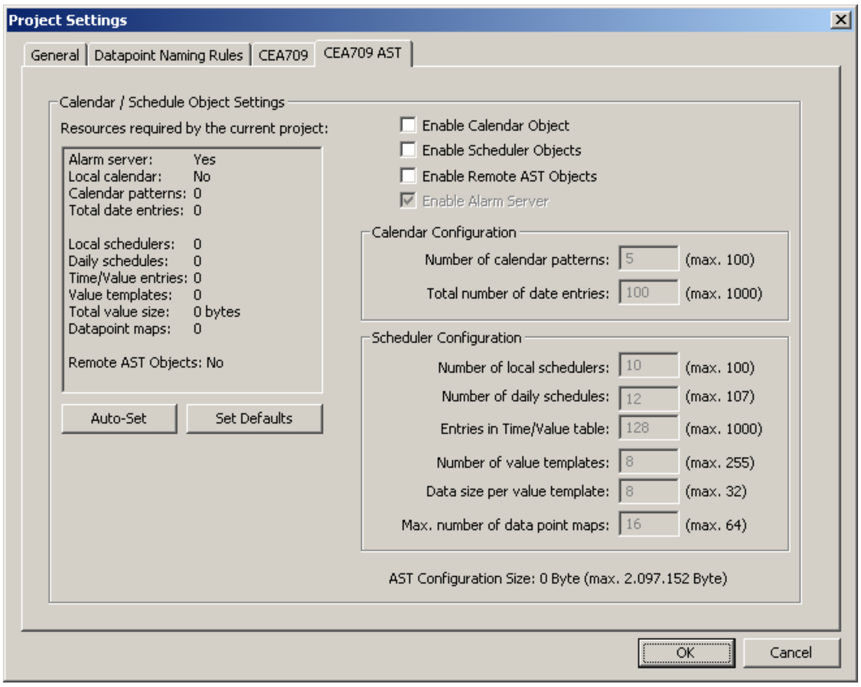
Figure 84: CEA-709 Project Settings.

7.3.4 AST Settings

For CEA709 devices, the use of alarming, scheduling, trending (AST) features requires additional resources (functional objects and NVs). This changes the static interface. Since the number of used resources also influences the performance, the CEA-709 AST tab allows configuring those resources for the project. In this tab the required number of scheduler units that may be instantiated and their capacity may be configured (how many time/value entries, value templates, bytes per value template, and so on). It contains the following options and settings, which are relevant to calendar and scheduler functionality of the device:

- **Enable Calendar Object:** This checkbox enables a LONMARK compliant calendar object on the device. It is automatically enabled together with local schedulers, since the two are always used together.
- **Enable Scheduler Objects:** This checkbox enables local LONMARK compliant scheduler objects on the device. Checking this box will automatically enable the calendar as well.
- **Enable Remote AST Objects:** This checkbox enables the functional object for NVs, which are used to access remote AST objects. If this box is checked, the *Clients* functional block is included in the static interface.
- **Number of calendar patterns:** Specifies the maximum number of different exception schedules (day classes like holiday, maintenance day) supported by this calendar object.
- **Total number of date entries:** Specifies the maximum number of date definitions which may be stored by the calendar. This is the sum of all date definitions from all calendar entries. A date definition is for example a single date, a date range, or a week and day pattern (every last Friday in April).
- **Number of local schedulers:** This is the number of local scheduler objects which should be available on the device. Each local scheduler data point created in the data point manager will connect to one of these scheduler objects. There may be more scheduler objects available on the device than are actually used at a certain time. It is a good idea to have some spare scheduler objects ready, in case another scheduler is needed.

- **Number of daily schedules:** This is the maximum number of schedules supported by each scheduler object. This number must at least be 7, since a scheduler always needs to provide one schedule for each day of the week (default weekly schedule). For each special day defined by the calendar, an additional daily schedule is required to support it.
- **Entries in Time/Value table:** This is the total number of entries in each scheduler defining a value template that should apply on a specific day starting at a specific time (the time table).
- **Number of value templates:** This is the maximum number of value templates supported by each scheduler.
- **Data size per value template:** This specifies the buffer size reserved to hold the data for each value template. More data points or bigger data structures require a bigger value buffer.
- **Max. number of data point maps:** Specifies the maximum number of individual data points that this scheduler is able to control.
- **AST Configuration Size:** This number in Bytes is calculated from the scheduler settings above and represents the total size of the LONMARK configuration properties file stored on the device. While certain settings can be freely edited within the given limits, the resulting configuration size is also limited.



Calendar / Schedule Object Settings

Resources required by the current project:

Alarm server:	Yes
Local calendar:	No
Calendar patterns:	0
Total date entries:	0
Local schedulers:	0
Daily schedules:	0
Time/Value entries:	0
Value templates:	0
Total value size:	0 bytes
Datapoint maps:	0
Remote AST Objects:	No

☐ Enable Calendar Object
☐ Enable Scheduler Objects
☐ Enable Remote AST Objects
☑ Enable Alarm Server

Calendar Configuration

Number of calendar patterns:	5	(max. 100)
Total number of date entries:	100	(max. 1000)

Scheduler Configuration

Number of local schedulers:	10	(max. 100)
Number of daily schedules:	12	(max. 107)
Entries in Time/Value table:	128	(max. 1000)
Number of value templates:	8	(max. 255)
Data size per value template:	8	(max. 32)
Max. number of data point maps:	16	(max. 64)

AST Configuration Size: 0 Byte (max. 2.097.152 Byte)

Figure 85: CEA-709 AST Project Settings.

As can be seen from the above list, it is not easy to configure a LONMARK scheduler object. There are many technical parameters which need to be set and which require some knowledge of how these scheduler objects work internally. Therefore, the configuration software provides the following mechanisms to help in choosing the right settings:

- **Resources required by the current project:** The absolute minimum settings required by the current project are shown in a table at the left side of the window. This data may be used to fill in the values at the right side, but some additional resources should be planned to allow for configuration changes which need more resources.
- **Auto-Set:** This button may be used to let the configuration software decide on the best settings to use, based on the current project. Since the current projects resource usage

is taken as a starting point, all schedulers and calendar patterns in the project should first be configured as required before this button is used.

- **Set Defaults:** This button will choose standard values for all settings. In most cases, these settings will provide more resources than necessary.

Note: *It is possible to enter anything here, until the project is actually saved or downloaded. At this point in time, the software will check that the resources configured here are sufficient to support the projects configuration. If this is not the case, this dialog will automatically open so that the settings may be adjusted.*

7.4 Workflows for the LINX-10X

This section discusses a number of work flows for configuring the LINX-10X 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 a flow diagram. The individual steps refer to later Sections, which describe each step in more detail. In principle, the LINX-10X Configurator supports the following use cases:

- Network Management Tool based on LNS 3.x (see Section 7.4.2)
- Non-LNS 3.x network management tool with polling (see Section 7.4.3)
- Non-LNS 3.x network management tool with bindings (see Section 7.4.4)

7.4.1 Involved Configuration Files

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

- 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 LINX-10X on-line. There exists a XIF for the FT port (LINX-10x_FT-10.xif) and one for the IP-852 port (LINX-10x_IP-10L.xif).
- LINX-10X Configurator project file: This file contains all ports, all data points and all connections of a project. These files end with ".linx0". It stores all the relevant configuration data and is intended to be saved on a PC to back up the LINX-10X's data point configuration.

7.4.2 Configure with LNS

The flow diagram in Figure 86 shows the steps that need to be followed in order to configure the LINX-10X in a network with LNS 3.x. In this scenario the LINX-10X will use dynamic NVs and bindings.

First, the LINX-10X device must be added to LNS (see Section 7.5). Then the LINX-10X Configurator must be started in plug-in mode to configure the LINX-10X (see Section 7.7.1). In the Configurator scan for the data points in the LNS database (see Section 7.7.4). Select the data points that the LINX-10X shall expose (see Section 7.7.7). Finally, the configuration needs to be downloaded onto the LINX-10X (see Section 7.7.12). It is recommended to save the complete configuration to a disk file for being able to replace an LINX-10X in the network.

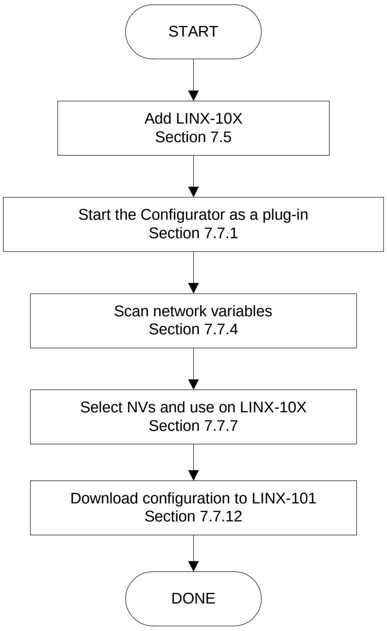


Figure 86: Basic design-flow with LNS.

To add more NVs when all bindings are in place and the LINX-10X is being used simply repeat the steps described above. The Configurator software will back up the bindings, create or delete the dynamic NVs, and re-create the bindings again.

7.4.3 Configure without LNS

The flow diagram in Figure 87 shows the steps that need to be followed in order to configure the LINX-10X without LNS 3.x. In this scenario the LINX-10X will use external NVs and polling. The advantage of this solution is that no bindings in the non-LNS tool (or self-binding nodes) need to be changed. This comes at the cost of a constant network load caused by polling.

Start the Configurator in stand-alone mode and connect to the LINX-10X via the FTP method (see Section 7.7.2). If changing an existing configuration upload the current configuration from the LINX-10X (see Section 7.7.3). In the Configurator import data points from a CSV import file (see Section 7.7.5). Select the data points that the LINX-10X shall expose (see Section 7.7.7). Alternatively, you can create external NVs manually (see Section 7.7.10). Finally, the configuration needs to be downloaded onto the LINX-10X (see Section 7.7.12). It is recommended to save the complete configuration to a disk file for being able to replace an LINX-10X in the network.

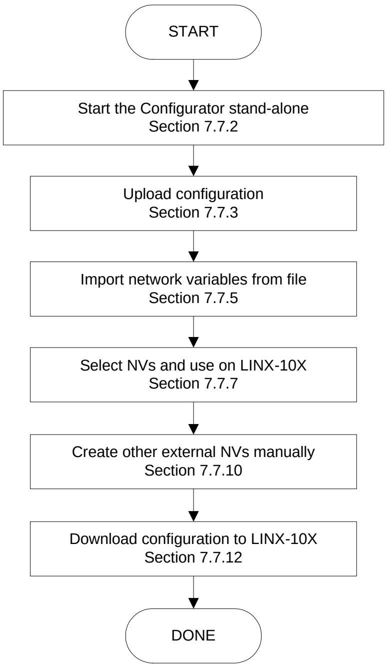

START
Start the Configurator stand-alone
Section 7.7.2
Upload configuration
Section 7.7.3
Import network variables from file
Section 7.7.5
Select NVs and use on LINX-10X
Section 7.7.7
Create other external NVs manually
Section 7.7.10
Download configuration to LINX-10X
Section 7.7.12
DONE

Figure 87: Basic design-flow without LNS.

7.4.4 Configure without LNS Using Bindings

The flow diagram in Figure 88 shows the steps that need to be followed in order to configure the LINX-10X without LNS 3.x. In this scenario the LINX-10X will use static NVs and bindings. The advantage of this solution is that the network load is minimized. However, the non-LNS management tool must create bindings for the LINX-10X and update an existing network.

Start the Configurator in stand-alone mode and connect to the LINX-10X via the FTP method (see Section 7.7.2). In the Configurator import data points from a CSV import file (see Section 7.7.5). Select the data points that the LINX-10X shall expose (see Section 7.7.7). For the NVs used on the LINX-10X select the “static NV” allocation type (see Section 7.7.8). Alternatively, you can create static NVs manually (see Section 7.7.9).

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 7.7.14). Please contact the tool’s vendor for information whether ECS is supported or not.

Download the configuration onto the LINX-10X (see Section 7.7.12). Finally, export a XIF file (see Section 7.7.13). It is recommended to save the complete configuration to a disk file for being able to replace an LINX-10X in the network.

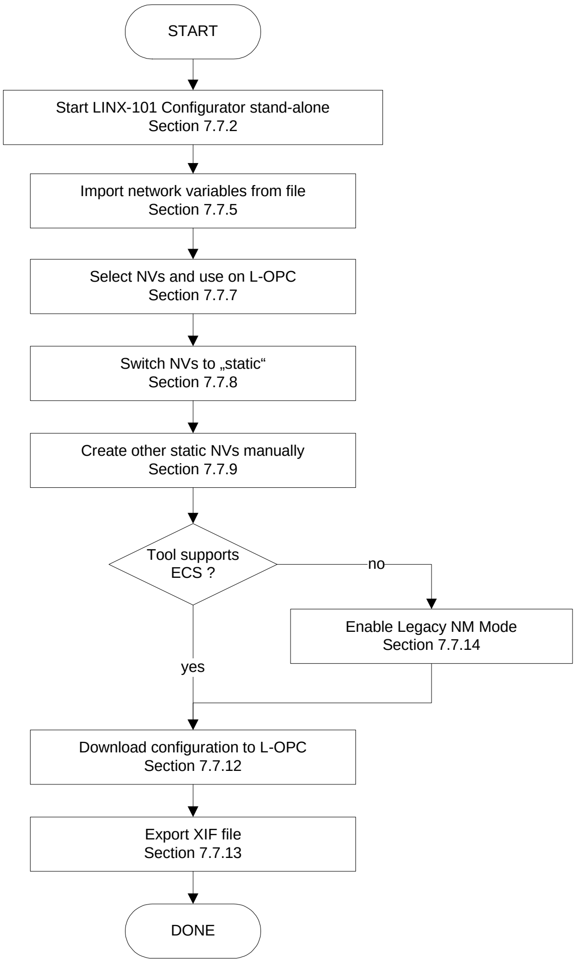


Figure 88: Basic design-flow without LNS using bindings.

To use the LINX-10X in the non-LNS management tool, commission the LINX-10X using the exported XIF file and create the bindings.

When changing a running LINX-10X configuration with existing bindings, it is recommended to create additional data points as external NVs with polling as described in Section 7.4.3. Otherwise, a new XIF file needs to be exported and replacing the LINX-10X in the non-LNS tool requires the user to create all bindings again from scratch (see Section 6.4.2).

7.4.5 Replace a LINX-10X

An LINX-10X can be replaced in the network by another unit. This might be necessary, if a hardware defect occurs. First of all, the replacement LINX-10X needs to be configured with the appropriate IP settings, including all relevant CEA-852 device settings. The remainder of this section focuses on the LINX-10X data point configuration. The work flow is depicted in Figure 89.

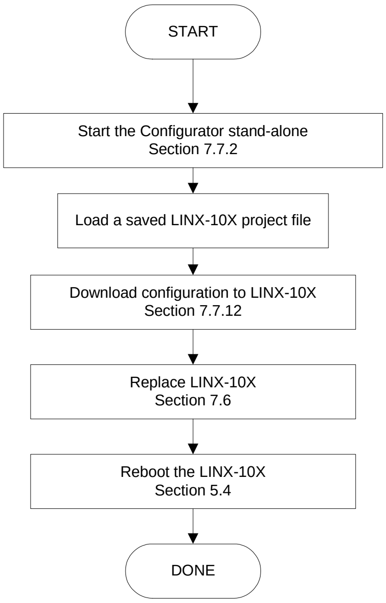

START
Start the Configurator stand-alone
Section 7.7.2
Load a saved LINX-10X project file
Download configuration to LINX-10X
Section 7.7.12
Replace LINX-10X
Section 7.6
Reboot the LINX-10X
Section 5.4
DONE

Figure 89: Basic work flow to configure a replacement device.

Start the Configurator software stand-alone and connect via the FTP method (see Section 7.7.2). Then load the LINX-10X Configurator project file from disk, which has been saved when the original LINX-10X has been configured or modified. Double-check, if the data point configuration seems sensible. Then download the configuration to the LINX-10X (see Section 7.7.12).

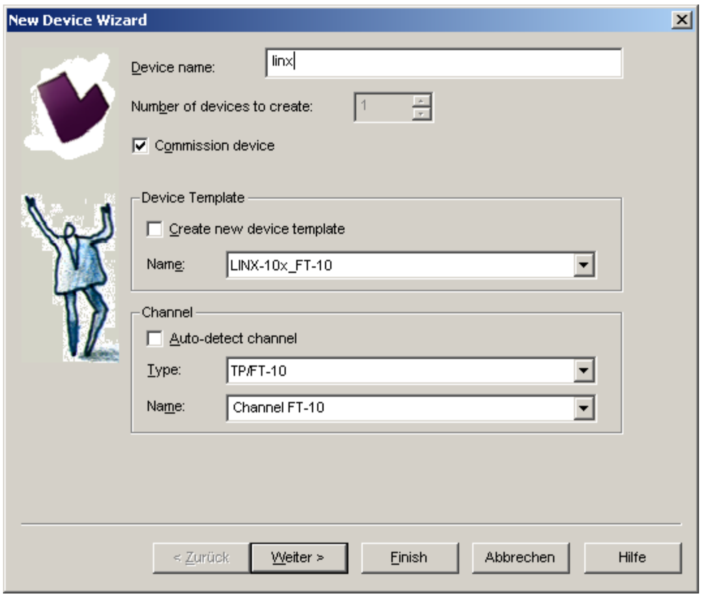
If using an LNS-based tool, the LINX-10X device needs to be replaced in that tool (see Section 7.6). If you are not using LNS, then refer to your network management tool's reference manual on how to replace a device. After replacing the device in the network management tool, reboot the LINX-10X (see Section 5.5).

7.5 Adding LINX-10X

To configure a LINX-10X in your LonMaker drawing, the device needs to be added to the LNS database and commissioned. This Section refers to LonMaker TE and describes how to add a LINX-10X to your database.

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 90.



New Device Wizard

Device name: linx

Number of devices to create: 1

☑ Commission device

Device Template

☐ Create new device template

Name: LINX-10x_FT-10

Channel

☐ Auto-detect channel

Type: TP/FT-10

Name: Channel FT-10

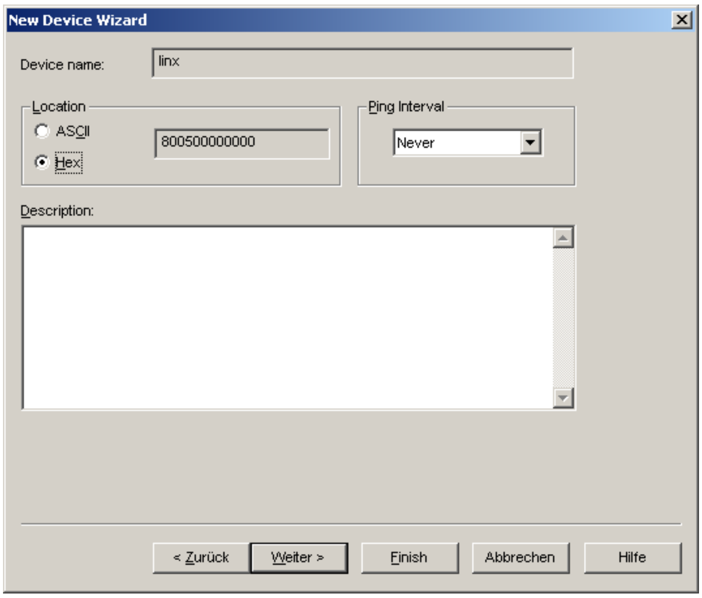
Figure 90: Create a new device in the drawing.

2. Select **Commission Device** if the LINX-10X is already connected to the network.

3. In the **Device Template** group box select the existing device template of the LINX-10X. Select "LINX-10x_FT-10", if the LINX-10X is configured to use the FT-10 interface, or "LINX-10x_IP-10L", if the LINX-10X 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 LINX-10X is connected to and click **Next**.

5. In the following dialog shown in Figure 91 appears. Click **Next**.



New Device Wizard

Device name: linx

Location

○ ASCII

● Hex

800500000000

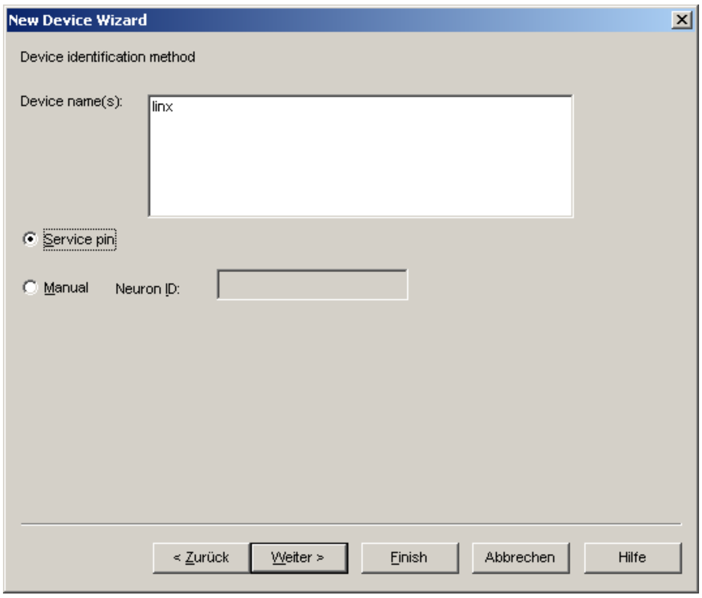
Ping Interval

Never

Description:

Figure 91: Leave defaults for Location.

6. Check Service Pin as the device identification method as shown in Figure 92 and click **Next**.



New Device Wizard

Device identification method

Device name(s): linx

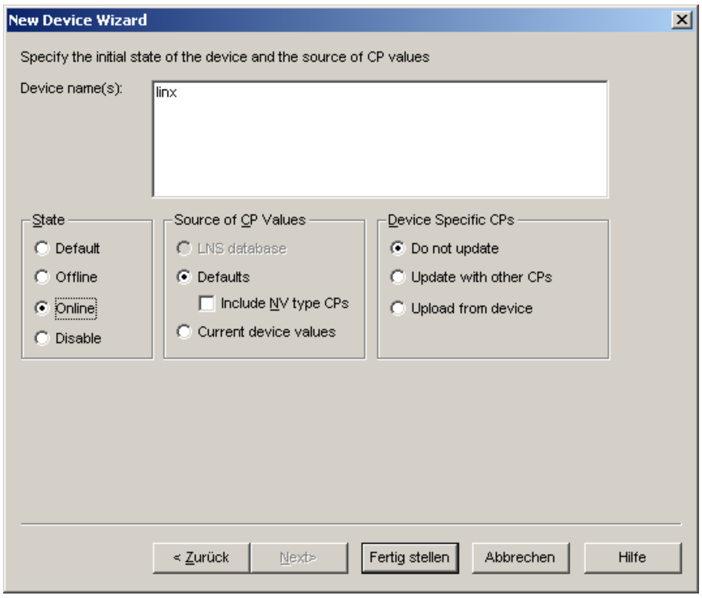
● Service pin

○ Manual Neuron ID:

Figure 92: Use Service Pin.

7. Click **Next** in the following screens until you get to the final dialog shown in Figure 93.

8. If the device is already on-net, select **Online**.



New Device Wizard

Specify the initial state of the device and the source of CP values

Device name(s): linx

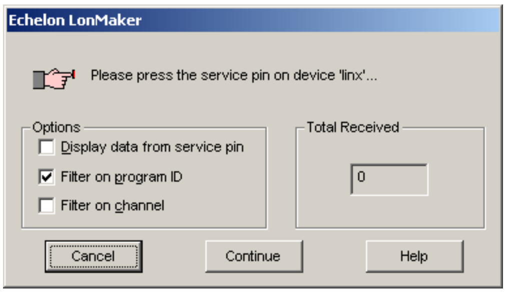
State
○ Default
○ Offline
● Online
○ Disable

Source of CP Values
○ LNS database
● Defaults
□ Include NV type CPs
○ Current device values

Device Specific CPs
● Do not update
○ Update with other CPs
○ Upload from device

Figure 93: Final dialog.

9. Click **Finish**. A dialog will prompt to press the service pin.



Echelon LonMaker

Please press the service pin on device 'linx'...

Options

□ Display data from service pin

☑ Filter on program ID

□ Filter on channel

Total Received

0

10. Finally, you should get the device added to your drawing as depicted in Figure 94.

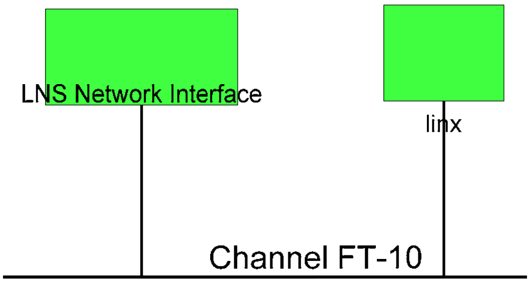


Figure 94: The LINX-10X has been added to the drawing.

7.6 Replace a LINX-10X

This Section describes how to replace as LINX-10X in your LNS database. The description refers to LonMaker TE. Let’s assume there is a device ‘linx’ in the LNS database as shown in Figure 95.

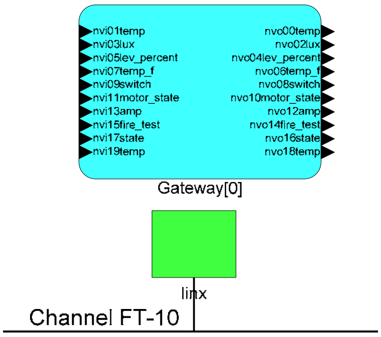
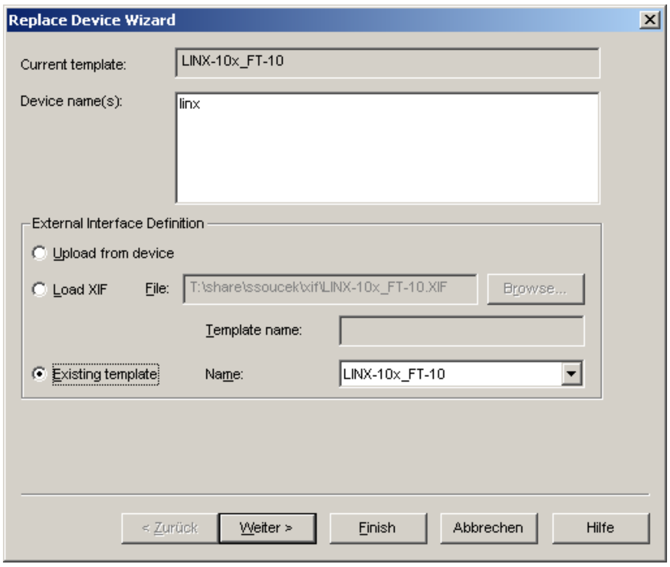


Figure 95: LonMaker drawing with one LINX-10X.

To Replace a Device in LonMaker TE

1. Select the device and right-click on the device shape.

2. Select **Commissioning → Replace…**. This opens the LonMaker Replace Device Wizard as shown in Figure 96.



Current template: LINX-10x_FT-10

Device name(s): linx

External Interface Definition

○ Upload from device

○ Load XIF File: T:\share\ssoucek\xif\LINX-10x_FT-10.XIF Browse...

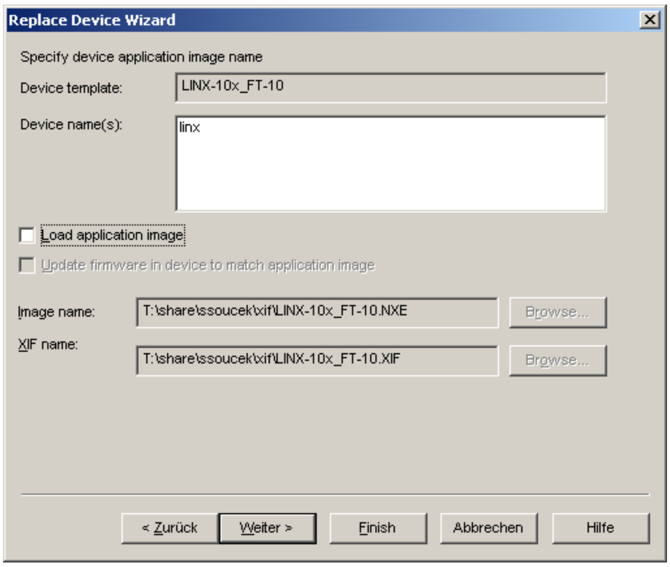
Template name:

● Existing template Name: LINX-10x_FT-10

Figure 96: LonMaker replace device wizard.

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

4. In the following window shown in Figure 97 click **Next**.



Specify device application image name

Device template: LINX-10x_FT-10

Device name(s): linx

□ Load application image

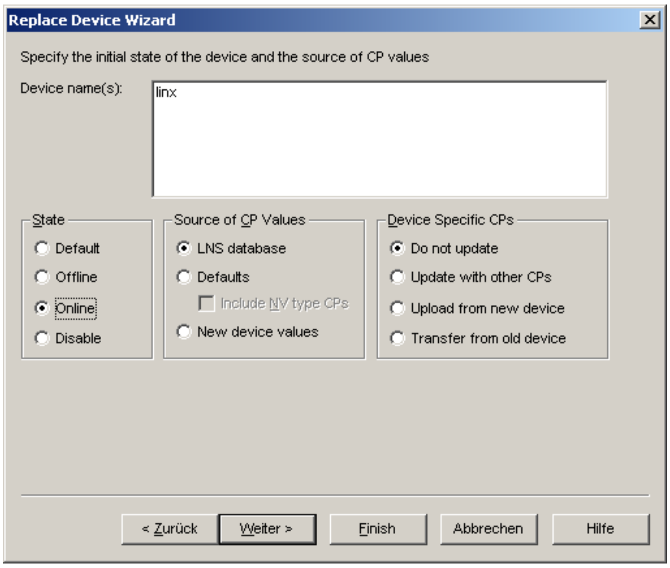
□ Update firmware in device to match application image

Image name: T:\share\ssoucek\xif\LINX-10x_FT-10.NXE Browse...

XIF name: T:\share\ssoucek\xif\LINX-10x_FT-10.XIF Browse...

Figure 97: Click Next without loading an application image.

5. Then select **Online** as shown in Figure 98.



Replace Device Wizard

Specify the initial state of the device and the source of CP values

Device name(s): linx

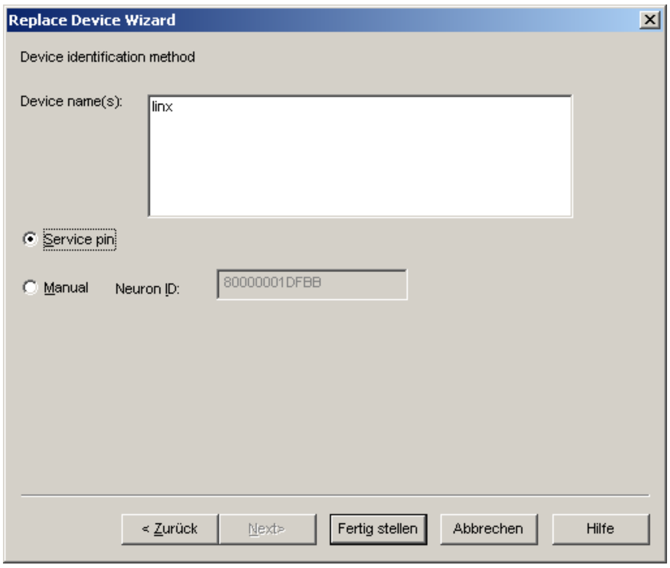
State
○ Default
○ Offline
● Online
○ Disable

Source of CP Values
● LNS database
○ Defaults
□ Include NV type CPs
○ New device values

Device Specific CPs
● Do not update
○ Update with other CPs
○ Upload from new device
○ Transfer from old device

Figure 98: Select online state.

6. Select the service pin method and click on **Finish** as shown in Figure 99.



Replace Device Wizard

Device identification method

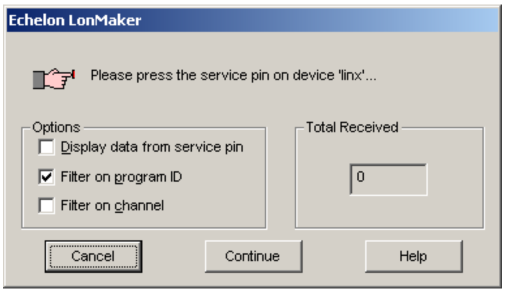
Device name(s): linx

● Service pin

○ Manual Neuron ID: 80000001DFBB

Figure 99: Select Service Pin and click Finish

7. Then the service pin requestor opens. Press the service pin on the replacement LINX-10X on the correct port. You can also send the service pin using the Web interface (see Section 5.1).



Echelon LonMaker

Please press the service pin on device 'linx'...

Options
☐ Display data from service pin
☑ Filter on program ID
☐ Filter on channel

Total Received: 0

8. After the service pin has been received, LonMaker commissions the replacement device, creates the dynamic NVs again (if any) and installs the bindings.

7.7 Using the LINX-10X Configurator

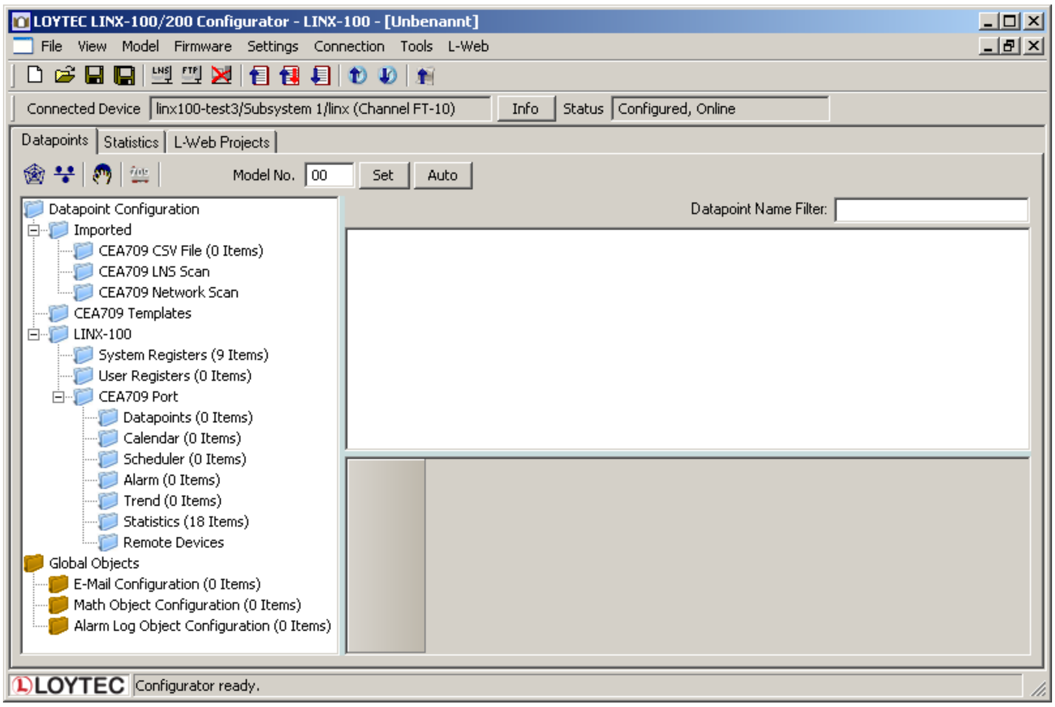
7.7.1 Starting as an LNS Plug-In

In LonMaker the plug-in is started by right clicking on the LINX-10X 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 LINX-10X node, then selecting the Option **LOYTEC LINX-10X Configurator** in the **PlugIns** sub menu.

In Alex the Plug-in is started by right clocking on the LINX-10X device and selecting the **LOYTEC LINX-10X Configurator** in the **Starte PlugIn** sub menu.

A window similar to what is shown in Figure 100 should appear.



LOYTEC LINX-100/200 Configurator - LINX-100 - [Unbenannt]

Connected Device: linx100-test3/Subsystem 1/linx (Channel FT-10)

Status: Configured, Online

Model No. 00

Datapoint Name Filter:

Configurator ready.

Figure 100: LINX-10X Configurator main window.

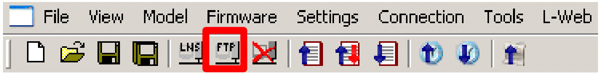
7.7.2 Starting Stand-Alone

The LINX-10X can also be used without LNS-based tools. In this case the LINX-10X Configurator needs to be started as a stand-alone application. Go to the Windows Start menu, select "Programs", "LOYTEC LINX-10X Configurator" and then click on "Configure LINX-10X". This starts the LINX-10X Configurator and the main connections screen is displayed.

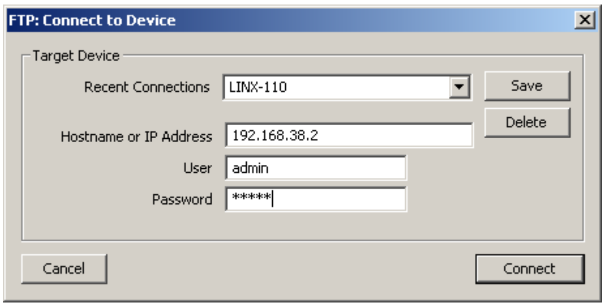
If the LINX-10X is not yet connected to the network, go to the Firmware menu and select the firmware version of the LINX-10X to be configured. If the LINX-10X is already connected to the network it is recommended to connect the configuration software to the LINX-10X.

To Connect to an LINX-10X Stand-Alone

1. Select the FTP connection method by clicking on the FTP connect button



in the tool bar of the main connections window. The FTP connect dialog as shown in Figure 101 opens.



Recent Connections: LINX-110
Hostname or IP Address: 192.168.38.2
User: admin
Password: *****

Figure 101: FTP connection dialog.

2. Enter the IP address of the LINX-10X, the user 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.

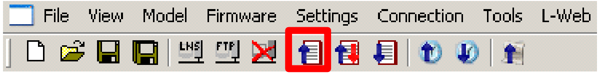
4. Click on **Connect**. This established the connection to the device.

7.7.3 Uploading the Configuration

To get the current network variable configuration of the LINX-10X, the port interface needs to be uploaded. This will upload the entire configuration from the LINX-10X, including data points, dynamic NVs and schedules.

To Upload a Configuration

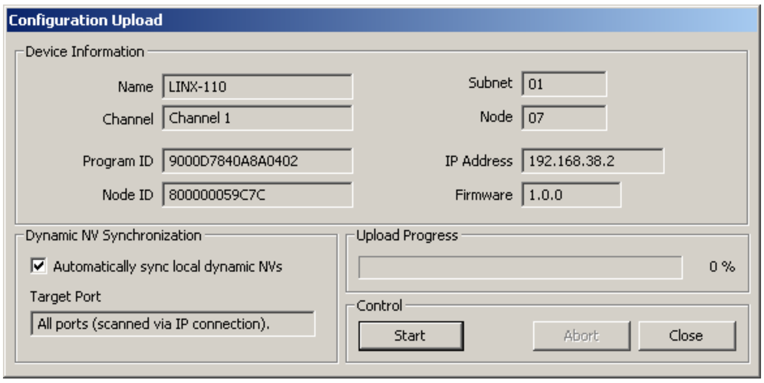
1. Click on the upload button



in the tool bar. The configuration upload dialog opens up as shown in Figure 102.

2. 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. If the LINX-10X is on-line, also

the current connection information and manually created dynamic NVs and schedules are uploaded.



Configuration Upload

Device Information

Name: LINX-110
Channel: Channel 1
Program ID: 9000D7840A8A0402
Node ID: 800000059C7C
Subnet: 01
Node: 07
IP Address: 192.168.38.2
Firmware: 1.0.0

Dynamic NV Synchronization

☑ Automatically sync local dynamic NVs

Target Port: All ports (scanned via IP connection).

Upload Progress: 0 %

Figure 102: Configuration upload dialog.

3. 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.

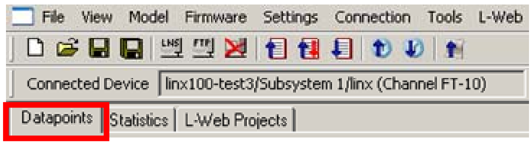
4. If dynamic NVs were synchronized, click on **Finish**.

7.7.4 Scanning for Network Variables

When the LINX-10X Configurator is connected to an LNS database, network variables can be scanned in from that data base.

To scan network variables from the LNS database

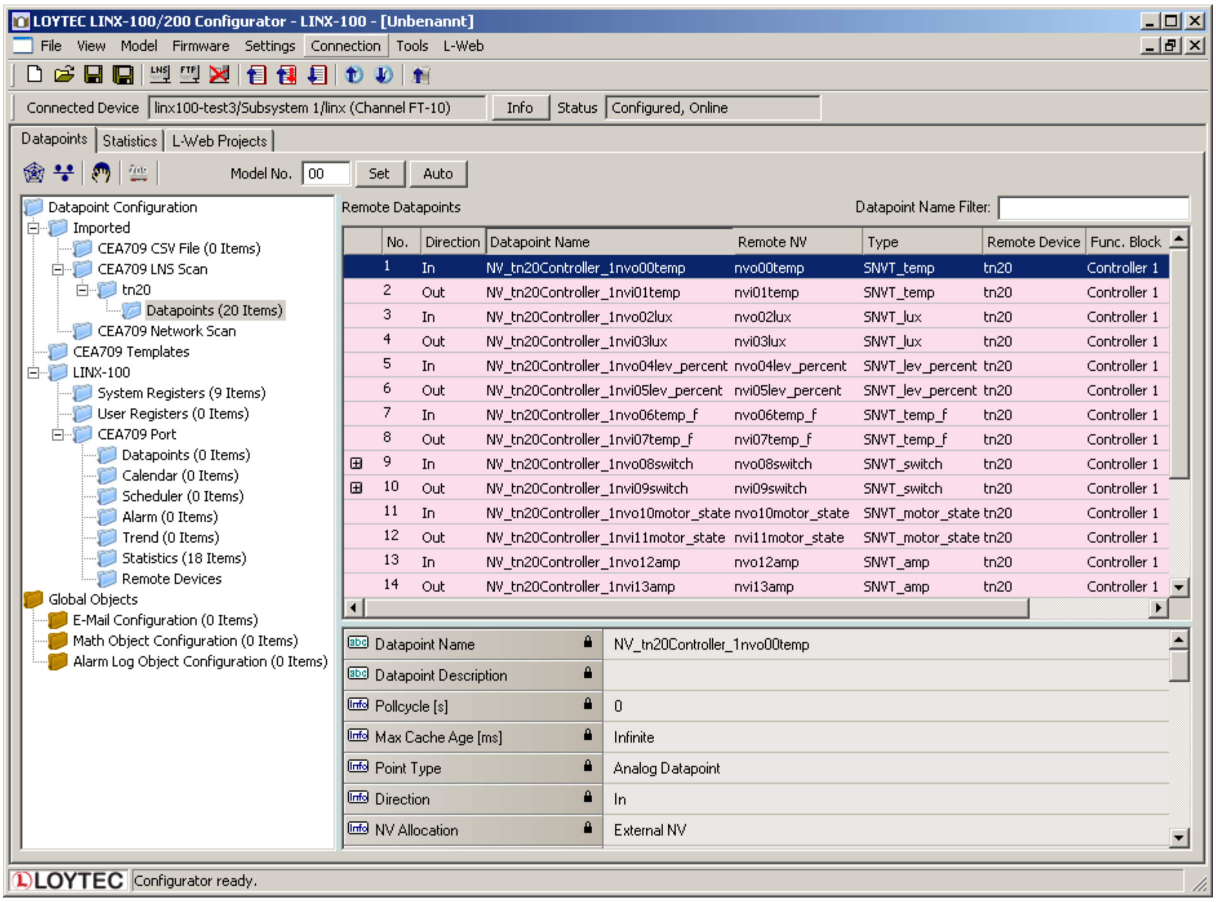
1. Click on the **Datapoints** tab.



Connected Device: linx100-test3/Subsystem 1/linx (Channel FT-10)

2. Click on the button **Scan channel**. This scans in all NVs on all devices connected to the CEA-709 channel of the LINX-10X.

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 convention "node name", "object name", "NV name". These names are ensured to be unique by adding a counter for multiple occurrences of the same name.



Connected Device: linx100-test3/Subsystem 1/linx (Channel FT-10)

Status: Configured, Online

Model No.: 00

No.	Direction	Datapoint Name	Remote NV	Type	Remote Device	Func. Block
1	In	NV_tn20Controller_1nvo00temp	nvo00temp	SNVT_temp	tn20	Controller 1
2	Out	NV_tn20Controller_1nvi01temp	nvi01temp	SNVT_temp	tn20	Controller 1
3	In	NV_tn20Controller_1nvo02lux	nvo02lux	SNVT_lux	tn20	Controller 1
4	Out	NV_tn20Controller_1nvi03lux	nvi03lux	SNVT_lux	tn20	Controller 1
5	In	NV_tn20Controller_1nvo04lev_percent	nvo04lev_percent	SNVT_lev_percent	tn20	Controller 1
6	Out	NV_tn20Controller_1nvi05lev_percent	nvi05lev_percent	SNVT_lev_percent	tn20	Controller 1
7	In	NV_tn20Controller_1nvo06temp_f	nvo06temp_f	SNVT_temp_f	tn20	Controller 1
8	Out	NV_tn20Controller_1nvi07temp_f	nvi07temp_f	SNVT_temp_f	tn20	Controller 1
⊞ 9	In	NV_tn20Controller_1nvo08switch	nvo08switch	SNVT_switch	tn20	Controller 1
⊞ 10	Out	NV_tn20Controller_1nvi09switch	nvi09switch	SNVT_switch	tn20	Controller 1
11	In	NV_tn20Controller_1nvo10motor_state	nvo10motor_state	SNVT_motor_state	tn20	Controller 1
12	Out	NV_tn20Controller_1nvi11motor_state	nvi11motor_state	SNVT_motor_state	tn20	Controller 1
13	In	NV_tn20Controller_1nvo12amp	nvo12amp	SNVT_amp	tn20	Controller 1
14	Out	NV_tn20Controller_1nvi13amp	nvi13amp	SNVT_amp	tn20	Controller 1

Datapoint Name	NV_tn20Controller_1nvo00temp
Datapoint Description	
Pollcycle [s]	0
Max Cache Age [ms]	Infinite
Point Type	Analog Datapoint
Direction	In
NV Allocation	External NV

Figure 103: Scanned NVs in the LNS Database Scan Folder

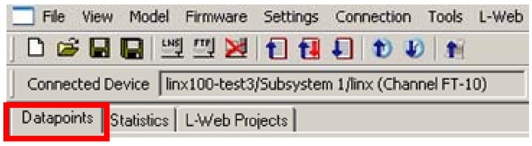
Figure 103 shows an example result of the database scan. The list can be sorted by each column. Selecting a line will display a number of associated properties in the property view below. Multiple items can be selected by using the <Ctrl> key and clicking with the mouse. All items can be selected by pressing <Ctrl-A>.

7.7.5 Importing Network Variables

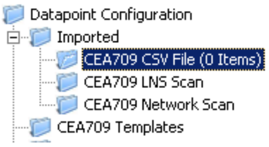
Without LNS, the tool cannot connect to an LNS database, where it scans for network variables (NVs). Therefore, the list of NVs to be used on LINX-10X has to be available in a CSV file. This file can be produced by external software or created by hand. The CSV format for importing NVs is defined in 10.2.1.

To Import NVs from a File

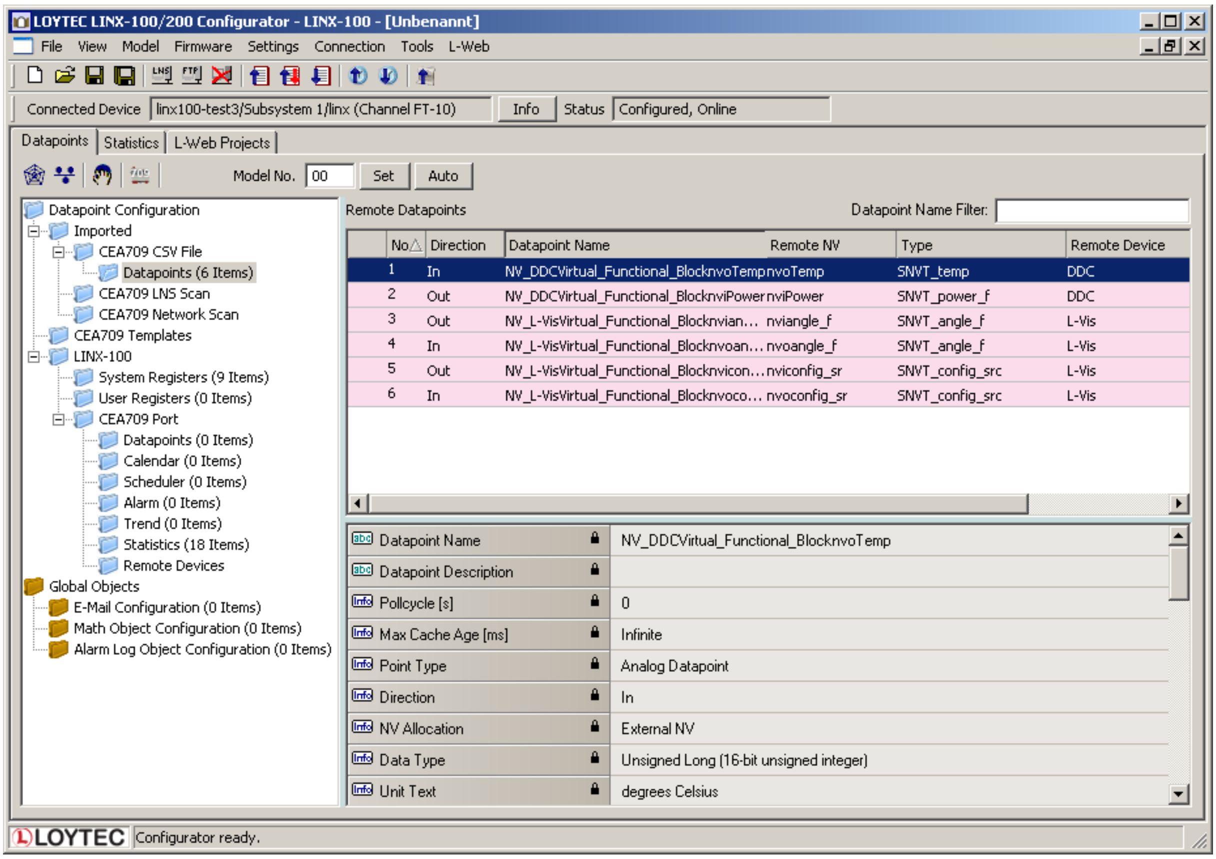
1. Click on the **Datapoints** tab.


File View Model Firmware Settings Connection Tools L-Web
Connected Device
linx100-test3/Subsystem 1/linx (Channel FT-10)
Datapoints
Statistics
L-Web Projects

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**.



Connected Device: linx100-test3/Subsystem 1/linx (Channel FT-10)

Status: Configured, Online

Model No.: 00

No△	Direction	Datapoint Name	Remote NV	Type	Remote Device
1	In	NV_DDCVirtual_Functional_BlocknvoTemp	nvoTemp	SNVT_temp	DDC
2	Out	NV_DDCVirtual_Functional_BlocknviPower	nviPower	SNVT_power_f	DDC
3	Out	NV_L-VisVirtual_Functional_Blocknvian...	nviangle_f	SNVT_angle_f	L-Vis
4	In	NV_L-VisVirtual_Functional_Blocknvoan...	nvoangle_f	SNVT_angle_f	L-Vis
5	Out	NV_L-VisVirtual_Functional_Blocknvicon...	nviconfig_sr	SNVT_config_src	L-Vis
6	In	NV_L-VisVirtual_Functional_Blocknvoco...	nvoconfig_sr	SNVT_config_src	L-Vis

Datapoint Name	NV_DDCVirtual_Functional_BlocknvoTemp
Datapoint Description	
Pollcycle [s]	0
Max Cache Age [ms]	Infinite
Point Type	Analog Datapoint
Direction	In
NV Allocation	External NV
Data Type	Unsigned Long (16-bit unsigned integer)
Unit Text	degrees Celsius

Configurator ready.

Figure 104: Imported NVs

4. Now the CSV File folder is populated with the imported NVs as shown in Figure 104.

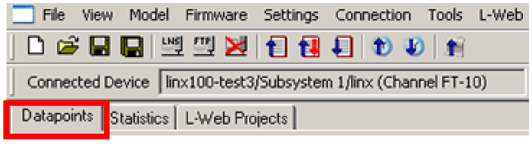
The list can be sorted by each column. Selecting a line will display a number of associated properties in the property view below. Multiple items can be selected by using the <Ctrl> key and clicking with the mouse. All items can be selected by pressing <Ctrl-A>.

7.7.6 Scanning NVs online from the Network

LINX-10X devices also support an online network scan on the CEA-709 network. In this scan the devices 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.

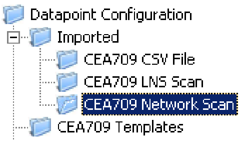
To scan NV online of the CEA-709 network

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



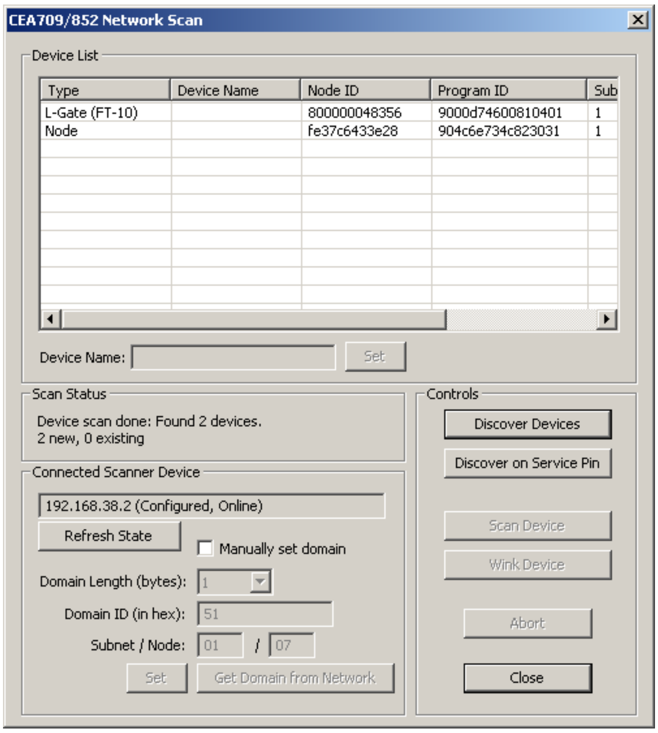
Connected Device: linx100-test3/Subsystem 1/linx (Channel FT-10)

2. Select the folder CEA709 Network Scan



3.

4. Right-click on that folder and select **Scan CEA709/852 Network…**. This opens the CEA709/852 Network Scan dialog as shown in Figure 105.



Type	Device Name	Node ID	Program ID	Sub
L-Gate (FT-10)		800000048356	9000d74600810401	1
Node		fe37c6433e28	904c6e734c823031	1

Device scan done: Found 2 devices.
2 new, 0 existing

192.168.38.2 (Configured, Online)

☐ Manually set domain

Domain Length (bytes): 1

Domain ID (in hex): 51

Subnet / Node: 01 / 07

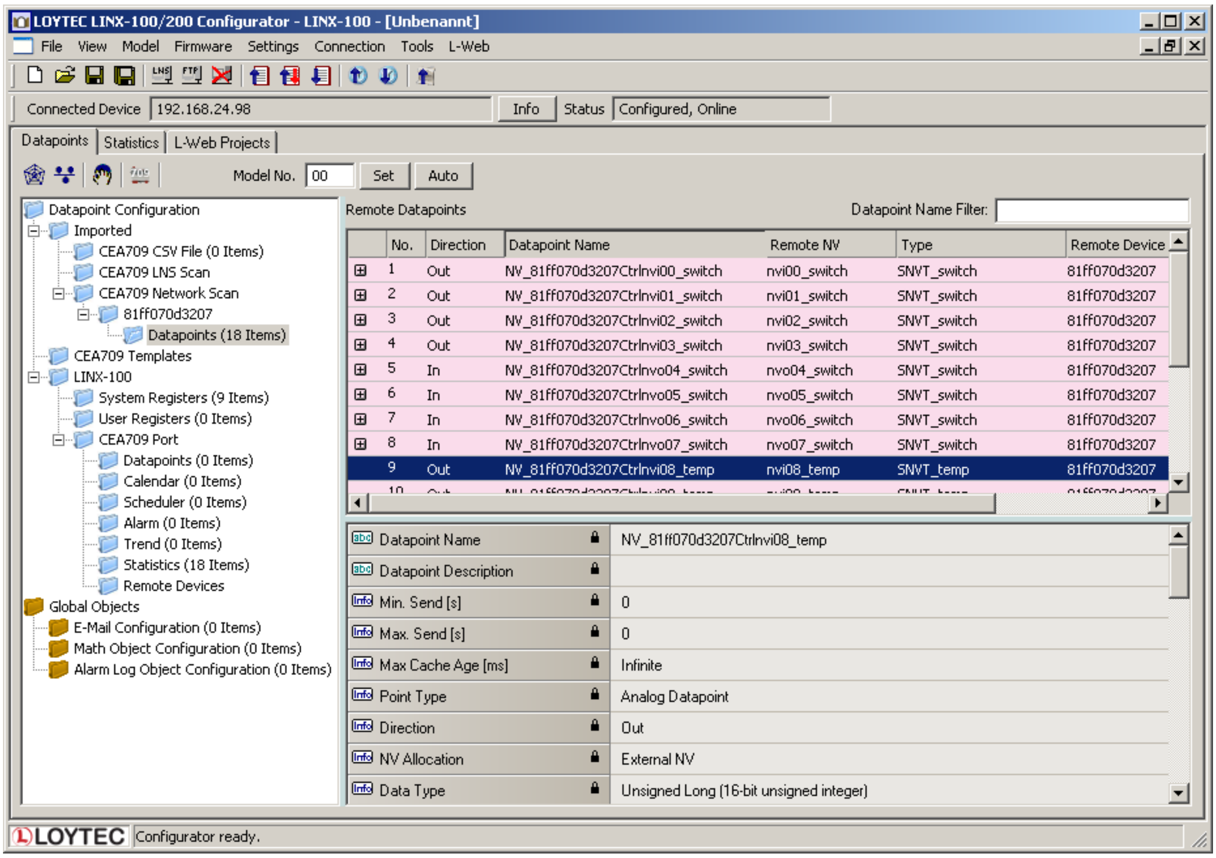
Figure 105: CEA-709 network scan dialog.

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

6. 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.

7. 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 106.

Tip! *If you are not sure, which device you have selected, click on **Wink Device**. The selected device will execute its wink sequence.*


LOYTEC LINX-100/200 Configurator - LINX-100 - [Unbenannt]
File View Model Firmware Settings Connection Tools L-Web
Connected Device 192.168.24.98
Info
Status Configured, Online
Datapoints Statistics L-Web Projects
Model No. 00
Set
Auto
Datapoint Configuration
Imported
CEA709 CSV File (0 Items)
CEA709 LNS Scan
CEA709 Network Scan
81ff070d3207
Datapoints (18 Items)
CEA709 Templates
LINX-100
System Registers (9 Items)
User Registers (0 Items)
CEA709 Port
Datapoints (0 Items)
Calendar (0 Items)
Scheduler (0 Items)
Alarm (0 Items)
Trend (0 Items)
Statistics (18 Items)
Remote Devices
Global Objects
E-Mail Configuration (0 Items)
Math Object Configuration (0 Items)
Alarm Log Object Configuration (0 Items)
Remote Datapoints
Datapoint Name Filter:
LOYTEC Configurator ready.

No.	Direction	Datapoint Name	Remote NV	Type	Remote Device
1	Out	NV_81ff070d3207CtrlnvI00_switch	nvi00_switch	SNVT_switch	81ff070d3207
2	Out	NV_81ff070d3207CtrlnvI01_switch	nvi01_switch	SNVT_switch	81ff070d3207
3	Out	NV_81ff070d3207CtrlnvI02_switch	nvi02_switch	SNVT_switch	81ff070d3207
4	Out	NV_81ff070d3207CtrlnvI03_switch	nvi03_switch	SNVT_switch	81ff070d3207
5	In	NV_81ff070d3207Ctrlnvo04_switch	nvo04_switch	SNVT_switch	81ff070d3207
6	In	NV_81ff070d3207Ctrlnvo05_switch	nvo05_switch	SNVT_switch	81ff070d3207
7	In	NV_81ff070d3207Ctrlnvo06_switch	nvo06_switch	SNVT_switch	81ff070d3207
8	In	NV_81ff070d3207Ctrlnvo07_switch	nvo07_switch	SNVT_switch	81ff070d3207
9	Out	NV_81ff070d3207CtrlnvI08_temp	nvi08_temp	SNVT_temp	81ff070d3207

Datapoint Name	NV_81ff070d3207CtrlnvI08_temp
Datapoint Description	
Min. Send [s]	0
Max. Send [s]	0
Max Cache Age [ms]	Infinite
Point Type	Analog Datapoint
Direction	Out
NV Allocation	External NV
Data Type	Unsigned Long (16-bit unsigned integer)

Figure 106: CEA-709 network scan results.

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

7.7.7 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 LINX-10X. Select those NVs, which shall be connected IEC61131 variables.

To Use NVs on the LINX-10X

1. Go to any of the "LNS database scan", "CEA709/852 Network Scan" or the "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 LINX-10X/CEA709 Port folder. All data points in that folder will actually be created on the LINX-10X 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.*

7.7.8 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 LINX-10X/CEA709 port folder. This default allocation can be changed, e.g., for imported NVs when they shall be allocated as static NVs on the LINX-10X.

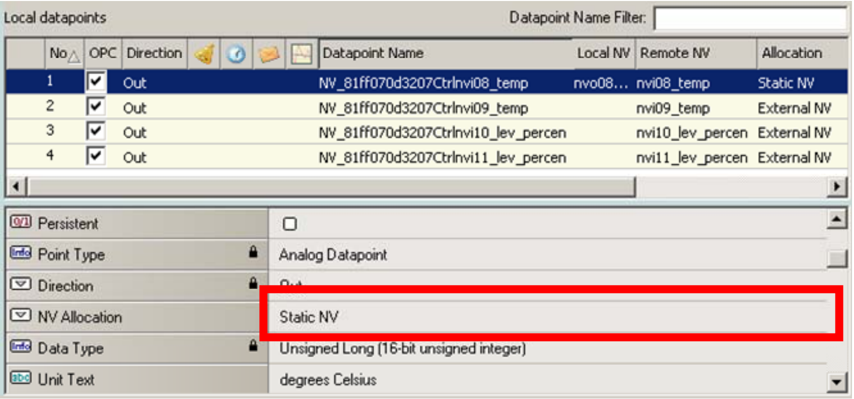
To Change the NV Allocation Type

1. In the data point view select the NVs in the LINX-10X/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 107.

3. To make the data points static NVs on the LINX-10X, select **Static NV**.



Local datapoints Datapoint Name Filter:

No	OPC	Direction					Datapoint Name	Local NV	Remote NV	Allocation
1	☑	Out					NV_81ff070d3207Ctrlnvi08_temp	nvo08…	nvi08_temp	Static NV
2	☑	Out					NV_81ff070d3207Ctrlnvi09_temp		nvi09_temp	External NV
3	☑	Out					NV_81ff070d3207Ctrlnvi10_lev_percen		nvi10_lev_percen	External NV
4	☑	Out					NV_81ff070d3207Ctrlnvi11_lev_percen		nvi11_lev_percen	External NV

Persistent	□
Point Type	Analog Datapoint
Direction	Out
NV Allocation	Static NV
Data Type	Unsigned Long (16-bit unsigned integer)
Unit Text	degrees Celsius

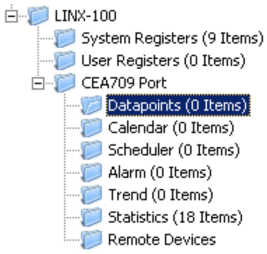
Figure 107: Change the NV allocation type.

7.7.9 Create Static NVs

The LINX-10X 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 LINX-10X/CEA-709 folder.

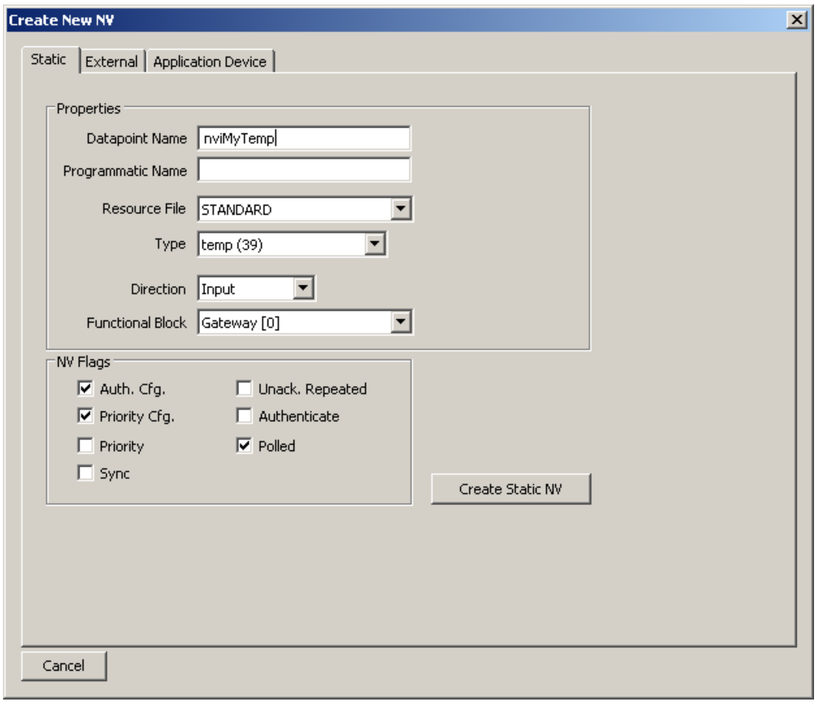
To Create Static NVs Manually

1. Select the LINX-10X/CEA-709 Port/Datapoint folder



- LINX-100
  - System Registers (9 Items)
  - User Registers (0 Items)
  - CEA709 Port
    - Datapoints (0 Items)
    - Calendar (0 Items)
    - Scheduler (0 Items)
    - Alarm (0 Items)
    - Trend (0 Items)
    - Statistics (18 Items)
    - Remote Devices

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 108.



Properties

Datapoint Name: nviMyTemp

Programmatic Name:

Resource File: STANDARD

Type: temp (39)

Direction: Input

Functional Block: Gateway [0]

NV Flags

☑ Auth. Cfg.

☑ Priority Cfg.

□ Priority

□ Sync

□ Unack. Repeated

□ Authenticate

☑ Polled

Figure 108: 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.

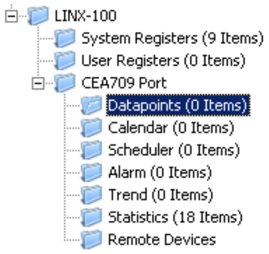
8. Note, that thse static interface of the LINX-10X will change as soon as static NVs are added or modified in the data point manager. This change is reflected in a new model number, which the LINX-10X will have after the configuration download (see Section 6.4.2). Also note that the manually created static NVs are not bound automatically by the LINX-10X Configurator. They simply appear on the device and need to be bound in the network management tool.

7.7.10 Create External NVs

External NVs are not actually allocated NVs on the LINX-10X. Instead, the LINX-10X uses polling to read data from and explicit updates to write data to external NVs. Since external NVs are not affecting the static NV interface of the LINX-10X, they can be used to extend an LINX-10X’s interface configuration at run-time, when no LNS with dynamic NVs is available.

To Create an External NV manually

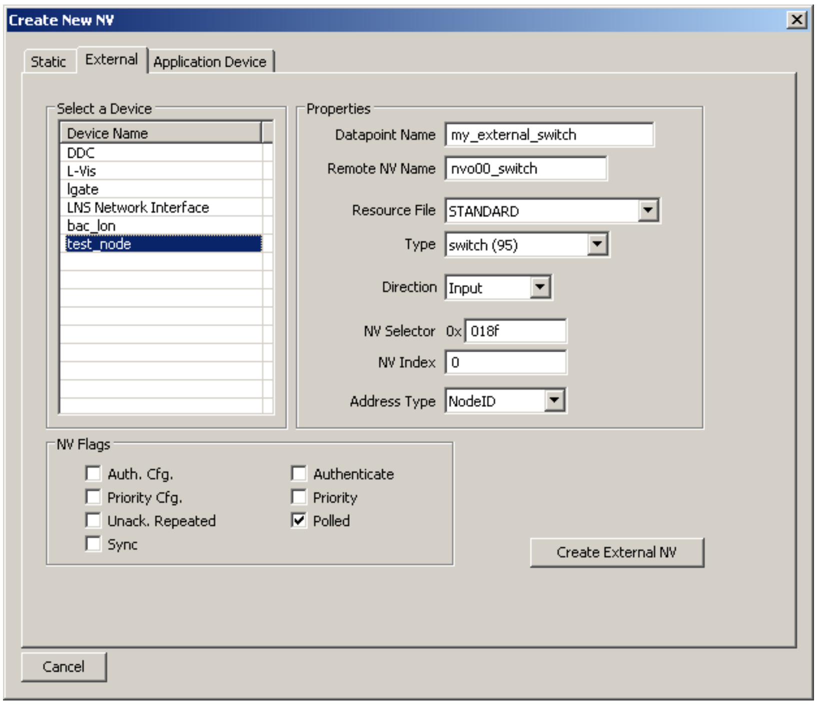
1. Select the LINX-10X/CEA-709 Port/Datapoints folder



LINX-100
- System Registers (9 Items)
- User Registers (0 Items)
- CEA709 Port
  - Datapoints (0 Items)
  - Calendar (0 Items)
  - Scheduler (0 Items)
  - Alarm (0 Items)
  - Trend (0 Items)
  - Statistics (18 Items)
  - Remote Devices

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 109.



Select a Device

Device Name
DDC
L-Vis
lgate
LNS Network Interface
bac_lon
test_node

Properties

Datapoint Name: my_external_switch
Remote NV Name: nvo00_switch
Resource File: STANDARD
Type: switch (95)
Direction: Input
NV Selector: 0x 018f
NV Index: 0
Address Type: NodeID

NV Flags

□ Auth. Cfg.
□ Priority Cfg.
□ Unack. Repeated
□ Sync
□ Authenticate
□ Priority
☑ Polled

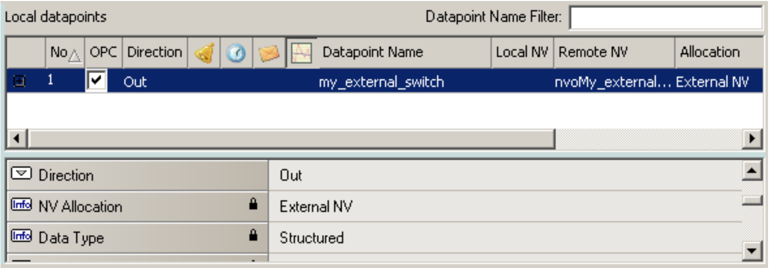
Figure 109: Create a new external NV.

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 LINX-10X. Therefore, the remote output NV nvo00_switch becomes an input on the LINX-10X. Also enter the NV selector in hexadecimal and the NV index in decimal. 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 port interface definition as shown in Figure 110. For external NVs, which are inputs to the LINX-10X, adapt the poll cycle property to your needs.



No	OPC	Direction	Datapoint Name	Local NV	Remote NV	Allocation
1	☑	Out	my_external_switch		nvoMy_external...	External NV

Direction	Out
NV Allocation	External NV
Data Type	Structured

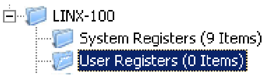
Figure 110: Manually created external NV in the port interface definition.

7.7.11 Create User Registers

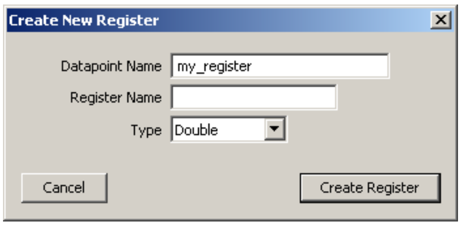
User registers are data points on the device that do not have a representation on the network. Thus, they are not accessible over a specific technology. A register merely serves as a container for intermediate data (e.g., results of math objects). Since a register has not network direction, it can be written and read. Therefore, two data points are generated for each register, one for writing the register (output) and one for reading the register (input).

To Create a User Register

1. Select the LINX-10X/User Registers folder



2. Right-click in the data point list and select **New Datapoint…** in the context menu. This opens the register creation dialog as shown in Figure 111.



Datapoint Name: my_register

Register Name:

Type: Double

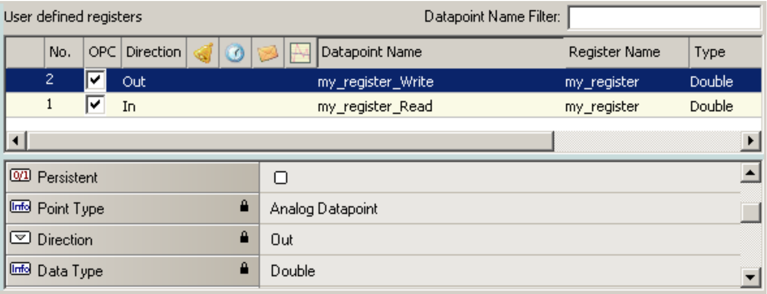
Figure 111: Create a user register.

3. Enter a **Datapoint Name** for the register. You may leave the **Register Name** blank to give the underlying register the same name as the data point.

4. Select a **Type**. Available are “Double”, “Boolean”, or “Signed Integer”.

5. Click **Create Register**.

6. Two data points now appear for the register, one for writing the register and one for reading the register as shown in Figure 112.



User defined registers

Datapoint Name Filter:

No.	OPC	Direction	Datapoint Name	Register Name	Type
2	☑	Out	my_register_Write	my_register	Double
1	☑	In	my_register_Read	my_register	Double

Persistent	□
Point Type	Analog Datapoint
Direction	Out
Data Type	Double

Figure 112: Manually created user register.

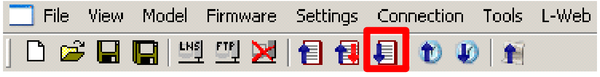
7.7.12 Configuration Download

After the data points have been configured, the configuration needs to be downloaded to the LINX-10X. For doing so, the LINX-10X must be online. If the LINX-10X 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 LINX-10X are "Static NV" or "Dynamic NV", the LINX-10X 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



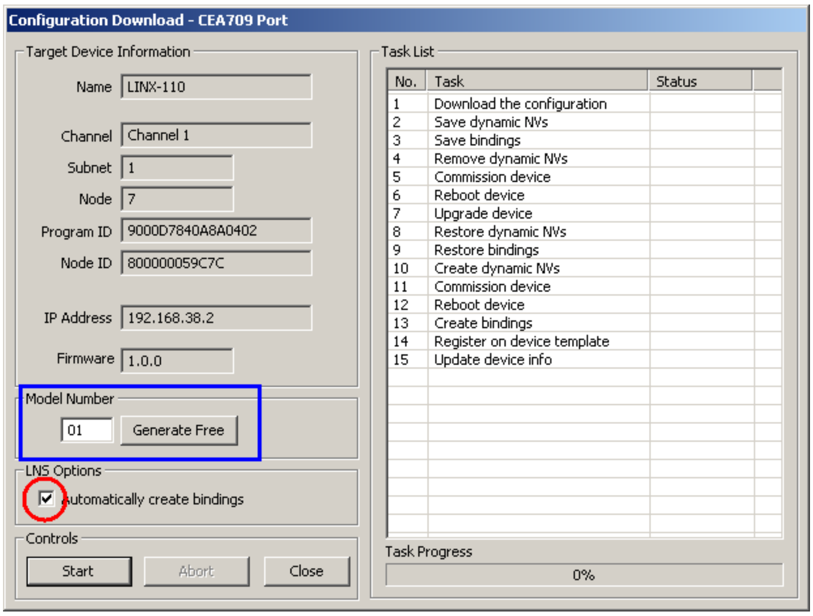
   in the tool bar of the main connections window. This will open the configuration download dialog as shown in Figure 113.

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

3. If the static NV interface has been changed, a new model number for the LINX-10X needs to be selected. This is necessary, as the static network interface of the LINX-10X changes on the CEA-709 network. The LINX-10X Configurator automatically selects a usable value, which can be overridden in the field **Model Number** marked by the blue rectangle in Figure 113.

4. 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.

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



Configuration Download - CEA709 Port

Target Device Information

Name: LINX-110

Channel: Channel 1

Subnet: 1

Node: 7

Program ID: 9000D7840A8A0402

Node ID: 800000059C7C

IP Address: 192.168.38.2

Firmware: 1.0.0

Model Number: 01

LNS Options

☑ Automatically create bindings

Controls

Task List

No.	Task	Status
1	Download the configuration	
2	Save dynamic NVs	
3	Save bindings	
4	Remove dynamic NVs	
5	Commission device	
6	Reboot device	
7	Upgrade device	
8	Restore dynamic NVs	
9	Restore bindings	
10	Create dynamic NVs	
11	Commission device	
12	Reboot device	
13	Create bindings	
14	Register on device template	
15	Update device info	

Task Progress

0%

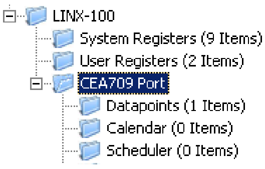
Figure 113: Configuration Download Dialog

Note, that after the download is complete, the interface changes become active on the LINX-10X (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 LINX-10X Configurator (e.g., use the menu "LonMaker|Refresh" in LonMaker or hit *F5* in NL-220).

7.7.13 Build XIF for Port Interface

When using static NVs on the LINX-10X, the LINX-10X Configurator can export a new XIF file for the changed static interface. To create a XIF file do the following:

1. Select the LINX-100/CEA-709 Port folder



```
LINX-100
  System Registers (9 Items)
  User Registers (2 Items)
  CEA709 Port
    Datapoints (1 Items)
    Calendar (0 Items)
    Scheduler (0 Items)
```

2. Right-click on that folder and in the context menu select **Build XIF …**.

3. This opens a file requestor where the XIF file name needs to be entered. Select a useful name to identify the LINX-10X, e.g. as "linx-10X_1.xif".

7.7.14 Enable Legacy NM Mode

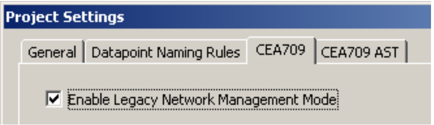
For network management tools, which do not support the ECS (enhanced command set) network management commands, the legacy network management mode must be configured. Please contact the tool's vendor for information whether ECS is supported or not. Note, that changing to legacy network management mode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

To Enable Legacy NM Mode

1. In the LINX-10X Configurator menu go to **Settings → Project settings …**

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

3. Put a check mark in **Enable Legacy Network Management Mode**.



☑ Enable Legacy Network Management Mode

4. Click **Ok.**

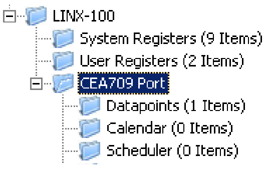
5. Download the configuration to activate the change.

7.7.15 Upload Dynamic NVs from Device

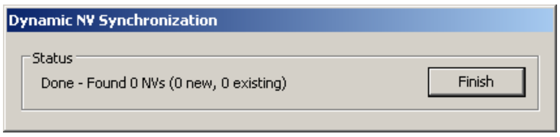
In LNS-based tools it is possible to create dynamic NVs on the device manually. This is a possible workflow to engineer the NV interface of the device in the LNS database. To use those manually created dynamic NVs, the LINX-10X Configurator must synchronize its dynamic NV information with the port.

To Upload Dynamic NVs

1. Select the **CEA709 Port** folder.



2. Right-click and select **Sync Dynamic NVs** in the context menu. The LINX-10X 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.



Done - Found 0 NVs (0 new, 0 existing)

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.

7.7.16 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 LINX-10X results in a file transfer.

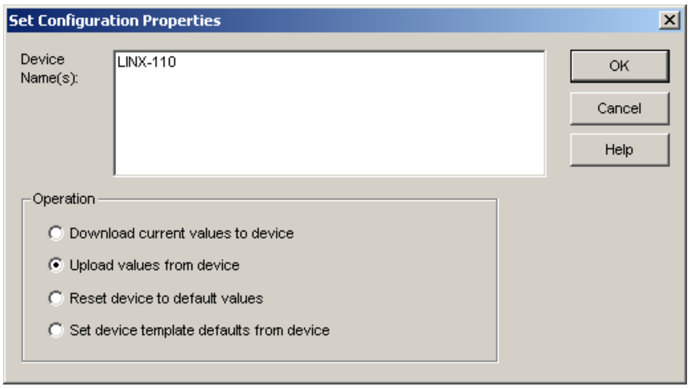
The LINX-10X supports both, the LONMARK file transfer and the simpler direct memory read/write method. In both cases, however, one has to keep in mind that a file transfer incurs more overhead than a simple NV read/write. Therefore, polling CPs should be done at a much slower rate than polling NVs.

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 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 115.



Set Configuration Properties

Device Name(s): LINX-110

Operation

○ Download current values to device
● Upload values from device
○ Reset device to default values
○ Set device template defaults from device

Figure 115: Set Configuration Properties in LonMaker TE.

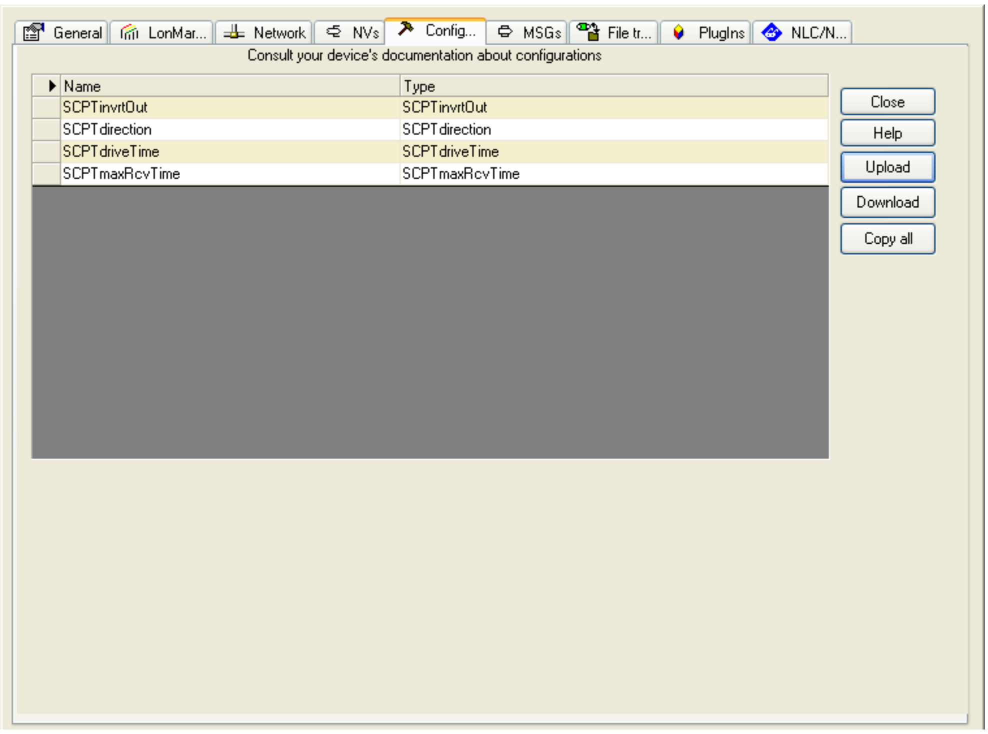
3. In this dialog select the radio button Upload values from device in the **Operation** group box. To use the current settings of the device as default values for new devices, select Set device template defaults from device.

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

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).



Consult your device's documentation about configurations

Name	Type
SCPTinvrtOut	SCPTinvrtOut
SCPTdirection	SCPTdirection
SCPTdriveTime	SCPTdriveTime
SCPTmaxRcvTime	SCPTmaxRcvTime

Figure 116: Configuration Tab for Configuration Properties in NL220.

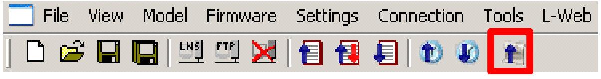
7.7.17 Upload the System Log

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 LINX-10X Configurator.

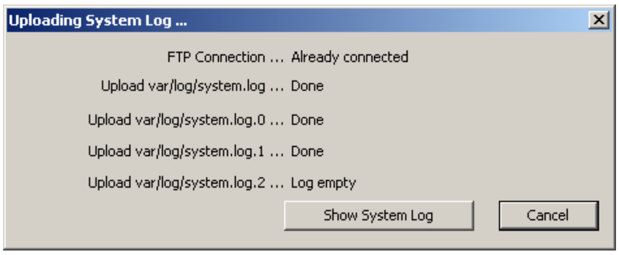
To Upload the System Log

1. Connect to the LINX-10X via the FTP or LNS method (see Section 7.7.2).

2. Click on the Upload system log button



in the tool bar. The upload system log dialog as shown in Figure 117 opens showing the upload progress.

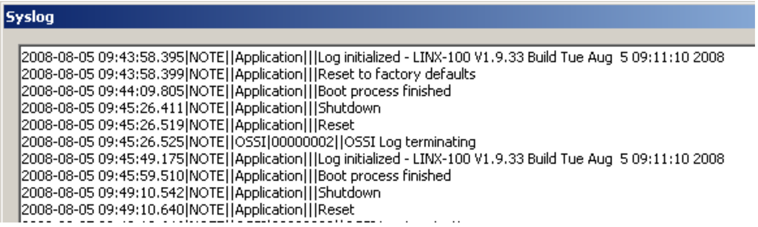


Uploading System Log ...

FTP Connection ... Already connected
Upload var/log/system.log ... Done
Upload var/log/system.log.0 ... Done
Upload var/log/system.log.1 ... Done
Upload var/log/system.log.2 ... Log empty

Figure 117: Upload system log dialog.

3. When the upload is finished, click on **Show System Log**. The system log window appears as shown in Figure 118.



```
2008-08-05 09:43:58.395|NOTE||Application|||Log initialized - LINX-100 V1.9.33 Build Tue Aug  5 09:11:10 2008
2008-08-05 09:43:58.399|NOTE||Application|||Reset to factory defaults
2008-08-05 09:44:09.805|NOTE||Application|||Boot process finished
2008-08-05 09:45:26.411|NOTE||Application|||Shutdown
2008-08-05 09:45:26.519|NOTE||Application|||Reset
2008-08-05 09:45:26.525|NOTE||OSSI|00000002||OSSI Log terminating
2008-08-05 09:45:49.175|NOTE||Application|||Log initialized - LINX-100 V1.9.33 Build Tue Aug  5 09:11:10 2008
2008-08-05 09:45:59.510|NOTE||Application|||Boot process finished
2008-08-05 09:49:10.542|NOTE||Application|||Shutdown
2008-08-05 09:49:10.640|NOTE||Application|||Reset
```

Figure 118: System log window.

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

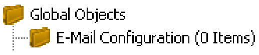
7.8 E-Mail Templates

7.8.1 Create an E-Mail Template

E-Mail templates are used to assemble and transmit E-Mails when certain trigger conditions occur. The E-Mail template contains the destination E-Mail address, the subject, and text. Variable parameters can be added to the text by using data point sources. The transmission of an E-Mail is triggered by one or more trigger data points. For setting up E-Mails, the E-Mail account information has to be configured on the device, e.g. on the Web UI (see Section 5.2.13).

To Create an E-Mail Template

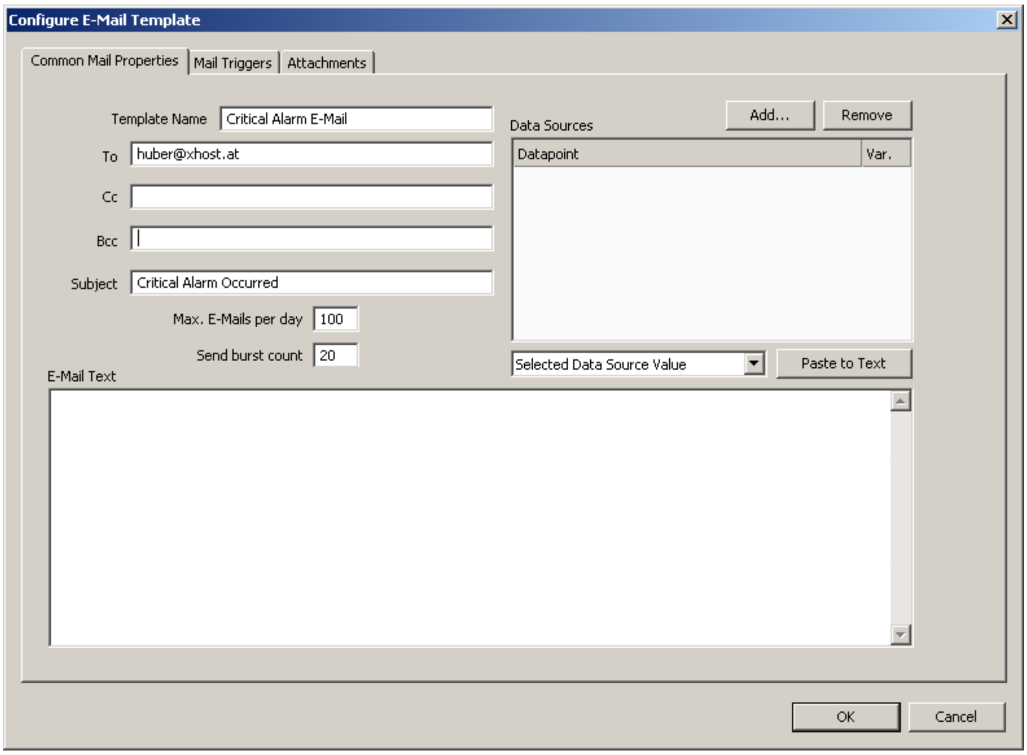
1. Under the **Global Objects** folder, select the **E-Mail Configuration** sub-folder.



Global Objects
E-Mail Configuration (0 Items)

2. Right-click and select **New E-Mail Template …** from the context menu.

3. In the **Configure E-Mail Template** dialog, which is shown in Figure 119 enter the **To** address and the **Subject**. Optionally, **Cc** and **Bcc** addresses can be specified.



Template Name: Critical Alarm E-Mail

To: huber@xhost.at

Cc:

Bcc:

Subject: Critical Alarm Occurred

Max. E-Mails per day: 100

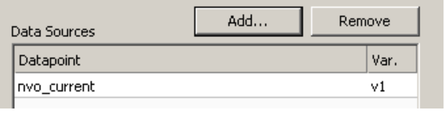
Send burst count: 20

Figure 119: Configure E-Mail Template Dialog.

4. Enter text in the **E-Mail Text** multi-line field.

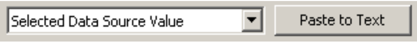
5. If the E-Mail text shall contain values of data points, add data points to the **Data Sources** list by clicking the **Add…** button.

6. A data point selector dialog opens. Select one or more data points and click **Ok**. The selected data point appears in the **Data Sources** list.



Datapoint	Var.
nvo_current	v1

7. Select the data point in the **Data Sources** list. In the drop-down box underneath select **Selected Data Source Value** and click the **Paste to Text** button.



Selected Data Source Value

8. A place holder `%{v1}` for the data point value appears now in the E-Mail text.

7.8.2 Trigger E-Mails

E-Mail templates are used to assemble and transmit E-Mails when certain trigger conditions occur. For an E-Mail template, one or more trigger conditions can be defined. The E-Mail will be sent, when one of the trigger conditions is activated. Depending of the trigger data point type, the trigger conditions can be refined.

Note, that the behavior of the trigger data point is influenced by the COV properties of the data point. If the **Only notify on COV** property is checked, the data point triggers only if its value changes to the value of the trigger condition. If that property is not checked, the data point triggers on every write with a value that matches the trigger condition.

The trigger for sending an E-Mail can be enabled or disabled altogether by using an *enable* data point. This data point must be of type *binary*. If the value of that enable data point is TRUE, the trigger conditions are evaluated. If the value of the enable is FALSE, no E-Mails are be triggered.

To Create an E-Mail Trigger

1. Under the **Global Objects** folder, select the **E-Mail Configuration** sub-folder.

2. Right-click and select **Configure E-Mail Template …** from the context menu.

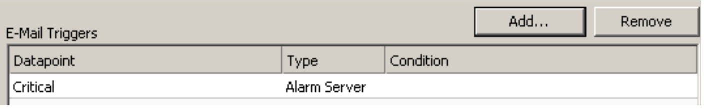
3. Change to the **Mail Triggers** tab.

Note: *Of course, you can also change directly to the* ***Mail Triggers*** *tab when creating an E-Mail template.*

4. Click the **Add…** button. A data point selection dialog opens.

5. Select one or more data point and click **Ok**.

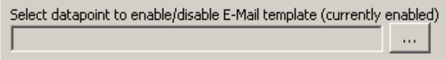
6. The triggers appear now in the **Mail Triggers** list. The data points that server as E-Mail triggers also appear with the E-Mail icon ✉ in the data point list.



Datapoint	Type	Condition
Critical	Alarm Server	

7. In the **Manage Trigger Conditions** you can refine the trigger condition depending on the trigger data point class.

8. If the trigger condition is depending on the value of an enabling data point, you can add an enable data point by clicking on the **…** button.


Select datapoint to enable/disable E-Mail template (currently enabled)
...

9. To remove such a trigger enable, click the **Remove Enable Trigger** button.

7.8.3 Attachments

E-Mail templates can be configured to have file attachments. Basically, any file of the device can be specified as an attachment.

To Configure Attachments

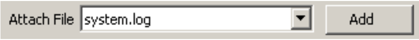
1. Under the **Global Objects** folder, select the **E-Mail Configuration** sub-folder.

2. Right-click and select **Configure E-Mail Template …** from the context menu.

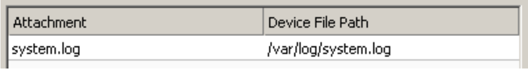
3. Change to the **Attachments** tab.

Note: *Of course, you can also change directly to the* ***Attachments*** *tab when creating an E-Mail template.*

4. Select an available file from the **Attach File** drop-down box.


Attach File: system.log

5. Click the **Add** button. The file appears in the **Attachments** list.



Attachment	Device File Path
system.log	/var/log/system.log

6. To remove an attachment, select the attachment file in the **Attachments** list and click the button **Remove**.

7.8.4 Limit E-Mail Send Rate

The transmission of E-Mails is triggered by the configured trigger conditions. It is not predictable, how often the trigger condition will cause the transmission of an E-Mail. The E-Mail template can be configured to limit the number of transmitted E-Mails. This is done in the Configure E-Mail Template dialog.

To configure an E-Mail Rate Limit, configure the settings:

- **Max. E-Mails per day**: This setting defines, how many E-Mail can be sent on average per day. The actual number of transmitted E-Mails on a specific day may be slightly higher than this setting, depending on burst rates. The default is 200 E-Mail per day. This results in an average interval of one E-Mail per 7 minutes.
- **Send burst count**: This setting defines how many E-Mails may be transmitted shortly after each other not limited by the above average interval. After the burst count, the average Mails per day limit takes effect. The default is a maximum of 20 E-Mails in a row.

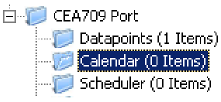
7.9 Local Schedule and Calendar

7.9.1 Create a Calendar

As the first step, the required data points must be created. A calendar must be created, if the schedules shall work with exception days, such as “Holidays”. If it suffices for schedules to define daily schedules for normal weekdays only, no calendar needs to be created.

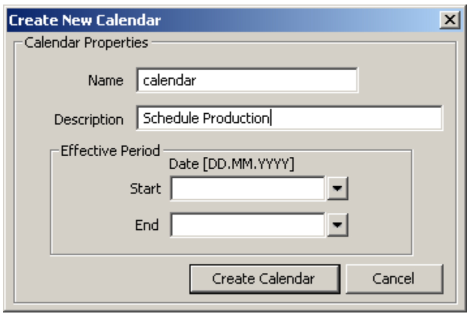
To Create a Calendar

1. Under the port folder, select the **Calendar** sub-folder to create a calendar.



2. Right-click in the data point list view and select **New local Calendar …**.

3. In the Create New Calendar dialog box (as shown in Figure 120) enter Name and Description of the calendar. Correct the effective period if necessary.



Name: calendar

Description: Schedule Production

Date [DD.MM.YYYY]

Start:

End:

Figure 120: Create New Calendar dialog box.

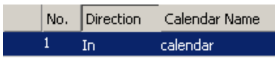
4. Click **Ok**. The calendar appears now in the data point list view.

7.9.2 Create Calendar Pattern

When a local calendar is used, it needs to be configured with calendar patterns. A calendar pattern represents a class of days such as “Holidays”. The calendar patterns can then be used in a schedule to define daily schedules for exception days. The available calendar patterns should be created when the system configuration is engineered. The actually dates in the calendar patterns can be modified later at run-time.

To Create a Calendar Pattern

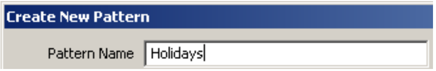
1. Select an existing calendar data point.



No.	Direction	Calendar Name
1	In	calendar

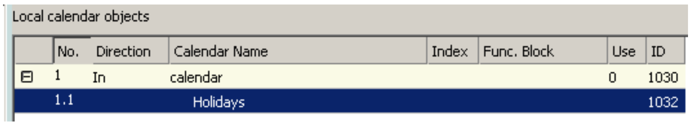
2. Right-click and select **Create Calendar Pattern…**

3. Enter a Pattern Name in the **Create Calendar Pattern** dialog



Pattern Name: Holidays

4. Click **Create Pattern**. The dialog closes and the calendar pattern appears beneath the calendar data point.



Local calendar objects

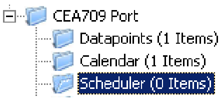
	No.	Direction	Calendar Name	Index	Func. Block	Use	ID
⊟	1	In	calendar			0	1030
	1.1		Holidays				1032

7.9.3 Create a Local Scheduler

For scheduling data points, a scheduler object must be created. On each port, multiple local scheduler objects can be created. These local schedulers can then be configured to schedule data points.

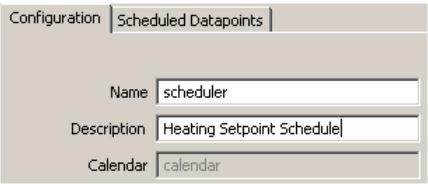
To Create a Local Scheduler

1. Under the port folder, select the Scheduler sub-folder to create a scheduler.



2. Right-click in the data point list view and select **New Local Scheduler …**.

3. Enter a name for the schedule and a description. Note, that the schedule automatically detects a calendar, if it has previously been created.



Name: scheduler
Description: Heating Setpoint Schedule
Calendar: calendar

4. Click **Create Schedule**. The new schedule appears in the data point list of the Scheduler sub-folder.

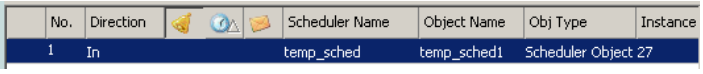
7.9.4 Configure Scheduled Data Points

When a local scheduler has been created, it needs to be configured, which data points it shall schedule. This is done by attaching data points to the scheduler. Note, that there may be limits, how many and which data points may be attached (see Section 7.9.8).

This configuration must be done as an initial setup. Which data points are scheduled cannot be changed at run-time. The daily schedules, however, can be changed later in the Web UI or over the network.

To Attach Data Points to a Scheduler

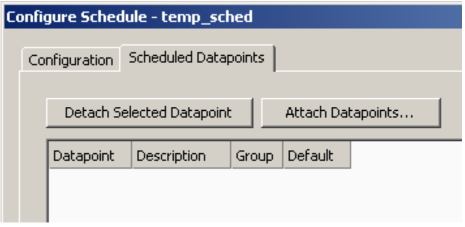
1. Select the scheduler data point in the Scheduler sub-folder.



No.	Direction				Scheduler Name	Object Name	Obj Type	Instance
1	In				temp_sched	temp_sched1	Scheduler Object	27

2. Right-click and select **Configure Schedule** from the context menu. The same dialog which appears when a new scheduler is created is shown and allows to configure the scheduler. Of course, this step can also be done directly when the point is created.

3. Select the tab Scheduled Datapoints.



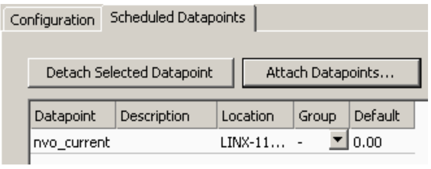
Datapoint	Description	Group	Default

4. Click the button **Attach Datapoints** . This opens another data point selector window.

5. Select the data points to attach and click **Ok**. For each of the attached data points, one or more lines appear in the list below the attach button. If the attached point is a structure, there will be one line for each element of the structure.

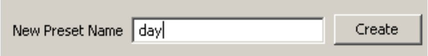
Tip! *Data points can also be attached to a scheduler by selecting a data point in the data point manager, drag it onto a scheduler data point and drop it on the scheduler data point.*

6. Enter a Description text in the second column of each line. This text will be shown when the user changes a value set on the device later on.

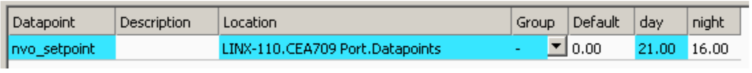


Datapoint	Description	Location	Group	Default
nvo_current		LINX-11…	-	0.00

7. Add new value presets by entering a name and pressing the **Create** button next to the input field.

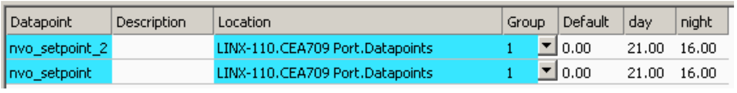


8. For each new preset, a new column will appear in the list. In this column, enter the desired value for each of the attached points, which will be set when this value template is scheduled. The user may later edit the values for each preset on the device but cannot add new value presets unless there is only one line (one value) in the list.



Datapoint	Description	Location	Group	Default	day	night
nvo_setpoint		LINX-110.CEA709 Port.Datapoints	-	0.00	21.00	16.00

9. If there are multiple output values which belong together, they can be grouped in order to save space on the device. For each group, the entered value is stored only once, even if there are more data points in the same group.



Datapoint	Description	Location	Group	Default	day	night
nvo_setpoint_2		LINX-110.CEA709 Port.Datapoints	1	0.00	21.00	16.00
nvo_setpoint		LINX-110.CEA709 Port.Datapoints	1	0.00	21.00	16.00

10. When done with the point and value setup, switch back to the **Configuration** tab or click **Save Changes** to leave the dialog.

7.9.5 Configure Daily Schedules

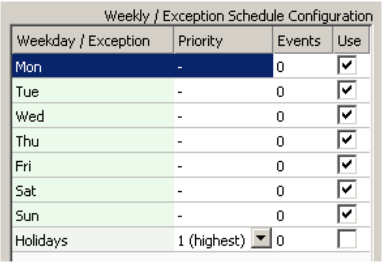
Once a scheduler is configured with attached data points and value presets, the daily schedules can be defined. This can be done on the device or over the network at run-time, or also in the configuration software. A daily schedule defines the time and value sequences in a 24-hour period starting at 00:00 and ending at 23:59 hours. For each weekday its own daily schedule can be configured.

In addition, daily schedules can be configured for exception days from a calendar, such as “Holidays”. An exception day always overrides a normal weekday. If more than one exception day is used, a priority must be assigned. This is necessary so that the system knows which schedule to follow on a day which is part of more than one calendar pattern.

To Configure a Daily Schedule

1. Open the **Configure Schedule** dialog and click on the **Configuration** tab (see Section 7.9.4).

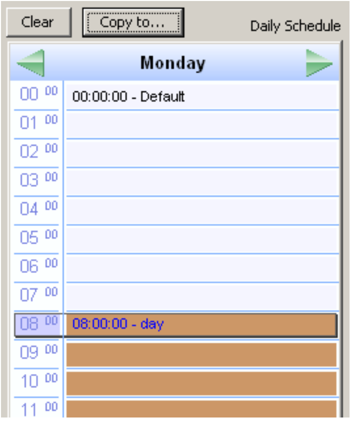
2. Select the day for which to configure a daily schedule.



Weekday / Exception	Priority	Events	Use
Mon	-	0	☑
Tue	-	0	☑
Wed	-	0	☑
Thu	-	0	☑
Fri	-	0	☑
Sat	-	0	☑
Sun	-	0	☑
Holidays	1 (highest)	0	□

3. Select a value preset in the **Available Data Presets** box on the upper right-hand side.

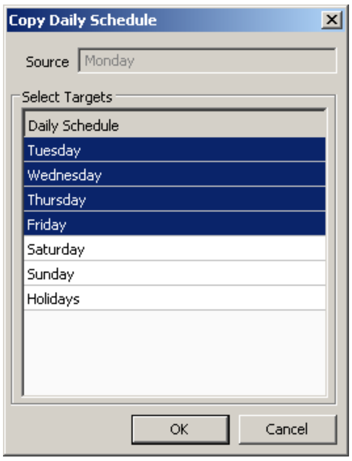
4. Drag and drop the preset from this list into the time table area to define the desired output values on the day schedule.



00:00:00 - Default

08:00:00 - day

5. Completed daily schedules may be copied to other days using the **Copy to** button. For example, the Monday may serve as the template for a regular work day and be copied to Tuesday till Friday. Then click **Ok**.

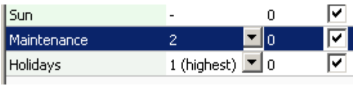


Source: Monday

Daily Schedule
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Holidays

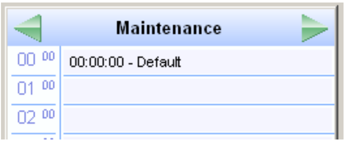
To Use Exception Days

1. Select a calendar pattern, which shall be used as an exception day and place a checkmark on it.



Sun	-	0	☑
Maintenance	2	0	☑
Holidays	1 (highest)	0	☑

2. Edit the daily schedule.



00:00:00 - Default

3. If more than one calendar pattern is used, edit the priorities. For example, if a given calendar day falls in both categories, "Holidays" and "Maintenance", the exception day with the higher priority becomes effective on that day. The highest available

priority is marked **highest**. Note that the actual priority values depend on the technology (see Section 7.9.8).

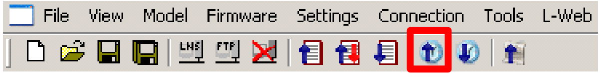
Important! ***Choose different priorities for different exceptions. If two exceptions are valid for a given day and their priorities are equal, it is not determined, which exception is in effect.***

7.9.6 Configure Exception Days

When a local calendar is used, its calendar patterns need to be configured with exception days (pattern entries). The calendar patterns can be configured in the LINX-10X configuration software or be modified at run-time over the Web UI or over the network. When configuring in the software, the current exception days should be uploaded from the device, to work on the current configuration.

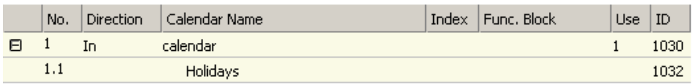
To Configure a Calendar Pattern

1. Click on the Upload calendar/scheduler configuration button



in the tool bar of the main connections window. Click **Ok** when the upload is finished.

2. Select the **Calendar** sub-folder and select the calendar pattern, which shall be configured

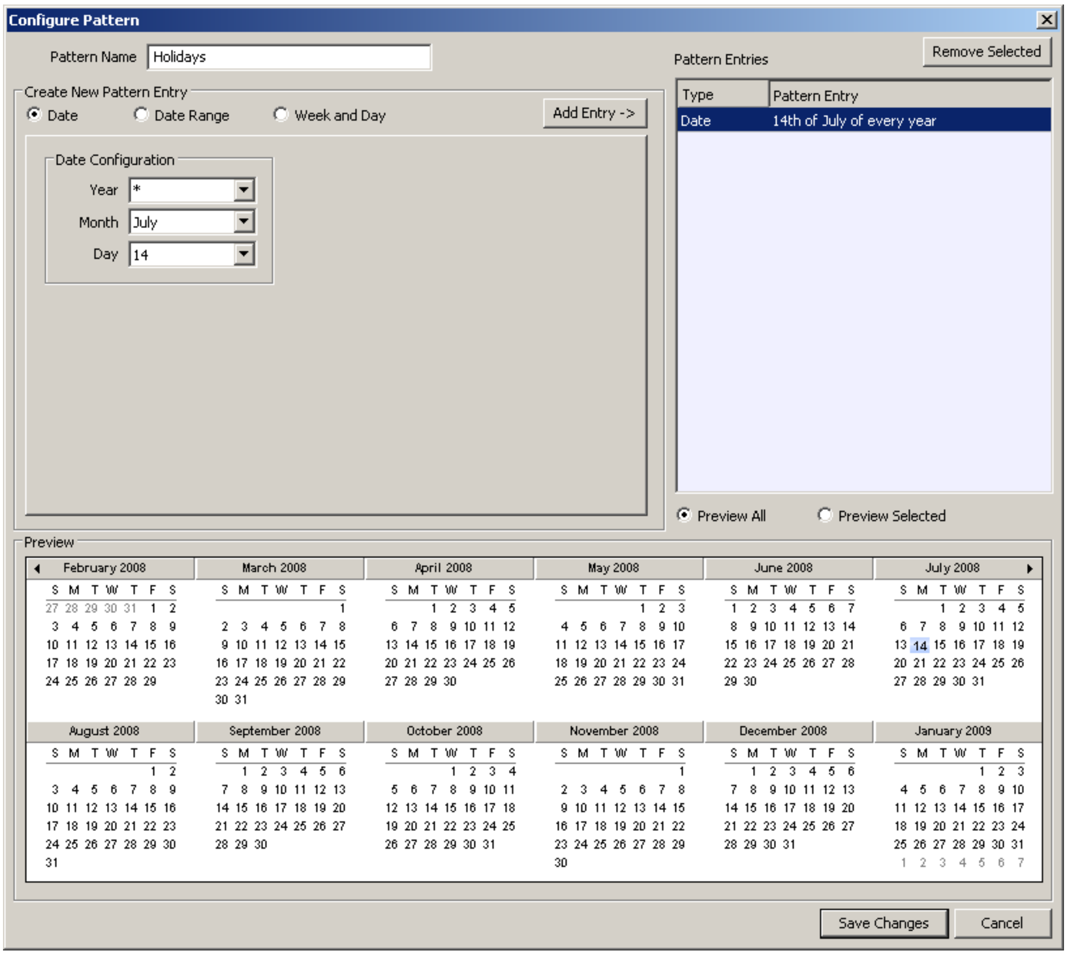


	No.	Direction	Calendar Name	Index	Func. Block	Use	ID
⊟	1	In	calendar			1	1030
	1.1		Holidays				1032

3. Right-click and select **Configure Pattern …** in the context menu.

4. The **Configure Pattern** dialog appears as shown in Figure 121. Add dates to the calendar pattern by entering a Date Configuration. Then click **Add Entry**. The date appears in the Pattern Entries list on the right-hand side.

5. Edit an exception by selecting the pattern entry in the **Pattern Entries** list. Then modify the date configuration in the **Date Configuration** group box.



Pattern Name: Holidays

● Date ○ Date Range ○ Week and Day

Year: *
Month: July
Day: 14

Type	Pattern Entry
Date	14th of July of every year

● Preview All ○ Preview Selected

Figure 121: Configure Calendar Pattern Dialog.

6. Click **Save Changes** when all exception days have been entered.

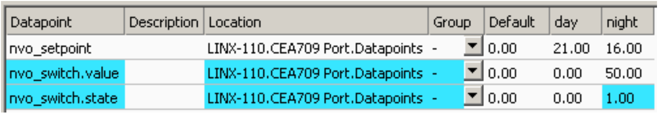
Tip!	*When not sure, how a date configuration affects the calendar days, click on a pattern in the **Pattern Entries** list and the affected days will be highlighted in the **Preview**.*

7.9.7 Using the Local Scheduler

Once the setup of the local scheduler is done, it is basically operational. It will immediately start to work based on the configuration data downloaded through the configuration software. You can verify the daily schedules and values of scheduled data points on the Web UI (see Section 5.2.10). The local schedule can be altered over the Web UI or using the network technology of the port, where the scheduler has been created.

7.9.8 Limitations for Local CEA-709 Schedulers

CEA-709 schedulers and the CEA-709 calendar adhere to the LONMARK standard objects. For CEA-709 certain restrictions exist that need to be kept in mind. Attached data points can only represent an entire NV, but not individual elements of a structured NV. CEA-709 schedulers may have several different groups of data points attached, i.e., the value preset may consist of more than one element. For example, a CEA-709 scheduler might schedule a SNVT_temp and a SNVT_switch and have 3 elements in each value preset as depicted in Figure 122.



Datapoint	Description	Location	Group	Default	day	night
nvo_setpoint		LINX-110.CEA709 Port.Datapoints	-	0.00	21.00	16.00
nvo_switch.value		LINX-110.CEA709 Port.Datapoints	-	0.00	0.00	50.00
nvo_switch.state		LINX-110.CEA709 Port.Datapoints	-	0.00	0.00	1.00

Figure 122: Example value presets in CEA-709 schedulers.

Priorities of exception days in a CEA-709 scheduler range from 0 (the highest) to 126 (the lowest). The value 127 is reserved as a default for weekdays.

Further, the implementation as LONMARK standard objects requires the use of configuration properties. If the number of CEA-709 schedulers or their capacities for daily schedules and value presets is changed, the resource and static interface of the CEA-709 port changes. The resources reserved for LONMARK calendar and scheduler objects can be changed in the project settings (see Section 7.3.4). When downloading a project, the software verifies, if sufficient resources have been configured. If it detects a problem, the user is notified to update the project settings. The Auto-Set feature automatically selects the right amount of resources.

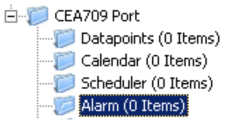
7.10 Local Alarming

7.10.1 Create an Alarm Server

To generate local alarms, an alarm server needs to be created at first. The local alarm sources will report alarms to that alarm server. The alarm server is the interface to access local alarms. This can be done over the network or the Web UI.

To Create an Alarm Server

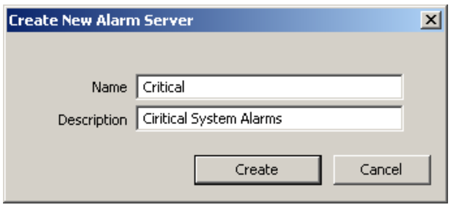
1. Under the port folder, select the **Alarm** sub-folder to create an alarm server.



CEA709 Port
Datapoints (0 Items)
Calendar (0 Items)
Scheduler (0 Items)
Alarm (0 Items)

2. Right-click in the data point list view and select **New Alarm Server …**.

3. In the **Create New Alarm Server** dialog box (as shown in Figure 123) enter **Name** and **Description** of the alarm server.



Create New Alarm Server

Name: Critical
Description: Ciritical System Alarms

Figure 123: Create New Alarm Server dialog box.

4. Click **Create**. The alarm server appears now in the data point list view.

7.10.2 Create an Alarm Condition

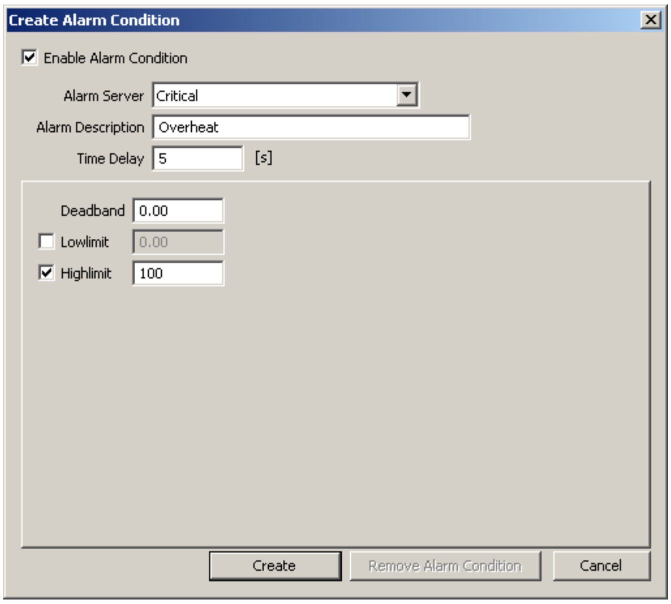
To generate alarms from data points, intrinsic reporting is used. For each data point an alarm condition must be defined. This condition employs an intrinsic algorithm to generate alarms based on the data point’s value. Depending on the data point type (analog, binary, multi-state), different conditions are defined. The alarm is reported to the attached alarm server.

To Create an Intrinsic Alarm Condition

1. Select a data point.

2. Right-click and select **Create Alarm Condition…** from the context menu.

3. For an analog data point the dialog as shown in Figure 124 appears. Select the **Alarm Server**. Optionally, enter an **Alarm Description**. If left empty, the description of the data point is used. Enter a **Time Delay**, after which the condition is evaluated. Select **Low Limit** and **High Limit** and put check marks, if they shall be employed. Enter a **Deadband**, to account for hysteresis.



Create Alarm Condition

☑ Enable Alarm Condition

Alarm Server: Critical

Alarm Description: Overheat

Time Delay: 5 [s]

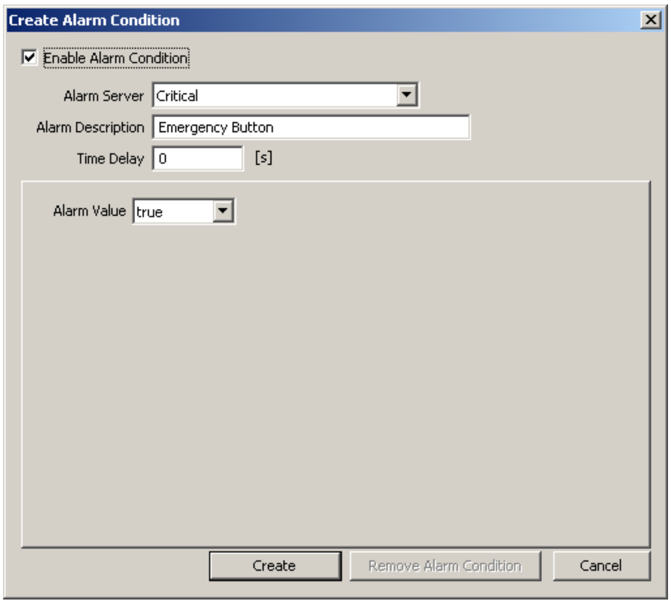
Deadband: 0.00

□ Lowlimit: 0.00

☑ Highlimit: 100

Figure 124: Alarm Condition for an Analog Data Point.

4. For a binary data point the dialog as shown in Figure 125 appears. Select the **Alarm Server**. Optionally, enter an **Alarm Description**. If left empty, the description of the data point is used. Enter a **Time Delay**, after which the condition is evaluated. Select the **Alarm Value**, which triggers the alarm.



Create Alarm Condition

☑ Enable Alarm Condition

Alarm Server: Critical

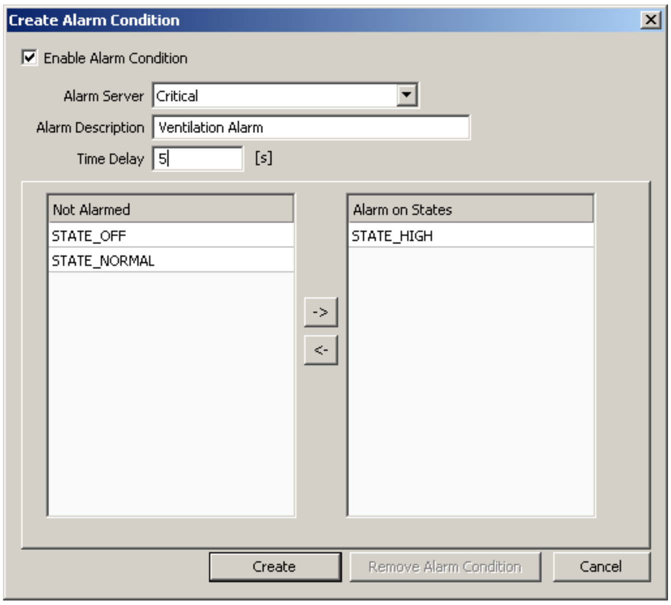
Alarm Description: Emergency Button

Time Delay: 0 [s]

Alarm Value: true

Figure 125: Alarm Condition for a Binary Data Point.

5. For a multi-state data point the dialog as shown in Figure 126 appears. Select the **Alarm** Server. Optionally, enter an **Alarm Description**. If left empty, the description of the data point is used. Enter a **Time Delay**, after which the condition is evaluated. Select the **Alarm States**, which triggers the alarm, by clicking the arrow buttons.



Create Alarm Condition

☑ Enable Alarm Condition

Alarm Server: Critical

Alarm Description: Ventilation Alarm

Time Delay: 5 [s]

Not Alarmed	Alarm on States
STATE_OFF	STATE_HIGH
STATE_NORMAL	

Figure 126: Alarm Condition for a Multi-State Data Point.

6. Click on **Create**. In the alarm column, the alarm sign 🔔 will be added for those data points that have an alarm condition.

7.10.3 Deliver Alarms via E-Mail

Updates in the alarm summary of an alarm object can be used as a trigger to send E-Mail. For setting up E-Mails, the account information has to be configured on the device, e.g. on the Web UI (see Section 5.2.13). Then an E-Mail template can be created and the alarm point attached as a trigger.

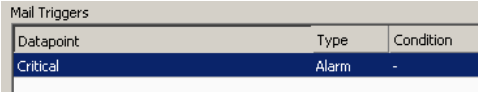
To Create an E-Mail Template for Alarms

1. Create or configure an E-Mail template as described in Section 7.8.1.

2. Change to the **Mail Triggers** tab.

3. Click the **Add…** button and select an alarm data point.

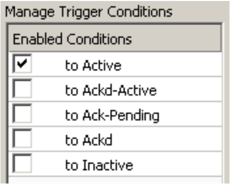
4. In the Mail Triggers list select the added trigger data point.



Mail Triggers

Datapoint	Type	Condition
Critical	Alarm	-

5. In the **Manage Trigger Conditions** list put a check mark on alarm conditions that shall invoke the transmission of the E-Mail.



Manage Trigger Conditions

Enabled Conditions

- ☑ to Active
- □ to Ackd-Active
- □ to Ack-Pending
- □ to Ackd
- □ to Inactive

6. Change to the Common Mail Properties tab.

7. Add the alarm data point as a data source and insert the place holder into the E-Mail text as described in Section 7.8.1.

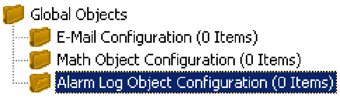
7.10.4 Create an Alarm Log

The alarm objects on the device contain an alarm summary (live list) of currently active and acknowledge-pending alarms. As soon as an alarm becomes inactive and has been acknowledged, it disappears from the alarm summary. To store a historical log of alarm transitions an *alarm log* needs to be created.

An alarm log can log transitions of one or more alarm objects. Its size is configurable. The alarm log is a ring buffer. As soon as its size limit is reached, the oldest alarm log records are overwritten by new alarm transitions.

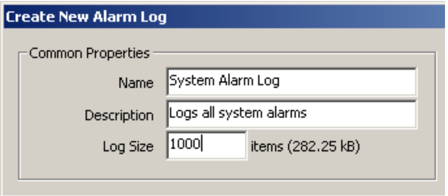
To Create an Alarm Log

1. Under the **Global Objects** folder, select the **Alarm Log Object Configuration** sub-folder.



Global Objects
- E-Mail Configuration (0 Items)
- Math Object Configuration (0 Items)
- Alarm Log Object Configuration (0 Items)

2. In the data point list right-click and select **New Alarm Log …** from the context menu.



Create New Alarm Log

Common Properties

Name: System Alarm Log

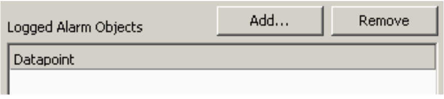
Description: Logs all system alarms

Log Size: 1000 items (282.25 kB)

3. In the **Create New Alarm Log** dialog enter a **Name** for the alarm log. Optionally enter a **Description**.

4. Enter a **Log Size**, which defines how many transitions are resident in the alarm log.

5. Click on the button **Add…** on top of the **Logged Alarm Objects** list.



6. A data point selector dialog opens. Select one or more alarm objects that shall be logged and click **Ok**. The alarm objects appear in the list.

7. Click **Create** to create the alarm log object.

7.10.5 Limitations for CEA-709 Alarm Servers

Local CEA-709 alarming supports only one alarm server object. This alarm server object is represented by the device's LONMARK node object and facilitates the SNVT_alarm2 output network variable. Acknowledging alarms in the alarm server is adhering to the LONMARK specification and relies on the RQ_CLEAR_ALARM mechanism.

7.11 Local Trending

7.11.1 Create a Local Trend

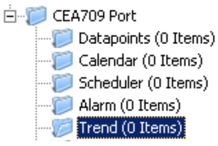
The value of a data point can be logged over time. This is referred to as trend data. To generate trend data a trend object has to be created. The trend data is stored in a data logger file. This file can be downloaded via FTP in binary or CSV format (see Section 10.1.2).

CEA-709 trend objects can generate trend logs for multiple data points and can be operated in one of three basic modes:

- **Interval Mode**: In this mode a snapshot of all trended data points is logged into the data logger file.
- **COV Mode**: In this mode each of the trended data points is logged separately, if and only if its value changes. For analog data points, a specific COV increment can be configured in the data point configuration properties of the trended data point.
- **Trigger Mode**: In this mode a snapshot of all trended data points is logged each time a trigger condition fires. The trigger condition is applied to a trigger data point.

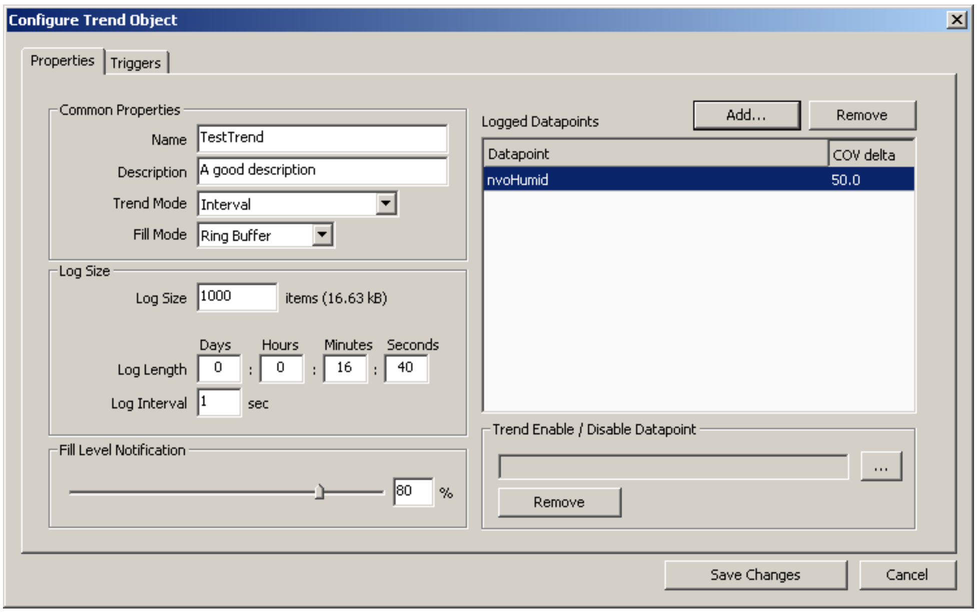
To Create a Trend Object

1. Under the port folder, select the **Trend** sub-folder to create a trend log object.



2. Right-click and select **New Trend …** from the context menu.

3. In the **Create New Trend Object** dialog (shown in Figure 127) enter a name and optionally a description for the trend log object.



Common Properties

Name: TestTrend

Description: A good description

Trend Mode: Interval

Fill Mode: Ring Buffer

Log Size

Log Size: 1000 items (16.63 kB)

	Days	Hours	Minutes	Seconds
Log Length	0	0	16	40

Log Interval: 1 sec

Fill Level Notification: 80 %

Logged Datapoints

Datapoint	COV delta
nvoHumid	50.0

Trend Enable / Disable Datapoint

Figure 127: Basic Trend Object Configuration.

4. Select the desired **Trend Mode**.

5. Select the **Log Size**. The display in the dialog will adapt the estimations for needed data logger file size in KB and duration of the trend log. Alternatively, for interval trends, the estimated log duration and log interval can be edited.

6. Select a **Fill Level Notification** percentage. This will decide after how many percent new log items a fill-level trigger will fire. A fill-level trigger can be used to trigger the transmission of an E-Mail (see Section 7.11.5).

7. Click **Save changes** to store the basic configuration of the trend object. The new trend log object appears in the data point list of the Trend folder.

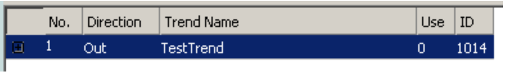
7.11.2 Configure Trended Data Points

When a local trend object has been created, it needs to be configured, which data points it shall log. This is done by attaching data points to the trend object. Only simple data points can be attached for trending, i.e., of class analog, binary, or multi-state. For CEA-709 trend log objects, multiple data points can be attached for trending.

The trending can be enabled/disabled on behalf of an *enable* data point. This data point must be of type *binary*. If the value of that enable data point is TRUE, the trend object logs data as defined by the trend mode. If the value of the enable is FALSE, trending is disabled. If no enable data point is configured, the trend log is always enabled.

To Attach Data Points for Trending

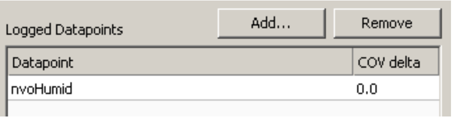
1. Select the trend object in the Trend sub-folder.



No.	Direction	Trend Name	Use	ID
1	Out	TestTrend	0	1014

2. Right-click and select **Configure Trend** from the context menu. The same dialog which appears when a new trend object is created is shown and allows configuring the trend object. Of course, this step can also be done directly when the object is created.

3. Add data points to be trended. Click on **Add …** which opens a data point selector window.



Datapoint	COV delta
nvoHumid	0.0

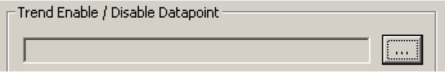
4. Select the data points and click **Ok**. For each of the attached data points, one or more lines appear in the list below the add button. The trended data points will also appear with the trend icon 📈 in the data point manager.

Tip! *Data points can also be attached to a trend by selecting a data point in the data point manager, drag it onto a trend object and drop it on the trend object.*

5. Data points can be removed from the trend by clicking **Remove**.

6. If COV mode was selected, the COV increment is displayed in the **COV delta** column. This value can be increased to produce less trend data. Note, that it cannot be lowered under the trended data point's own COV increment. Go to the data point configuration to change the COV increment in this case.

7. In addition, a special **Trend Enable** data point can be selected. If configured, the trend log will only log data, if the value of this data point evaluates **true**, i.e., is not zero. Click the **…** button to select a data point.



8. To remove the enable data point, click the **Remove** button.

9. When done with the data point setup click **Save Changes** to leave the dialog.

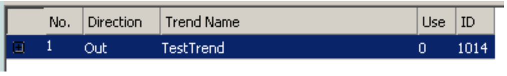
7.11.3 Trend Triggers

Local trend objects in CEA-709 can be operated in *trigger mode*. In this mode, one ore more trigger data points cause the generation of a snapshot containing the values of the trended data points at the time instant the trigger is activated. For a trend object, one or more trigger conditions can be defined. Depending of the trigger data point type, the trigger conditions can be refined.

Note, that the behavior of the trigger data point is influenced by the COV properties of the data point. If the **Only notify on COV** property is checked, the data point triggers only if its value changes to the value of the trigger condition. If that property is not checked, the data point triggers on every write with a value that matches the trigger condition.

To Configure Trigger Data Points for Trending

1. Select the trend object in the **Trend** sub-folder.



No.	Direction	Trend Name	Use	ID
1	Out	TestTrend	0	1014

2. Right-click and select **Configure Trend** from the context menu.

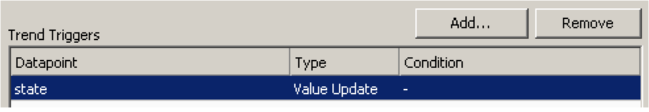
3. Change to the **Triggers** tab.

Note: *Of course, you can also change directly to the **Triggers** tab when creating a trend object.*

4. Click the **Add…** button. A data point selection dialog opens.

5. Select one or more data points and click **Ok**.

6. The triggers appear now in the **Trend Triggers** list.



Datapoint	Type	Condition
state	Value Update	-

7. In the **Manage Trigger Conditions** you can refine the trigger condition depending on the trigger data point class.

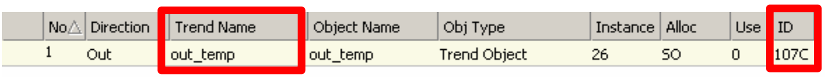
8. When done with the data point setup click **Save Changes** to leave the dialog.

7.11.4 Download Trend Data in CSV Format

Trend logs can be downloaded from the device via FTP in CSV format (see Section 10.1.2). The CSV contents are generated on-the-fly from the internal binary storage when accessing the file. Each trend log point has one CSV file. The files are located in

`/data/trend/`*TrendLogName_UID*`.csv`

Where *TrendLogName* is the data point name of the trend (Trend Name). The *UID* is the unique ID of the trend log object. The UID can be obtained from the ID column in the data point list of trend log data points as shown in Figure 128. This would result in the trend CSV file ‘`/data/trend/out_temp_107C.csv`’.



	No△	Direction	Trend Name	Object Name	Obj Type	Instance	Alloc	Use	ID
	1	Out	out_temp	out_temp	Trend Object	26	SO	0	107C

Figure 128: UID of data points.

Because the contents are generated on-the-fly, the file size in the FTP client will appear as 0 Bytes. The decimal point and CSV column separator can be configured over in the system configuration of the Web UI (see Section 5.2.1) of the LINX-10X. Note, that for a comma “,” as the separator, the decimal point is a point. This is useful for English/U.S. applications. For countries that use the comma as the decimal point, select the semicolon as the CSV separator.

7.11.5 Deliver Trend Data via E-Mail

Trend logs can be downloaded from the device via FTP. This requires an active action by the user. Alternatively, trend data can be sent as an E-Mail attachment. For doing that, an E-Mail template has to be set up for the trend log to be transmitted. The fill-level condition in the trend object can be used as a trigger to send an E-Mail with the trend’s data logger CSV file as an attachment.

For setting up E-Mails, the account information has to be configured on the device, e.g. on the Web UI (see Section 5.2.13). Then an E-Mail template can be created and the trend object attached as a trigger.

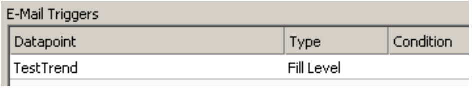
To Create an E-Mail Template for Trends

1. Create or configure an E-Mail template as described in Section 7.8.1.

2. Change to the **Mail Triggers** tab.

3. Click the **Add…** button and select a trend object.

4. In the **Mail Triggers** list the added trigger data point appears with the **Fill Level** condition.

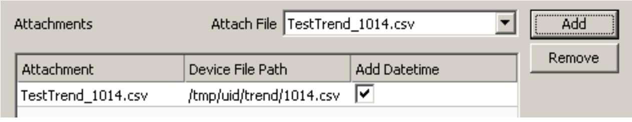


E-Mail Triggers

Datapoint	Type	Condition
TestTrend	Fill Level	

5. Change to the **Attachments** tab.

6. Select the trend log CSV file of the trend object used as a trigger in the **Attach File** drop-down box and click **Add**.



Attachments

Attach File: TestTrend_1014.csv

Attachment	Device File Path	Add Datetime
TestTrend_1014.csv	/tmp/uid/trend/1014.csv	☑

7. Click **Ok** to complete the E-Mail template configuration.

7.11.6 Limitations for Local CEA-709 Trends

Local CEA-709 trend objects supports trending multiple data points in all trend modes, interval, COV, and trigger. The enable data point is also supported. All data points can be NVs, registers or of any other technology. There is no LONMARK object linked to the trend object. Consequently, trend data cannot be accessed over a LONMARK mechanism.

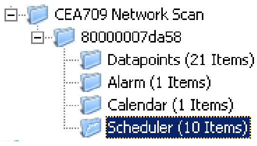
7.12 Remote AST Objects

7.12.1 Remote Scheduler and Calendar

Adding remote access to the configuration of a scheduler and calendar, which is located on another device, is done by creating remote scheduler and calendar objects. These objects can be created from data obtained by a network scan or LNS scan.

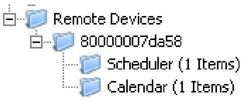
To Create a Remote Scheduler

1. Execute a network scan, as described earlier in this document. The scan folder is filled with available schedulers.



CEA709 Network Scan
80000007da58
Datapoints (21 Items)
Alarm (1 Items)
Calendar (1 Items)
Scheduler (10 Items)

2. From the data points in the import folder, select the scheduler objects you are interested in and click the **Use on Device** speed button. This creates suitable remote scheduler and the corresponding calendar objects in the **Remote Devices** folder.



Remote Devices
80000007da58
Scheduler (1 Items)
Calendar (1 Items)

3. Adjust the basic settings for the newly created objects, such as the object name and description. The object name will be used as the name for the scheduler, as seen on the Web UI.

4. A static NV is created to receive information from the remote device about changes to the scheduler configuration, so that the local device does not need to poll the remote device. Set a name for this NV (default is nviSchedLink<number>) and assign it to a suitable function block.

Note: *Due to the static input NV, which is required for a remote CEA709 scheduler object, adding remote scheduler points will change the static interface of the device.*

The new static input NV representing the remote calendar on the local device (this NV is normally called *nviCalLink*) needs to be bound to the output NV called *nvoCalLink* located in the Calendar functional block of the remote device and the new static *nviSchedLink* NVs which were created for each remote scheduler point need to be bound to the respective *nvoSchedLink* variable located in the Scheduler functional block of the remote device. The binding between the *nvoSchedLink* variable on the remote device to the *nviSchedLink* variable on the local device defines which of the scheduler data points on the local device connect to which scheduler unit on the remote device. All required information is transmitted over the link NVs, so it is possible to later change the binding to any other remote scheduler without rescanning the network.

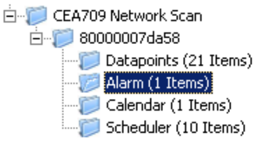
Note: *If connected via LNS, the bindings to the nvoCalLink and nvoSchedLink NVs are made automatically by the configuration software in the download process.*

7.12.2 Alarm Clients

Accessing alarm server objects on remote devices is done by creating remote alarm data points. These points may be created from data obtained by a network scan. The local device is configured as an alarm client and subscribes to alarm updates from the remote alarm server. The alarm client can also be used to acknowledge alarms on the remote alarm server. Any updates are synchronized back to the alarm client.

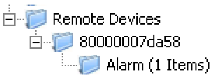
To Create an Alarm Client

1. Execute a network scan, as described earlier in this document. The scan folder is filled with available remote alarm servers.



CEA709 Network Scan
80000007da58
Datapoints (21 Items)
Alarm (1 Items)
Calendar (1 Items)
Scheduler (10 Items)

2. From the points in the import folder, select the alarm server points you are interested in and click the **Use on Device** speed button. This creates the corresponding alarm client points in your project.



Remote Devices
80000007da58
Alarm (1 Items)

3. Select the new alarm client point and adjust the name of the local NV (default name is *nviAlarm_2*). This NV is located in the *Clients* functional block.

Note: *Due to the static input NV which is required for a CEA709 alarm client point, adding alarm clients will change the static interface of the device.*

The new static input NVs representing the alarm clients on the local device need to be bound to the alarm outputs of the remote device. A CEA709 device normally delivers alarms through an output NV of type *SNVT_alarm_2* located in the node object of the device, therefore the new input NV on the local device must be bound to the alarm output NV of the remote devices node object. All required information is transmitted over the alarm input NV, so it is possible to later bind the alarm client to any other alarm server without rescanning the network.

Note: *If connected via LNS, the binding to the nvoAlarm2 NV is made automatically by the configuration software in the download process.*

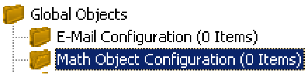
7.13 Math Objects

7.13.1 Create a Math Object

Math objects are advanced application objects that can execute mathematical operations on data points. A math object takes a number of input data points (variables v_1, v_2, …, v_n) and calculates a result value according to a specified formula. When configuring a math object, the input data points, output data points and the formula must be configured by the user.

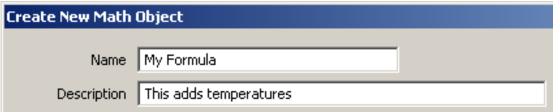
To Create a Math Object

1. Under the **Global Objects** folder, select the **Math Object** sub-folder.


Global Objects
E-Mail Configuration (0 Items)
Math Object Configuration (0 Items)

2. Right-click and select **New Math Object …** from the context menu.

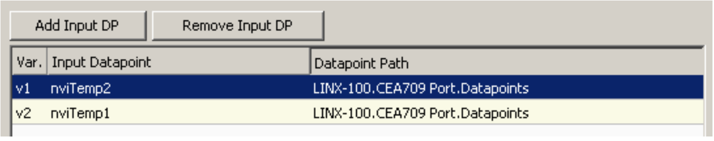
3. In the Create New Math Object dialog, enter a name and optionally a description for the math object.


Create New Math Object

Name: My Formula

Description: This adds temperatures

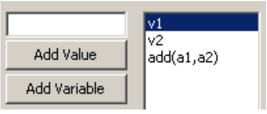
4. Attach input data points by clicking the **Add Input DP** button.



Var.	Input Datapoint	Datapoint Path
v1	nviTemp2	LINX-100.CEA709 Port.Datapoints
v2	nviTemp1	LINX-100.CEA709 Port.Datapoints

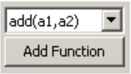
5. In the data point selector dialog select the input data points and click **Ok**. The data points appear as v1, v2, etc.

6. Select the input data point and click **Add Variable** to push the variable on the evaluation stack.



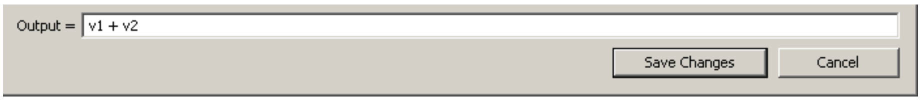
v1
v2
add(a1,a2)

7. Select a function to be applied on the variables and click the **Add Function** button.



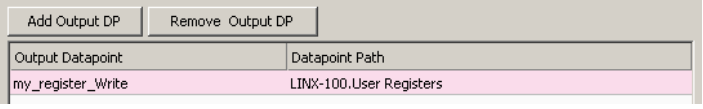
add(a1,a2)

8. Te resulting formula is displayed at the bottom of the dialog. Alternatively, the formula can be entered there.



Output = v1 + v2

9. Add output data points by clicking the **Add Output DP button**.



Output Datapoint	Datapoint Path
my_register_Write	LINX-100.User Registers

10. In the data point selector dialog select the output data points and click **Ok**.

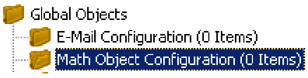
11. To create the math object click **Create**.

7.13.2 Editing a Math Object

Math objects can be edited once created. The formula can be changed, new variables added, or additional output data points added.

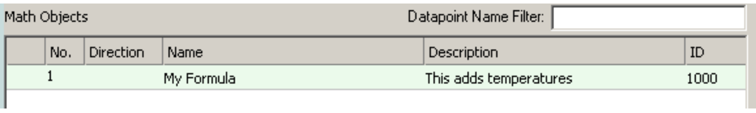
To Edit a Math Object

1. Under the **Global Objects** folder, select the **Math Object** sub-folder.



Global Objects
E-Mail Configuration (0 Items)
Math Object Configuration (0 Items)

2. Select the math object in the data point list.



Math Objects Datapoint Name Filter:

No.	Direction	Name	Description	ID
1		My Formula	This adds temperatures	1000

3. Right-click and select **Configure Math Object …** from the context menu.

4. Edit the math object as described in Section 7.13.1.

5. To finalize the edit click on **Save Changes**.

8 The LINX-101 Router

The LINX-101 is equipped with a standard CEA-709 router (i.e., an embedded L-IP), which connects the FT port and the CEA-852 port. Depending on the use case the LINX-101's router supports different operating modes how packets are routed between the CEA-709 side and the IP-852 side. The LINX-101 also contains a configuration server (CS) to manage members on an IP-852 channel.

8.1 CEA-709 Router

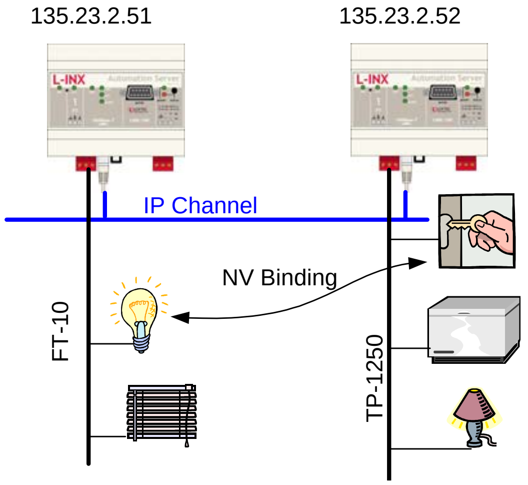


Figure 129: The LINX-101 supports different methods to route packets between the CEA-709 and IP-852 channel.

Depending on the CEA-709 router configuration (see Section) the LINX-101 supports 4 different methods to route packets between the CEA-709 and the IP-852 channel. The 4 operating modes are listed below and described in more detail in the subsequent sections.

- Configured Router: The LINX-101 acts like a standard CEA-709 configured router (*i*.LON 1000/600 alike)
- Smart Switch: The LINX-101 acts as a self-learning plug&play router ("smart switch mode")
- Store-and-Forward Repeater: To freeze a learned configuration and operate the switch based on the existing forwarding tables, disable group learning and Subnet/Node learning.
- Smart switch with no broadcast flooding: Set Subnet/Node Learning set to "subnet". In this mode the LINX-101 learns the network topology but doesn't flood subnet broadcasts.

8.1.1 Configured Router Mode

In this operating mode the LINX-101 acts like a standard configured router, which can be configured with standard network management tools like LonMaker or NL-220. This operating mode is compatible with the *i*.LON 1000 and the *i*.LON 600.

This operating mode uses the "channel routing" routing strategy on the IP channel. In this mode the LINX-101 is fully compatible with *i*.LON 1000/600 devices This operating mode should also be used in networks with more than 10 LINX-101 devices on one IP channel and heavy network traffic on the IP channel (more than 500 packets/s) since channel routing sends the IP packet only to the LINX-101 device(s) that connect to the CEA-709 node(s) addressed in this IP packet and not to all LINX-101 devices on the IP channel. This is the standard operating mode.

8.1.2 Smart Switch Mode

The LINX-101 can be configured to act as a learning switch in a CEA-709 network. This operating mode is called smart switch mode. In this operating mode the LINX-101 decides if the message has to be forwarded or not, based on the destination address of a message. Thus, it isolates local network traffic (e.g. in case of heavily loaded networks).

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

Important: ***Whenever a network is reconfigured, it is recommended to clear the forwarding tables in the LINX-101 by pressing the status button for at least 20 seconds (see Section 3.5.1).***

The router supports learning of up to 4 Domains.

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

The subnet/node learning algorithm supports segmentation of the network traffic on a subnet/node basis. Thus, the user does NOT need to take care of any subnets spanning multiple physical channels. Even when a node is moved from one channel to another, the LINX-101 keeps track and modifies its forwarding tables accordingly.

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

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

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

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

The router has no learning strategy for broadcast addresses. As a result, all subnet or domain wide broadcasts are always forwarded. If subnet wide broadcasts shall not be forwarded please use the smart switch operating mode without subnet broadcast forwarding (see Section 8.1.4).

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

This operating mode uses the "channel routing" strategy on the IP channel to distribute IP packets. It uses flooding to send all packets on the IP channel to all IP devices on this IP channel. The advantage of this operating mode is that it is fully plug&play and no router configuration is required. The disadvantage is that this operating mode doesn't scale very well with larger networks. We do not recommend this operating mode for IP channels with more than 10 IP-852 devices and packet rates of more than 500 packets/s. Please use the configured router mode from Section 8.1.1 for larger IP channel configurations.

Further, it is recommended to configure a multi-cast group for routers in the smart switch mode to reduce the traffic burden and improve scalability. Refer to Section 8.5 on how to configure the LINX-101 to use multi-cast.

8.1.3 Store-and-Forward Repeater

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

1. DIP-switch number 1 must be on, see Table 2.

2. DIP-switch number 2 must be off, see Table 2.

3. The forwarding tables must be reset by pressing the status button for at least 20 seconds (see Section 3.5.1).

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

Further, it is recommended to configure a multi-cast group for router in repeater mode to reduce the traffic burden and improve scalability. Refer to Section 8.5 on how to configure the LINX-101 to use multi-cast.

8.1.4 Smart Switch Mode with No Subnet Broadcast Flooding

This operating mode is the same as the smart switch mode from Section 8.1.2 with the only difference that subnet wide broadcasts are not flooded in this mode. This operating mode can be used in large network installations where the network management tool uses group overloading to replace group addresses with subnet wide broadcasts. In this operating mode the network installer must ensure that one subnet address may only exist behind one and no more than one network port. This condition is met if nodes are installed, using an LNS based tool, on different channels that are separated either with a router shape.

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

Further, it is recommended to configure a multi-cast group for the router in the smart switch mode to reduce the traffic burden and improve scalability. Refer to Section 8.5 on how to configure the LINX-101 to use multi-cast.

8.2 CEA-852 Device of the Router

Every LINX-101 acts as a device on the IP channel. It either needs to contact a configuration server or a configuration server needs to contact the device in order to set up the proper routing tables. Before a device can become a member of the IP-852 channel it needs to have proper IP settings (see Section 4.6):

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

Please consult Sections 4.6 and 4.7 on how to setup a CEA-852 device.

The L-IP can be used together with the PC-based *i*.LON Configuration Server utility or with the built-in configuration server. If multiple CEA-852 devices behind one NAT router are added, the Auto-NAT setting in the CEA-852 devices is recommended to be used with the LINX-101 configuration server or an L-IP configuration server. Please refer to the following sections on how to setup the device and the configuration server.

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

8.3 Configuration Server for Managing the IP-852 Channel

8.3.1 Overview

Every logical IP-852 channel requires one configuration server that manages all CEA-852 devices (LINX-101, L-IP, LOYTEC NIC852, *i*.LON 1000, *i*.LON 600, LonMaker, etc.) on this channel. A simple example is shown in Figure 130. A configuration server keeps a list of all devices on a logical IP-852 channel and distributes the routing information between those devices. If a device wants to join an IP-852 channel it needs to register itself at the configuration server. Traditionally, a dedicated Windows PC is used to act as the configuration server. The LINX-101 contains an embedded configuration server and can therefore replace the PC.

The configuration server can be enabled in the LINX-101 in the CEA-852 server configuration menu in Section 4.3.7. This configuration server can manage one IP-852 channel and up to 256 devices on this IP-852 channel. In order to setup the configuration server one must specify the following parameters:

- IP address/netmask/gateway (either via DHCP or manual entry), see Section 4.6
- NAT address if used behind a firewall/NAT router, see Section 4.6
- MD5 secret if authentication is required, see Section 4.7
- Enable the configuration server, see Section 4.9.1 (server LED lights up green)
- A list of CN/IP channel members, see Section 4.9.11.

Note: *If the LINX-101 is used as a configuration server it needs a fixed IP address.*

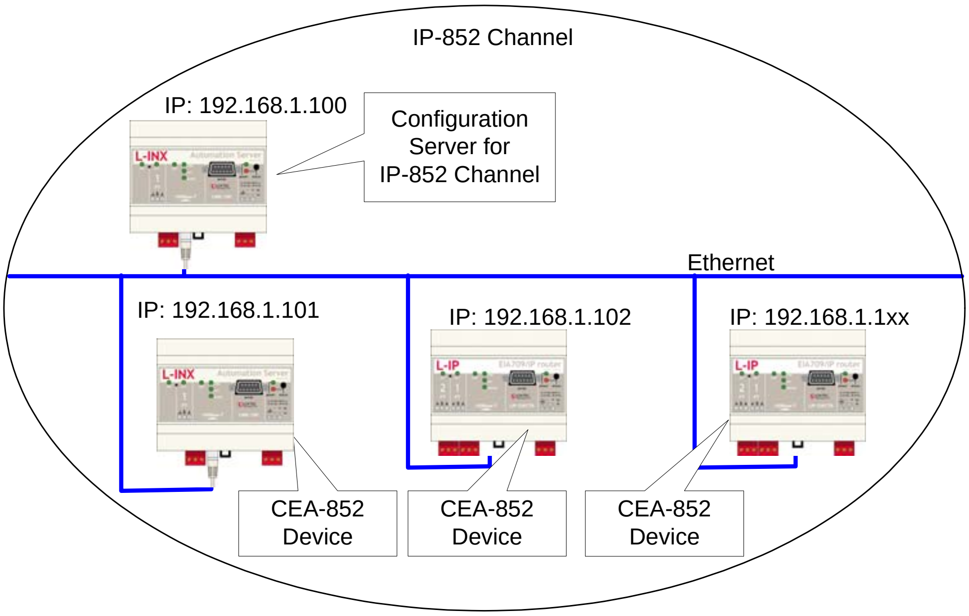


Figure 130: The configuration server manages the devices on an IP-852 channel.

8.3.2 Configuration Server Contacts IP-852 Device

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

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

If multiple IP-852 devices behind one NAT router are added, the Auto-NAT setting in the LINX-101 is recommended to be used with the LINX-101 configuration server.

8.3.3 IP-852 Device Contacts Configuration Server

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

- IP address/netmask/gateway (either via DHCP or manual entry), see Section 4.6
- Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 4.6
- MD5 secret if authentication is required, see Section 4.7
- Configuration server IP address and port number, see Section 4.7.1

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

8.3.4 Using the Built-In Configuration Server

For security purposes the configuration server contacts each IP-852 device on the IP-852 channel. Therefore one must enter a list of all channel members in the CEA-852 Configuration Server menu (see Section 4.9). This ensures that no unwanted device can join the IP-852 channel. A properly configured IP-852 channel list can look like Figure 131.

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

No     Name                 IP Address           Status              Flags
---------------------------------------------------------------------------
000    local                128.168.1.253:1628   registered
---------------------------------------------------------------------------
NAT Router                  128.168.1.250
+ 001  lip-n1               10.0.2.2:1628        registered
+ 002  lip-n2               10.0.2.3:1631        registered
---------------------------------------------------------------------------
003    pc37                 128.168.1.37:1628    not responding
---------------------------------------------------------------------------
Press <RETURN> to continue
```

Figure 131: Properly configured IP-852 channel with 4 channel members.

Note that also *i*.LON 1000/600, VNI and LOYTEC NIC852 based network nodes (e.g. LonMaker or NL-220 applications) can join the IP-852 channel managed by the configuration server.

Note that the built-in configuration server should be used if LINX-101 or L-IP devices are communicating across firewalls/NAT routers.

For adding multiple devices behind a NAT router the L-IP configuration server supports the extended NAT mode (see Section 8.4.2). The configuration server automatically switches the channel mode to extended NAT if needed. Note that the *i*.LON 600 must be configured with the *i*.LON CS to extended NAT mode before adding the *i*.LON 600 to the configuration server, because the *i*.LON 600 does not switch to that mode automatically.

8.4 Firewall and NAT Router Configuration

The LINX-101's router can be used behind a firewall and/or NAT (Network Address Translation) router as shown in Figure 132. Note, that in general only one CEA-852 device can be used behind the NAT router. This mode of operation is referred to as "Standard" channel mode. It is fully compliant with CEA-852.

LOYTEC's newer devices such as the L-IP and the LINX-101 support more than one CEA-852 channel member behind a NAT router. This mode of operation is referred to as "Extended NAT" channel mode. This mode introduces extensions to the standard mode which need to be supported by all members. Other devices supporting the extended NAT mode are the *i*.LON 600. See Section 8.3.4 on compatibility with the *i*.LON 600.

8.4.1 Automatic NAT Configuration

In order to use the LINX-101 behind a firewall the public NAT address and the local IP address must be set in the IP configuration menu (see Section 4.6). By default the NAT address is determined automatically when adding the LINX-101 to the channel in the configuration server. Alternatively, the NAT address can be configured manually. Furthermore the NAT router must be configured to forward ports 1628 and 1629 for UDP and TCP packets to the private IP address of the LINX-101 (192.168.1.100 in Figure 132). In summary we can say the following parameters must be set in order to operate an LINX-101 behind a NAT router.

- Specify the IP address (private IP address: 192.168.1.100),

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

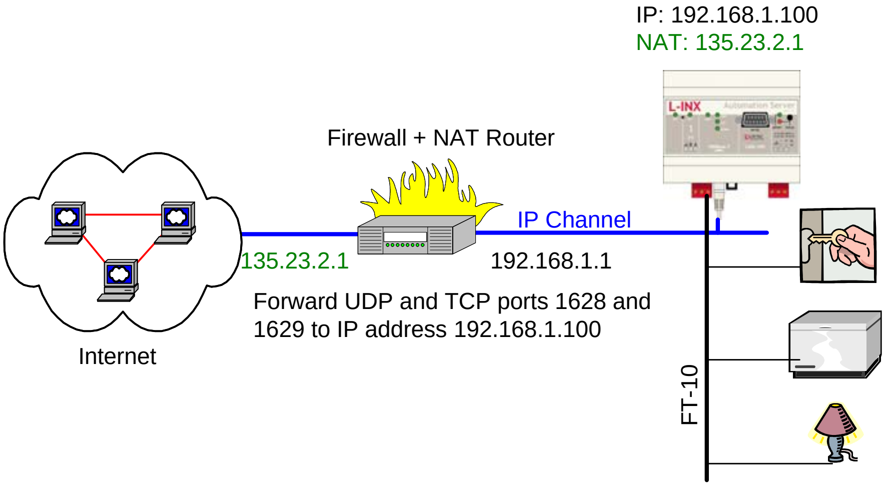


Figure 132: Operating an LINX-101 behind a NAT router and firewall.

Note that an LINX-101 must be used as configuration server when the device is installed behind a firewall or NAT router. The LINX-101 with the configuration server can also be located behind a firewall.

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

When using more than one IP-852 device behind a single NAT router the recommended method in the LINX-101 configuration server is to use the extended NAT mode. This mode requires that all devices support this feature. Currently these are LINX-101, L-IP 3.0, *i*.LON 600, and the NIC852 PC software from LOYTEC. If there are other devices in the channel, this method does not work. Incompatible devices are disabled from the channel in this case. Please refer to the classic method in Section 8.4.3 to setup this network.

When using multiple devices behind a NAT router, each device needs a separate port-forwarding rule in the NAT router. This implies, that each device must use a unique client port (e.g. 1628, 1630, 1631, etc). The port-forwarding rules must be setup that each port points to one of the IP-852 devices. In the LINX-101 change the client port in the CEA-852 device configuration menu. Figure 133 shows an example configuration for three LINX-101s behind the NAT router 135.23.2.1.

It is recommended that both ports 1628 and 1629 are forwarded to the same private address. It is then also possible to turn on the configuration server behind a NAT router. In this case activate the CS on the LINX-101 which has port-forwarding to 1628 and 1629. In the example in Figure 133 the LINX-101 with private address 192.168.1.100 also acts as a configuration server.

If the CS is activated on an LINX-101 behind a NAT router, the NAT router must have a fixed public IP address. The LINX-101 with the CS also cannot use automatic NAT discovery. In this case enter the NAT address of the NAT router manually in the IP configuration menu (Auto-NAT can no longer be enabled on an LINX-101 with a CS). To diagnose possible problems in the NAT configuration with port forwarding use the enhanced communications test (see Section 4.11.5).

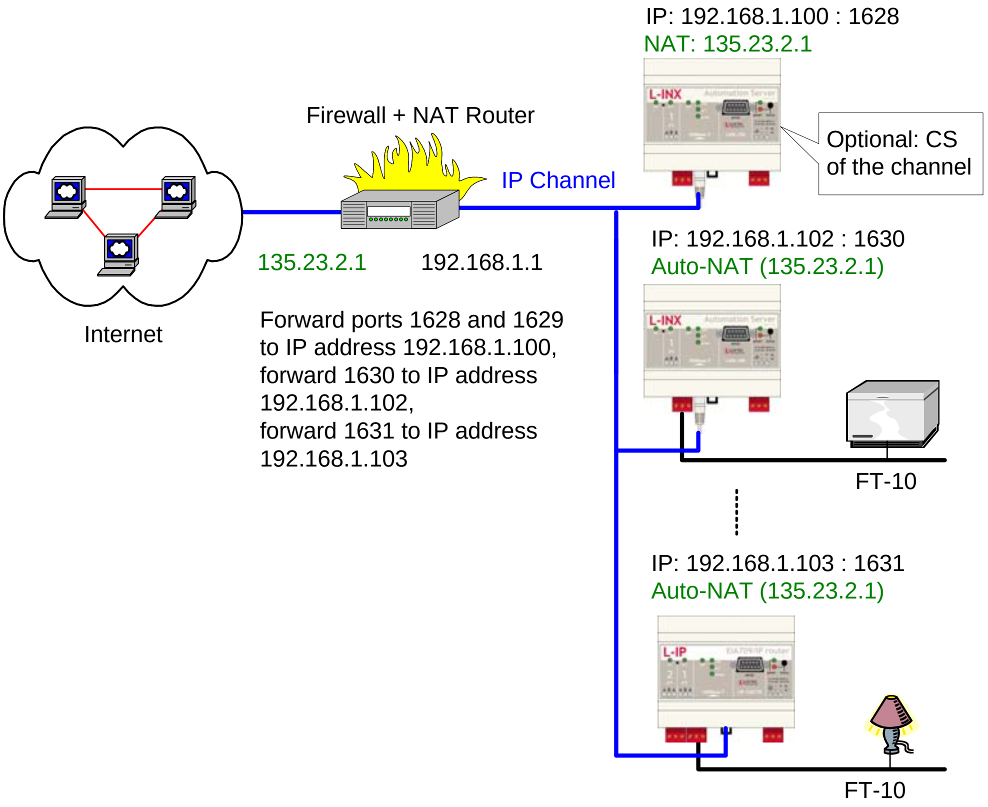


Figure 133: Multiple LINX-101 devices behind a NAT: Extended NAT Mode.

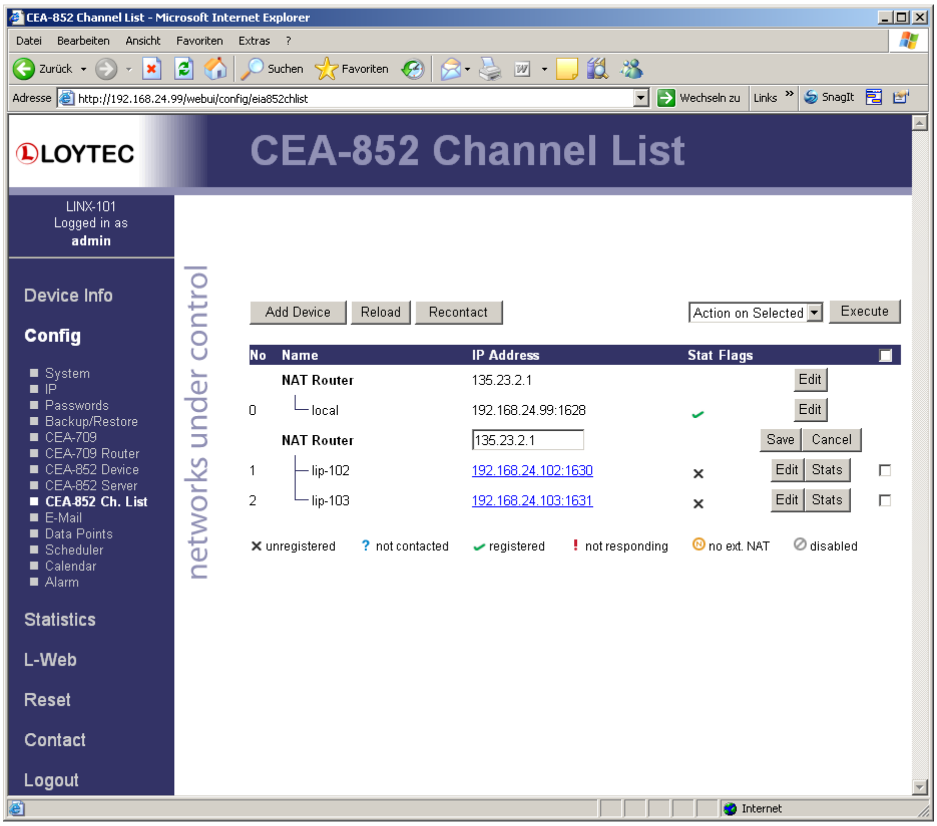
After the NAT router has been configured with the port-forwarding settings and the CS has been turned on, the channel members can be added. This can be done either on the console UI or through the Web interface of the CS.

On the console UI add the devices to the channel in the configuration server menu 7. Choose ‘a’ to add a device. Enter the private address of the device in the IP address field. Enter the public address of the NAT router in the NAT address field. Modify the port as needed. For example, to add the LINX-101 with port 1631 in Figure 133, enter the values as shown in Figure 134.

```
CEA-852 Member Menu
===================

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

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

Figure 134: Adding a member with extended NAT Mode on the console UI.

In the Web UI add the members with their private IP addresses and the client ports as defined by the port-forwarding. Then select the added member by checking the check box and select the action “Assign to NAT”. Enter the public NAT address of the NAT router. An example to add the two IP-852 devices in Figure 133 through the Web UI is depicted in Figure 135. To remove a device from a NAT router but not delete it, select it and choose “Remove from NAT” as the action.



No	Name	IP Address	Stat	Flags	
	NAT Router	135.23.2.1		Edit	
0	local	192.168.24.99:1628	✓	Edit	
	NAT Router	135.23.2.1		Save Cancel	
1	lip-102	192.168.24.102:1630	×	Edit Stats	□
2	lip-103	192.168.24.103:1631	×	Edit Stats	□

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

Figure 135: Adding a member with extended NAT Mode on the Web UI.

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

If more than one LINX-101 must be used behind the NAT router and there are devices which do not support the extended NAT mode, we propose the setup from Figure 136.

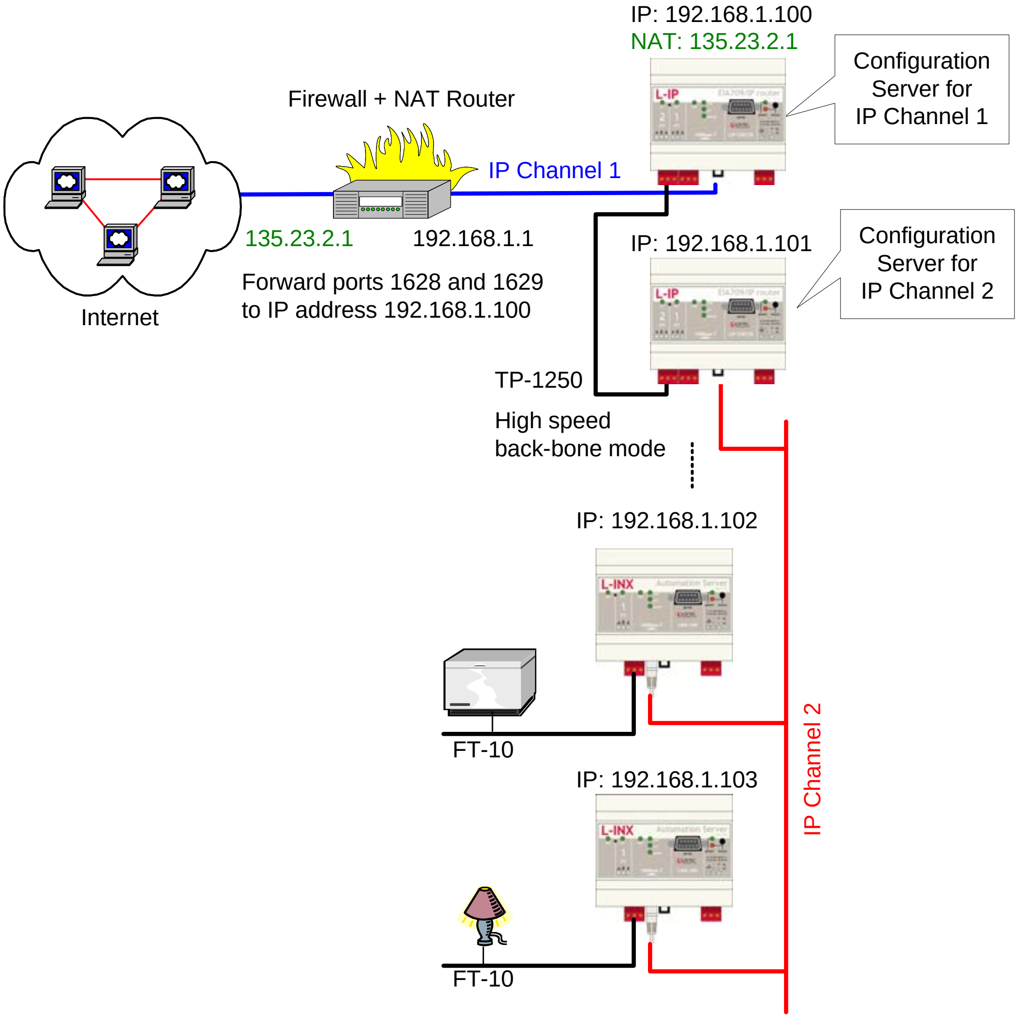


Figure 136: Application that uses multiple LINX-101 devices behind a NAT router firewall.

The LINX-101 with IP address 192.168.1.100 is member of IP Channel 1 and can be accessed through the Internet. The LINX-101 devices with IP addresses 192.168.101 to 192.168.1.110 form another logical IP Channel 2 that communicates with the devices on the IP Channel 1 over the TP-1250 channel, which is used in high-speed backbone mode for optimum networking performance. Note that devices on both IP Channels 1 and 2 can of course connect to the same physical network wiring. Furthermore both IP Channels 1 and 2 must have a separate configuration server that manages the LINX-101 devices on the different channels. In the example in Figure 136 the LINX-101 with address 192.168.1.100 acts as the configuration server for IP Channel 1 and the LINX-101 with IP address 192.168.1.101 acts as the configuration server for IP Channel 2.

8.5 Multi-Cast Configuration

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

The LINX-101 supports both unicast and multi-cast delivery of CNIP data packets. Using multi-cast is recommended when using the LINX-101's router in the Smart Switch Mode. For those LINX-101s configure a multi-cast address in the IP configuration menu. Please contact your system administrator to obtain a valid multi-cast address for your network.

Note, that all channel members must be configured with the same multi-cast address and use the same client port (1628 is recommended). Also note, that multi-cast addresses cannot be routed on the Internet. They can only be used in a LAN or VPN environment.

If you configure multi-cast there may be some devices, which do not support this feature. In this case, the LINX-101 uses a hybrid scheme and sends unicast to those devices, which are not configured for multi-cast. Note, that the LINX-101 determines automatically, when to switch to the multi-cast mode depending what types of devices are in the channel and on the traffic burden for those devices. As a rule of thumb multi-cast is used when there are only switches/repeaters in the channel and it is not used when there are only configured routers.

To detect, if the LINX-101's router utilizes the multi-cast feature to send to other devices, contact the Extended CEA-852 device statistics in the statistics menu (Section 5.2.6). The entry "Channel Routing Mode" reads SL (send list) if packets are routed to the multi-cast group. It reads CR (channel routing) if the normal unicast method is employed. Also the entry "Multi-cast packets sent" in the CEA-852 device statistics menu (Section 5.2.6) counts the number of multicast packets transmitted to the group. If this item remains zero, no multi-cast is used by the LINX-101.

8.6 Remote LPA Operation

The LINX-101 supports remote LPA access. This means that a protocol analyzer connected to the Ethernet network can connect to the LINX-101 and record all packets on the CEA-709 channel (FT-10). Our LPA-IP supports this sophisticated feature. The principle functionality is shown in Figure 137.

The LPA-IP runs on a Windows PC that is connected to the Ethernet network. In a LINX-101 device selection window one can e.g. select the LINX-101 with IP address 192.168.1.210 and display all packets on the FT-10 channel connected to the LINX-101 with IP address 192.168.1.210. For this operation the LPA-IP does not need to be a member of the CN/IP channel. Note that this functionality is only possible with LINX-101 Internet routers.

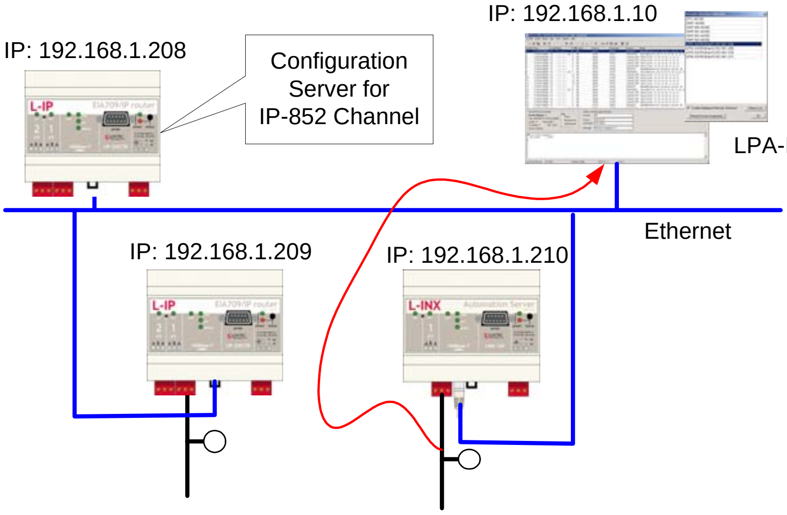


Figure 137: Remote LPA principle.

8.7 Internet Timing Aspects

If the LINX-101's router is used over the Internet or in a large Intranet with unpredictable network delays the user should become familiar with the following advanced timing aspects. Channel Timeout is set in the configuration server whereas escrowing and aggregation are set in the CEA-852 client device whereas the Channel Delay is a channel property of LNS and can be set in NL-220, LonMaker or other network management tools.

Table 9 summarizes the timing values that must be set when operating the LINX-101 under WAN conditions.

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

Table 9: Advanced IP-852 timing parameters.

Please use a PC to determine the average ping delay between the different LINX-101s in the network. If multiple LINX-101s are communicating with each other always use the largest measured average ping delay for the input value for the calculations in Table 9.

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

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

8.7.1 Channel Timeout

The Channel Timeout is a property of the CN/IP channel. If a packet travels across this CN/IP channel for longer than what is specified in Channel Timeout in ms the packet is discarded. The LINX-101s always needs to synchronize with a SNTP timeserver when a Channel Timeout is set other than 0 ms.

Channel Timeout is highly recommended if MD5 authentication is enabled in order to prevent replay. Set Channel Timeout to 200 ms and Channel Delay to 20 ms in a LAN environment. Please refer to Section 4.9.6 on how to enable or disable the Channel Timeout.

If an LNS based network management tool like LonMaker or NL220 is used on a network that has channel timeout enabled please install an NTP client program (e.g. achron4.exe) on this PC that synchronizes the PC clock to the NTP time. Otherwise the PC clock and the clock inside the LINX-101 will drift apart and communication between the PC and the LINX-101 will terminate.

8.7.2 Channel Delay

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

8.7.3 Escrowing Timer (Packet Reorder Timer)

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

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

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

8.7.4 SNTP Time Server

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

In larger CN/IP networks like the Internet with possibly long packet delays one must specify a SNTP server to synchronize the local clocks of the LINX-101 devices. The local clocks must be synchronized to a common notion of time in order to make CN/IP protocol features like escrowing (Channel Timeout) work properly.

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

A primary and a secondary SNTP server can be defined please refer to Section 4.7.5 and Section 4.9.5 on how to enable the SNTP server.

8.8 Advanced Topics

8.8.1 Aggregation

Aggregation (or packet bunching) is a technique that collects multiple CEA-709 packets into a single larger CN/IP packet. Aggregation improves overall system performance since one CN/IP packets now carries multiple CEA-709 packets und with the same number of CN/IP transactions more CEA-709 packets can be exchanged between LINX-101 devices thus reducing protocol overhead. The Aggregation Timeout defines the time period in ms in which the transmitting device collects the CEA-709 packets before it transmits the CN/IP packet over the CN/IP channel. Please refer to Section 4.7.7 on how to enable aggregation. Note, that aggregation adds a delay to the transactions but dramatically improves the throughput of your CN/IP channel. Use aggregation if you have a high channel load but can tolerate some additional propagation delay given by the aggregation time value.

8.8.2 MD5 Authentication

MD5 authentication is a method to verify the authenticity of the sending device. Only devices that have MD5 enabled and use the same MD5 secret can share information with each other. If the configuration server has MD5 enabled only devices that have MD5 enabled and use the same MD5 secret as the configuration server can join the logical CN/IP channel. Please refer to Section 4.7.8 and Section 4.9.9 for details.

8.8.3 Dynamic NAT Addresses

A common practice for Internet providers is to assign addresses on a per-session basis to a client. Each time a connection is established (e.g., an ADSL link is set up) the Internet provider may choose an IP address from a pool. Since this address will be the public address of a NAT router, the NAT address configured in the LINX-101 would need to be updated. The Auto-NAT feature in the LINX-101 permanently monitors the current NAT address. When the LINX-101 detects a change in the NAT address it re-registers with the configuration server using this new address. This feature requires an LOYTEC configuration server (e.g., LINX-101, L-IP) and "Roaming Members" enabled on that CS.

A consequence of this monitoring process is that the LINX-101 contacts the CS every 45 seconds to probe for the NAT address. This causes a small amount of additional traffic on the Internet link. The Auto-NAT feature also causes any shut-down connection to be re-established. The NAT monitoring functions as a keep-alive for the connection. If neither the additional traffic nor the automatic initiation of a new connection is tolerable, then the Auto-NAT feature must be disabled and the NAT address configured manually. In this case, the Internet service provider needs to assign a fixed public IP address to the NAT router.

9 OPC Server

9.1 XML-DA OPC Server

9.1.1 Access Methods

The primary function of the LINX-10X is to expose data points to the built-in OPC server. The OPC tag namespace is built from the data point hierarchy, which has been configured by the Configurator software. The OPC server on the device implements the data access standard via the Web service interface XML-DA. The OPC XML-DA Web service is accessible via the URI

http://192.168.24.100/DA

where the IP address has to be replaced with the actual IP address of the LINX-10X. The Web service is accessible over the same TCP port as the Web server. The default TCP port is 80. The Web server port can only be changed via the console (see Section 4.4.4) or in the L-Config tool.

Since the Web service is easily routable on the Internet, the LINX-10X OPC server implements the basic authentication method to protect the system from unauthorized write access. Read access is available without authentication. The basic authentication involved the operator user and the password configured for this user. On how to configure the operator's password please refer to Section 5.1. To disable the basic authentication clear the operator's password.

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

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

- Use LOYTEC's L-Web visualization tool that comes free with the LINX-10X,
- use a standard OPC client or SCADA package, or
- create your own Web service client with custom Web Pages.

The easiest way to visualize the network's data points over a Web-based interface using the LINX-10X is the L-Web software. This software is fully integrated into the LINX-10X Configurator and allows designing graphical page content. The tool is intuitive to use like the L-Vis graphical page designer. The resulting L-Web application is stored on the LINX-10X and can be directly accessed in your Web browser or other Internet appliances, such as PDAs. For more information on the L-Web refer to Section 9.2.

Standard OPC clients and SCADA packages, which shall visualize the LINX-10X's data points, must conform to the OPC XML-DA standard. This means they must support the OPC Web service and not only the COM/DCOM protocol. If your SCADA package does not support OPC XML-DA, a PC-based bridge from XML-DA to the COM-based protocol can be used. The bridge software is running on a PC and translates from COM/DCOM requests into XML-DA Web service requests. The system is depicted in Figure 138.

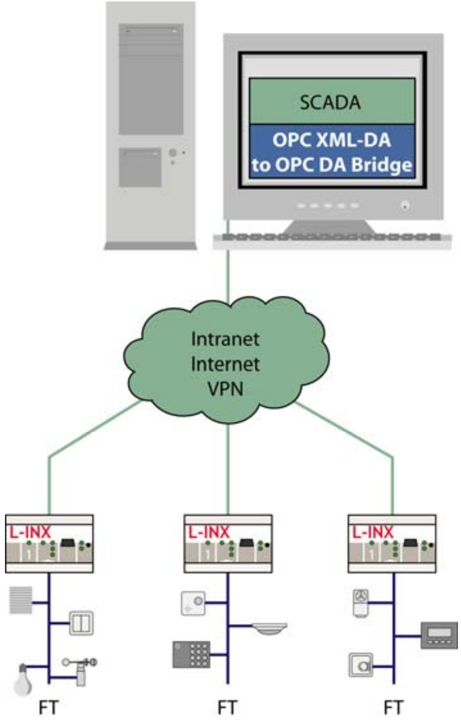


Figure 138: Using a XML-DA/DCOM bridge.

With the bridge configured to access a number of LINX-10X, the COM-based SCADA application can access a COM-based OPC server for each LINX-10X. The bridge software OPCBR-800 can be purchased and installed on any PC. This is discussed in Section 9.3.

Finally, customers can create their own XML-DA clients based on the WSDL for OPC XML-DA. Refer to Section 9.4 for more information.

9.1.2 Data Points

The data point hierarchy as configured by the LINX-10X Configurator software is exposed to the OPC tag namespace by the LINX-10X. This is done internally for all data points, which are marked for OPC exposure (i.e., have the OPC check-mark set).

Folders are translated into OPC nodes. Any of the data point classes analog, binary, multi-state, string, and user are exposed as OPC tags. Each OPC tag contains the value of the data point and some of its meta-data as available in OPC. An example of browsing the OPC tags on the LINX-10X is shown in Figure 139.

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

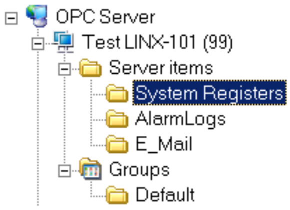

OPC Server
Test LINX-101 (99)
Server items
System Registers
AlarmLogs
E_Mail
Groups
Default

Figure 139: Client browsing the OPC tag namespace on a LINX-10X.

9.1.2.1 Analog

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

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

9.1.2.2 Binary

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

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

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

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

9.1.2.3 Multi-state

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

- Item Canonical Data Type (SmallInt): This property indicates the data type ‘3’ (Integer).

- Item Value (Integer): The present data point value.

- Item Quality (SmallInt): The value quality. It is “good” if the data point is in normal state, or “uncertain” if the data point has an off-normal state, e.g., offline or unreliable.

- Item Timestamp (Date): This property contains the timestamp of the last value update.

- Item Access Rights (Integer): This property defines, if the tag is read-only or read/write.

- Item Description (String): This is the description of the data point.

- Item EU Type (Integer): This property is ‘2’ for multi-state.

- Enumerated EU (Array of String): This property contains the state texts of the data point.

9.1.2.4 User Type

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

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

- Item Value (String): A hex string without whitespace representing the byte array.

- Item Quality (SmallInt): The value quality. It is “good” if the data point is in normal state, or “uncertain” if the data point has an off-normal state, e.g., offline or unreliable.

- Item Timestamp (Date): This property contains the timestamp of the last value update.

- Item Access Rights (Integer): This property defines, if the tag is read-only or read/write.

- Item Description (String): This is the description of the data point.

9.1.2.5 Structured Data Points

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

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

9.1.3 AST Objects

The alarming, scheduling, and trending (AST) objects are more complex than regular data points. The OPC XML-DA standard does not have appropriate tags for those objects. Therefore, the LINX-10X exposes AST objects as a set of OPC tags describing the object. All tags for one AST object are collected under an OPC node representing the AST object.

9.1.3.1 Scheduler Object

The LINX-10X exposes the schedule objects to OPC XML-DA tags. Each schedule object is represented by a node in the OPC name space. The content of the schedule XML contents referred to in this Section must be compliant to the scheduleCfg schema. This schema can be found at the LOYTEC Web site. The XML documents can refer to the target namespace 'http://www.loytec.com/xsd/scheduleCfg/1.0/'.

In that node, the following OPC tags are available:

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

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

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

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

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

9.1.3.2 Calendar Object

The LINX-10X exposes the calendar objects to OPC XML-DA tags. Each calendar object is represented by a folder in the OPC name space. In that folder, the following OPC tags shall be available:

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

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

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

9.1.3.3 Alarm Objects

The LINX-10X alarm objects provide the *alarm summary* and can be used to acknowledge alarms. The alarm objects are exposed to XML-DA tags. Each alarm is uniquely identified by an XML alarm ID (XAID). The XAID must identify the alarm object and the alarm ID in that object. The XAID is used in the acknowledge service to identify the alarm. The XAID can also be transmitted in E-Mail notifications.

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

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

- Summary (string, Read-only): Reading from this tag, the current alarm summary can be obtained. The data type is string and the tag contains an XML document. This tag should not be subscribed to. The root element of the XML document is the *alarmSummary* element.

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

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

9.1.3.4 Trend Log Objects

Each trend log object on the LINX-10X is represented as a folder in the OPC name space. This folder contains a number of tags describing and controlling the trend log. To retrieve log records, however, the XML-DA tag interface cannot be used. There are two options: (1) retrieve the complete log as a CSV file, or use the proprietary Data Log Web service (XML-DL). That Web service uses the logHandle provided by a tag. The CSV file location can be obtained from a tag also.

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

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

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

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

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

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

- CentralDL0, CentralDL1 (string, read/write): These tags serve as placeholders for the central data logger to store its URI. The tag CentralDL0 is intended for the primary, CentralDL1 for the secondary central data logger. The tags are stores in non-volatile memory and retain their values over a power-on reset.

9.1.3.5 E-Mail Templates

E-Mail templates can be configured in the LINX-10X Configurator software. When an E-Mail template is triggered, the corresponding E-Mail is transmitted. The E-Mail template can also be triggered over the OPC interface. Therefore, a node is added to the OPC name space for each E-Mail template under the "E_Mail" node.

Each E-Mail node is named after the E-Mail template and contains the following OPC tags:

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

- Send (boolean, read/write): When writing TRUE to this tag, the E-Mail transmission is triggered.

9.2 Using L-Web

The L-Web is a Web-based visualization software that comes free with the LINX-10X. It uses the standard Web technologies to visualize and control data provided by one or more LINX-100 or LINX-200 Automation Servers on a Windows PC.

The L-Web software uses the standardized OPC XML-DA Web service to communicate between L-Web and remote LINX-100 or LINX-200 Automation Servers, which makes it extremely firewall-friendly and easy to setup.

The graphical design of the L-Web user interface consists of pages, which can simply be created by using the L-Vis Configurator software without any know-how in HTML, Java, etc. Dynamic information is shown in the form of numeric values, text, changing icons, bar graphs, trend logs, alarm and event lists, or schedule controls.

The complete set of automation functions of the LINX-100 or LINX-200 Automation Server is fully supported by L-Web. The automation services are residing in the embedded LINX-100 or LINX-200 Automation Servers and distributed over the network to build up a dependable system with L-Web only accessing these services. Furthermore, any kind of calculations, data point connections, etc., are implemented on the embedded Automation Server, which makes the application on the Automation Server completely independent from the connection to the L-Web application.

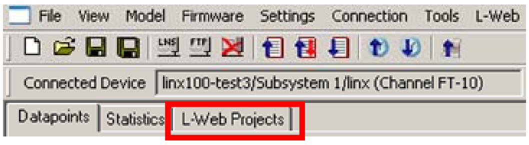
Starting from the LINX-10X data point configuration, the user can create an L-Web project. The L-Web project contains the data point configuration of the Web service interface and a graphical design for the L-Web user interface. For more information on creating graphical designs using the L-Vis Configurator software refer to [1].

9.2.1 Create a new L-Web Project

The LINX-10X Configurator provides the data point configuration, which is downloaded into the device. On top of that configuration, an L-Web design can be created for visualization.

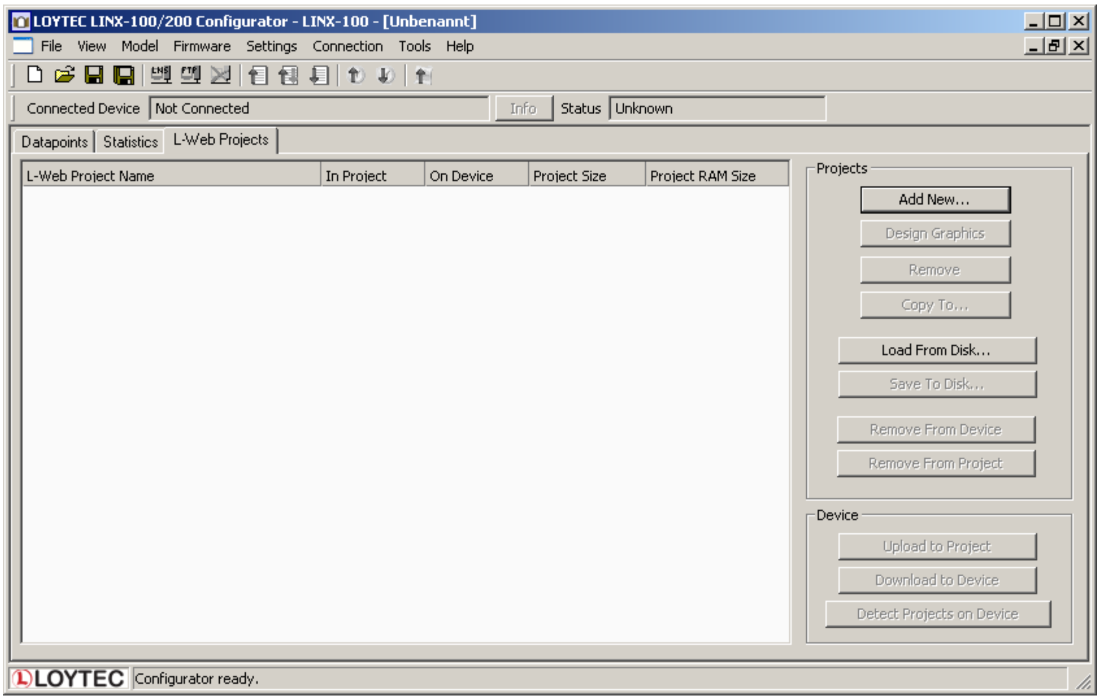
To Create an L-Web Project

1. Start the Configurator software and change to the **L-Web Projects** tab.



Connected Device: linx100-test3/Subsystem 1/linx (Channel FT-10)

2. The L-Web project tab appears as in Figure 140.



Connected Device: Not Connected

Status: Unknown

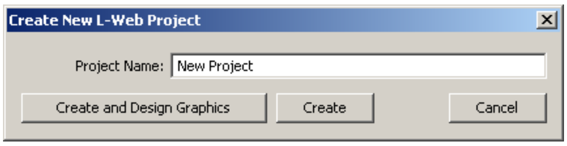
L-Web Project Name	In Project	On Device	Project Size	Project RAM Size

Configurator ready.

Figure 140: L-Web Projects Tab.

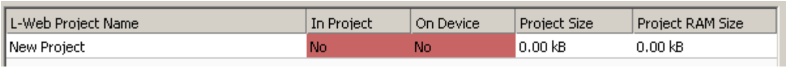
3. Click on **Add New …**

4. Enter a new **Project Name**.



Project Name: New Project

5. Click on **Create**. The new project appears in the projects list.



L-Web Project Name	In Project	On Device	Project Size	Project RAM Size
New Project	No	No	0.00 kB	0.00 kB

9.2.2 Start a Graphical L-Web Design

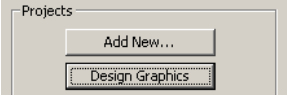
The L-Web graphical design tool is started from within the L-Web projects tab. The graphical design for the L-Web project is created in the L-Vis design tool. The data point configuration created in the LINX-10X configuration project is available for the L-Web project and its graphical design.

To Start a Graphical Design

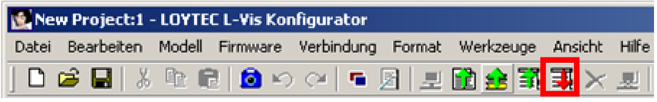
1. Select the **L-Web Projects** tab.

2. Select an L-Web project.

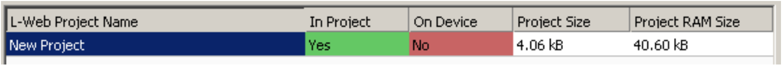
3. Click **Design Graphics**.



4. This opens the L-Vis graphical design tool. Complete the graphical design in the tool and click the **Download to Device** speed button



5. The graphical design is now part of the project.



L-Web Project Name	In Project	On Device	Project Size	Project RAM Size
New Project	Yes	No	4.06 kB	40.60 kB

Note: *If the Configurator had been connected to the device, the graphical design would have been added to the device in the same step.*

9.2.3 Organize L-Web Projects

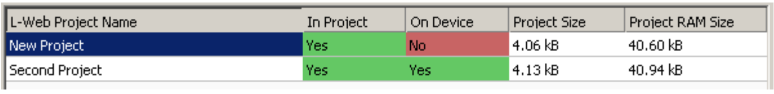
L-Web projects can be organized within the LINX-10X configuration project. L-Web projects can be part of the configuration project and/or stored on the device. For instance, the configuration project may contain a number of L-Web projects, but for saving space on the device, only one of them is downloaded on the device. The L-Web projects tab provides a number of tools to organize a set of L-Web projects.

To Organize L-Web Projects

1. Connect to the device as described in Section 7.7.2.

2. Select the **L-Web Projects** tab.

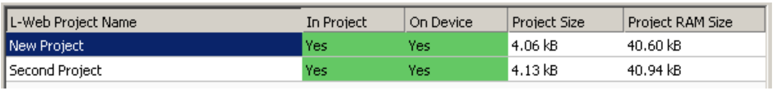
3. Click **Detect Projects on Device**. This scans for all projects found on the device.



L-Web Project Name	In Project	On Device	Project Size	Project RAM Size
New Project	Yes	No	4.06 kB	40.60 kB
Second Project	Yes	Yes	4.13 kB	40.94 kB

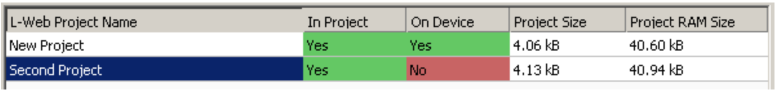
Projects marked as a green **Yes** in the **In Project** column are L-Web projects, which are part of the current LINX-10X configuration project. Projects marked as a green **Yes** in the **On Device** column are L-Web projects, which are part of the current LINX-10X configuration project. A red **No** identifies the L-Web project to be missing in the project or on the device, respectively.

4. If you want to download an L-Web project to the device, which is missing there, select the project and click **Download to Device**. After the download the project appears with a green **Yes** in **On Device**.



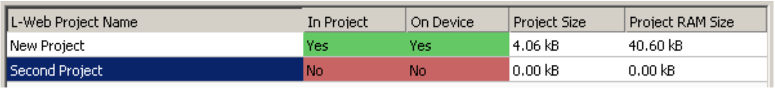
L-Web Project Name	In Project	On Device	Project Size	Project RAM Size
New Project	Yes	Yes	4.06 kB	40.60 kB
Second Project	Yes	Yes	4.13 kB	40.94 kB

5. If you want to remove a project from the device, click **Remove from Device**.



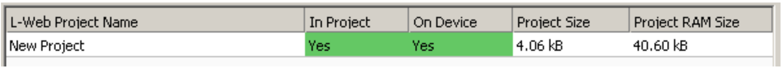
L-Web Project Name	In Project	On Device	Project Size	Project RAM Size
New Project	Yes	Yes	4.06 kB	40.60 kB
Second Project	Yes	No	4.13 kB	40.94 kB

6. If you want to remove the project from the current LINX-10X project file, click **Remove from Project**.



L-Web Project Name	In Project	On Device	Project Size	Project RAM Size
New Project	Yes	Yes	4.06 kB	40.60 kB
Second Project	No	No	0.00 kB	0.00 kB

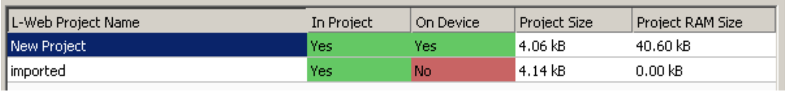
7. If you want to remove the L-Web project altogether, click **Remove**.



L-Web Project Name	In Project	On Device	Project Size	Project RAM Size
New Project	Yes	Yes	4.06 kB	40.60 kB

8. If you want to export the L-Web project into a separate L-Web project file, click **Save to Disk …** and select a file name in the file requestor dialog.

9. If you want to import an L-Web project from a separate L-Web project file, click **Load from Disk …** and select the file in the file requestor dialog. The L-Web project appears in the project but not on the device.



L-Web Project Name	In Project	On Device	Project Size	Project RAM Size
New Project	Yes	Yes	4.06 kB	40.60 kB
imported	Yes	No	4.14 kB	0.00 kB

9.3 Using the OPC Bridge

9.3.1 Software Installation

The LOYTEC OPC Bridge software LOPC-BR800 is installed as a separate application on a PC. A license for the LOYTEC OPC Bridge software must be purchased separately. With one software license for the OPC Bridge, multiple LINX-10X devices can be accessed. With the OPC Bridge software installed, each configured LOYTEC LINX-10X device appears as a separate COM/DCOM server. The OPC Bridge software can be used with LOYTEC LINX OPC servers only. The bridge won't connect to third-party OPC servers.

System requirements:

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

The OPC Bridge software is available on the LOYTEC Software CD or via download from the LOYTEC Web site www.loytec.com. For installing the software, a registration code must be purchased.

To Install the OPC Bridge

1. Double click on 'lopc-br800_1_0_setup.exe' and follow the installation steps.

2. When asked type in the bridge's registration code. Click **Next**.

3. Finalize all remaining installation steps by clicking **Next** and **Finish**.

When the installation is complete, the OPC Bridge software is available under Programs → LOYTEC OPC Bridge.

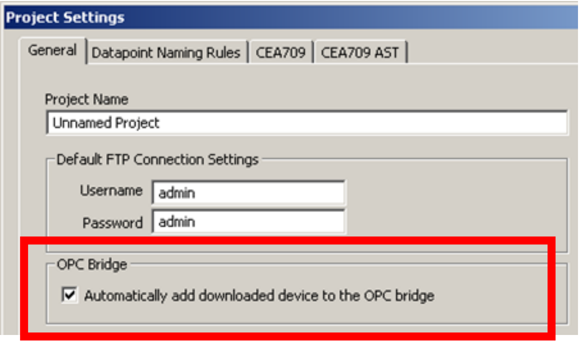
9.3.2 Configure the Bridge Locally

If the bridge software is installed on the same PC as where the LINX-10X Configurator software is used to configure the LINX-10X OPC server, the server information can be automatically made available as a COM OPC server. This is done when the LINX-10X configuration is downloaded into the device.

To Configure the Bridge Locally

1. Open the Configurator software and configure the LINX-10X as described in Section 7.7.

2. In the LINX-10X Configurator menu go to "Settings|Project settings …". This opens the project settings dialog on the tab **General** as shown in Figure 141.



Project Name: Unnamed Project

Default FTP Connection Settings

Username: admin

Password: admin

OPC Bridge

☑ Automatically add downloaded device to the OPC bridge

Figure 141: Enable bridge export in the project settings.

3. Put a check mark on **Automatically add downloaded device to the OPC bridge**.

4. Click **Ok.**

5. Downloading the configuration also makes the LINX-10X available as a COM OPC server through the local bridge.

9.3.3 Export OPC Servers for another PC

If the bridge software is not installed locally on the same PC as where the LINX-10X configuration is created, it must be exported to make the OPC server information available. The exported file can then be transferred to the OPC bridge.

To Export the Bridge Configuration

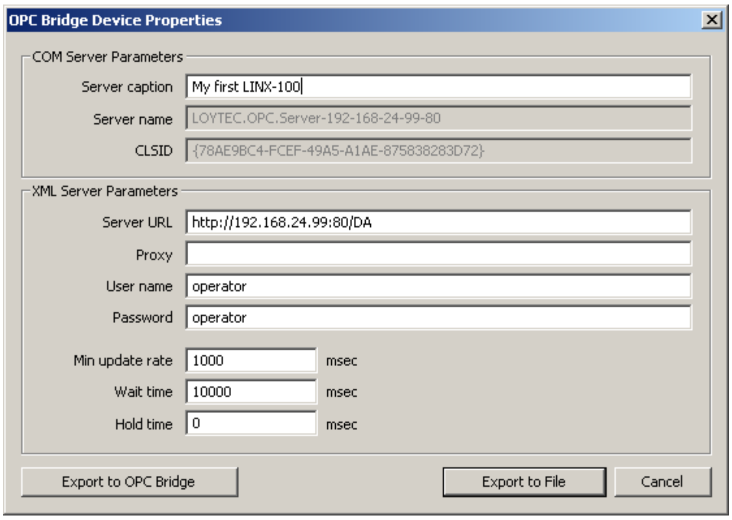
1. Open the LINX-10X Configurator.

2. Connect to the LINX-10X, which shall be available in the bridge.

3. Select the menu **File → Export to OPC Bridge**.

4. In the **OPC Bridge Device Properties** dialog as shown in Figure 142 add information, which is not default, i.e., Min update rate, Wait time and Hold Time. If the operator user has a non-default password, enter the password.

5. Click **Export to File**.



OPC Bridge Device Properties

COM Server Parameters

Server caption: My first LINX-100

Server name: LOYTEC.OPC.Server-192-168-24-99-80

CLSID: {78AE9BC4-FCEF-49A5-A1AE-875838283D72}

XML Server Parameters

Server URL: http://192.168.24.99:80/DA

Proxy:

User name: operator

Password: operator

Min update rate: 1000 msec

Wait time: 10000 msec

Hold time: 0 msec

Figure 142: Bridge Export dialog.

9.3.4 Import OPC Servers Using the Configurator

When using OPC server information exported by the Configurator, the exported server definition must be imported to the OPC bridge. This can be also done using the Configurator software. The Configurator software must be installed on the same PC as the OPC bridge for doing so.

To Import a Server Definition

1. Open the Configurator software.

2. Select the menu **File → Import Bridge Configuration**.

3. In the file requestor select the bridge configuration XML file, which has previously been exported and click **Ok**.

4. The **OPC Bridge Device Properties** dialog displays the imported bridge information.

5. Click **Export to Bridge** to add the respective COM server to the bridge.

6. Click **Save**.

9.3.5 Manually Configure Servers

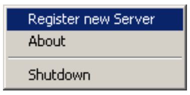
The OPC bridge configuration can also be edited manually. The same procedure is also applicable to verify imported OPC server definitions in the bridge software. After adding a server definition in the bridge software, the LINX-10X will be available as a COM OPC server through the bridge.

To Configure a Server in the Bridge

1. Start the OPC bridge from the Windows Start menu under Programs → LOYTEC OPC Bridge → OPC Bridge manual Setup.

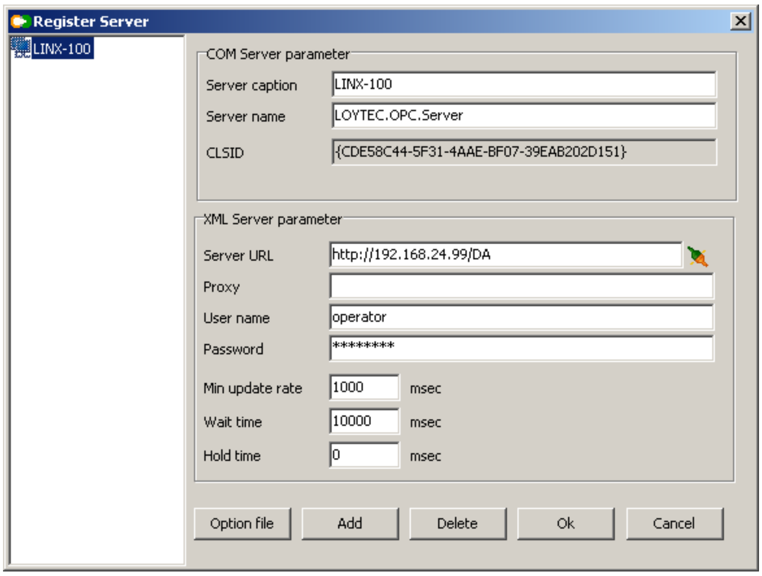
2. In the system tray, right-click on the bridge icon .

3. In the context menu select **Register new Server**.



4. In the Register Server dialog click **Add**.

5. A new server entry is added. Enter the information on **Server caption** (this is displayed), **Server name** (this is the COM object name), and the **Server URL** (the URL of the LINX-10X device) as shown in Figure 143.



Server caption: LINX-100
Server name: LOYTEC.OPC.Server
CLSID: {CDE58C44-5F31-4AAE-BF07-39EAB202D151}
Server URL: http://192.168.24.99/DA
Proxy:
User name: operator
Password: ********
Min update rate: 1000 msec
Wait time: 10000 msec
Hold time: 0 msec

Figure 143: Register Server dialog in the bridge software.

6. Additionally, enter the “operator” as the **User name** and its **Password** on the device.

7. Click **Ok**.

9.4 Using Custom Web Pages

Custom Web pages can also be developed for the LINX-10X. For doing so, the applications engineer must implement an OPC XML-DA Web service client, which adheres to the WSDL interface. This can be done in C++ or script languages such as Perl. The WSDL must be obtained from the OPC Foundation’s Web site following the OPC XML-DA namespace http://opcfoundation.org/webservices/xmlda/1.0/.

Any Web content, including scripts, applications or static Web pages can be stored directly on the LINX-10X’s file system. Use the admin account to upload the content via FTP into the directory

```
/var/www
```

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

10 Operating Interfaces

10.1 Common Interface

10.1.1 Schedule and Calendar XML Files

The daily schedule and calendar pattern configuration can be changes at run-time over the Web UI or the network. An alternate way to change that configuration is to download a schedule and calendar XML file via FTP onto the device. After the file has been downloaded, the new configuration becomes effective immediately. The device does not need to be rebooted. The files are located in

```
/tmp/uid/sched/UID.xml
/tmp/uid/cal/UID.xml
```

The *UID* is the unique ID of the data point. The UID can be obtained from the ID column in the data point list as shown in Figure 128. A schedule data point with UID 107C would result in the schedule XML file ‘`/tmp/uid/sched/107C.xml`’. The UID remains constant for the life time of the data point even when the name or description is changed.

The content of the XML file must be compliant to the scheduleCfg schema. This schema can be found at the LOYTEC Web site. The XML documents can refer to the target namespace ‘http://www.loytec.com/xsd/scheduleCfg/1.0/’.

10.1.2 Trend Log CSV File

The CSV file format for a trend log and the location of those files are defined in this section. The trend log CSV files are accessible either via their UID only, or in combination with contents of the trend log object name. The files are located in

```
/tmp/uid/trend/UID.csv
/data/trend/Datapointname_UID.csv
```

The *UID* is the unique ID of the data point. The UID can be obtained from the ID column in the data point list as shown in Figure 128. For a more user-friendly listing of the files, the *Datapointname* contains the trend log’s object name. It is truncated after 23 ASCII characters to fit the requirements of the file system. A trend CSV file for the trend object ‘trend0’ and the UID ‘107C’ would result in the CSV file ‘`/data/trend/trend0_107C.csv`’. The UID remains constant for the life time of the object even when the name is changed.

The CSV file format for a trend log is defined in this section. The CSV file starts with a header, containing at least the first line, which specifies the CSV format (log_csv_ver). The current version is 2. The next line contains the field log_device. It has trailing fields that specify the vendor, product code, firmware version and device ID string. The Device ID String can be one of the following: (IP) 192.168.24.100, (BACnet Device) 224100, (CEA-709 NID) NID.

The log_info line specifies the fields UID and name of the trend log object. The line log_create has two fields specifying the date and time when this CSV log was generated. The line log_capacity has two fields: the current number of log entries in the file and the log capacity.

Following are one or more lines of log_item. Each line specifies a trended data point. The first field is the index, the second the ID of the logged data point, the third the data point name. The data point name can be augmented by engineering units in square brackets. Log entries in the CSV refer to the item index to identify the data point, for which the entry was logged.

```
#log_csv_ver,2
#log_device;LOYTEC;Product Code;Firmware Version;Device ID String
#log_info;Log-ID;Log Name
#log_create;YYY-MM-DD;HH:MM:SS
#log_capacity;filled;capacity
#log_item;index;UID;data point name [units]
```

After those lines any number of comment lines starting with a hash character ‘#’ are allowed. One line contains the column headings. Lines that are not comments specify one log record per line, using the column information as described below. The columns are separated by commas ‘,’ or semi-colons ‘;’. If commas are used as a separator, the decimal point must be a point ‘.’. If semi-colons are used, the decimal point must be a comma ‘,’.

Column	Field	Example	Description
A	Sequence Number	50	The log record sequence number. This is the monotonously increasing sequence number, which is unique for each log record.
B	Source	0	Data point source identifier. Indexes into logger_entry header. For value lines in a multi-column CSV, this field indexes the first column, which has a value. For the ERROR record type, the field indexes the data source that caused the error. For LOGSTATE, TIMECHANGE records this field is not applicable and can be left at zero.
C	Record Type	2	The record type: LOGSTATE (0), BOOL (1), REAL (2), ENUM (3), UNSIGNED (4), SIGNED (5), NULL (7), ERROR (8), TIMECHANGE (9)
D	Error/Time Change/Log Status	1	This field is valid for records of type ERROR, TIMECHANGE, and LOGSTATUS.
E	Date/Time	2007-11-02 15:34:22	The date/ime of the log record. This is in the format YYYY-MM-DD HH:MM:SS.
F	Value 0	24,5	Logged value from source 0 or empty
G	Value 1	200	Logged value from source 1 or empty
…	…		
…	Value *n* – 1	5000	Logged value from source *n* – 1 or empty

Table 10: Columns of the Trend Log CSV File

There are as many value columns as value sources specified in the header. If at a given date/time more values are logged, all of them appear in the same line. If at that given time some sources did not log values, those columns are left empty. The “Source” column in a multi-value CSV refers to the first data source that supplied a value in a given line.

10.1.3 Alarm Log CSV File

The historical alarm logs are also accessible as CSV-formatted files. The alarm log CSV files are accessible either via their UID only, or in combination with contents of the alarm log object name. The files are located in

```
/tmp/uid/allog/UID.csv
/data/allog/Alarmlogname_UID.csv
```

The *UID* is the unique ID of the alarm log object. The UID can be obtained from the ID column in the data point list of the alarm log folder, similar to obtaining the UID of trend log objects. For a more user-friendly listing of the files, the *Alarmlogname* contains the alarm log's object name. It is truncated after 23 ASCII characters to fit the requirements of the file system. A trend CSV file for the alarm log object 'alarmlog0' and the UID '100C' would result in the CSV file '`/data/allog/alarmlog0_100C.csv`'. The UID remains constant for the life time of the object even when the name is changed.

The CSV format of the alarm log CSV file is identical to the trend log CSV format as described in Section 10.1.2.

10.2 CEA-709 Interface

10.2.1 NV Import File

Network variables can be imported to the LINX-10X 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 11. 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 of the NV on the network node. Indices start at 0.
C	NV selector	1	The NV selector in decimal 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 11: CSV Columns of the NV Import File

10.2.2 Node Object

The LINX-10X provides a node object conforming to the LONMARK guidelines. A diagram of the node object is depicted in Figure 144.

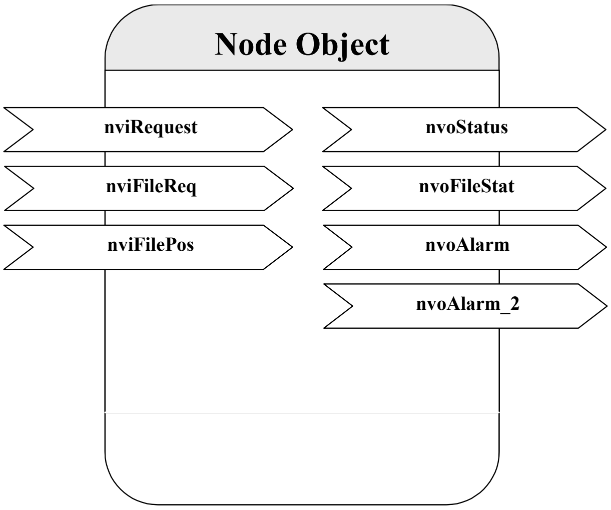


Figure 144: Node Object

- The Node Object accepts the following commands via *nviRequest*: RQ_NORMAL, RQ_UPDATE_STATUS, RQ_REPORT_MASK, RQ_ENABLE, RQ_DISABLE, RQ_UPDATE_ALARM, RQ_CLEAR_ALARM, 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 LINX-10X and react with a defined action (e.g. send an email). By supporting both alarm SNVTs, SNVT_alarm and SNVT_alarm_2, legacy and state-of-the-art alarm handling is supported.
- nviDateEvent (*SNVT_date_event*), nvoDateResync (*SNVT_switch*): These NVs are part of the standard LONMARK node object, if schedulers are used. If not bound, the local calendar is used. If a global calendar shall be used, both of these NVs must be bound to the respective NVs of the global calendar object.
- nviTimeSet (*SNVT_time_stamp*): When writing to this NV, the system is set. The time value is interpreted as local time
- nvoSystemTemp (*SNVT_temp*): This NV can be used to poll the system temperature of the LINX-10X. It does not send updates and must be polled.
- nvoSupplyVolt (*SNVT_volt*): This NV can be used to poll the supply voltage of the LINX-10X. It does not send updates and must be polled.
- nvoIpAddress (*SNVT_str_asc*): This NV can be used to poll the IP address of the LINX-10X. It does not send updates.
- nciEarthPos (*SNVT_earth_pos*): This configuration property can be used to set the earth position of the LINX-10X. It has been implemented as an NV to make other devices send that configuration to the LINX-10X over the network (e.g., from a GPS device).
- nviClearStat (*SNVT_switch*): When writing {100.0 1} to this NV, the channel monitor objects' statistics data are cleared.
- nvoUpTime (*SNVT_elapsed_tm*): This NV contains the elapsed time since the last reboot.

10.2.3 Real-Time Keeper Object

When the scheduler objects are enabled in the project settings, the LINX-10X includes the standard LONMARK real-time keeper object.

10.2.4 Channel Monitor Object

Figure 145 shows the Channel Monitor Object functional block. This functional block is responsible for network monitoring. There is one object for each channel the LINX-10X is attached to: The channel monitor object with index 0 corresponds to the FT port of the LINX-10X, while the object with index 1 corresponds to the IP-852 port of the LINX-10X. If a port is not available in the current system configuration, the nvoElapsedTime is set to the invalid value and nvoPort is set to 255.

Each object has the following network variables:

- nvoPort (*SNVT_count*): Index of port associated with this Channel Monitor Object instance. Port 1 corresponds to the FT port of the LINX-10X, while port 2 corresponds to the IP-852 port of the LINX-10X. If the monitored port is not available in a system configuration, the value is 255. This NV is polled only.
- nvoElapsedTime (*SNVT_elapsed_tm*): Time since LINX-10X powered up or since the statistics for this port where reset. The statistics can be reset with the network variable *nviClearStat* in the node object (see Section 10.2.2) or if the node is reset with a network management command (e.g. while the device is commissioned). If the monitored port is not available in a system configuration, the value is set to the invalid value. The NV is polled only.
- nvoAvgPkts (SNVT_count_32): The average number of packets per second received or transmitted via the associated channel since power-up or since the statistics for this port where reset.
- nvoIvalBandUtl (*SNVT_lev_cont*): Bandwidth utilization of associated channel during the last interval. For a smooth operation of the CEA-709 segment the bandwidth utilization must remain below 50%.

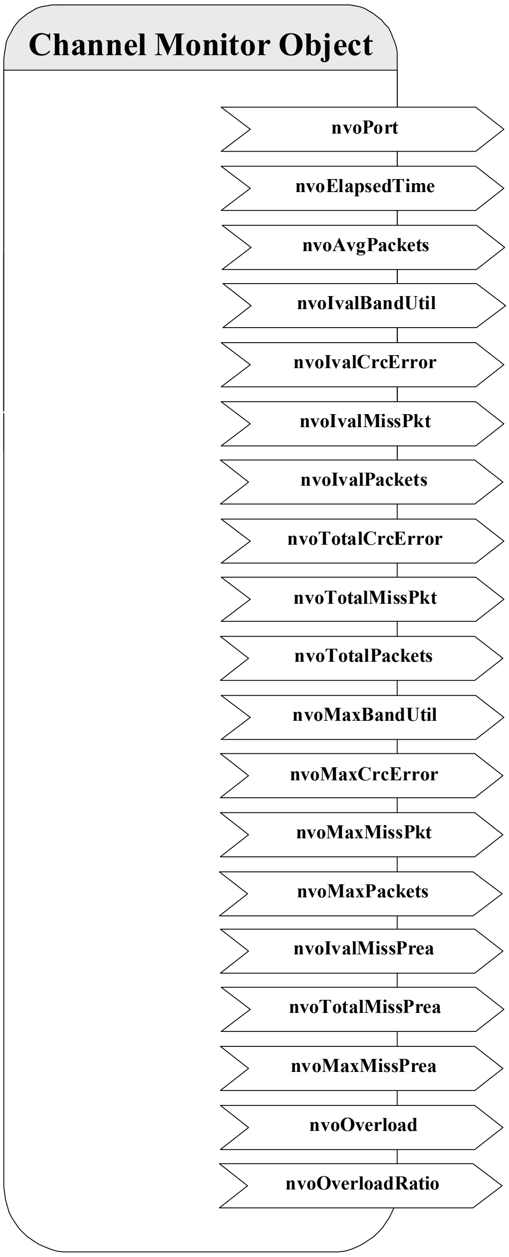


Figure 145: Channel Monitor Object

- nvoIvalCrcErr (*SNVT_lev_cont*): Percentage of packets with CRC error received on the associated channel during the last interval.
- nvoIvalMissed (*SNVT_lev_cont*): Percentage of packets from the associated channel which could not be processed during the last interval.
- nvoIvalPkts (*SNVT_count_32*): Number of packets received or transmitted via the associated channel during the last interval.
- nvoTotalCrcErr (*SNVT_count_32*): Total number of packets with CRC error received via the associated channel since power-up or since the statistics for this port where reset.
- nvoTotalMissed (*SNVT_count_32*): Total number of packets from the associated channel which could not be processed since power-up or since the statistics for this port where reset.
- nvoTotalPkts (*SNVT_count_32*): Total number of packets received or transmitted via the associated channel since power-up or since the statistics for this port where reset.

- nvoMaxBandUtl (*SNVT_lev_cont*): Maximum value of *nvoIvalBandUtl* since power-up or since the statistics for this port where reset. For a smooth operation of the CEA-709 segment the bandwidth utilization must remain below 50%.
- nvoMaxCrcErr (*SNVT_lev_cont*): Maximum value of *nvoIvalCrcErr* since power-up or since the statistics for this port where reset.
- nvoMaxMissed (*SNVT_lev_cont*): Maximum value of *nvoIvalMissed* since power-up or since the statistics for this port where reset.
- nvoMaxPkts (*SNVT_count_32*): Maximum value of *nvoIvalPkts* since power-up or since the statistics for this port where reset.
- nvoIvalMisPre (*SNVT_count_32*): Number of missed preambles per second on the associated channel measured during the last interval. A missed preamble is detected, whenever the link layer receives a preamble, which is shorter then the defined preamble length. A large number in this counter is usually due to noise on the channel.
- nvoTotalMisPre (*SNVT_count_32*): Total number of missed preambles per second on the associated channel measured since power-up or since the statistics for this port where reset.
- nvoMaxMisPre (*SNVT_count_32*): Maximum value of *nvoIvalMisPre* since power-up or since the statistics for this port where reset.
- nvoChnlAlarm (*SNVT_switch*): Signals an overload alarm condition of the channel during the last statistic interval. A channel can be overloaded due to one of the following conditions:
  - The bandwidth utilization during the last statistic interval (*nvoIvalBandUtl*) exceeded the limit defined by the *SCPThighLimit1* (default 70%) OR
  - The CRC Error Rate during the last statistic interval (*nvoIvalCrcErr*) exceeded the limit defined by the *SCPThighLimit1* (default 5%) OR
  - The Missed Packets Rate during the last statistic interval (*nvoIvalMissed*) was not zero OR
  - The Missed Preamble Rate during the last statistic interval (*nvoIvalMisPre*) exceeded the limit defined by the *SCPThighLimit1* (default switched off).

  If an overload is detected the network variable is set to {100, ON}, while if no error occurred it is set to {0, OFF}.
- nvoChnlAlarmRat (*SNVT_lev_cont*): Ratio between statistic intervals during which the channel was in overload alarm condition and intervals during which the channel was not in overload alarm condition since power-up or since the statistics for this port where reset.

In addition, each channel monitor object has the following SCPTs:

- SCPTifaceDesc: This configuration property contains a human-readable name of the monitored port. Possible values on the LINX-10X are "CEA-709", "IP", "inactive".
- SCPTmaxSndT: Defines how often output NVs are transmitted. Exceptions are nvoPort, nvoElapsedTime, which are polled-only.

10.2.5 Calendar Object

When the scheduler objects are enabled in the project settings, the LINX-10X includes the standard LONMARK calendar object.

10.2.6 Scheduler Object

When the scheduler objects are enabled in the project settings, the LINX-10X includes the configured number of standard LONMARK scheduler objects.

10.2.7 Clients Object

When the remote AST object feature is enabled in the project settings, the LINX-10X includes a proprietary object, which is a container for network variables required to implement the remote object features.

For remote schedulers and calendars, *nviSchedLink* and *nviCalLink* NVs are created. For alarm clients nviAlarm_2 NVs are created.

10.2.8 Gateway Objects

The LINX-10X contains eight proprietary Gateway objects. These are containers for all NVs, which are configured on the LINX-10X’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.

11 Network Media

11.1 FT

The LINX-10X 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 LINX-10X 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.

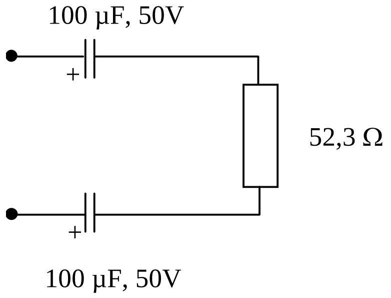


Figure 146: FT Free Topology Termination

In a double terminated 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.

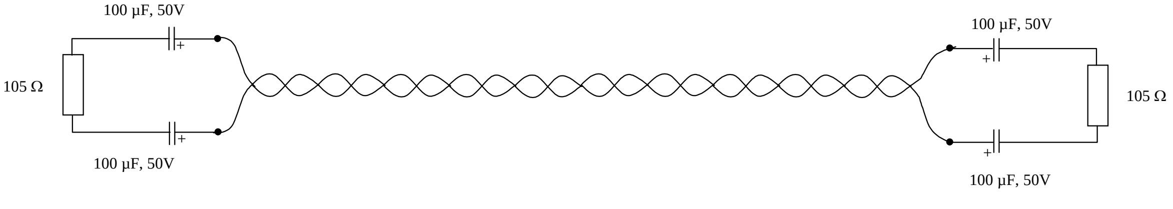


Figure 147: Termination in an FT Bus Topology

12 LINX-10X Firmware Update

The LINX-10X firmware supports remote upgrade over the network and the serial console.

To guarantee that the LINX-10X is not destroyed due to a failed firmware update, the LINX-10X firmware consists of two images:

- LINX-10X fallback image,
- LINX-10X primary image.

The LINX-10X 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 LINX-10X boots up with the fallback image, the OPC LED, the CEA-709 port LED and the CNIP LED are flashing red.

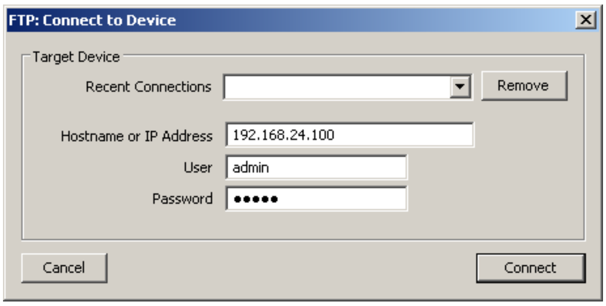
12.1 Firmware Update via the LINX-10X Configurator

The LINX-10X primary image can be updated using the LINX-10X Configurator. For this purpose, the LINX-10X must be connected to the Ethernet and must have a valid IP configuration (see Section 4.6 and 5.2.2). The LINX-10X Configurator must be installed (see Section 0).

To Update the Firmware using the LINX-10X Configurator

1. Start the LINX-10X Configurator from the Windows Start menu: Start → Programs → LOYTEC LINX-10X Configuration → Configure LINX-10X.

2. Select the menu: Operations → Connect to LINX-10X → FTP. This opens the FTP connection dialog as shown in Figure 148.



Hostname or IP Address: 192.168.24.100
User: admin
Password: ●●●●●

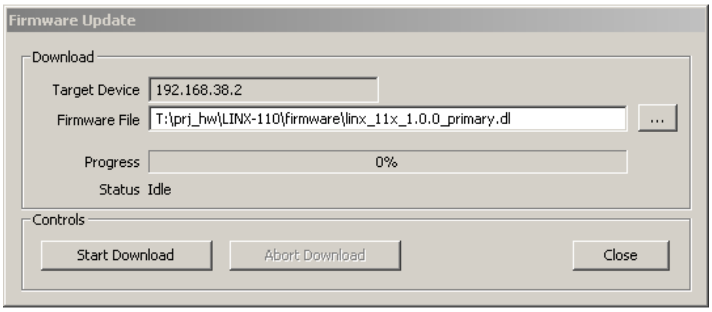
Figure 148: FTP connection dialog.

3. In the FTP connection dialog enter the IP address of the LINX-10X to upgrade and 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 4.10.2).

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 (“linx_lc3k_3_0_0_primary.dl”).



Firmware Update

Download

Target Device 192.168.38.2

Firmware File T:\prj_hw\LINX-110\firmware\linx_11x_1.0.0_primary.dl

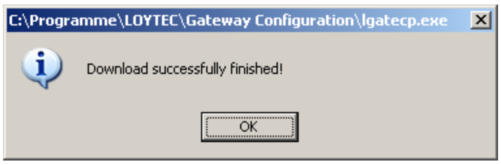
Progress 0%

Status Idle

Figure 149: Firmware Update dialog of the LINX-10X Configurator.

7. Click on Start Download.

8. Observe the download progress. When the download is complete the dialog shown in Figure 150 appears.



C:\Programme\LOYTEC\Gateway Configuration\lgatecp.exe

Download successfully finished!

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.

12.2 Firmware Update via the Console

To download the firmware via the console interface, the LINX-10X 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 LINX-10X console shows the main menu otherwise navigate to the main menu or simply reset the LINX-10X.

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.

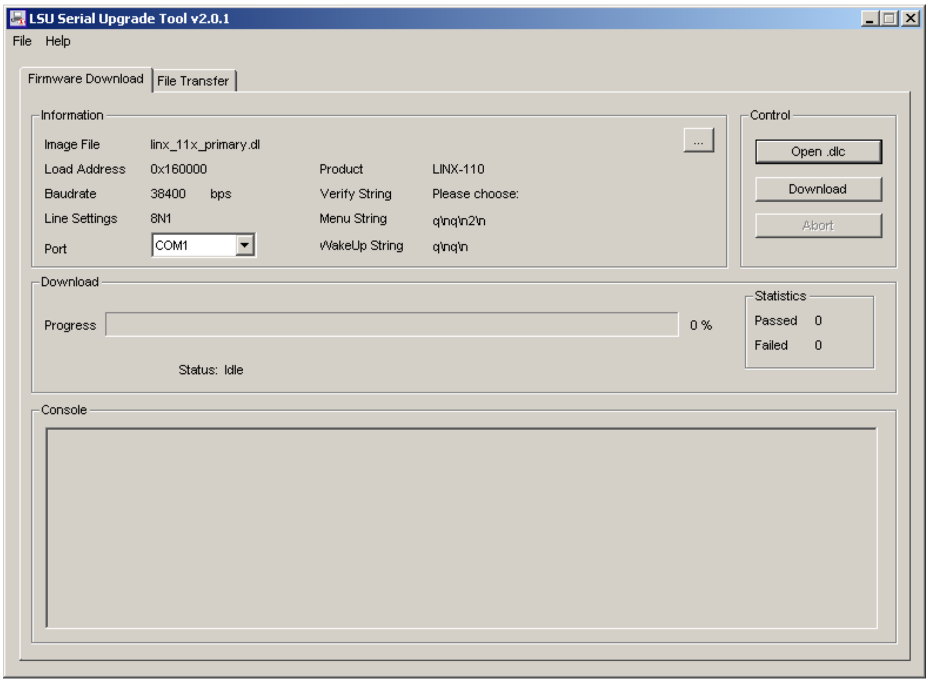


Image File linx_11x_primary.dl

Load Address 0x160000

Product LINX-110

Baudrate 38400 bps

Verify String Please choose:

Line Settings 8N1

Menu String q\nq\n2\n

Port COM1

WakeUp String q\nq\n

Progress 0 %

Status: Idle

Passed 0

Failed 0

Figure 151: LSU Serial Upgrade Tool in Idle Mode

2. If the LINX-10X 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.

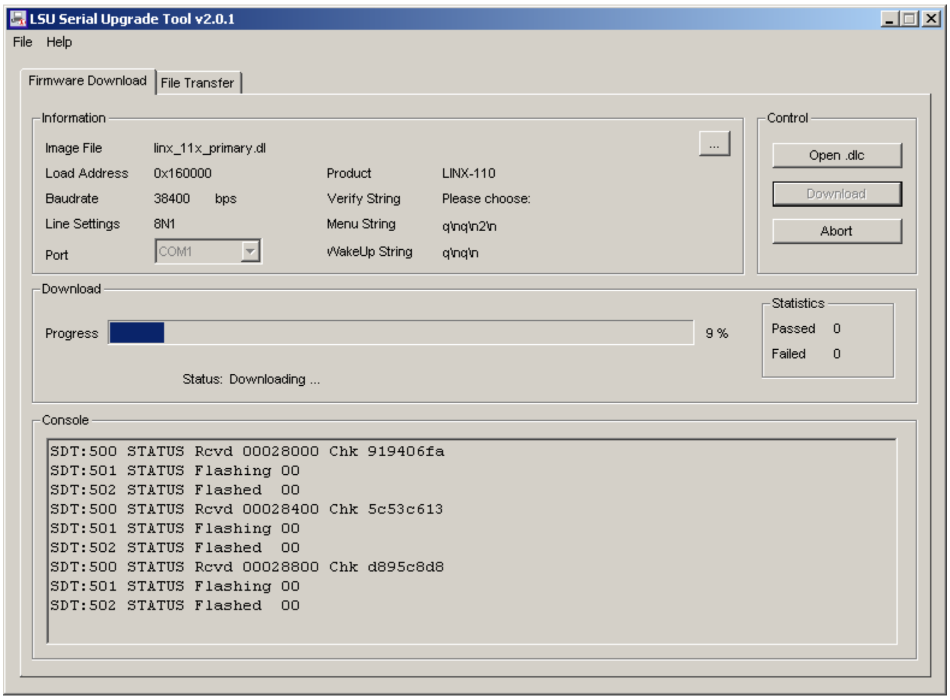


Image File linx_11x_primary.dl

Load Address 0x160000

Baudrate 38400 bps

Line Settings 8N1

Port COM1

Product LINX-110

Verify String Please choose:

Menu String q\nq\n2\n

WakeUp String q\nq\n

Progress 9 %

Status: Downloading ...

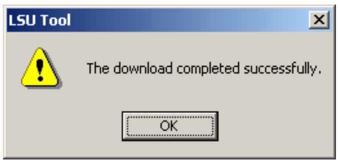
Passed 0

Failed 0

```
SDT:500 STATUS Rcvd 00028000 Chk 919406fa
SDT:501 STATUS Flashing 00
SDT:502 STATUS Flashed  00
SDT:500 STATUS Rcvd 00028400 Chk 5c53c613
SDT:501 STATUS Flashing 00
SDT:502 STATUS Flashed  00
SDT:500 STATUS Rcvd 00028800 Chk d895c8d8
SDT:501 STATUS Flashing 00
SDT:502 STATUS Flashed  00
```

Figure 152: Progress Bar during Firmware Download.

3. If the upgrade is successful, the following window appears (Figure 153).



The download completed successfully.

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.

13 Troubleshooting

13.1 Technical Support

LOYTEC offers free telephone and e-mail support for our LINX-10X 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

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

or

LOYTEC Americas Inc.
11258 Goodnight Lane
Suite 101
Dallas, Texas 75229
USA

Email:	***support@loytec-americas.com***
web:	***http://www.loytec-americas.com***
tel:	***+1/512/402 5319***
fax:	***+1/972/243 6886***

14 Application Notes

14.1 The LSD Tool

Please refer to application note "AN002E LSD Tool" for further information about the LOYTEC system diagnostics tool for the LINX-10X.

14.2 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.

15 Firmware Versions

Table 12 shows the most important features available only in certain firmware versions.

Firmware Version/ Features	3.0.0			
OPC XML-DA Server	√			
CEA-709 Network Scan	√			
UNVTs, SCPTs	√			
XML configuration	√			
Scheduler	√			
Trend Log	√			
Alarming	√			
Alarm Log	√			
E-Mail	√			
Backup/Restore Configuration	√			

Table 12: Available Features depending on Firmware Version

16 Specifications

16.1 LINX-10X

16.1.1 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 +85°C
Humidity (non condensing) operating	10 to 90% RH @ 50°C
Humidity (non condensing) storage	90% RH @ 50°C
Enclosure	Installation enclosure 6 TE, DIN 43 880
Environmental Protection	IP 40 (enclosure); IP 20 (screw terminals)
Installation	DIN rail mounting (EN 50 022) or wall mounting

16.1.2 Resource Limits

Total number of data points	10000
OPC tags	1000
User registers	1000
NVs (static, dynamic)	1000
External NVs	1000
Alias NVs	1000 (both ECS and legacy mode)
Address table entries	512 (15 in legacy mode)
LONMARK Calendar objects	1 (25 calendar patterns)

LONMARK Scheduler objects	100 (max. AST configuration size 384KB)
LONMARK Alarm Servers	1
Trend Logs	100 (total aggregated size 2MB)
E-Mail templates	100
Math objects	100
Alarm logs	10

17 References

[1] L-Web User's Manual, LOYTEC electronics GmbH, Document No. 88074201 , August 2008.

18 Revision History

Date	Version	Author	Description
08-02-07	1.0	STS	Initial revision V1.0 for L-OPC 1.0
01-08-08	3.0	STS	Initial revision V3.0 for LINX-10X 3.0