
L-Gate™

CEA-709/BACnet Gateway

User's Manual

LOYTEC electronics GmbH



Contact

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

Version 3.0.1

Document 88072405

LOYTEC MAKES AND YOU RECEIVE NO WARRANTIES OR CONDITIONS,
EXPRESS, IMPLIED, STATUTORY OR IN ANY COMMUNICATION WITH YOU,
AND

LOYTEC SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THIS
PRODUCT IS NOT DESIGNED OR INTENDED FOR USE IN EQUIPMENT
INTENDED FOR SURGICAL IMPLANT INTO THE BODY OR OTHER
APPLICATIONS INTENDED TO SUPPORT OR SUSTAIN LIFE, FOR USE IN
FLIGHT CONTROL OR ENGINE CONTROL EQUIPMENT WITHIN AN
AIRCRAFT, OR FOR ANY OTHER APPLICATION IN WHICH IN THE FAILURE
OF SUCH PRODUCT COULD CREATE A SITUATION IN WHICH PERSONAL
INJURY OR DEATH MAY OCCUR.

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

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

LonTalk®, LONWORKS®, Neuron®, LONMARK®, LonMaker®, *i.LON*®, and LNS® are
trademarks of Echelon Corporation registered in the United States and other countries.

Contents

1	Introduction	11
1.1	Overview	11
1.2	Scope.....	12
2	Quick-Start Guide	13
2.1	Hardware installation	13
2.2	Configuration of the L-Gate.....	14
2.2.1	IP Configuration on the console	14
2.2.2	IP Configuration via the Web-Interface.....	15
2.2.3	BACnet Configuration	17
2.3	Gateway Configuration with LNS-based Tools.....	18
3	Hardware Installation	19
3.1	Enclosure	19
3.1.1	LGATE-900.....	19
3.2	Product Label.....	20
3.3	Mounting.....	20
3.4	LED signals.....	20
3.4.1	Power LED	20
3.4.2	Status LED.....	20
3.4.3	MSTP Activity LED	20
3.4.4	FT Activity LED	21
3.4.5	Ethernet Link LED.....	21
3.4.6	Ethernet Activity LED	21
3.4.7	CN/IP LED	21
3.4.8	BACnet/IP LED.....	22
3.4.9	Wink Action.....	22
3.4.10	Network Diagnostics.....	22
3.5	Status Button	22
3.6	DIP Switch Settings.....	22
3.7	Power Supply.....	23
3.8	Terminal Layout	23
3.9	Wiring	23
4	Console Interface	25
4.1	Console Connection.....	25
4.2	Self Test.....	25
4.3	L-Gate Device Main Menu	26

4.3.1	Option 1 - Show device information	26
4.3.2	Option 2 – Serial firmware upgrade	27
4.3.3	Option 3 – System configuration.....	27
4.3.4	Option 4 – CEA-709 configuration.....	27
4.3.5	Option 5 – IP configuration.....	27
4.3.6	Option 6 – CEA-852 client configuration	27
4.3.7	Option 7 – BACnet configuration	27
4.3.8	Option 8 - Reset configuration (factory defaults).....	27
4.3.9	Option 9 – Device statistics.....	27
4.3.10	Option 0 – Reset Device.....	28
4.3.11	Option a – Data Points	28
4.4	System Configuration Menu.....	28
4.4.1	Option 1 - Configure Date/Time	28
4.4.2	Option 2 - Configure Earth Position.....	29
4.4.3	Option 7 – FTP server, 8 – FTP server port.....	29
4.4.4	Option 9 – Web server, 0 – Web server port.....	29
4.4.5	Option c – E-Mail Account Configuration.....	29
4.5	CEA-709 Configuration Menu	30
4.5.1	Option 0 – Port configuration.....	30
4.6	IP Configuration Menu.....	30
4.6.1	Option 1 – DHCP	31
4.6.2	Option 2 – IP Address, 3 - IP Netmask, 4 – IP Gateway	31
4.6.3	Option 5 – Hostname, 6 – Domainname	31
4.6.4	Option 7 – DNS Servers.....	31
4.6.5	Option 9 – MAC Address.....	32
4.6.6	Option 0 – NTP Servers	32
4.6.7	Option b – Link Speed & Duplex.....	32
4.7	CEA-852 Device Configuration Menu.....	32
4.7.1	Option 2 – Config server address, 3 – Config server port.....	33
4.7.2	Option 4 – Config client port	33
4.7.3	Option 5 – Device name.....	33
4.7.4	Channel Mode	33
4.7.5	SNTP server, channel timeout.....	33
4.7.6	Option 6 - Escrow timeout	33
4.7.7	Option 7 – Aggregation Timeout	34
4.7.8	Option 8 – MD5 authentication.....	34
4.7.9	Option 9 – MD5 secret.....	34
4.7.10	Option 0 – Location string	34
4.7.11	Option a – NAT Address.....	34

4.7.12 Option b – Multicast Address	35
4.8 BACnet Configuration Menu.....	35
4.8.1 Option 1 – Device ID.....	35
4.8.2 Option 2 – Device name, 3 – Device description, 4 – Device location ...	35
4.8.3 Option 9 – Data Link Layer	35
4.8.4 Option 0 – Configure Data Link Layer.....	35
4.9 Reset configuration (load factory defaults).....	36
4.9.1 Option 1 – Reset everything to factory defaults	37
4.9.2 Option 3 – Reset all passwords.....	37
4.9.3 Option 4 – Clear data point configuration	37
4.10 Device Statistics Menu	37
4.10.1 Option 1 – CEA-852 device statistics.....	37
4.10.2 Option 2 – CEA-709 Application Statistics.....	38
4.10.3 Option 4 – IP statistics	39
4.10.4 Option 6 – Enhanced Communications Test.....	41
4.10.5 Option 7 – Show BACnet MS/TP Statistics	41
4.11 Data Point Menu	42
4.11.1 Option 1 – List Data Points.....	42
4.11.2 Option 2 – Get Value	43
4.11.3 Option 3 – Set Value.....	43
5 Web Interface	44
5.1 Device Information and Account Management	44
5.2 Device Configuration	47
5.2.1 System Configuration	47
5.2.2 IP Configuration	48
5.2.3 CEA-709 Configuration.....	50
5.2.4 CEA-852 Device Configuration	51
5.2.5 BACnet Configuration	53
5.2.6 Data Points.....	55
5.2.7 Scheduler	56
5.2.8 Calendar	58
5.2.9 Alarm	58
5.2.10 E-Mail Configuration.....	59
5.3 Device Statistics.....	60
5.3.1 IP Statistics	60
5.3.2 CEA-852 Statistics.....	61
5.3.3 Enhanced Communications Test.....	62
5.3.4 CEA-709 Statistics.....	63
5.3.5 BACnet MS/TP Statistics	64

5.4	Scheduler Statistics Page.....	65
5.5	Reset, Contact, Logout.....	65
6	L-Gateway Configuration Software	66
6.1	Overview.....	66
6.1.1	Data Points	66
6.1.2	Connections.....	67
6.1.3	Static Interface Changes.....	68
6.1.4	Timing Configuration.....	68
6.2	AST Features	68
6.2.1	Alarming.....	68
6.2.2	Scheduling.....	69
6.2.3	Trending	71
6.2.4	E-Mail.....	71
6.3	Installing the Configuration Software	72
6.4	Registration as a Plug-In.....	72
6.5	Operating Modes of the Configuration Software	73
6.5.1	On-line mode.....	73
6.5.2	Off-line mode	73
6.5.3	Stand-alone mode.....	74
6.6	Data Point Manager	74
6.6.1	Folder List.....	74
6.6.2	Data Point List.....	75
6.6.3	Property View	76
6.7	Project Settings	76
6.7.1	General	76
6.7.2	Data Point Naming Rules	77
6.7.3	CEA-709 Settings.....	78
6.7.4	BACnet Settings.....	79
6.7.5	AST Settings	80
7	L-Gate in a Network.....	83
7.1	Workflows for the L-Gate.....	83
7.1.1	Involved Configuration Files	83
7.1.2	Configure with LNS	83
7.1.3	Configure without LNS.....	84
7.1.4	Configure without LNS Using Bindings.....	85
7.1.5	Replace an L-Gate	86
7.1.6	Configure from BACnet.....	87
7.2	Adding L-Gate	88
7.3	Replace an L-Gate	91

7.4	Using the L-Gateway Configuration Software.....	93
7.4.1	Starting as an LNS Plug-In	93
7.4.2	Starting Stand-Alone.....	94
7.4.3	Uploading the Configuration	95
7.4.4	Scanning for Network Variables.....	96
7.4.5	Importing Network Variables	97
7.4.6	Scanning NVs online from the Network.....	98
7.4.7	Select and Use Network Variables	100
7.4.8	Change the NV Allocation.....	100
7.4.9	Create Static NVs.....	101
7.4.10	Create External NVs	102
7.4.11	Generate BACnet Objects.....	104
7.4.12	Configuration Download	105
7.4.13	Build XIF for Port Interface.....	106
7.4.14	Enable Legacy NM Mode.....	107
7.4.15	Upload Dynamic NVs from Device.....	107
7.4.16	Working with Configuration Properties	108
7.5	Connections	109
7.5.1	Create a New Connection	109
7.5.2	Delete a Connection.....	112
7.5.3	Edit a Connection.....	112
7.6	BACnet Configuration.....	113
7.6.1	Scan for BACnet Objects.....	113
7.6.2	Import from EDE File.....	115
7.6.3	Use Imported BACnet Objects	115
7.6.4	Edit a Client Mapping.....	116
7.6.5	Create Server Object.....	116
7.6.6	Enable International Character Support.....	117
7.7	E-Mail Templates.....	118
7.7.1	Create an E-Mail Template	118
7.7.2	Trigger E-Mails.....	119
7.7.3	Attachments	120
7.7.4	Limit E-Mail Send Rate	121
7.8	Local Schedule and Calendar	121
7.8.1	Create a Calendar.....	121
7.8.2	Create Calendar Pattern	122
7.8.3	Create a Local Scheduler	122
7.8.4	Configure Scheduled Data Points	123
7.8.5	Configure Daily Schedules	124

7.8.6	Configure Exception Days	126
7.8.7	Using the Local Scheduler	127
7.8.8	Limitations	127
7.9	Local Alarming	128
7.9.1	Create an Alarm Server	128
7.9.2	Create an Alarm Condition.....	129
7.9.3	Deliver Alarms via E-Mail	131
7.9.4	Generate Alarms from NVs.....	132
7.10	Local Trending.....	132
7.10.1	Create a Local Trend	132
7.10.2	Trend NVs	132
7.10.3	Download Trend Data in CSV Format	133
7.10.4	Deliver Trend Data via E-Mail.....	133
7.11	Remote AST Objects	134
7.11.1	Remote Scheduler and Calendar	134
7.11.2	Alarm Clients	135
7.12	Mapping CEA-709 and BACnet Schedules.....	136
7.12.1	Mapping and Limitations	136
7.12.2	Map from CEA-709 to BACnet	137
7.12.3	Map from BACnet to CEA-709	138
8	Operating Interfaces	140
8.1	Common Interface.....	140
8.1.1	Schedule and Calendar XML Files	140
8.1.2	Trend Log CSV File	140
8.2	CEA-709 Interface.....	141
8.2.1	Resource Limits.....	141
8.2.2	NV Import File	142
8.2.3	Node Object	143
8.2.4	Extended Node Object Interface	144
8.2.5	Real-Time Keeper Object.....	145
8.2.6	Calendar Object.....	145
8.2.7	Scheduler Object	145
8.2.8	Clients Object.....	145
8.2.9	Gateway Objects	145
8.3	BACnet Interface.....	145
8.3.1	Resource Limits.....	145
8.3.2	Device Object.....	145
8.3.3	Client Mapping CSV File.....	148
8.3.4	EDE Export of BACnet Objects.....	149

9 Network Media	150
9.1 FT	150
10 L-Gate Firmware Update	151
10.1 Firmware Update via FTP.....	151
10.2 Firmware Update via the Console	152
11 Troubleshooting.....	154
11.1 Technical Support.....	154
12 Application Notes	155
12.1 The LSD Tool	155
12.2 Use of Static, Dynamic, and External NVs on a Device.....	155
13 Firmware Versions	156
14 Specifications	157
14.1 LGATE-900	157
15 Revision History	158

Abbreviations

100BaseT	100 Mbps Ethernet network with RJ-45 plug
Aggregation	Collection of several CEA-709 packets into a single CEA-852 packet
AST	Alarming, Scheduling, Trending
BACnet	Building Automation and Control Network
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
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
MS/TP	Master/Slave Token Passing (this is a BACnet data link layer)
NAT	Network Address Translation, see Internet RFC 1631
NV	Network Variable
RTT	Round-Trip Time
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

Introduction

Overview

The L-Gate is a high performance, reliable and secure network infrastructure component that provides data access to a defined set of data points, which are mapped from one control network technology to another control network technology. In particular, the CEA-709/BACnet Gateway (LGATE-900) implements mappings between a set of CEA-709 network variables (NVs) and a set of standard BACnet server objects. Which NVs are mapped to BACnet objects can be configured by an LNS plug-in or stand-alone configuration software. Easy to understand diagnostic LEDs allow installers and system integrators to install and troubleshoot this device without expert knowledge and dedicated troubleshooting tools. The LGATE-900 is equipped with a 100-BaseT Ethernet port (IP), an FT-10 port (CEA-709), and an RS-485 port (MS/TP). The device is fully compliant with ANSI/CEA-709 and ENV14908, ANSI/ASHRAE-135-2004 and ISO 16484.

On the CEA-709 side of the L-Gate, there can be up to 1000 NVs. The 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 L-Gate. In this case, address information is supplied by the configuration software by importing e.g. a CSV file. As communications media on the CEA-709 side, the L-Gate supports either the FT-10 channel or an CEA-852 channel (IP channel over the Intranet/Internet). Which of the two interfaces is used is configurable. The CEA-852 interface 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 BACnet objects on the L-Gate can be of the type analog input/output, binary input/output, and multistate input/output. There can be up to 750 of such objects. They are mapped to NVs as configured by the Gateway configuration software. This software is able to automatically create BACnet object as counterparts to NVs. In particular, BACnet properties such as Object_Name, Description, Units, Max_Pres_Value, Min_Pres_Value, Resolution, Number_Of_States, and State_Text are derived from the Standard Network Variable Types (SNVTs)¹. Further, the automatically assigned default values can be edited in the configuration software. BACnet properties updated during run-time by the gateway are Present_Value, Status_Flags, Reliability, Out_Of_Service. Structured NVs are mapped to one BACnet object per structure member. The BACnet server objects are accessible from the BACnet network. In addition, the L-Gate also includes BACnet client functionality. For each server object a “client mapping” can be defined. These mappings specify other BACnet objects on the network where the L-Gate can read values from (poll or COV subscribe) or write updates to.

¹ This is based on the recommendation in CEN/TS 15231:2006.

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.

In firmware 1.2 and up, the L-Gate supports user-defined network variable types (UNVTs) as dynamic or external NVs, and can access configuration properties (CPs) on other devices through file transfer. To transfer CPs it 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 mapped automatically to BACnet objects.

In firmware versions from 3.0 and up, the L-Gate also supports Trendlog, Schedule and Notification Class objects. These objects can be used to operate on any of the basic BACnet objects, which are mapped to CEA-709 NVs. This allows the L-Gate to provide trend data of one or more NVs, schedule NVs and BACnet objects, and report alarms based on NV conditions directly in BACnet. There can be up to 100 scheduler and calendar objects, up to 32 notification class objects, and up to 100 trend log objects with an aggregated total log buffer size of 2MB.

Furthermore, the L-Gate provides LonMark scheduler/calendar objects, which can directly schedule NVs or be translated to BACnet schedules/calendars. For alarm conditions, the L-Gate can be configured to send E-Mails to pre-defined addresses.

The L-Gate is used for:

- connecting BACnet and CEA-709 networks,
- communicating on BACnet with either BACnet/IP or BACnet/MSTP,
- communicating on CEA-709 with either FT-10 or CEA-852 (IP channel on the Intranet/Internet),
- accessing ANSI/CEA-709 network variables (NVs) and configuration properties (CPs) in BACnet,
- supporting standard (SNVT, SCPT) and user-defined (UNVT, UCPT) types,
- accessing BACnet objects in ANSI/CEA-709 networks,
- scheduling BACnet objects and ANSI/CEA-709 network variables,
- translating BACnet schedules/calendars to LonMark schedules/calendars,
- trending BACnet objects,
- generating alarms using intrinsic reporting on BACnet objects,
- sending E-Mails on alarms or scheduled events.

Scope

This document covers L-Gate devices with firmware version 3.0 and the L-Gateway Configuration Software version 3.0. See Chapter 0 for differences between the different L-Gate firmware versions.

Quick-Start Guide

This Chapter shows step-by-step instructions on how to configure the L-Gate for a simple network architecture, mapping CEA-709 network variables to BACnet server objects.

Hardware installation

Connect power (9-35 VDC or 12-24 VAC), the CEA-709 network, and the Ethernet cable as shown in Figure 1. More detailed instructions are shown in Chapter 0.

Important: *Do not connect terminal 17 with ground!*

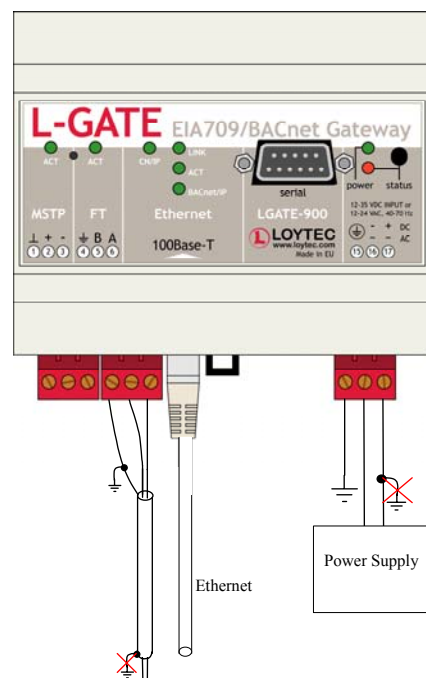


Figure 1: Basic Hardware Installation

If the L-Gate is connected to a BACnet MS/TP network, the MS/TP EIA-485 network must be properly terminated with a termination resistance of 120 Ohms connected at each of the two ends of the segment media. Figure 2 shows how to connect the L-Gate to an MS/TP network.


```
IP Configuration Menu
=====

[1] DHCP                : disabled
[2] IP Address          : 192.168.1.254
[3] IP Netmask          : 255.255.255.0
[4] IP Gateway          : 192.168.1.1
[5] Hostname            : new
[6] Domainname          : <unset>
[7] DNS Servers         : <unset>
[9] MAC Address         : 00:0A:B0:01:0C:9F (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 4: Enter basic IP settings.

Press x to save the IP settings and reset the L-Gate 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.***

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 L-Gate. Note that if your PC has an IP address in a subnet other than 192.168.1.xxx please open a command tool and enter the following route command to add a route to the L-Gate:

Windows START => Run

command.com

route add 192.168.1.254 %COMPUTERNAME%

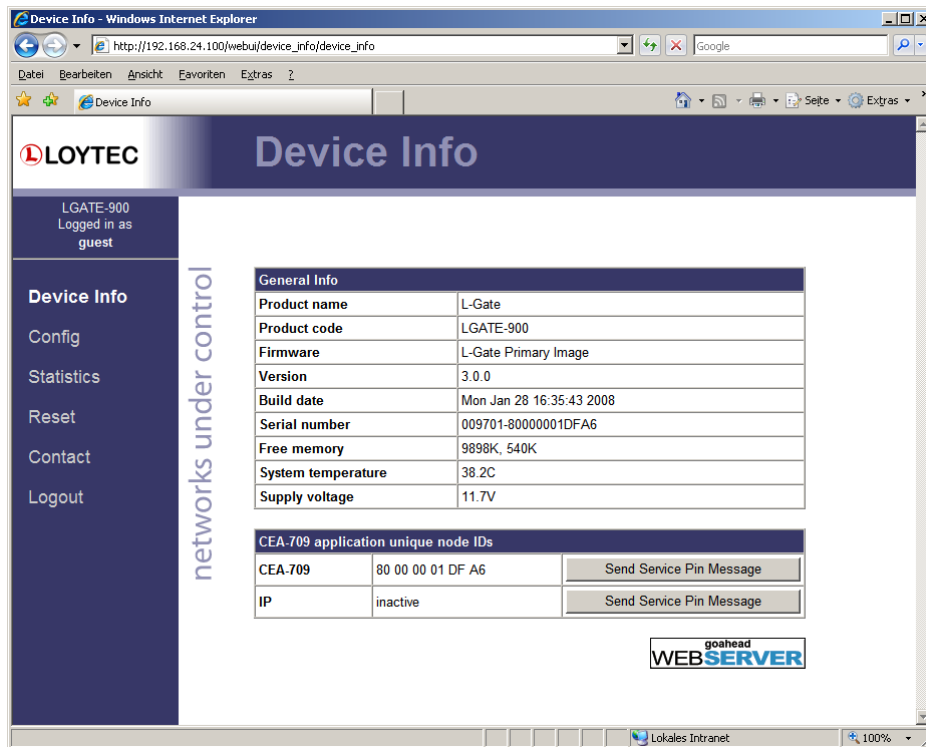


Figure 5: Example Start Screen

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

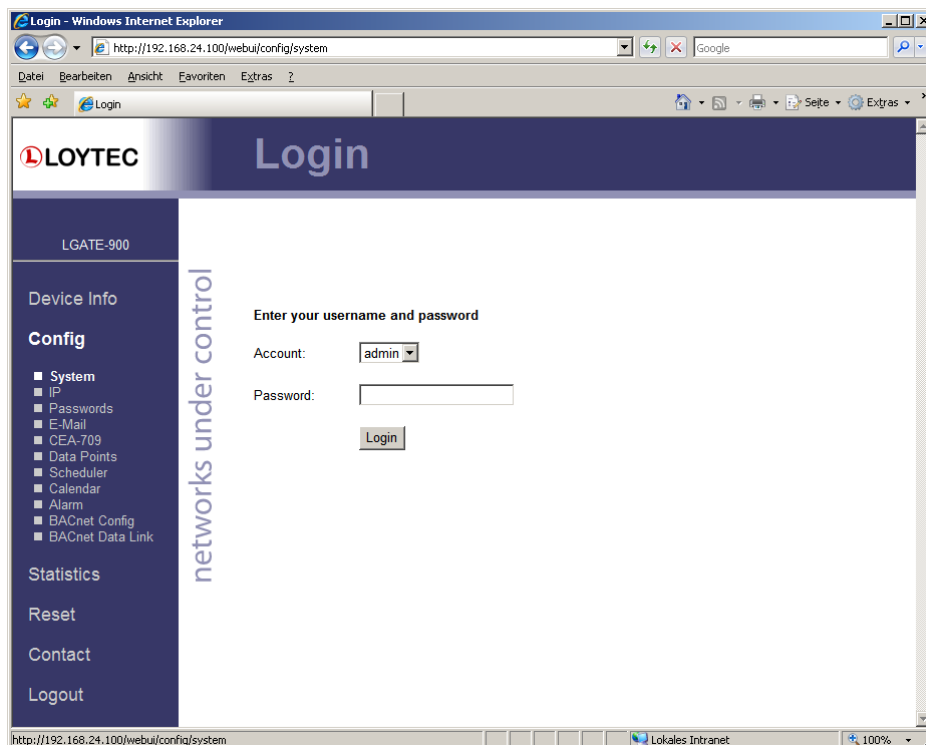


Figure 6: Enter admin as the default administrator password.

The Config menu opens. Click on IP in the Config menu and enter the IP address, the IP netmask, and IP gateway for this L-Gate as shown in Figure 7.



Figure 7: Enter IP address and gateway.

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

BACnet Configuration

To configure the BACnet interface, at least the Device ID and the Device Name must be configured (see Figure 8).

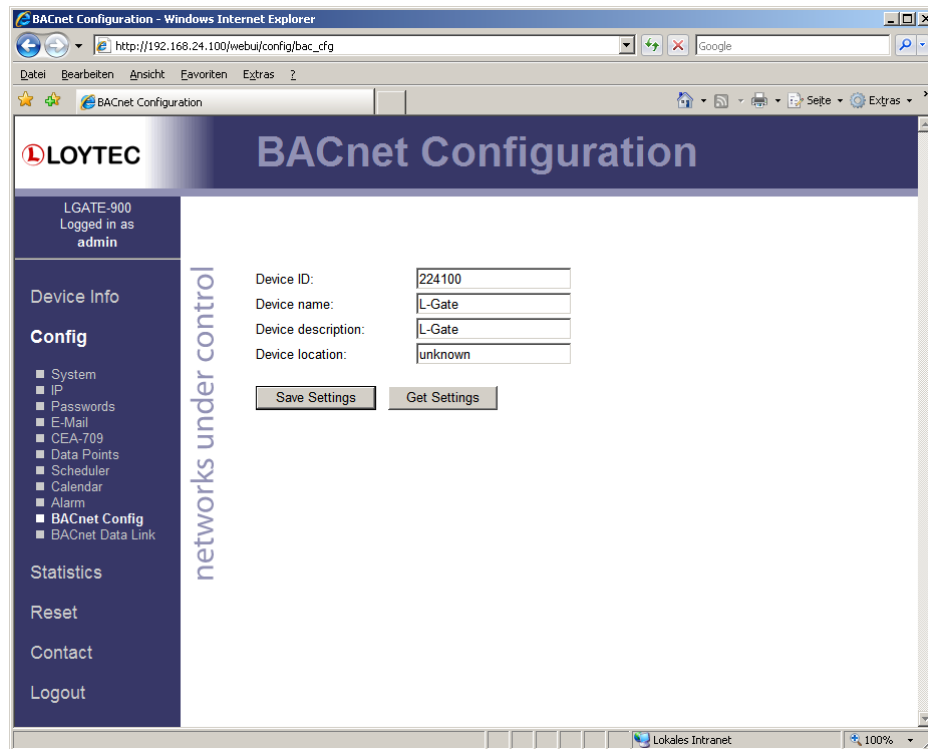


Figure 8: BACnet Device Configuration

The device ID corresponds to the instance number of the BACnet device object. It must be a unique ID on the BACnet internetwork. Also the Device Name must be a unique name on the BACnet internetwork.

By default the BACnet/IP data link layer is used. If the L-Gate shall be used with the BACnet MS/TP data link layer, please refer to Section 0 for further information.

Gateway Configuration with LNS-based Tools

Install the L-Gateway configuration software from the setup.exe. This file can be downloaded from www.loytec.com. In your LNS-based tool register the L-Gateway configuration software as an LNS plug-in.

The detailed guide to configuring the L-Gate and downloading the configuration can be found in section 0 (Configure with LNS).

Hardware Installation

Enclosure

LGATE-900

The L-Gate enclosure is 6 TE (1 TE = 17.5 mm) wide for DIN rail mounting, following DIN 43 880 (see Figure 9).

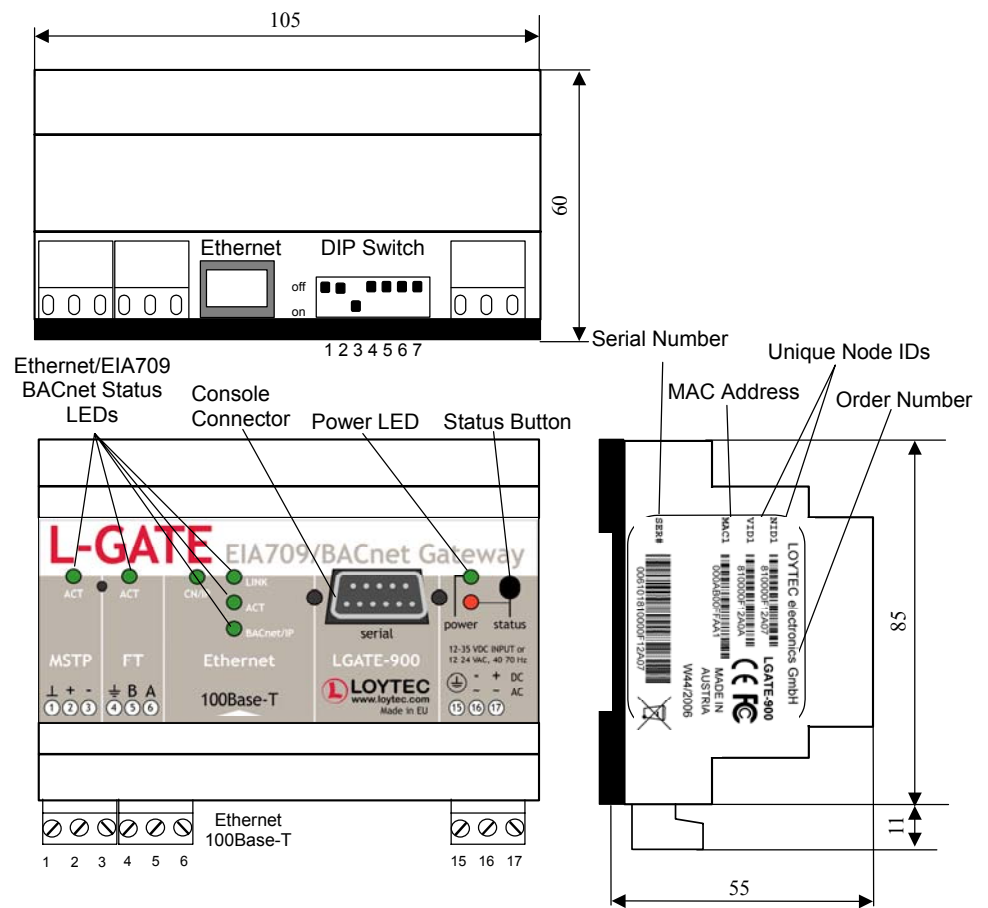


Figure 9: L-Gate Enclosure (dimensions in mm)

Product Label

The product label on the side of the L-Gate contains the following information (see Figure 9):

- L-Gate order number with bar-code (e.g., LGATE-900),
- 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).

Unless stated otherwise, all bar codes are encoded using “Code 128”. An additional label is also supplied with the L-Gate for documentation purposes. A virtual ID (VID) is a Node ID on the IP channel.

Mounting

The device comes prepared for mounting on DIN rails following DIN EN 50 022. The device can be mounted in any position. However, an installation place with proper airflow must be selected to ensure that the L-Gate's temperature does not exceed the specified range (see Chapter 0).

LED signals

Power LED

The L-Gate power LED lights up green when power is supplied to terminals 15, 16, and 17.

Status LED

The L-Gate is equipped with a red status LED (see Figure 9). 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.

MSTP Activity LED

The MS/TP port has a three-color MSTP Activity LED (see Figure 9). Table 2 shows the different LED patterns of the port and their meaning. A permanent color reflects a state, flicker is for 25 ms when there is activity on the MS/TP data link layer.

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

Table 1: MS/TP Activity LED Patterns

FT Activity LED

The FT port on the L-Gate has a three-color LED (green, red, and orange, see Figure 9). Table 2 shows different LED patterns of the port and their meaning.

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

Table 2: CEA-709 Activity LED Patterns

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.

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.

CN/IP LED

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

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

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

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

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

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

BACnet/IP LED

The BACnet/IP LED flashes green for 25 ms when BACnet packets are transmitted or received over the BACnet/IP interface.

Wink Action

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

Network Diagnostics

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

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

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

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

A port overload condition occurs if

- the average bandwidth utilization of this port was higher than 70% or
- the collision rate was higher than 5% or
- more than 15% CRC errors have occurred on a port with a power-line transceiver or more than 5% on a port with a transceiver other than power-line or
- the L-Gate 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.

Status Button

The L-Gate is equipped with a status button (see Figure 9). When pressing the status button shortly during normal operation of the L-Gate, it sends a "Service Pin Message" on the active CEA-709 network port (FT-10 or CEA-852). It also sends a BACnet "I-Am" message on all active BACnet data link layers. As an alternative to pressing the status button, a service pin message can be sent via the Web interface (see Section 0).

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. 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 0).

DIP Switch Settings

The L-Gate has seven switches to select the mode of operation. The DIP switch assignment for the L-Gate is shown in Table 3.

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

Table 3: DIP Switch Settings for L-Gate

Power Supply

The L-Gate can either be DC or AC powered. The L-Gate power terminals are listed in Table 4.

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

Table 4: Power Terminals on LGATE-900.

Important: *Do not ground the power supply wire on terminal 17 as shown in Figure 10!*

Terminal Layout

The L-Gate 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 mm²/AWG12.

Terminal	Function
1	BACnet MS/TP Reference
2	BACnet MS/TP Non-Inverting Input
3	BACnet MS/TP Inverting Input
4	Earth Ground
5, 6	CEA-709 A, B of FT-10 Channel Port
8	Ethernet 100BaseT
15	Main Earth Ground
16, 17	Power Supply (do not connect 17 to ground)

Table 5: L-Gate Terminals LGATE-900.

Wiring

The CEA-709 network segment connected to the L-Gate needs to be terminated according to the rules found in the specification of the transceiver (see Section 0). If BACnet is configured to run over MS/TP, the MS/TP network segment must be properly terminated

with a termination resistance of 120 Ohms connected at each of the two ends of the segment media.

Important: *All Earth ground terminals must be connected to the main Earth ground terminal 15. When using shielded network cables only one side of the cable should be connected to ground. Thus, the shield must be connected to earth ground either at the L-Gate terminals or somewhere else in the network, but never at more than one place (see Figure 10)!*

Important: *If BACnet MS/TP is used, the negative power terminal 16 on the L-Gate must be connected to functional ground (see Figure 10). Do not connect to earth ground! If 2-wire MS/TP cabling is used, also connect the MS/TP reference wire on terminal 1 to functional ground.*

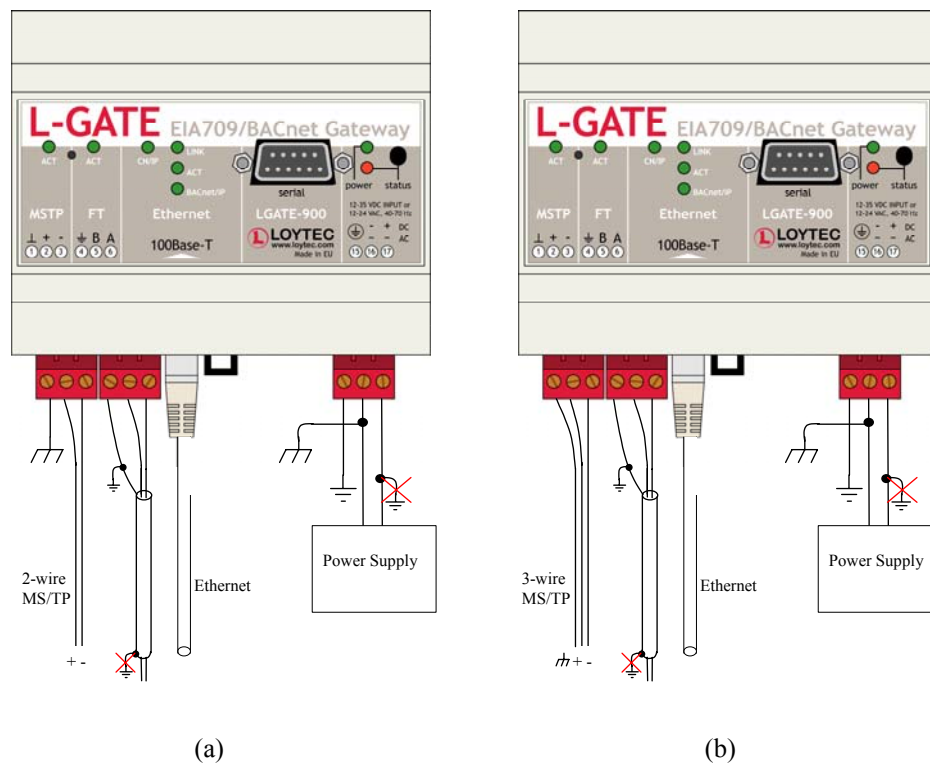


Figure 10: Connecting the Earth Ground to the L-Gate: (a) 2-wire MS/TP, (b) 3-wire MS/TP

Console Interface

Console Connection

The L-Gate is equipped with a serial interface to

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

To use the serial interface, the console connector (see Figure 9) of the L-Gate can be connected to the RS-232 port of a PC. The PC can communicate with the L-Gate using a standard terminal program with communication settings of 38,400 bps / 8 data bits / no parity / 1 stop bit. Use a standard null-modem cable with full handshaking to connect the L-Gate serial console interface to your PC.

Self Test

Whenever the L-Gate comes out of reset it performs a self-test.

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

```

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
L-Gate 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 CEA-852 device             Passed
Detecting CEA-709 port 1 (FT)      Passed
Starting BACnet networking          Passed
Starting CEA-709 networking         Passed
Starting Web server                 Passed

L-Gate(c)
LOYTEC electronics GmbH
Mon Jan 28 16:35:43 2008 - v3.0.0

```

Figure 11: Console messages during the boot phase.

The duration of a successful boot sequence of an L-Gate is typically 30 seconds.

L-Gate Device Main Menu

After booting has completed, the L-Gate displays the console menu as shown in Figure 12.

```

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] BACnet configuration
[8] Reset configuration (factory defaults)
[9] Device statistics

[a] Data Points

[0] Reset device

Please choose:

```

Figure 12: L-Gate Device Main Menu.

The menu items are described in the following sections.

Option 1 - Show device information

This menu item shows information about the L-Gate and the current firmware version. The output should look like what is shown in Figure 13.

```
Device Information
=====

Product:      L-Gate
Product code: LGATE-900
Firmware:     L-Gate Primary Image
Version:      1.0.0
Build date:   Mon Sep 25 13:06:20 2006
Serial number: 009701-800000048326
Free memory:  12099K,218K
System temp:  44.7C
Supply volt:  15.1V

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

CEA-709      : 80 00 00 04 83 26
IP           : inactive

Press <RETURN> to continue
```

Figure 13: Device Information

Option 2 – Serial firmware upgrade

This menu item allows updating the L-Gate firmware via the serial interface (console). See Section 0 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.

Option 3 – System configuration

Select this menu item to change system configuration settings. See Section 0 for details.

Option 4 – CEA-709 configuration

Select this menu item to change the CEA-709 configuration settings. See Section 0 for details.

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 0 for details.

Option 6 – CEA-852 client configuration

Select this menu item to change the CEA-852 client configuration settings like configuration server IP address, device name, SNTP server, escrow timeout, aggregation timeout, MD5 authentication secret. See Section 0 for details.

Option 7 – BACnet configuration

Select this menu item to change the BACnet configuration settings like device ID, device name, and data link layer related configuration setting. See Section 0 for details.

Option 8 - Reset configuration (factory defaults)

This menu item resets the L-Gate to factory defaults. See Section 0 for details.

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 0 for details.

Option 0 – Reset Device

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

Option a – Data Points

This menu option takes the user to the data point menu. In this menu the configured data points in the L-Gate can be viewed and set with values. See Section 0 for details.

System Configuration Menu

The system configuration menu holds various system configuration settings. Typically the system configuration menu looks like shown in Figure 14.

```
System Configuration Menu
=====

[1] Configure date/time : Tue Jan 29 10:50:15 2008 (GMT+01:00)
[2] Configure earth pos : 0:00:00 S 0:00:00 E 0 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 14: System Configuration Menu

Option 1 - Configure Date/Time

This menu item allows to configure the L-Gate's system time. It provides several sub-items as shown in Figure 15. With menu option '1' the time source is defined. The following options are available: 'auto', 'manual', 'NTP', 'BACnet', 'LonMark'. In the 'auto' mode the device switches to the first external time source that is discovered (e.g., synchronizes to BACnet, if a BACnet time sync is received). 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 0).

```
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 15: 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.

Option 2 - Configure Earth Position

This menu item allows to configure the L-Gate'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 16). For moving locations, this setting can be updated over the network using the network variable nciEarthPos (see Section 0).

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

[1] Set latitude       : 0:00:00 S
[2] Set longitude     : 0:00:00 E
[3] Set altitude      : 0 m

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

Please choose:
```

Figure 16: 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.

Option 7 – FTP server, 8 – FTP server port

Allows to enable and disable the FTP server and configure 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 0).

Option 9 – Web server, 0 – Web server port

These menu items allow enabling and disabling the Web server and configuring the Web server port on the L-Gate. You can disable the Web server if you do not want to provide access to the L-Gate 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.

Option c – E-Mail Account Configuration

This menu item allows configuring the L-Gate'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 17.

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 an 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 L-Gate (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 17: E-Mail Account Configuration Menu

For testing the e-mail setup, enter <0> to send a test e-mail. The user is prompted for an E-Mail address. If none is entered, the test E-Mail is sent to the Reply-To address (if given) or the Source E-Mail address. For debugging delivery problems, turn on logging information by selecting <9>. The e-mail transmission log is then output to the console.

CEA-709 Configuration Menu

This menu allows to change the CEA-709 port of the L-Gate. The menu looks like shown in Figure 18.

```

CEA-709 Configuration Menu
=====

[0] Port configuration          : CEA-709
    CEA-709                    : FT
    IP                         : IP-852 (inactive)

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

Please choose:

```

Figure 18: CEA-709 Configuration Menu

Option 0 – Port configuration

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

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 19.

```

IP Configuration Menu
=====
[1] DHCP                : disabled
[2] IP Address          : 192.168.1.254
[3] IP Netmask          : 255.255.255.0
[4] IP Gateway          : 192.168.1.254
[5] Hostname            : new
[6] Domainname         : <unset>
[7] DNS Servers         : <unset>
[9] MAC Address         : 00:0A:B0:01:45:1F (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 19: IP Configuration Menu when DHCP is disabled

The IP configuration menu, when DHCP is enabled, is shown in Figure 20.

```

IP Configuration Menu
=====
[1] DHCP                : enabled
    IP Address          : 192.168.1.254
    IP Netmask          : 255.255.255.255
    IP Gateway          : 0.0.0.0
[5] Hostname            : new
    Domainname         : <unset>
    DNS Servers         : <unset>
[9] MAC Address         : 00:0A:B0:01:45:1F (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 20: IP Configuration Menu when DHCP is enabled

Option 1 – DHCP

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”.

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

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

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

Option 5 – Hostname, 6 – Domainname

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

Option 7 – DNS Servers

You can configure up to 3 Domain Name Servers. Currently, these entries are not used.

Option 9 – MAC Address

The L-Gate 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.

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 0). The text appended to this menu item displays the current NTP synchronization status (out-of-sync, or in-sync).

Option b – Link Speed & Duplex

If the L-Gate 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
```

CEA-852 Device Configuration Menu

This menu holds relevant information regarding the configuration of the CEA-852 device. In principle, there are two ways to add the L-Gate to an IP channel. The recommended method is to enter the information at the configuration server. The configuration server will then contact the L-Gate and configure the relevant information. If for some reason the L-Gate 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 the L-Gate starts to contact the configuration server to register. The device configuration menu is shown in Figure 21.


```
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 21: CEA-852 Device Configuration Menu

In case that the configuration server contacts the L-Gate, 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.

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

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

Option 4 – Config client port

If only one L-Gate 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.

Option 5 – Device name

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

Channel Mode

This field reflects the current channel mode of the device. It is configured by the configuration server. If there are any two devices in the channel which use the same IP address but different ports (e.g. multiple L-Gates 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.

SNTP server, channel timeout

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

Option 6 - Escrow timeout

Defines how long the CEA-852 device on the L-Gate 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.

Option 7 – Aggregation Timeout

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

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*.

Option 9 – MD5 secret

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

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

Option 0 – Location string

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

Option a – NAT Address

If the CEA-852 device on the L-Gate is used behind a NAT router, the public IP address of the NAT router or firewall must be known. This address can either be entered manually or can be determined automatically. Automatic NAT router discovery allows to operate the CEA-852 device of the L-Gate 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 22: Enable/Disable automatic NAT Router Discovery

To enable/disable automatic NAT router discovery select this menu option. The question in Figure 22 will be prompted on the console. Choose 'y' to enable automatic NAT router discovery. To manually enter a NAT address, choose 'n' and enter the NAT address when requested to do so. To completely disable the NAT router support, choose 'n' and enter the IP address 0.0.0.0 when requested to enter the NAT address.

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

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

Option b – Multicast Address

This menu option allows the user to add the CEA-852 device of the L-Gate 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.

BACnet Configuration Menu

This menu allows to configure the BACnet interface of the L-Gate. The BACnet configuration menu is shown in Figure 23.

```
BACnet Configuration Menu
=====

[1] Device ID           : 17800
[2] Device name        : L-Gate
[3] Device description  : L-Gate
[4] Device location    : unknown

[9] Data Link Layer     : BACnet/IP
[0] Configure BACnet/IP Data Link Layer

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

Please choose:
```

Figure 23: BACnet Configuration Menu

Option 1 – Device ID

This configuration option allows to set the instance part of the “Object_Identifier” property of the BACnet Device object. Note that this instance number must be unique within the BACnet internetwork.

Option 2 – Device name, 3 – Device description, 4 – Device location

These menu items allow to set the value of the properties “Object_Name”, “Description”, and “Location” of the BACnet Device object. Note that the “Object_Name” property must be unique within the BACnet internetwork.

Option 9 – Data Link Layer

This menu item allows to choose the BACnet data link layer used. The following options are given:

```
Select Data Link Layer
=====

[1] BACnet/IP
[2] MS/TP

Please choose:
```

Option 0 – Configure Data Link Layer

Depending on the currently selected BACnet data link layer one of the following menus appears:

BACnet/IP Configuration Menu

The BACnet/IP configuration menu is shown in Figure 24. Its only option allows to set the UDP port used for the BACnet/IP protocol (Option 3). Enter a port number of 0 to use the default port (47808/0xBAC0).

```
BACnet/IP Configuration Menu
=====

[3] BACnet/IP port      : 47808 (default)

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

Please choose:
```

Figure 24: BACnet/IP Configuration Menu

MS/TP Configuration Menu

The MS/TP configuration menu is shown in Figure 25.

```
MS/TP Configuration Menu
=====

[3] MS/TP node number : 127
[4] Baud rate         : 9600
[5] Max info frames   : 1
[6] Max master        : 127

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

Please choose:
```

Figure 25: MS/TP configuration menu.

The menu offers the following options:

Option 3 – MS/TP node number

This menu item is used to set the MS/TP node number of the L-Gate. It must be in the range 0 to the number configured with the “Max master” configuration option.

Option 4 – Baud rate

This menu item allows to configure the baud rate on the MS/TP channel. Possible options are 9600, 19200, and 38400 baud.

Option 5 – Max info frames

This menu item allows to set the maximum number of info frames on the MS/TP channel. The default value is 1. It is recommended to leave this configuration option at the default setting.

Option 6 – Max master

This menu item allows to set the maximum number of masters on the MS/TP channel. The default value is 127. It is recommended to leave this configuration option at the default setting.

Reset configuration (load factory defaults)

This menu item allows to reset the device into its factory default state. The menu appears as shown in Figure 26.

```
Reset Configuration Menu
=====

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

[q] Quit

Please choose:
```

Figure 26: Reset to Factory Defaults Menu

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.).

Option 3 – Reset all passwords

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

Option 4 – Clear data point configuration

Select this option to clear all CEA-709 network variables and BACnet objects configured on the L-Gate. This effectively clears all the port configuration. The L-Gate needs to be rebooted to let the changes take effect.

Device Statistics Menu

This menu holds relevant information regarding the device statistics of the L-Gate. The device statistics menu is shown in Figure 27. 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
[7] Show BACnet MS/TP statistics

[q] Quit

Please choose:
```

Figure 27: Device Statistics Menu

Option 1 – CEA-852 device statistics

A sample console output is shown in Figure 28. 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 28: CEA-852 Device Statistics

A sample console output of the extended CEA-852 device statistics is shown in Figure 29. 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 29: Extended CEA-852 Device Statistics

Option 2 – CEA-709 Application Statistics

A sample console output is shown in Figure 30.

```
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 30: CEA-709 Application Statistics

Option 4 – IP statistics

A sample console output is shown in Figure 31.

```

***** 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 31: IP Statistics

The IP statistics menu has the additional feature of displaying any IP address conflicts. If the L-Gate's IP address conflicts with another host on the network, the banner shown in Figure 32 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 32: 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.

Option 6 – Enhanced Communications Test

This menu item allows testing the communication path between the CEA-852 device of the L-Gate 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 33.

```
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 33: Enhanced Communication Test Console Output

The round-trip value (RTT) is measured as the time a packet sent to the peer device needs to be routed back to the CEA-852 device of the L-Gate. 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 6.

A warning “Incorrect NAT configuration detected!” is displayed if the enhanced communications test determines that the CEA-852 device of the L-Gate is operated behind a NAT router, but it has no NAT address configured. In this case, go to the IP configuration menu and configure the correct NAT address or set it to Auto-NAT.

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

Table 6: Possible Communication Problems

Option 7 – Show BACnet MS/TP Statistics

This menu option is available, if the BACnet port is configured for MS/TP. A sample output is shown in Figure 34. When prompted to clear the MS/TP statistics, hit <y> to reset the counters or <n> to keep them. The following describes the most important statistics data.

The MS/TP token status reports the current token passing state. In state ‘OK’, the token is circulating between the masters. This is the normal state, when multiple masters are on the

MS/TP network. The state 'SOLE MASTER' is the normal state when the L-Gate is the only master on the network. If there are multiple masters on the network (e.g., an MS/TP BACnet router), this state is a hint to a broken cable. In state 'TOKEN LOST', the token is currently not circulating.

The counters 'Rcv ok' and 'Send ok' reflect the number of successfully received or transmitted MS/TP frames. Check these counters to verify that communication is flowing on the MS/TP segment. The counter 'MS/TP lost tokens' is an indicator for communication problems on the MS/TP network. If it increases, there is a cabling, ground, or termination problem.

```

BACnet MS/TP Statistics
=====

MS/TP token status      : OK
Rcv OK                  : 200
Send OK                 : 173
Rcv Idle Errors         : 0
Rcv Preamble Timeouts  : 0
Rcv Preamble Errors    : 0
Rcv Header Frame Too Long : 0
Rcv Header Timeouts    : 0
Rcv Header Errors      : 0
Rcv Header BAD CRC     : 0
Rcv Header No Data     : 0
Rcv Header Not For Us  : 0
Rcv Data Timeout       : 0
Rcv Data Error         : 0
Rcv Data Bad CRC       : 0
MSTP Lost Tokens       : 0
MSTP Master Polls     : 0
MSTP Rcvd Tokens       : 0
MSTP Rcvd Unwanted Frame : 0
MSTP Rcvd Unexpected Frame : 0
MSTP Rcvd Invalid Frame : 0
MSTP Rcvd FPM         : 0
MSTP Rcvd Data No Reply : 0
MSTP Rcvd Data Needing Reply : 0
MSTP Rcvd Reply Timeouts : 0
MSTP Rcvd Replies     : 0
MSTP Rcvd Postpone    : 0

Clear BACnet MS/TP statistics (y/n)?

```

Figure 34: BACnet MS/TP Statistics Menu.

Data Point Menu

The L-Gate data point menu as shown in Figure 35 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 0).

```

Data Point Menu
=====

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

[q] Quit without saving

Please choose:

```

Figure 35: L-Gate Data Point Menu.

Option 1 – List Data Points

Select this option to list all data points on the L-Gate. The list is flat and displays the values and status of each data point. An example is shown in Figure 36.

```
Data Points:
-----
BACnet 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 36: Example data point listing.

Option 2 – Get Value

This option allows to retrieve 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”.

Option 3 – Set Value

This option allows to set 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.

Web Interface

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

Device Information and Account Management

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

Windows START → Run

command.com

Route add 192.168.1.254 %COMPUTERNAME%

Also make sure that the Web server has not been disabled in the console interface (see Section 0). The device information page should appear as shown in Figure 37.



Figure 37: Device Information Page

The device information page shows information about the L-Gate and the current firmware version. It includes the unique node IDs (“Neuron IDs”) of the CEA-709 network interfaces. This page can also be used to send the CEA-709 service pin messages. This is a useful feature when commissioning the L-Gate, 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 38. Enter the default administrator password “admin” and select “Login”.

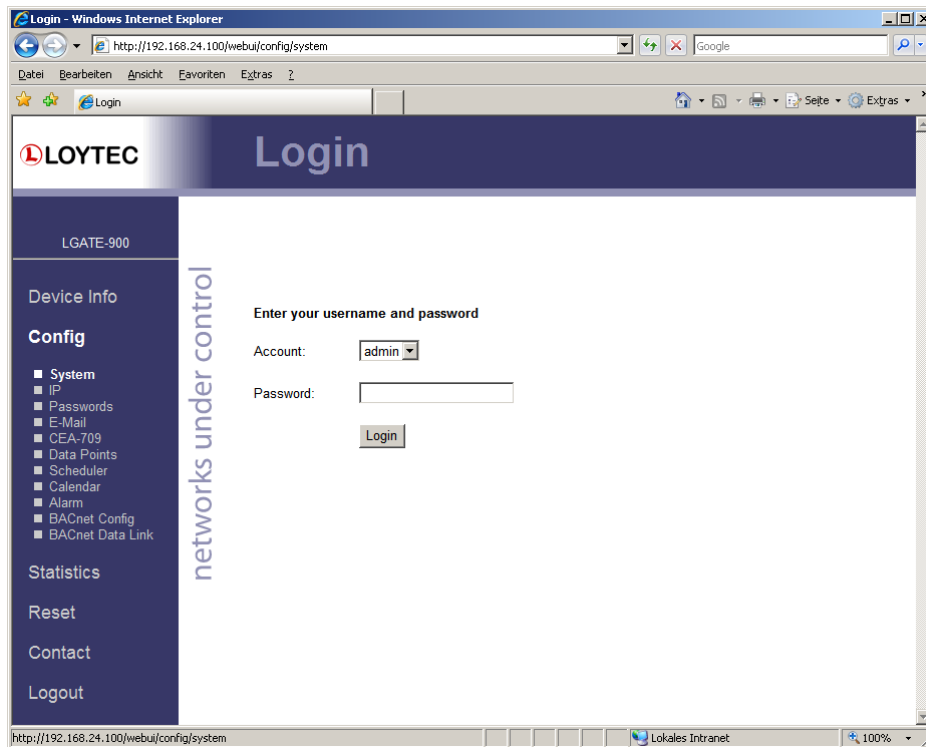


Figure 38: Enter admin as the default administrator password.

The Config menu opens. Click on “Passwords” in the Config menu, which opens the password configuration page as shown in Figure 39. The L-Gate has two 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) “admin” has full access to the L-Gate and can make changes to its configuration. Note that the user accounts are also used to log on to the FTP and Telnet server.

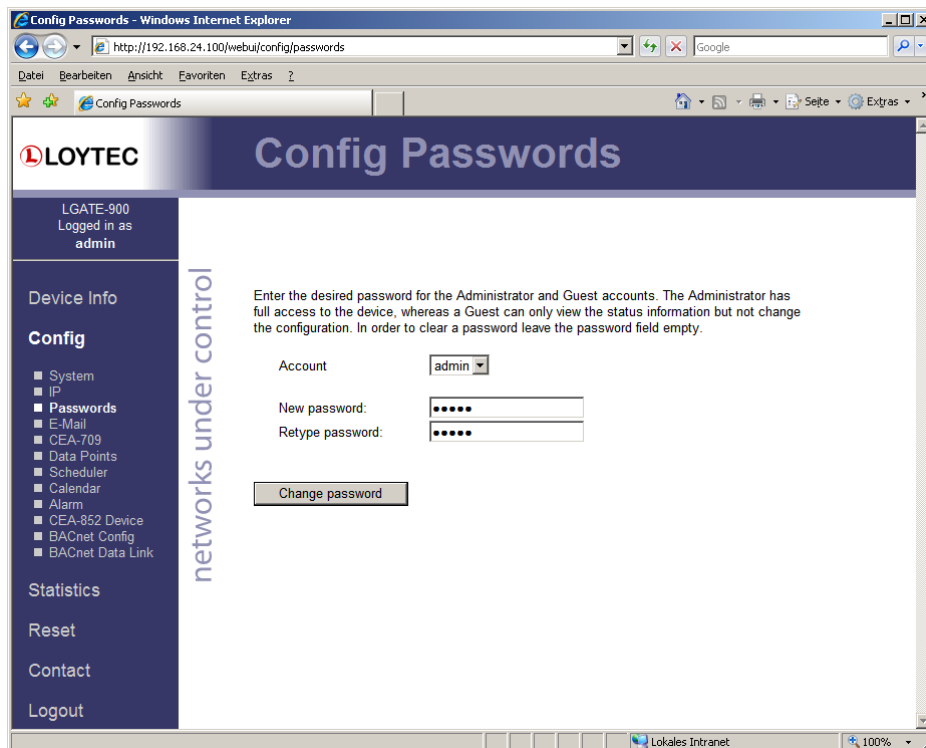


Figure 39: Password Configuration Screen

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

Device Configuration

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

System Configuration

The system configuration page as shown in Figure 40. This page allows to configure the L-Gate's system time. The time sync source can be set to 'auto', 'manual', 'NTP', 'BACnet', 'LonMark'. In the 'auto' mode the device switches to the first external time source that is discovered (e.g., synchronizes to BACnet, if a BACnet time sync is received). 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 0).

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.

The screenshot shows the 'Config System' web interface. The browser window title is 'Config System - Windows Internet Explorer'. The address bar shows 'http://192.168.24.100/webui/config/system'. The page header includes the LOYTEC logo and the title 'Config System'. A sidebar on the left contains the following menu items: Device Info, Config (with sub-items: System, IP, Passwords, E-Mail, CEA-709, Data Points, Scheduler, Calendar, Alarm, CEA-852 Device, BACnet Config, BACnet Data Link), Statistics, Reset, Contact, and Logout. The main content area is titled 'networks under control' and contains the following sections:

- Date/Time:** Time sync source (manual), Local Date (2008-01-29), Local Time (13:50:26), Timezone offset (+00:00), Daylight saving time (DST) (None), DST start (1st Su Jan 00:00), DST end (1st Su Jan 00:00). Buttons: Save Date/Time, Get Date/Time.
- Earth Position:** Latitude (0:00:00 S), Longitude (0:00:00 E), Altitude (0 m). Buttons: Save Earth Position, Get Earth Position.
- Webservice:** Webserver port (80), CSV delimiter (,). Buttons: Save Webservice Settings, Get Webservice Settings.
- FTP Server:** FTP enabled (checked), FTP port (21). Buttons: Save FTP Settings, Get FTP Settings.

Figure 40: System Configuration Page

The next section on the page allows to configure the L-Gate'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 0).

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 0) 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.

IP Configuration

Figure 41 shows the IP configuration page with DHCP disabled, while Figure 42 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.

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.

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.

The screenshot displays the 'Config IP' web interface for a LOYTEC device. The browser window title is 'Config IP - Windows Internet Explorer' and the address bar shows 'http://192.168.24.100/webui/config/ip'. The page header includes the LOYTEC logo and the title 'Config IP'. A sidebar on the left shows the user is logged in as 'admin' and provides navigation options: Device Info, Config (with sub-items: System, IP, Passwords, E-Mail, CEA-709, Data Points, Scheduler, Calendar, Alarm, BACnet Config, BACnet Data Link), Statistics, Reset, Contact, and Logout. The main content area is titled 'networks under control' and contains the following configuration fields:

- Enable DHCP:
- IP Address*: 192.168.24.100
- IP Netmask*: 255.255.192.0
- IP Gateway*: 192.168.1.1
- Hostname: new
- Domainname: (empty)
- 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:9F
- NTP Server 1: (leave empty to disable)
- NTP Server 2: (leave empty to disable)
- NTP Status: out-of-sync
- Link Speed & Duplex: Auto Detect

Buttons for 'Save Settings' and 'Get Settings' are located below the fields. A note at the bottom states: 'The entries marked with (*) are required for proper operation'.

Figure 41: IP Configuration Page with DHCP disabled



Figure 42: IP Configuration Page with DHCP enabled

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

The device can be configured to synchronize its clock with NTP time. Enter the IP address of a primary and, optionally, a secondary NTP server. The L-Gate will use NTP as a time source, if the time sync source in the system configuration page is set to 'NTP' (see Section 0). The field 'NTP status' below the NTP server settings displays the current NTP synchronization status (out-of-sync, or in-sync).

If the L-Gate 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.

CEA-709 Configuration

On the CEA-709 configuration page (shown in Figure 43) the user can configure, which of the available CEA-709 ports of the L-Gate shall be active. Select "CEA-709" from the drop-down box to use the L-Gate on an FT-10 channel, or "CEA-852" to use the L-Gate on an IP channel. Click on the tabs "CEA-709" and "IP" to learn more about the current transceiver settings.

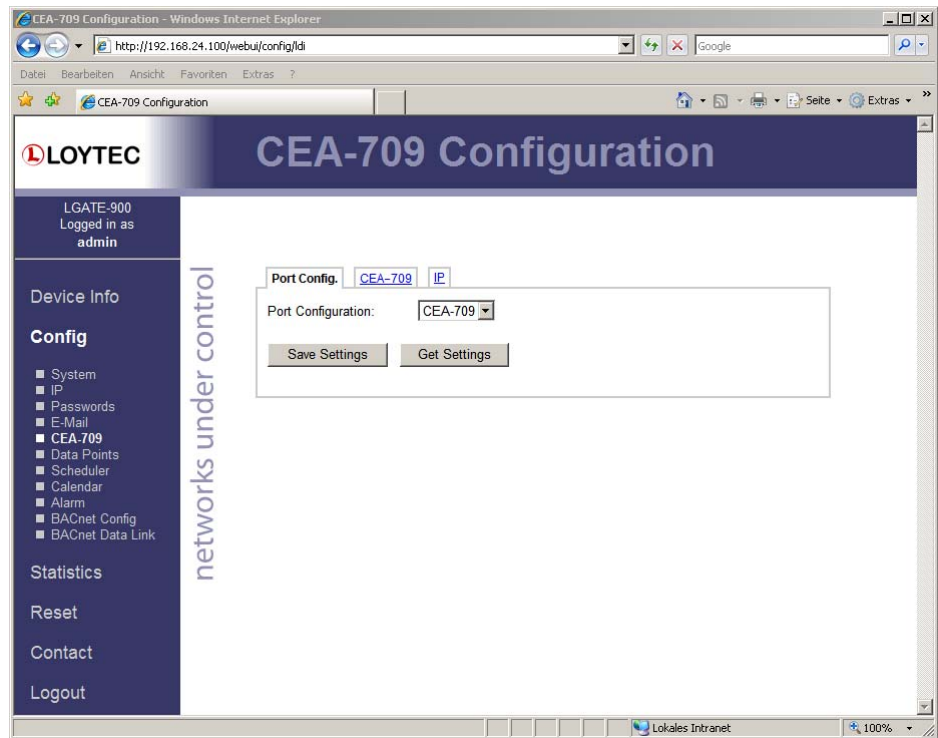


Figure 43: CEA-709 Configuration Page

CEA-852 Device Configuration

The CEA-852 device of the L-Gate can be configured in the CEA-852 device configuration page, which is depicted in Figure 44. Typically, the L-Gate is added to an IP channel by entering the relevant information on a configuration server. The configuration server then contacts the CEA-852 device of the L-Gate and sends its configuration.

The field “Config server address” and “Config server port” display the IP address and port of the configuration server, which manages the L-Gate and the IP channel. The field “Config client port” represents the IP port of the L-Gate’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 L-Gate, which will appear in the IP channel to identify this device. You can enter a device name with up to 15 characters. It is recommended to use unique device names throughout the IP channel.

The “Channel mode” field reflects the current channel mode of the CEA-852 device. It is configured by the configuration server. If there are any two devices in the channel which use the same IP address but different ports (e.g. multiple L-Gates 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 field “Escrow timeout” defines how long the CEA-852 device on the L-Gate waits for out-of-sequence CEA-852 data packets before they are discarded. Please enter the time in ms or 0 to disable escrowing. The maximum time is 255 ms.

The field “Aggregation timeout” defines the time interval in which multiple CEA-709 packets are combined into a single CEA-852 data packet. Please enter the time in ms or 0

to disable aggregation. The maximum time is 255 ms. Note that disabling aggregation will negatively affect the performance of the CEA-852 device of the L-Gate.

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. Either enter the 16 bytes as one string or with spaces between each byte.

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

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 0).

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 text which identifies the physical location of the L-Gate. A location string can have a maximum length of 255 characters. This is optional and for informational purposes only.

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

The "Multicast Address" field allows the user to add the CEA-852 device of the L-Gate 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.



Figure 44: CEA-852 Device Configuration Page

BACnet Configuration

Figure 45 shows the BACnet device configuration page. This configuration page allows to set the device ID, which is the instance part of the “Object_Identifier” property of the BACnet Device object. The field “Device name” holds the name of the BACnet device object (property Object_Name).

Important: *The device ID and device name must be unique within the BACnet internetwork.*

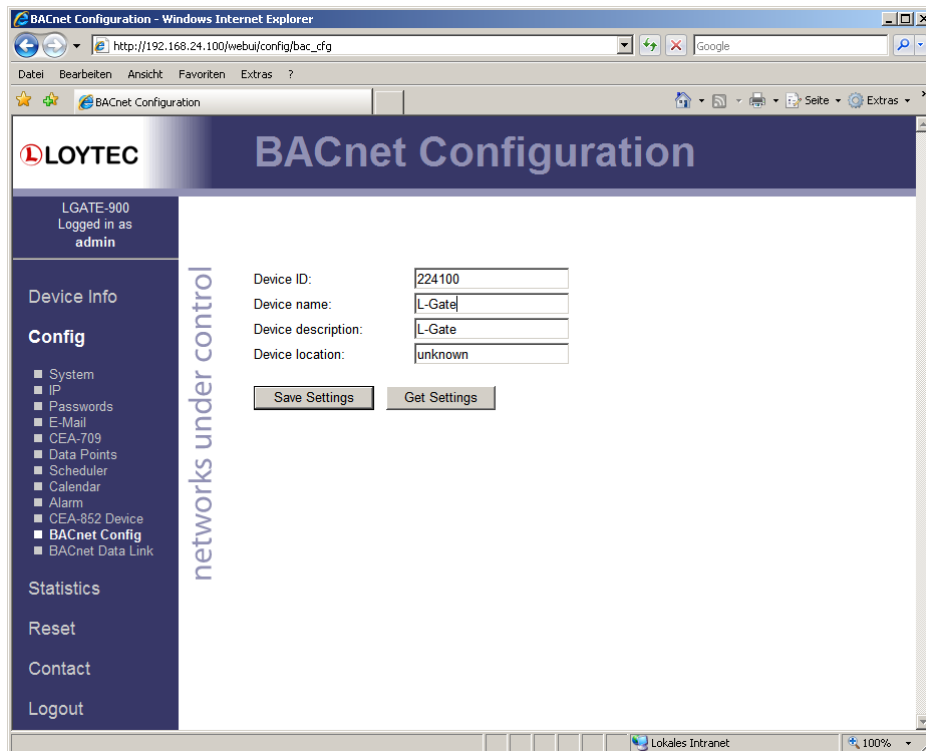


Figure 45: BACnet Device Configuration

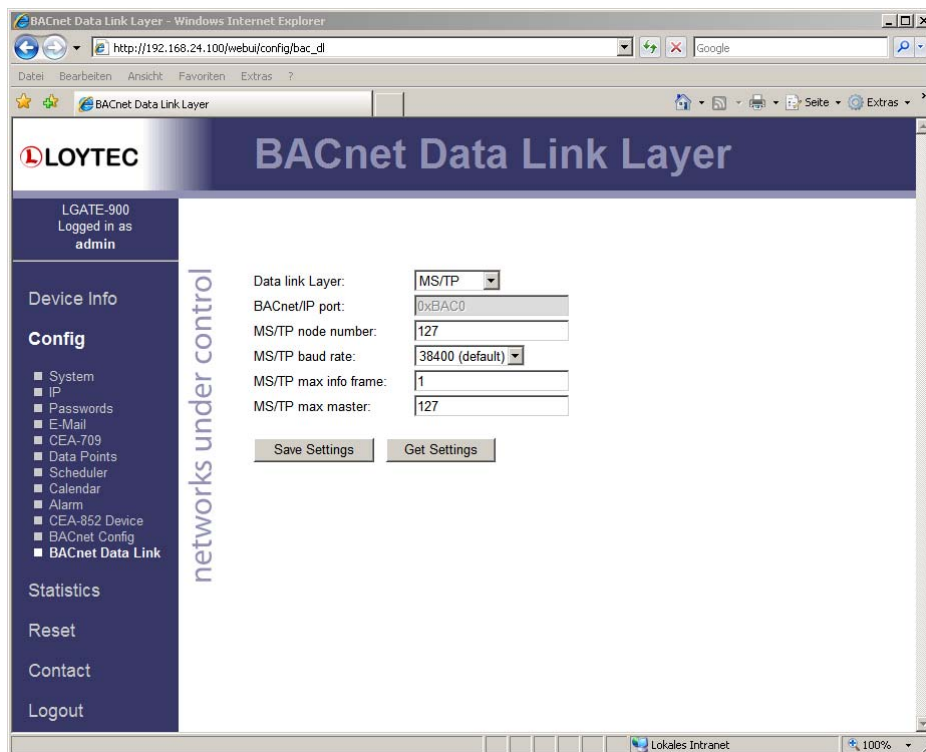


Figure 46: BACnet Data Link Layer Configuration

Further, the description and location can be configured. These configuration items correspond to the properties "Description", and "Location" respectively of the BACnet Device object.

Figure 46 shows the BACnet data link layer configuration page. This configuration page allows to select the data link layer used – BACnet/IP or BACnet MS/TP – and configure the chosen data link layer.

For the BACnet/IP data link layer, the UDP port used can be configured. For the BACnet MS/TP data link layer the MS/TP node number, the baud rate, the maximum number of info frames, and the maximum number of masters can be configured. The MS/TP node number determines the physical address of the L-Gate on the MS/TP channel and must be in the range 0 to the number configured with the “Max master” configuration option. It must be unique within the MS/TP channel. The baud rate on the MS/TP channel can be set to 9600, 19200, and 38400 baud. It is strongly recommended to leave the “max info frames” and the “max master” configuration options at their default settings.

Data Points

The L-Gate's Web interface provides a data point page, which lists all configured data points on the L-Gate. An example is shown in Figure 47. 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.

The screenshot shows the LOYTEC Data Points web interface. The browser address bar indicates the URL: http://192.168.24.100/webui/config/lgtw_dp. The page title is "Data Points" and the user is logged in as "admin".

The interface features a sidebar on the left with navigation options: Device Info, Config (System, IP, Passwords, EIA-709, Data Points, BACnet Config, BACnet Data Link), Statistics, Reset, Contact, and Logout. A vertical label "networks under control" is positioned next to the sidebar.

The main content area displays a tree view on the left with the following structure:

- ROOT
 - BACnet Port
 - EIA709 Port

A "Reload" button is located above the data point table. The table lists data points with the following columns: Name, Dir., Type, Value, and State.

Name	Dir.	Type	Value	State
/BACnet Port/				
NV_node1Ctrlm17state_bit0	input	binary	invalid value	invalid value
NV_node1Ctrlm16state_bit0	output	binary	1	normal
NV_node1Ctrlm15fire_test	input	multistate	invalid value	invalid value
NV_node1Ctrlm14fire_test	output	multistate	1	normal
NV_node1Ctrlm13amp	input	analog	invalid value	invalid value
NV_node1Ctrlm12amp	output	analog	1860.700000	normal
NV_node1Ctrlm10mctor_state	output	multistate	4	normal
NV_node1Ctrlm09switch_state	input	binary	invalid value	invalid value
NV_node1Ctrlm08switch_state	output	binary	0	normal
NV_node1Ctrlm07temp_f	input	analog	invalid value	invalid value
NV_node1Ctrlm06temp_f	output	analog	5137.600098	normal
NV_node1Ctrlm05lev_percent	input	analog	invalid value	invalid value
NV_node1Ctrlm04lev_percent	output	analog	32.500000	normal
NV_node1Ctrlm03lux	input	analog	invalid value	invalid value
NV_node1Ctrlm02lux	output	analog	51376.000000	normal
NV_node1Ctrlm01temp	input	analog	-246.100006	normal
NV_node1Ctrlm00temp	output	analog	4863.600000	normal
NV_node1Ctrlm11motor_state	input	multistate	invalid value	invalid value
/EIA709 Port/				
NV_node1Ctrlm17state	output	user	invalid value	invalid value
NV_node1Ctrlm16state	input	user	0000000000000000	normal
NV_node1Ctrlm15fire_test	output	multistate	invalid value	invalid value
NV_node1Ctrlm14fire_test	input	multistate	0	normal
NV_node1Ctrlm13amp	output	analog	invalid value	invalid value
NV_node1Ctrlm12amp	input	analog	1860.800000	normal
NV_node1Ctrlm11motor_state	output	multistate	invalid value	invalid value
NV_node1Ctrlm10mctor_state	input	multistate	3	normal
NV_node1Ctrlm09switch	output	user	invalid value	invalid value
NV_node1Ctrlm08switch	input	user	0000	normal
NV_node1Ctrlm07temp_f	output	analog	invalid value	invalid value
NV_node1Ctrlm06temp_f	input	analog	5137.600098	normal

At the bottom of the table, there are page enumerator links: "Goto Page: 1 2 3 4 5 6 Next".

Figure 47: 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 48. Clicking on the “Set” button writes the new value to the L-Gate's data server.

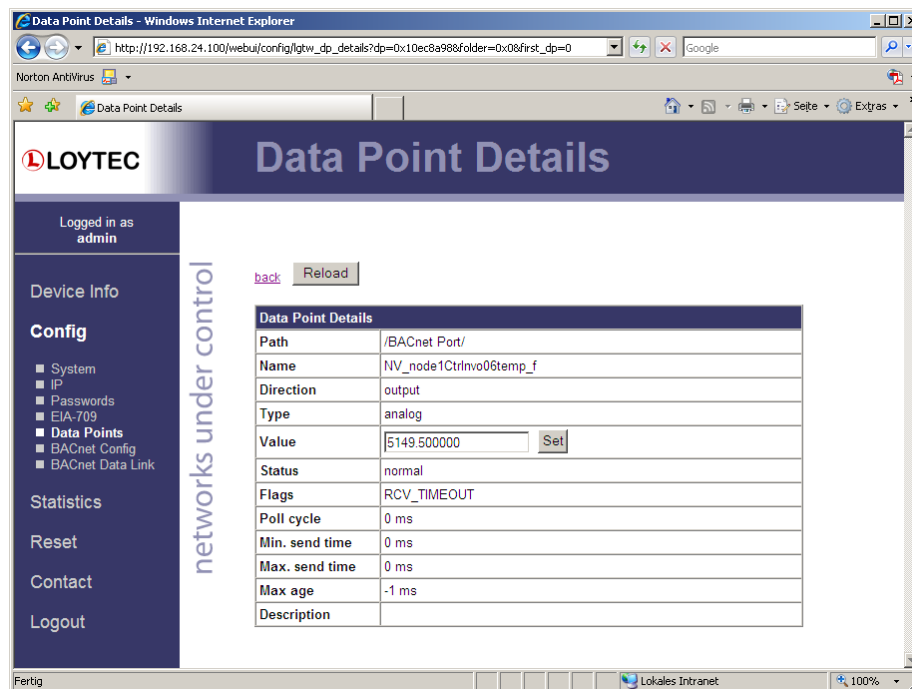


Figure 48: Data point details page

Scheduler

From firmware 3.0 and up, the L-Gate supports schedules and calendars. 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 0). 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 49.

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 49, 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 0.

To define actual values for the names such as “day” click on the tab “Scheduled Data Points” as shown in Figure 50. 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.

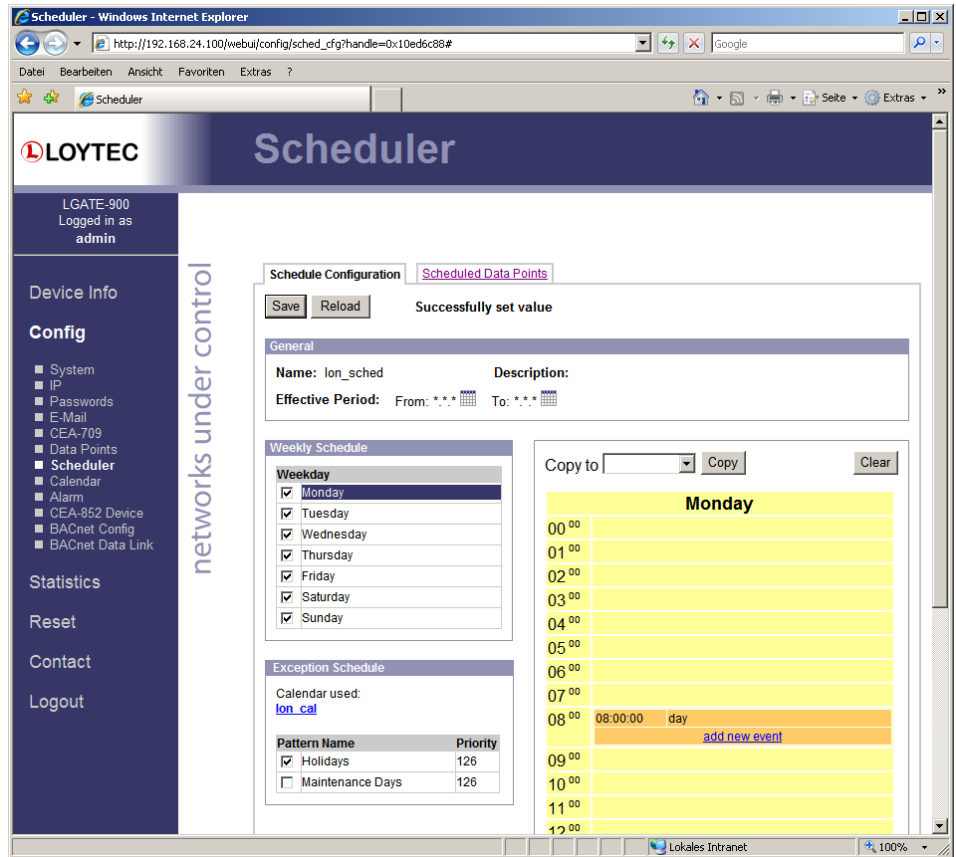


Figure 49: Schedule Configuration Page

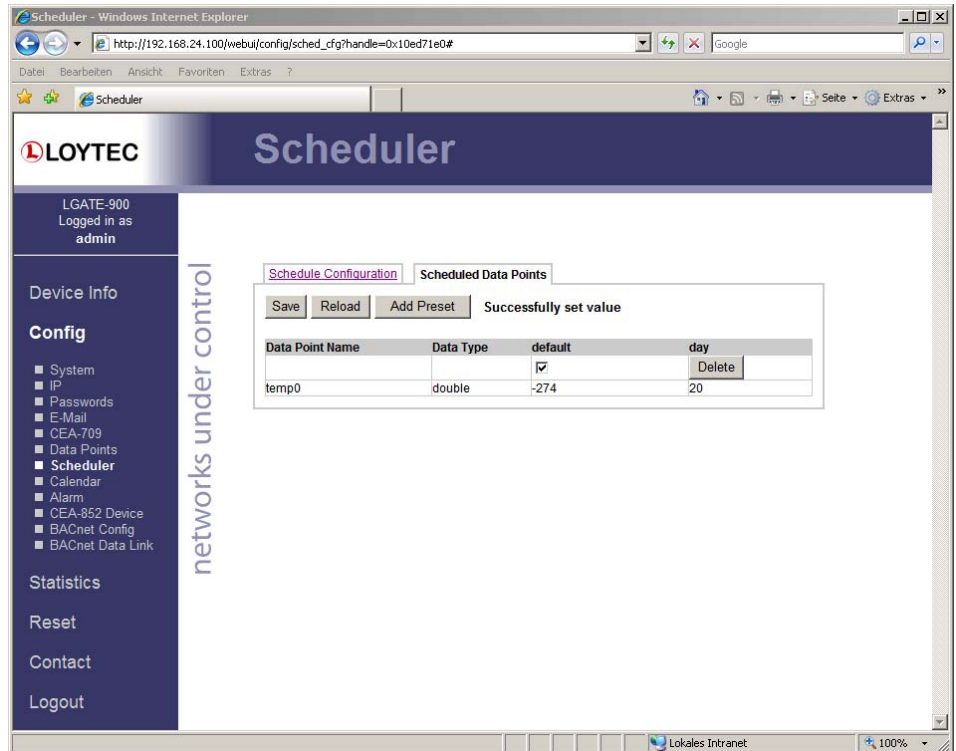


Figure 50: Scheduled Data Point Value Configuration Page

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.

Calendar

From firmware 3.0 and up, the L-Gate supports schedules and calendars. 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 51.

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’.

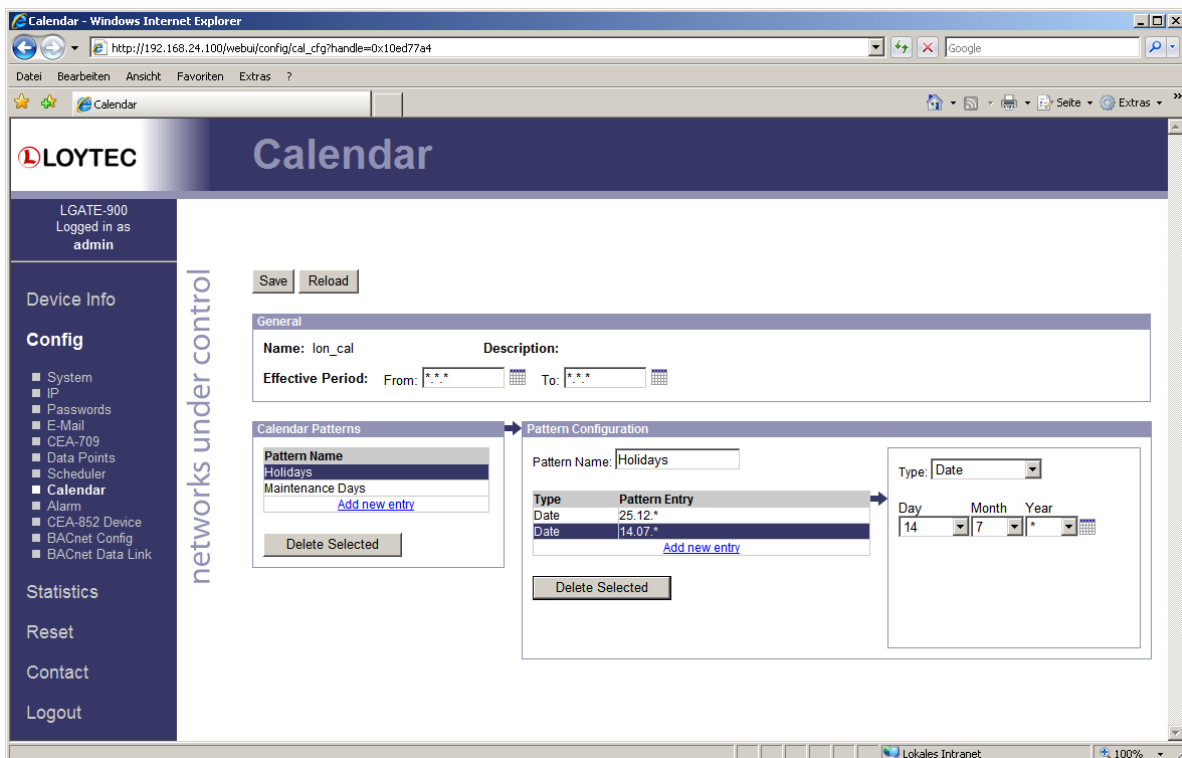


Figure 51: Calendar Configuration Page

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 51 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 51 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 0 for more information about defining exception dates.

Alarm

From firmware 3.0 and up, the L-Gate supports alarming. 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 51.

The screenshot shows the 'Alarm Summary Page' in a web browser. The page title is 'Alarm' and the URL is 'http://192.168.24.100/webui/config/alarm_obj?handle=0x10ede95c'. The page is divided into a sidebar and a main content area. The sidebar contains navigation options: Device Info, Config (System, IP, Passwords, E-Mail, CEA-709, Data Points, Scheduler, Calendar, Alarm, BACnet Config, BACnet Data Link), Statistics, Reset, Contact, and Logout. The main content area features a 'Reload' button, the alarm object name 'Critical', a 'Summary' table, and a 'Details' table. The 'Summary' table shows one active not acknowledged alarm. The 'Details' table shows two alarm events: a ventilation alarm and a high temperature alarm.

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

Alarm Time	Type	Priority	Description	Source Name	Value	Ack
05.02.2008 21:06:14	off-normal	127	Ventilation Alarm	dev 224100 (multistate-input.27)	(unknown)	Ack
05.02.2008 21:05:41	high-limit	127	High Temperature	dev 224100 (analog-input.29)	(unknown)	

Figure 52: Alarm Summary Page

Active alarms are rendered red. 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. Click on **Reload** to refresh your alarm list.

E-Mail Configuration

From firmware 3.0 and up, the L-Gate supports the transmission of E-Mails. 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 53.

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 L-Gate'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 L-Gate (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 0) 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.

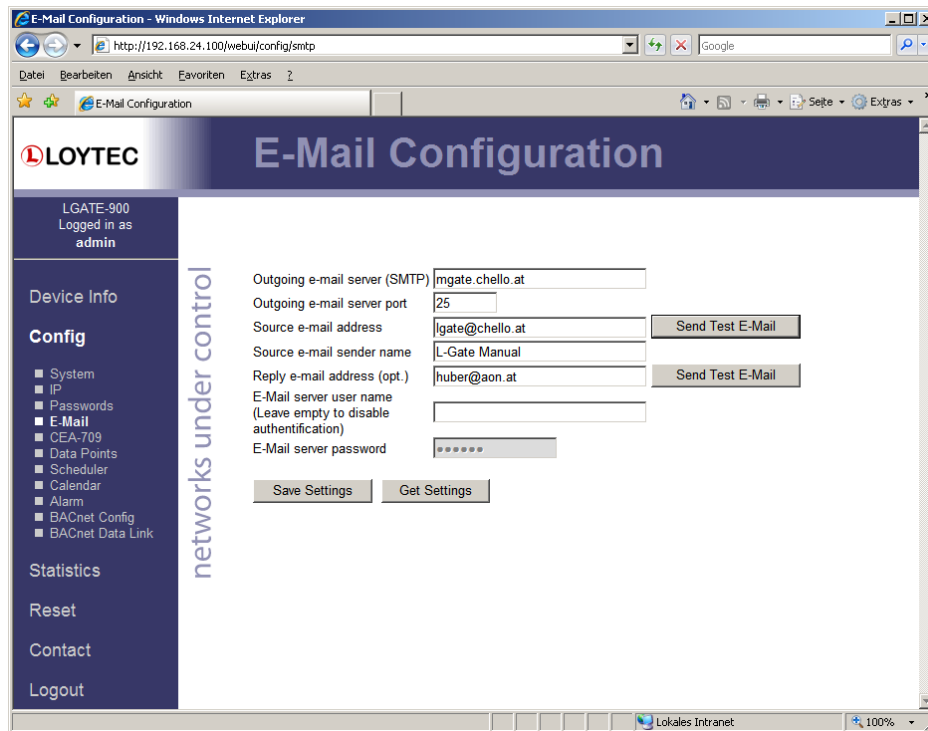


Figure 53: E-Mail Configuration Page

Device Statistics

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

IP Statistics

Figure 54 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 L-Gate's IP address conflicts with a different host on the network).

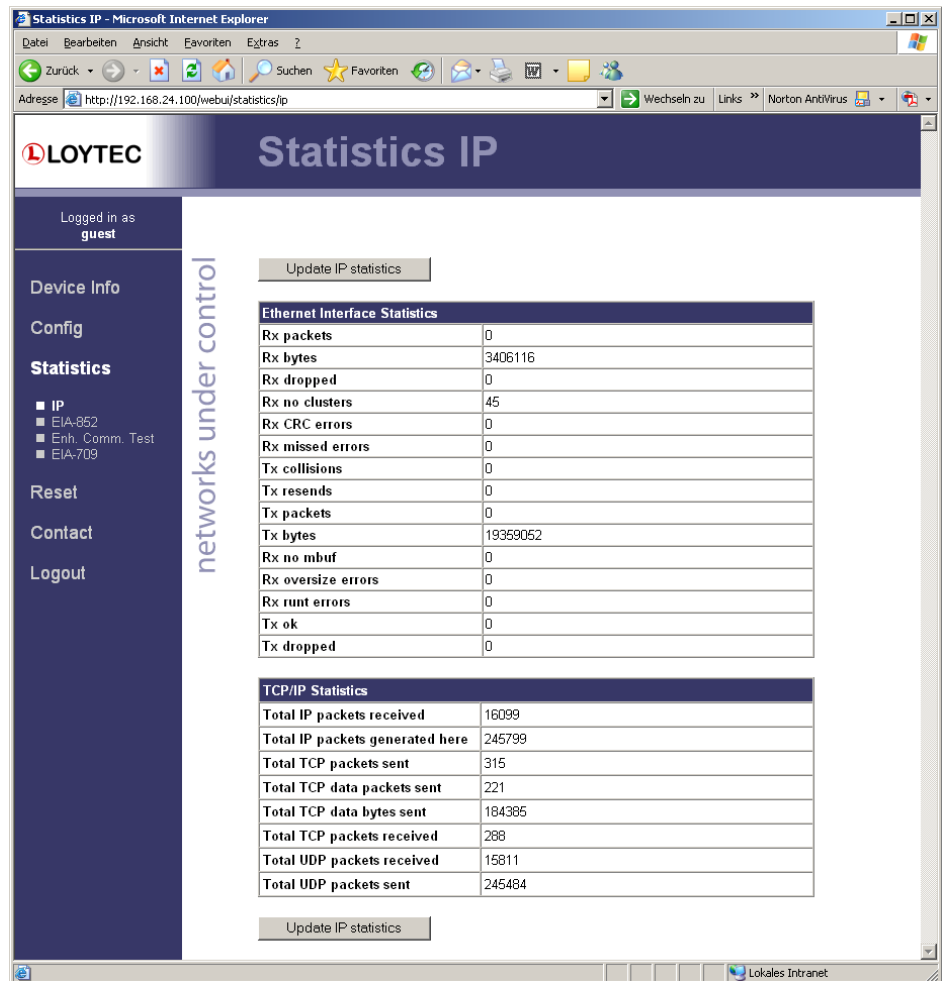


Figure 54: IP Statistics Page

CEA-852 Statistics

The CEA-852 statistics page displays the statistics data of the CEA-852 device on the L-Gate. The contents are the same as available through the console UI (see Section 0). The upper part of the CEA-852 statistics page is depicted in Figure 55. To update the statistics data press the button “Update all CEA-852 statistics”. To reset all statistics counters to zero click on the button “Clear all CEA-852 statistics”. The field “Date/Time of clear” will reflect the time of the last counter reset.

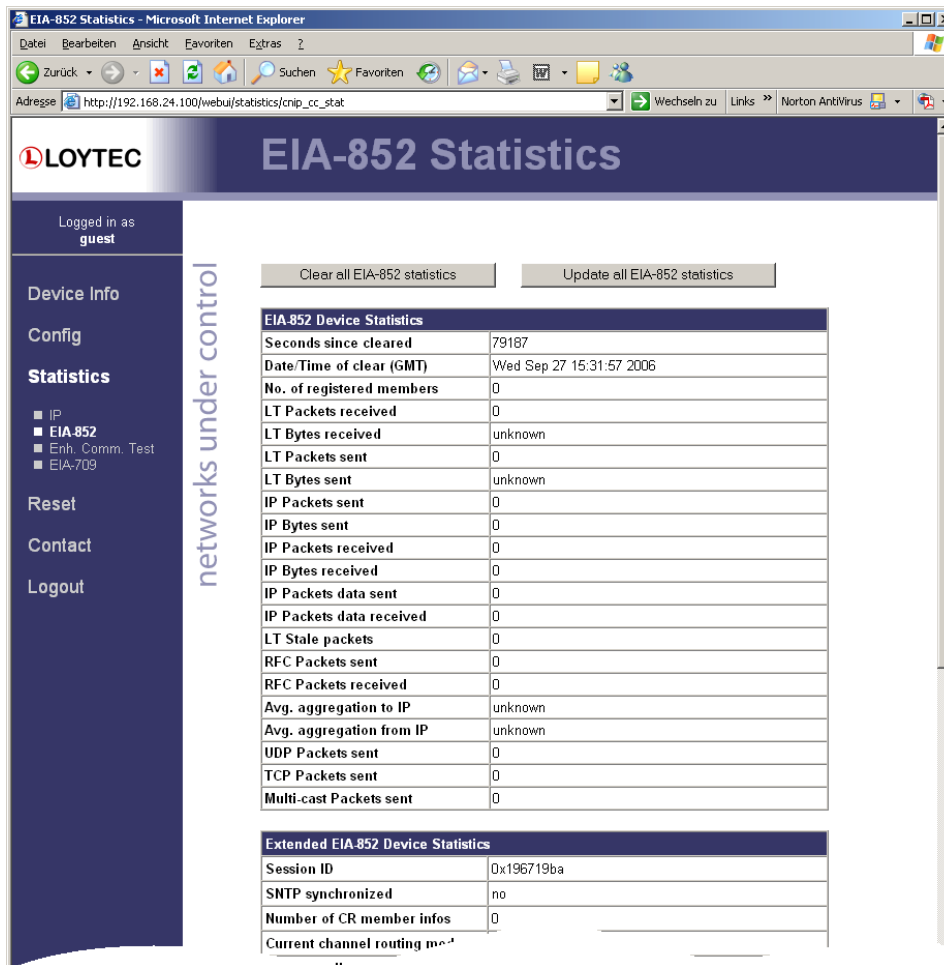


Figure 55: Part of the CEA-852 Statistics Page

Enhanced Communications Test

The Enhanced Communications Test allows testing the CEA-852 communication path between the CEA-852 device on the L-Gate 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 56.

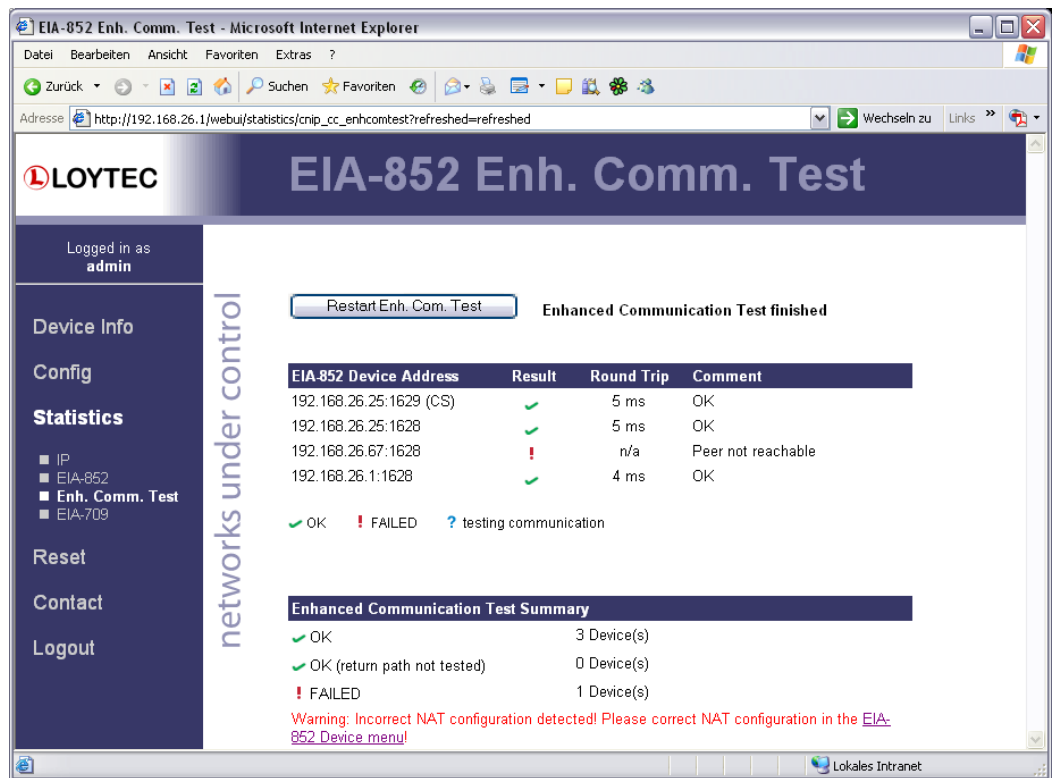


Figure 56: Enhanced Communication Test Output

The round-trip value (RTT) is measured as the time a packet sent to the peer device needs to be routed back to the L-Gate. 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 6.

CEA-709 Statistics

The CEA-709 statistics page displays statistics data of the CEA-709 port on the L-Gate as shown in Figure 57. This data can be used to troubleshoot networking problems. To update the data, click on the button "Update CEA-709 statistics".

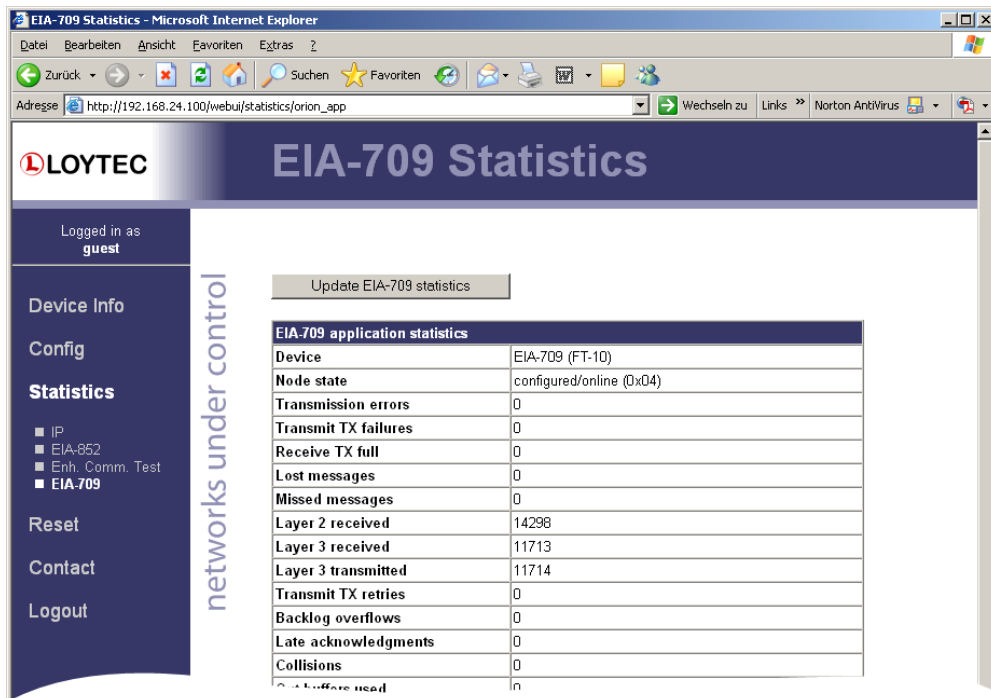


Figure 57: CEA-709 Statistics Page

BACnet MS/TP Statistics

The BACnet MS/TP statistics page is only available, when the BACnet port is configured for the MS/TP data link layer (see Section 0). An example is shown in Figure 58. The separated part on the top of the table contains the most important statistics data.

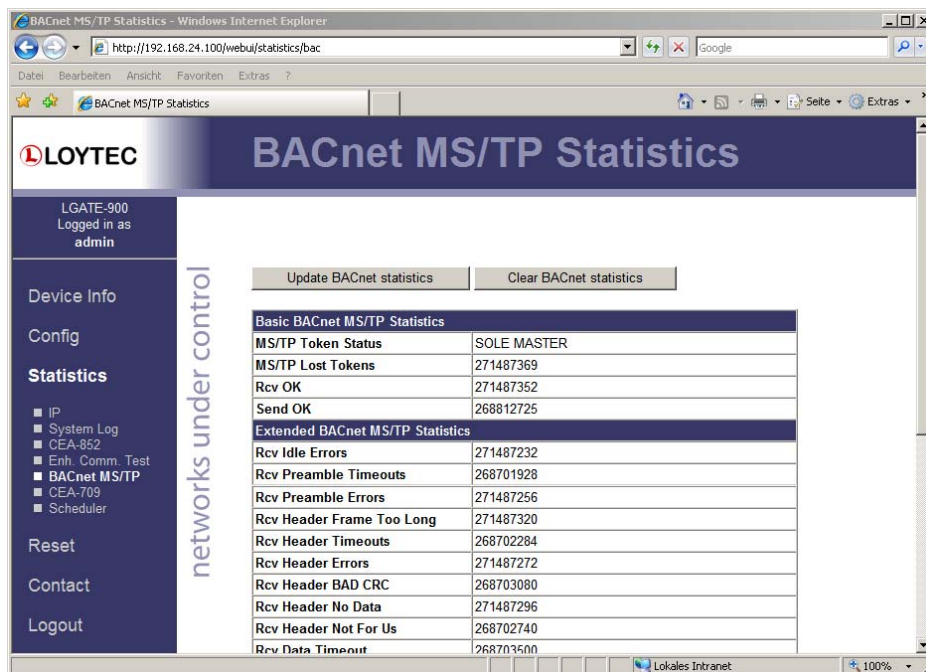


Figure 58: BACnet MS/TP Statistics Page

The MS/TP token status reports the current token passing state. In state 'OK', the token is circulating between the masters. This is the normal state, when multiple masters are on the MS/TP network. The state 'SOLE MASTER' is the normal state when the L-Gate is the only master on the network. If there are multiple masters on the network (e.g., an MS/TP BACnet router), this state is a hint to a broken cable. In state 'TOKEN LOST', the token is currently not circulating.

The counter 'MS/TP lost tokens' is an indicator for communication problems on the MS/TP network. If it increases, there is a cabling, ground, or termination problem. The counters 'Rcv ok' and 'Send ok' reflect the number of successfully received or transmitted MS/TP frames. Check these counters to verify that communication is flowing on the MS/TP segment.

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 59.

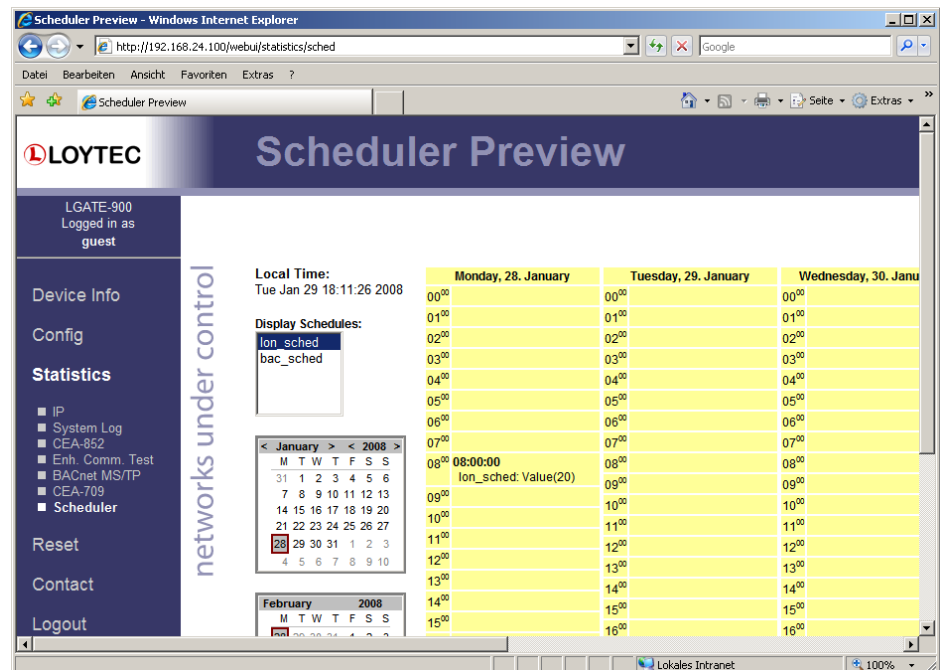


Figure 59: Scheduler Statistics Page

Reset, Contact, Logout

The menu item "Reset" allows resetting the L-Gate from a remote location. The "Contact" item provides contact information and a link to the latest user manual and the latest firmware version. The Logout item closes the current session.

L-Gateway Configuration Software

Overview

Data Points

The operating principle of the L-Gate is to connect data points of one network technology to data points of another technology. Data points in the CEA-709 network are known as network variables (NVs). They have a direction, a name, and a type. The type can be either a standard network variable type (SNVT) or a 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. Data points in the BACnet technology are known as BACnet server objects. They have a specific type (e.g. analog input or binary output) and a set of properties, which describe the data point more closely. The actual value is stored in the "Present_Value".

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

1. Select the data points of the network to be mapped (e.g., select the NVs in the CEA-709 network nodes)
2. Select or create matching counterparts of the other technology (e.g., create matching BACnet objects)
3. Create connections between the data points (e.g. connect NVs and BACnet objects).

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

- **Static NV:** For each selected NV on the network there is a static NV created on the L-Gate. This NV can be bound to the NV on the network. Note that adding static NVs to the L-Gate results in a change to the default XIF file. The L-Gate is assigned a new "model number" to reflect this change (see Section 0). Static NVs are the way to use NVs in non-LNS systems, where NVs shall be bound instead of using polling.
- **Dynamic NV:** For each selected NV on the network there is a dynamic NV created on the L-Gate. Compared to static NVs, dynamic NVs do not change the XIF interface of the L-Gate. The dynamic NVs are created by the network management tool. Currently, only LNS-based tools can manage dynamic NVs. As for static NVs, with dynamic NVs it is possible to use bindings instead of polling.
- **External NV:** The selected NVs on the network are treated as external NVs to the L-Gate. The L-Gate 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.

For more information on the different types of network variables and their implications please refer to the application note in Section 0. For CPs the allocation type "File" is used.

For BACnet data points, the L-Gate always creates BACnet server objects. These objects can be accessed by the BACnet building control system or operating workstations. They support COV subscriptions to deliver value changes in an event-driven way.

For certain applications however, it is necessary that the L-Gate acts as a BACnet client. This functionality can be configured by activating a "client mapping". Client mappings can be of the type "Poll", "COV", "Write", or "Auto". This specifies how the BACnet client accesses other BACnet objects on the BACnet network. The "Auto" method determines the best way (poll, COV, or write) to talk with other server objects. Poll is used for objects that need to read data from other BACnet objects in a periodic manner. COV is used to subscribe for COV at other BACnet objects in order to get updates in an event-driven fashion. Write is used to send updates to other BACnet objects.

When generating matching counter parts to NVs, there are two types of NVs to be considered: Simple NVs that hold only one value (scalar or enumeration), and structured NVs, that consist of a number of fields. For simple NVs only one BACnet object per NV is generated. For structured NVs, one BACnet object is generated for each structure member.

Which type of BACnet object is created depends on the type of the simple NV or of the structure member. For scalar types, analog objects are created. The scaling factors are applied to the NV to get the resulting scalar value for the Present_Value property. Other properties of analog objects are derived from the SNVT, including the engineering units, min and max present value. Multi-state objects are created for NV enumeration types. The CEA-709 state IDs are sorted and renumbered to start at '1' in BACnet (i.e., a '-1' of MOTOR_NUL in CEA-709 maps to a '1' of MOTOR_NUL in BACnet). This is necessary as the SNVT states '-1' and '0' cannot be represented in BACnet as a raw value, because allowed BACnet multi-states start at 1. Which state IDs exist is documented in the BACnet multi-state texts array. Optionally, binary objects are created for enumerated NVs with three states, excluding the '-1' state.

In BACnet commandable objects can be written with values at a certain priority. The value with the highest priority is in effect. When revoking a written value, the NULL value is written. This takes back the value. When all written values are withdrawn, the Relinquish_Default value is in effect. In CEA-709 there is no notion of taking a value back. To model this behavior, a distinctive *invalid* value can be written to an NV. Most SNVTs have such an invalid value. For those that do not an invalid value, it can be specified when editing the data point. To make a BACnet object convey that invalid value to the CEA-709 side, enable the property "Relinquish to Invalid".

Connections

A connection in the L-Gate specifies which data points exchange values with each other. The L-Gate supports both "1:n" and "m:1" connections. The single data point is referred to as the "hub" data point, whereas the other data points are the "target" data points. Only data points of the same technology can be configured on a single side of the connection.

This means, the following connections are possible:

- 1 input from an CEA-709 point is output to n BACnet points,
- m inputs from CEA-709 points are output to one BACnet point,
- 1 input from a BACnet point is output to n CEA-709 points,

- m inputs from BACnet points are output to 1 CEA-709 point.

The most common connection will be the 1:1 connection. This is the type of connection that is auto-generated by the Gateway configuration software.

Static Interface Changes

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

Each time the static interface of the L-Gate 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 L-Gate configuration software is connected via LNS, it supports the process of changing the device template for the new static interface. It automatically upgrades the device template of the L-Gate device in the LNS database and restores the previous bindings and dynamic NVs. If the L-Gate 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 0.

Timing Configuration

Data points in the L-Gateway configuration software can be configured with a number of timing parameters. The following properties are available to input or output data points, respectively:

- Polycle (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.

AST Features

Alarming

The alarming architecture comprises a number of entities. Objects that monitor values 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.

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 value is scheduled, the scheduler maintains its state for this value. 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 60 for an example of a daily schedule.



Figure 60: 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*, e.g., *Holidays*. Each calendar pattern describes a pattern of dates through a number of *pattern entries*, e.g., “July 14th every year”.

When a calendar is defined on a system, the exception days are available in all schedules. When a schedule want to define daily schedules for some of the available exception days, they need to be enabled in the schedule. See Figure 61 for an example where *Holidays* is used.

Weekday / Exception	Priority	Events	Use
Mon	-	2	<input checked="" type="checkbox"/>
Tue	-	0	<input checked="" type="checkbox"/>
Wed	-	0	<input checked="" type="checkbox"/>
Thu	-	0	<input checked="" type="checkbox"/>
Fri	-	0	<input checked="" type="checkbox"/>
Sat	-	0	<input checked="" type="checkbox"/>
Sun	-	0	<input checked="" type="checkbox"/>
Holidays	126 (lowest)	0	<input checked="" type="checkbox"/>
Maintenance Days	126 (lowest)	0	<input type="checkbox"/>

Figure 61: 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 single 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, that 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.

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.

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 L-Gate. This can be done on the Web UI (see Section 0). It is recommended to use the E-Mail server of your Internet provider. For public mailers enable the required authentication. Please note that the L-Gate does currently not support the SSL/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.

Installing the Configuration Software

The L-Gateway Configuration software must be used to setup the data point configuration of the L-Gate. This configuration utility 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, and Windows 2003 Server.

The L-Gateway configuration software can be downloaded from the LOYTEC website <http://www.loytec.com>. To install the configuration utility, double click on Setup and follow the installation steps. 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.

Registration as a Plug-In

If the L-Gate shall be configured using LNS-based tools (e.g. NL200 or LonMaker), the Gateway configuration software 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.

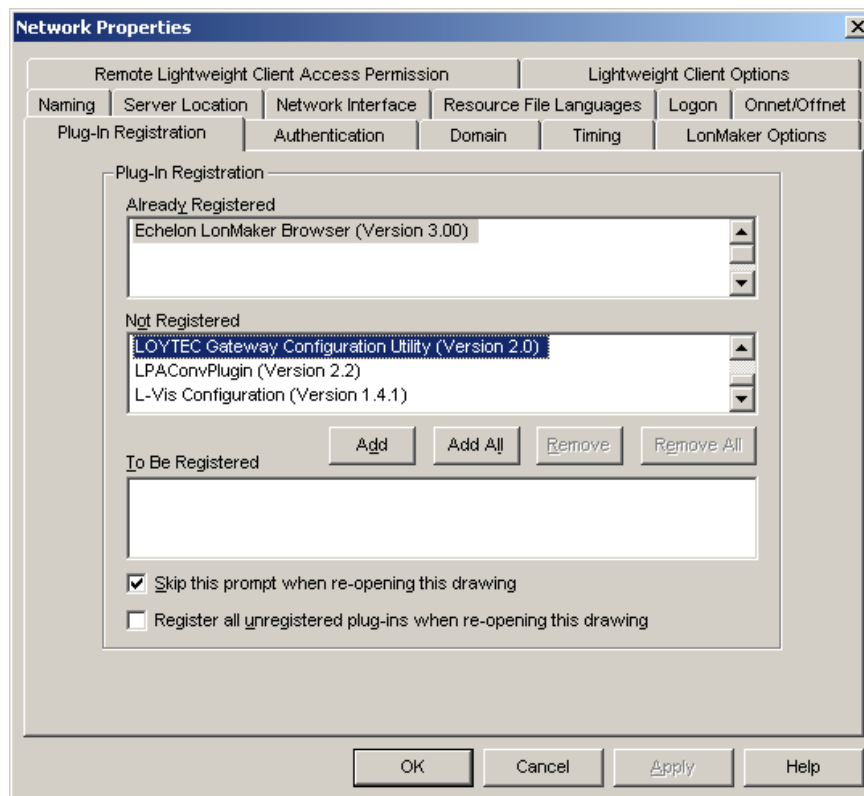


Figure 62: Select the Plug-in to be registered and click Add.

Open LonMaker and create a new network. When the “Plug-in Registration” dialog window pops up select the **LOYTEC Gateway Configuration Utility Version 3.0** from the list of “Not Registered Plug-Ins” (see Figure 62). Click “Add” and then “Ok” to

register the plug-in. Device templates for the L-Gate are added automatically and XIF files are copied into the LNS import directory.

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

Under LonMaker → Network Properties → Plug-In Registration make sure that the **LOYTEC Gateway Configuration Utility (Version 3.0)** shows up under “Already Registered”.

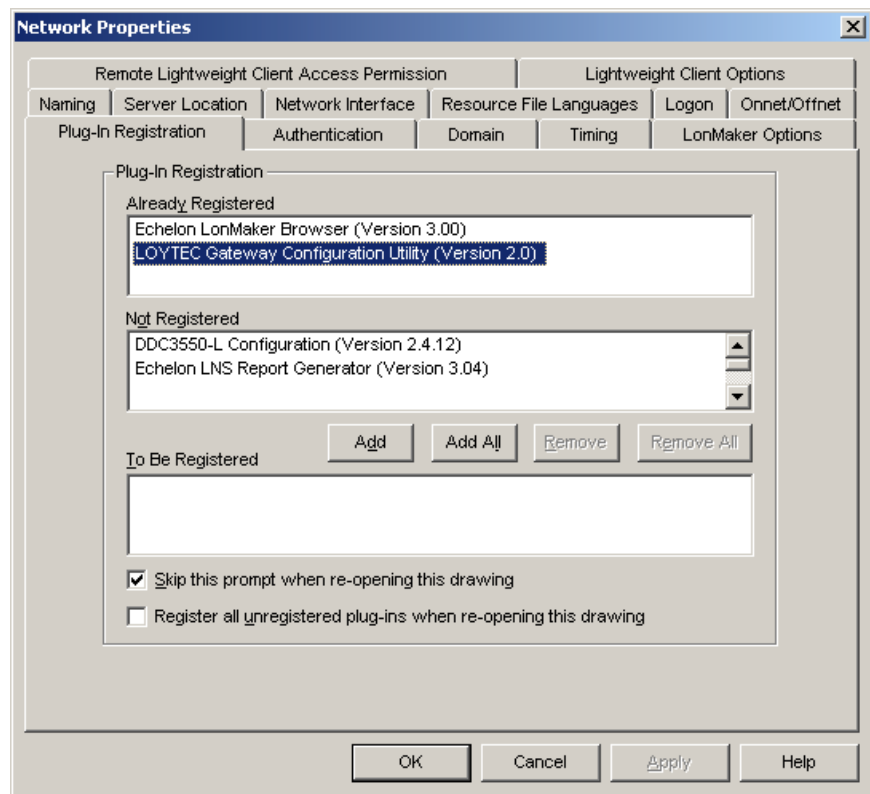


Figure 63: Double check that the Gateway configuration software is properly registered.

Operating Modes of the Configuration Software

The L-Gateway configuration utility 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 L-Gate 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 L-Gateway configuration utility 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.

Data Point Manager

The configuration software uses a central concept to manage data points. The data point manager as shown in Figure 64 is used to select, create, edit and delete data points. The dialog is divided into three sections:

- The folder list (number 1 in Figure 64),
- The data point list (number 2 in Figure 64),
- And a property view (number 3 in Figure 64).

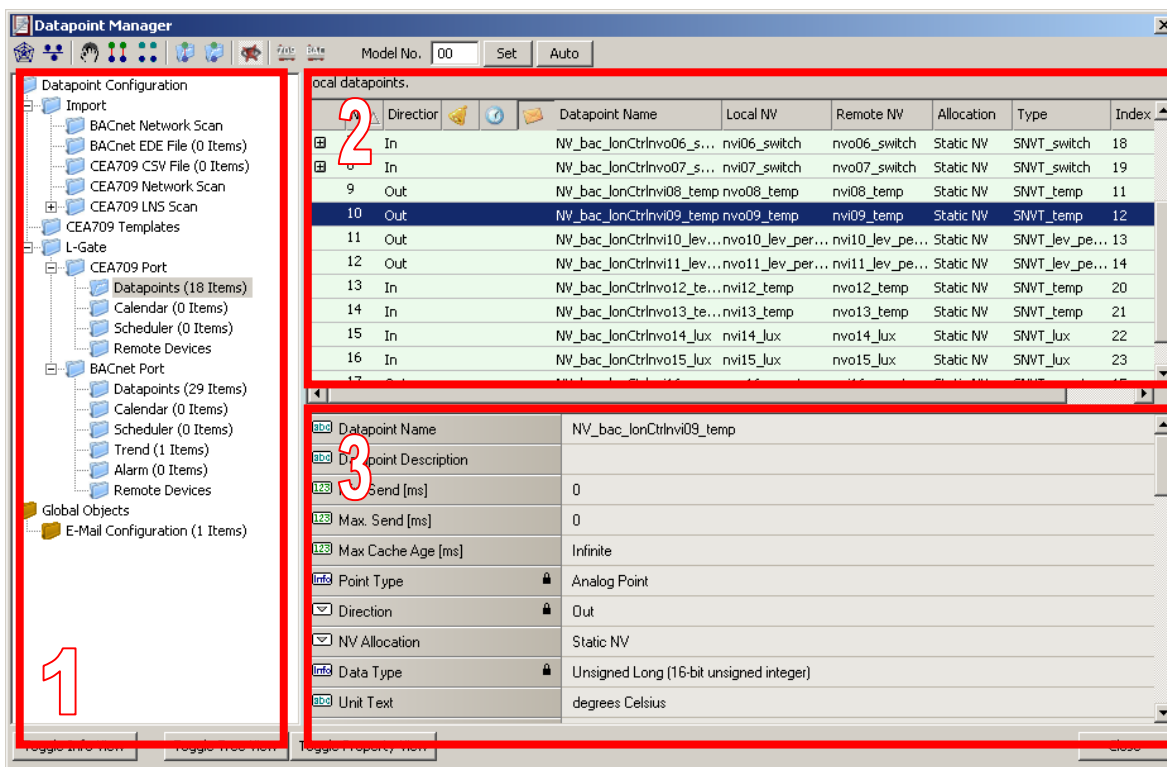


Figure 64: Datapoint Manager Dialog

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 several sub-folders. The LNS Database Scan folder is used to hold data retrieved from a network database scan. The CEA709/852 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. The BACnet Network Scan folder is used to display data points retrieved by an online scan of the BACnet network. The EDE File folder is used to display data points imported from an EDE file. 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 L-Gate.
- **L-Gate:** This is the device folder of the L-Gate. It contains all the necessary data points which constitute to the L-Gate's port interface definition. These data points are created on the L-Gate when the configuration is downloaded. The two subfolders represent the CEA-709 and BACnet ports on the L-Gate.
- **Datapoints:** Each port folder contains a data points sub-folder. This folder holds all data points, that 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.

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.

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.

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  sign in the list indicates that the data point contains sub-points. These can be structure members for structured SNVTs. Clicking on the  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 7 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

Table 7: Icons for used data points in the data point list view.

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. In a 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.

Some important properties include:

- **Datapoint Name:** This is the technology-independent data point name. This name may be used for the actual network variable, but can be different (e.g. longer). Datapoint names must be unique within a given folder. On the L-Gate the datapoint name is used as the BACnet object name.
- **Description:** This is a human readable description of the data point. There are no special restrictions for a description.
- **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.
- **Enable 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.
- **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.

Project Settings

The project settings allow to define 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.

General

The general tab of the project settings as shown in Figure 65 contains settings independent of the technology port. The settings are:

- **Project Name:** This setting allows to enter a descriptive name for the project.
- **Default Polycle for External NVs:** When using external NVs, this polycle is set as a default for input data points. The polycle 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 to set the UNSET state explicitly. As a binary point the UNSET state is implicitly chosen when the invalid value is written.
- **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. Instead the default username and default password from the project settings are used.

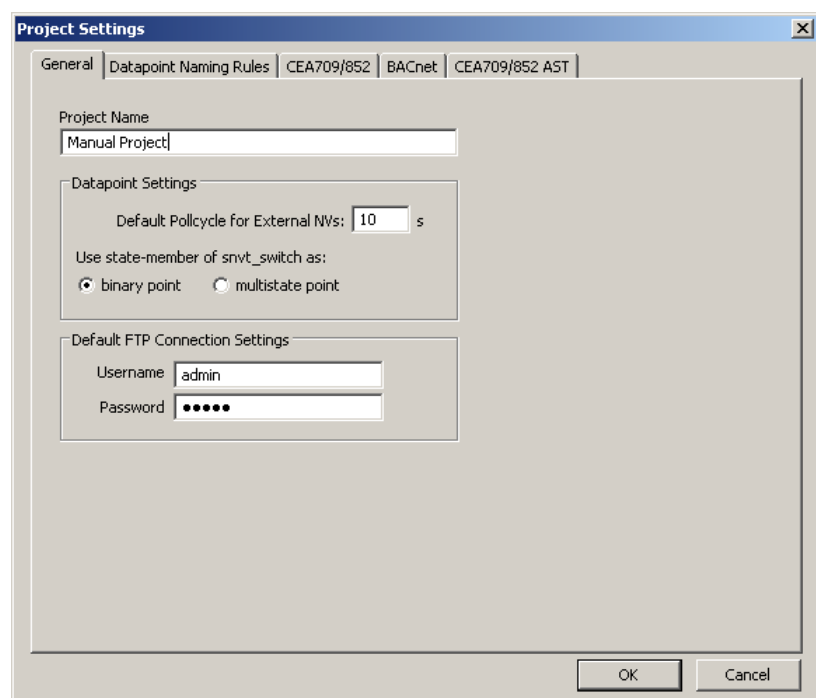


Figure 65: General Project Settings.

Data Point Naming Rules

The data point naming rules tab (see Figure 66) allows to specify, how data point names are automatically derived from scanned network variables. The preview shows how names would look like, when the check marks are modified.

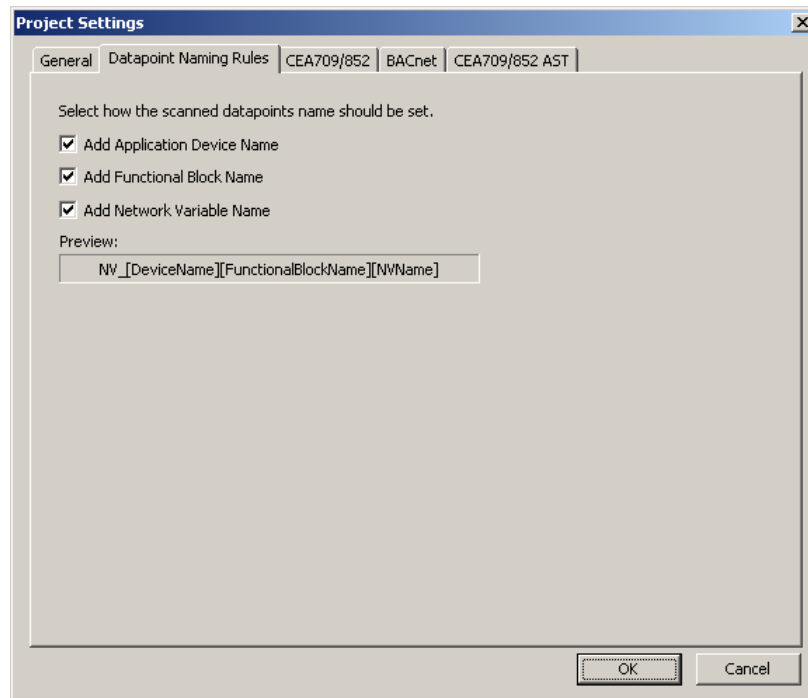


Figure 66: Data Point Naming Rules Project Settings.

CEA-709 Settings

The CEA-709 configuration tab as shown in Figure 67 allows to configure 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. See Section 0 for more information on how to configure such a system.
- **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 0) 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.

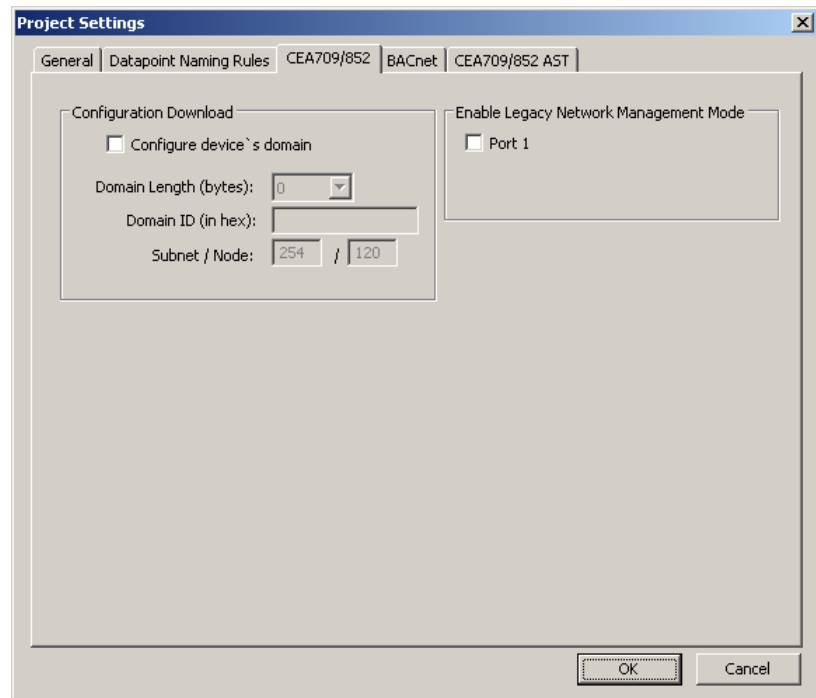


Figure 67: CEA-709 Project Settings.

BACnet Settings

The BACnet configuration tab as shown in Figure 68 allows to configure properties of the device's BACnet port. The options are:

- **Enable Unsolicited COV:** Put a check mark on this option to enable COV-U on the BACnet port. When active, the device sends unsolicited COV broadcast on all BACnet objects, when their value changes in accordance to the respective COV rules.
- **Always create value objects on auto-create:** If activated, the auto-create BACnet points function of the configuration software creates commandable value objects (AV, BV, MV) instead of output objects (AO, BO, MO) and non-commandable value objects (AV, BV, MV) instead of input objects (AI, BI, MI). This feature can be activated if the regular input/output model is not desired.
- **Encode all strings:** This setting defines, how strings in BACnet objects are encoded. By default it is ASCII, which is compatible with most BACnet software. To support characters of Western European languages, choose ISO-8859-1. To support Unicode character sets (e.g., Japanese) select UCS-2.

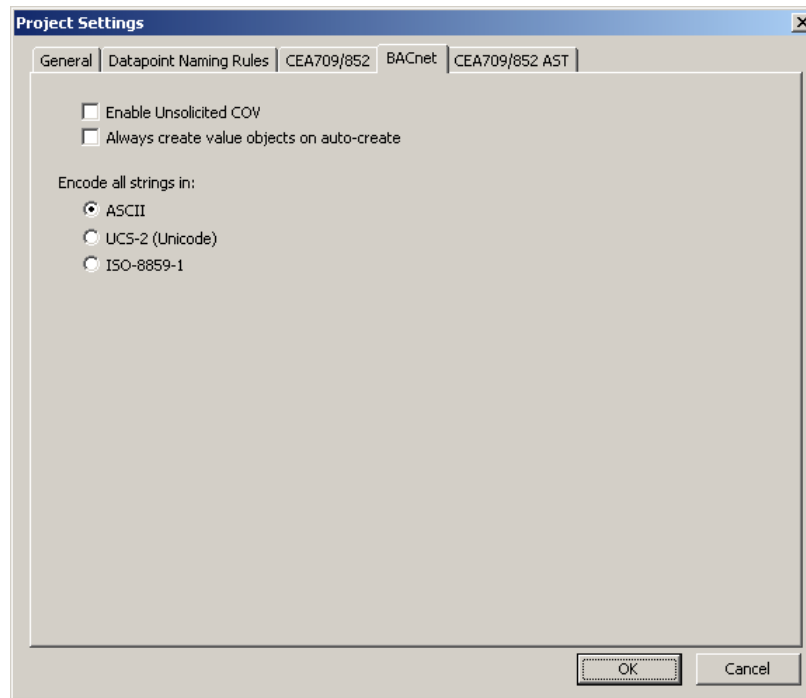


Figure 68: BACnet Project Settings.

AST Settings

For CEA709 devices, the use of alarming, scheduling, trending (AST) features requires additional resources (functional objects and NVs). The dialog is shown in Figure 69. Changes made there affect the static interface. Since the number of used resources also influences the performance, the CEA-709 AST tab allows to configure 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.

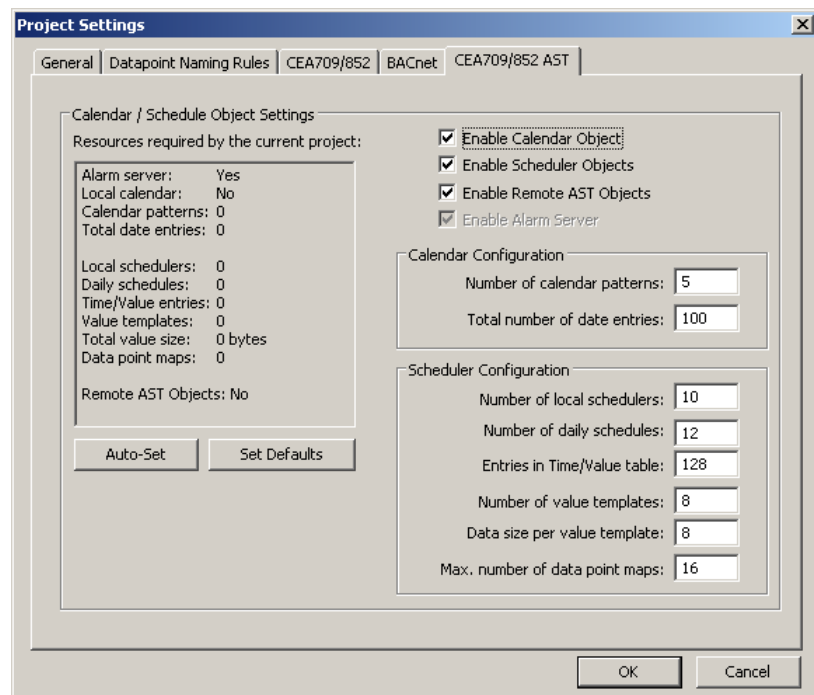


Figure 69: CEA-709 AST Project Settings.

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.

L-Gate in a Network

Workflows for the L-Gate

This section presents a number of work flows for configuring the L-Gate in different use cases in addition to the simple use case in the quick-start scenario (see Section 0). 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 L-Gateway configuration software supports the following use cases:

- Network Management Tool based on LNS 3.x (see Section 0)
- Non-LNS 3.x network management tool with polling (see Section 0)
- Non-LNS 3.x network management tool with bindings (see Section 0)

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 L-Gate online.
- Gateway configuration project file: This file contains all ports, all data points and all connections of a project. These files end with “.gtw”. It stores all the relevant configuration data and is intended to be saved on a PC to back up the L-Gate's data point configuration.

Configure with LNS

The flow diagram in Figure 70 shows the steps that need to be followed in order to configure the L-Gate in a network with LNS 3.x. In this scenario the L-Gate will use dynamic NVs and bindings.

First, the L-Gate device must be added to LNS (see Section 0). Then the L-Gateway configuration utility must be started in plug-in mode to configure the L-Gate (see Section 0). In the utility scan for the data points in the LNS database (see Section 0). Select the NVs that the L-Gate shall expose to BACnet (see Section 0). Generate BACnet objects and connections from the used NVs (see Section 0). Finally, the configuration needs to be downloaded onto the L-Gate (see Section 0). It is recommended to save the complete configuration to a disk file for being able to replace an L-Gate in the network.

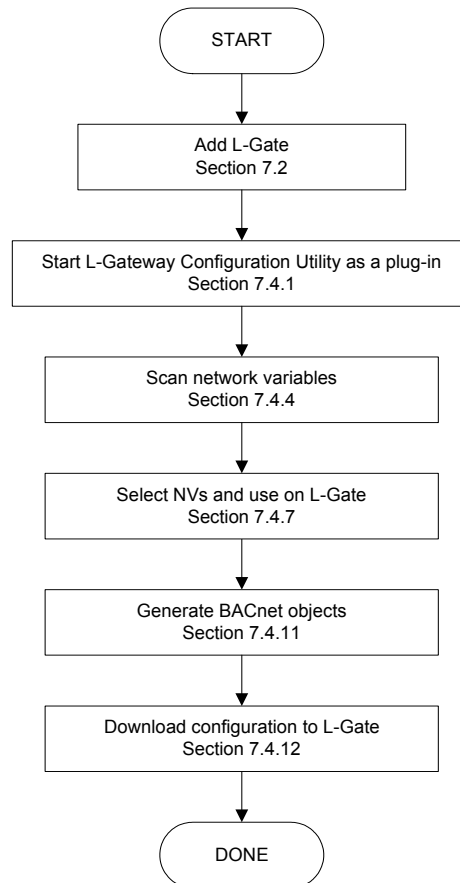


Figure 70: Basic design-flow with LNS.

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

Configure without LNS

The flow diagram in Figure 71 shows the steps that need to be followed in order to configure the L-Gate without LNS 3.x. In this scenario the L-Gate 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 L-Gateway configuration utility in stand-alone mode and connect to the L-Gate via the FTP method (see Section 0). If changing an existing configuration upload the current configuration from the L-Gate (see Section 0). In the utility import data points from a CSV import file (see Section 0) or scan an CEA-709 network online (see Section 0). Select the NVs that the L-Gate shall expose to BACnet (see Section 0). Alternatively, you can create external NVs manually (see Section 0). Generate BACnet objects and connections from the used NVs (see Section 0). Finally, the configuration needs to be downloaded onto the L-Gate (see Section 0). It is recommended to save the complete configuration to a disk file for being able to replace an L-Gate in the network.

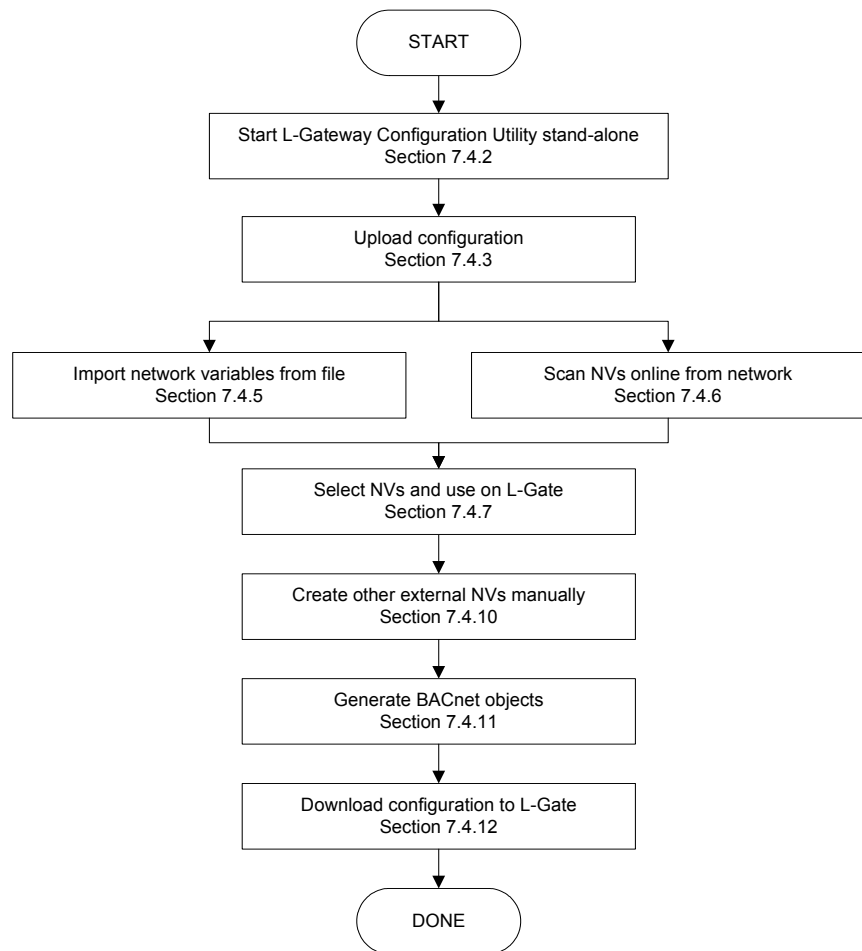


Figure 71: Basic design-flow without LNS.

Configure without LNS Using Bindings

The flow diagram in Figure 72 shows the steps that need to be followed in order to configure the L-Gate without LNS 3.x. In this scenario the L-Gate 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 L-Gate and update an existing network.

Start the L-Gateway configuration utility in stand-alone mode and connect to the L-Gate via the FTP method (see Section 0). In the utility import data points from a CSV import file (see Section 0) or scan an CEA-709 network online (see Section 0). Select the NVs that the L-Gate shall expose to BACnet (see Section 0). For the NVs used on the L-Gate select the “static NV” allocation type (see Section 0). Alternatively, you can create static NVs manually (see Section 0).

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

Generate BACnet objects and connections from the used NVs (see Section 0). Download the configuration onto the L-Gate (see Section 0). Finally, export a XIF file (see Section 0). It is recommended to save the complete configuration to a disk file for being able to replace an L-Gate in the network.

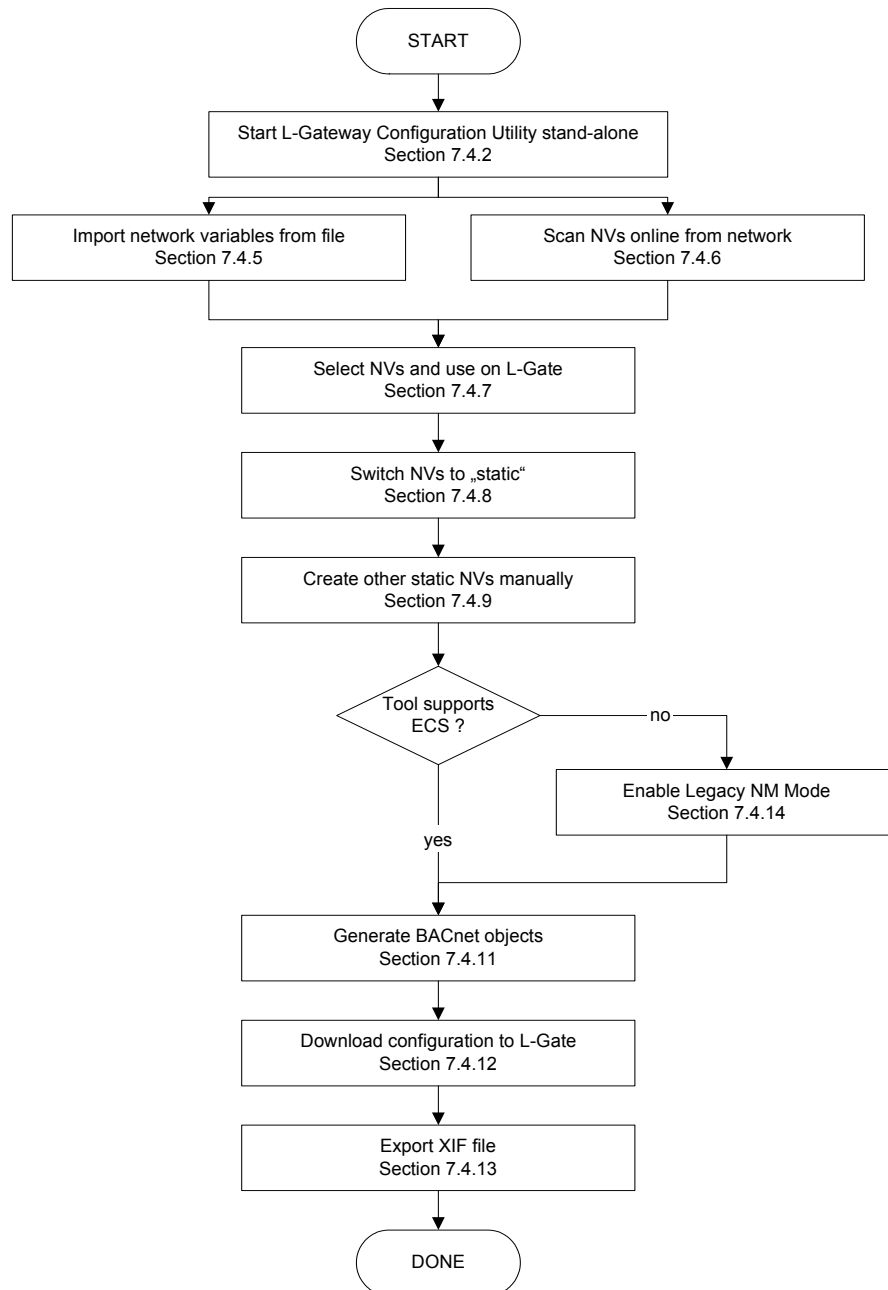


Figure 72: Basic design-flow without LNS using bindings.

To use the L-Gate in the non-LNS management tool, commission the L-Gate using the exported XIF file and create the bindings.

When changing a running L-Gate configuration with existing bindings, it is recommended to create additional data points as external NVs with polling as described in Section 0. Otherwise, a new XIF file needs to be exported and replacing the L-Gate in the non-LNS tool requires the user to create all bindings again from scratch (see Section 0).

Replace an L-Gate

An L-Gate can be replaced in the network by another unit. This might be necessary, if a hardware defect occurs. First of all, the replacement L-Gate needs to be configured with the appropriate IP settings, including all relevant BACnet device settings. The remainder of this section focuses on the L-Gate data point configuration. The work flow is depicted in Figure 73.

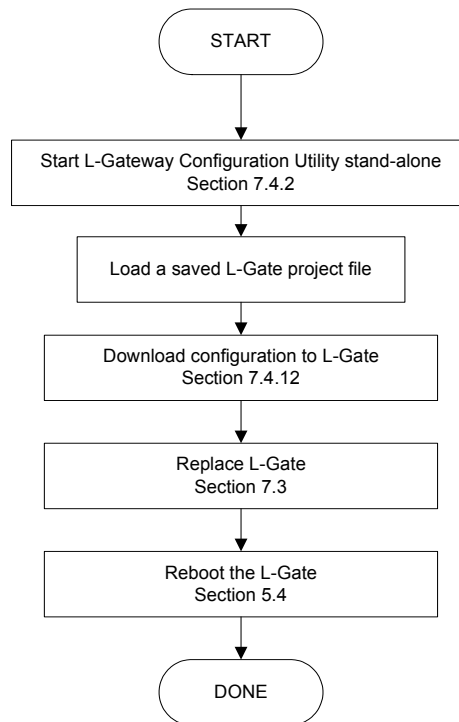


Figure 73: Basic work flow to configure a replacement device.

Start the L-Gateway configuration software stand-alone and connect via the FTP method (see Section 0). Then load the L-Gate configuration project file from disk, which has been saved when the original L-Gate has been configured or modified. Double-check, if the data point configuration seems sensible. Then download the configuration to the L-Gate (see Section 0).

If using an LNS-based tool, the L-Gate device needs to be replaced in that tool (see Section 0). 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 L-Gate (see Section 0)

Configure from BACnet

The flow diagram in Figure 74 shows the steps that need to be followed in order to configure the L-Gate from the BACnet side. In this scenario the L-Gate will be configured with BACnet data points from the BACnet network. The CEA-709 side of the gateway has to be engineered as described in the previous section, but without automatic BACnet object creation. The remainder of this section assumes, that NVs and the static interface have been configured already.

Start the L-Gateway configuration utility in stand-alone mode and connect to the L-Gate via the FTP method (see Section 0). In the utility use the BACnet network scan to find BACnet objects in the network (see Section 0) or import BACnet objects from an EDE file (see Section 0). Select the remote BACnet objects, that the L-Gate shall access and use them on the device to create client mappings on the L-Gate (see Section 0). Alternatively, you can create BACnet server objects manually (see Section 0).

Once the BACnet client mappings or server objects have been created on the BACnet port, connections need to be created (see Section 0). This has to be done manually by selecting the BACnet object and the NV, where this BACnet object shall be exposed to.

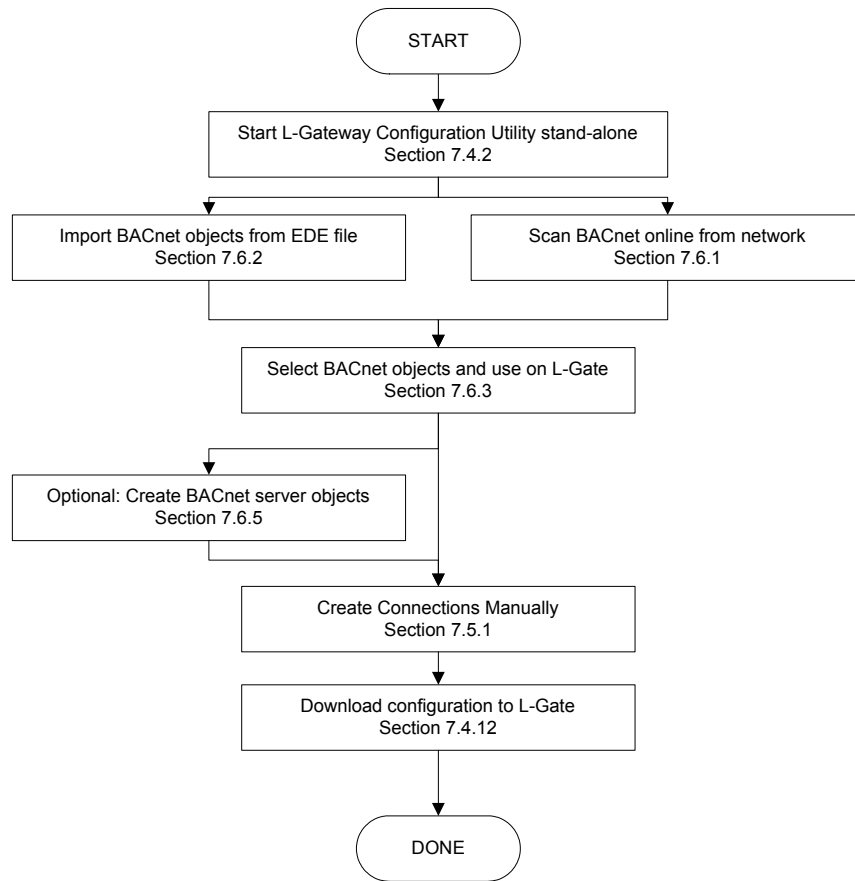


Figure 74: Basic design-flow from BACnet.

Adding L-Gate

To add an L-Gate to your LonMaker drawing, drag a device stencil into the drawing. Enter an appropriate name, select “Commission Device” if the L-Gate is already connected to the network, and hit next as shown in Figure 75.

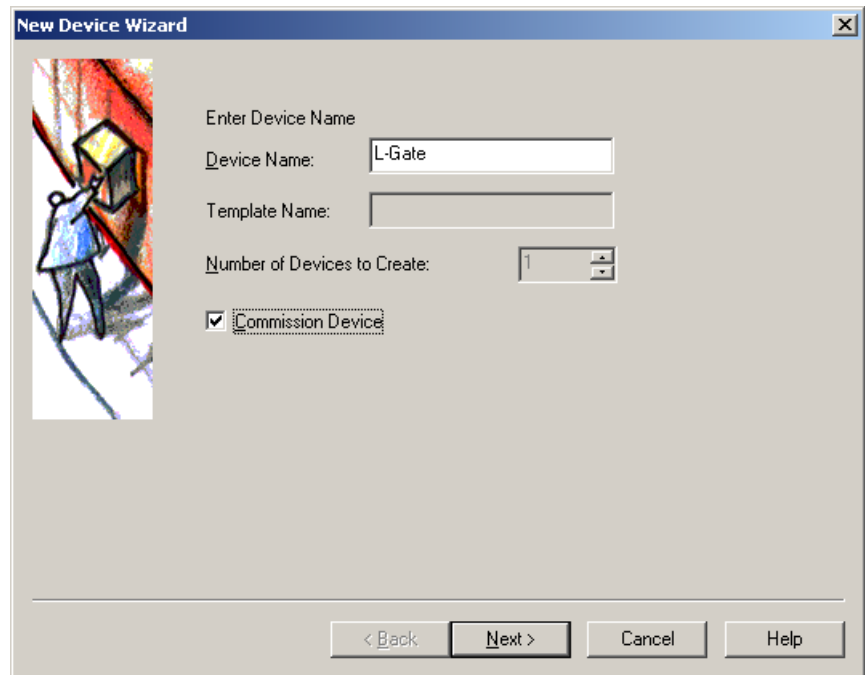


Figure 75: Create a new device in the drawing.

Then select the existing device template of the L-Gate. Select “L-Gate-900 FT-10”, if the L-Gate is configured to use the FT-10 interface, or “L-Gate-900 IP-10L”, if the L-Gate is configured to be on the IP channel. Figure 76 assumes the L-Gate to use the FT-10 port. For information on how to configure which port to use, refer to Section 0 for the console UI or Section 0 for the Web UI.

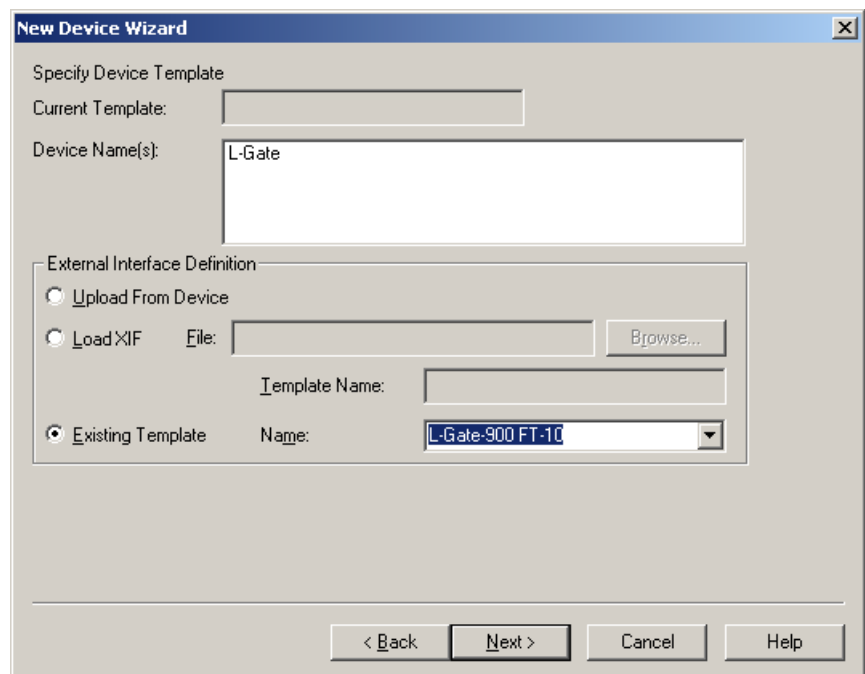


Figure 76: Select the installed L-Gate-900 device template.

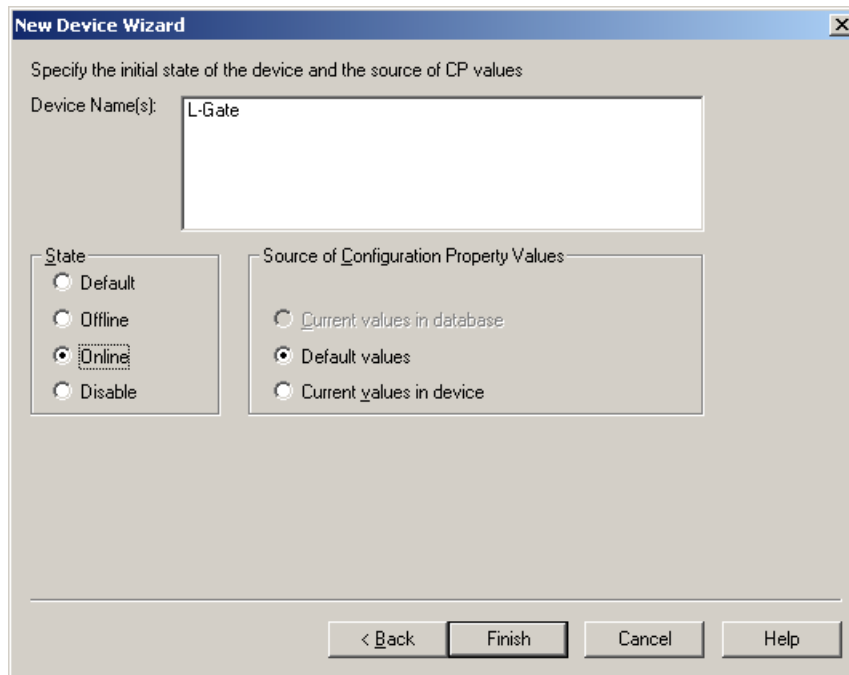


Figure 77: Finish adding the L-Gate.

Click “Next” in the following screens and complete the process by clicking “Finish” in the last screen as shown in Figure 77. You may choose to set the configuration values if prompted in a following dialog window. Finally, you should get an L-Gate device added to your drawing as depicted in Figure 78.

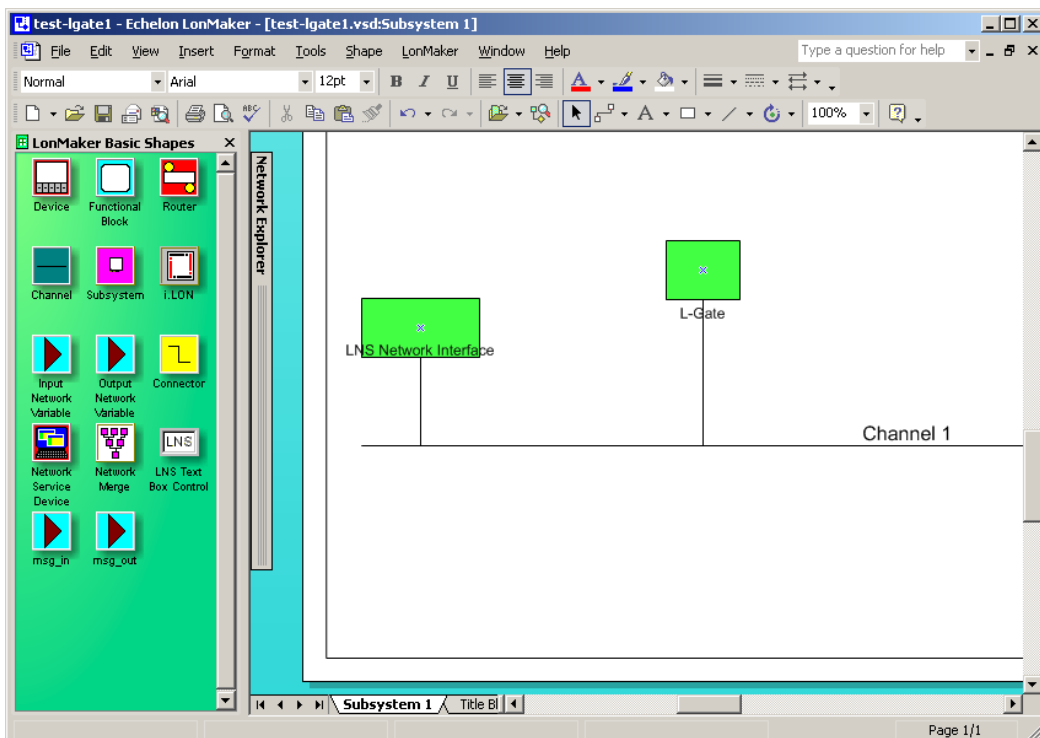


Figure 78: The L-Gate has been added to the drawing.

Replace an L-Gate

Let's assume there is a device 'lgate1' in the LNS database as shown in Figure 79. To replace the device right-click on the device shape and select 'Replace...'. This opens the LonMaker replace wizard as shown in Figure 80.

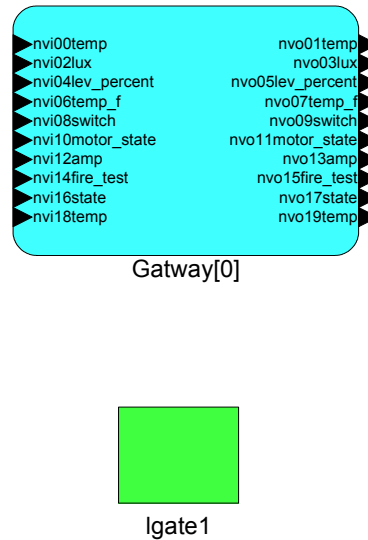


Figure 79: LonMaker drawing with one L-Gate device.

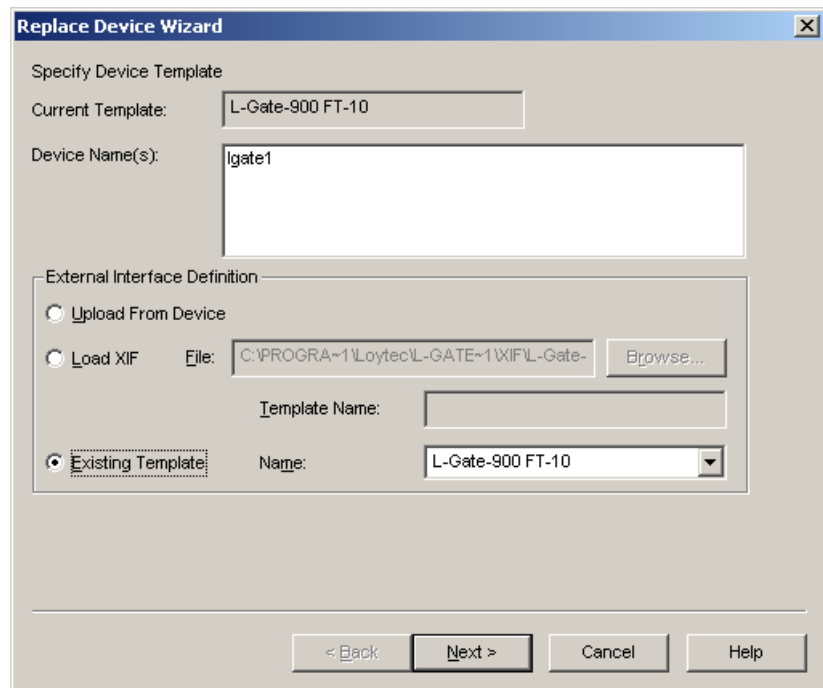


Figure 80: LonMaker replace wizard.

Choose the existing template and click Next.

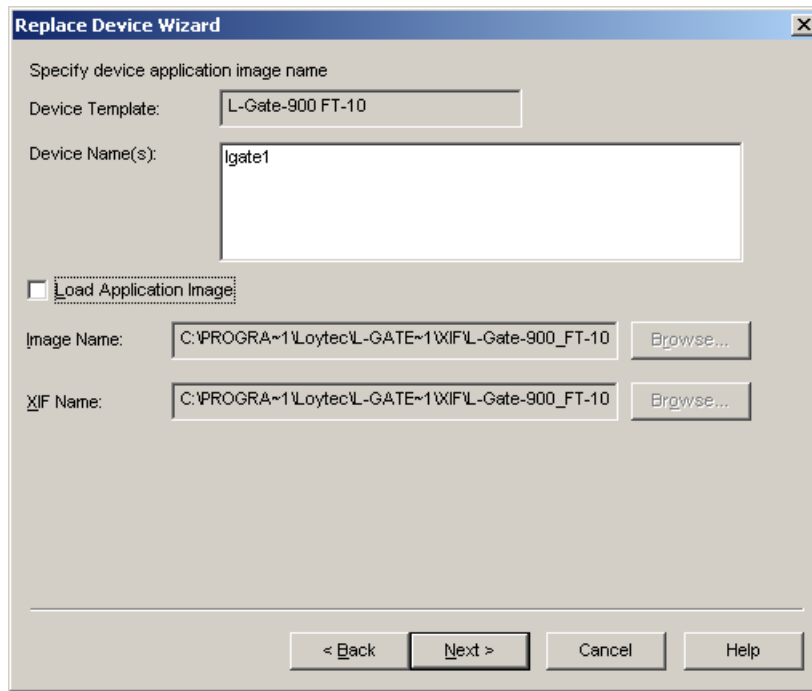


Figure 81: Click Next without loading an application image.

In the following window shown in Figure 81 click Next. Then select 'Online' as shown in Figure 82.

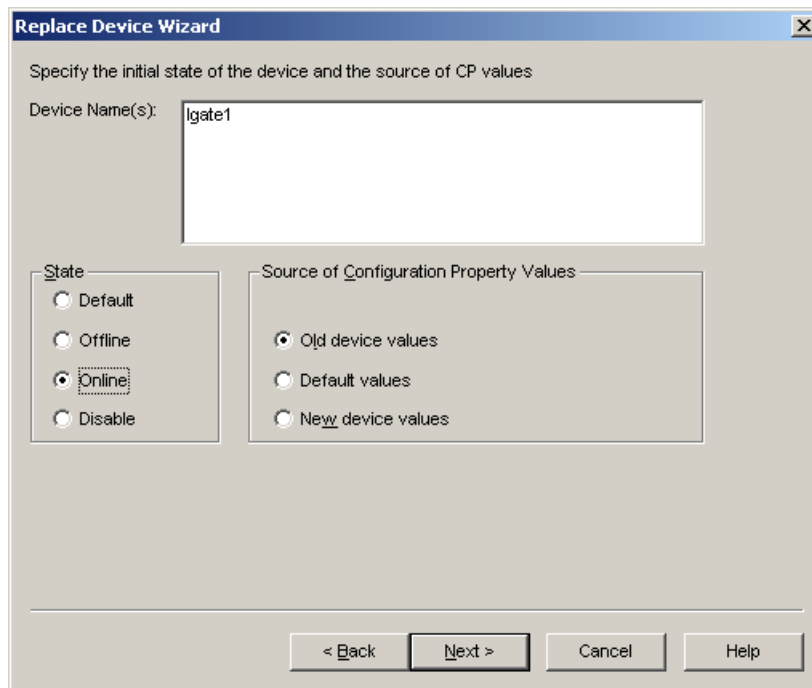


Figure 82: Select online state and click Next.

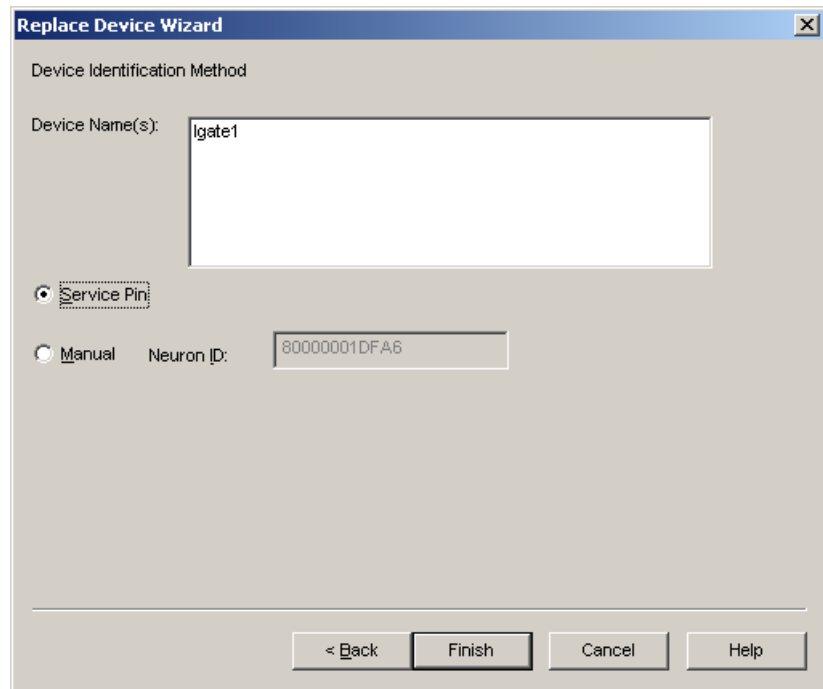


Figure 83: Select Service Pin and click Finish

Finally select the service pin method and click on Finish as shown in Figure 83. Then the service pin requestor opens as shown in Figure 84. Press the service pin on the replacement L-Gate on the correct port. You can also send the service pin using the Web interface (see Section 0).

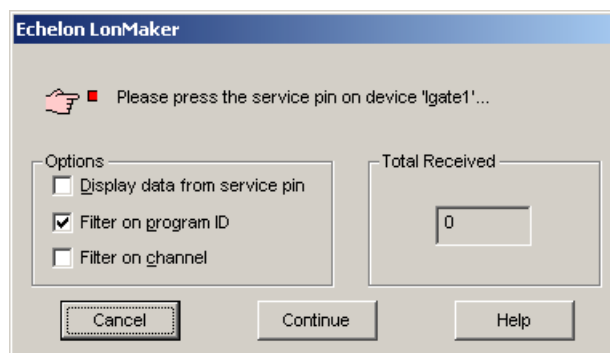


Figure 84: Waiting for the service pin on the replacement unit

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

Using the L-Gateway Configuration Software

Starting as an LNS Plug-In

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

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

In Alex the Plug-in is started by right clicking on the L-Gate device and selecting the **LOYTEC Gateway Configuration Utility** in the **Starte PlugIn** sub menu.

A window similar to what is shown in Figure 85 should appear.

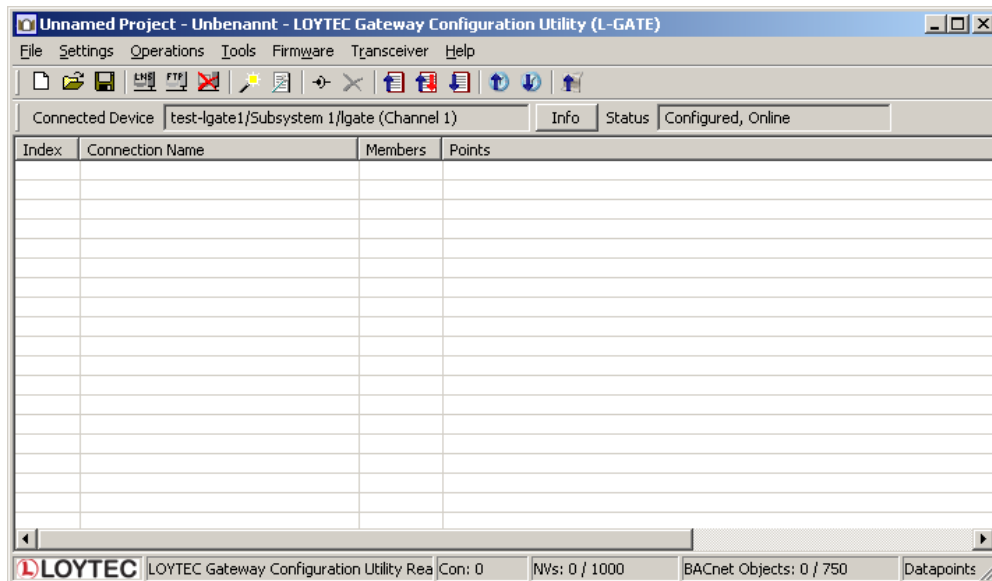


Figure 85: L-Gateway configuration software main window.

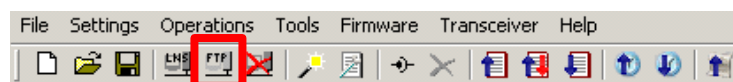
Starting Stand-Alone

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

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

To Connect to an L-Gate 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 86 opens.

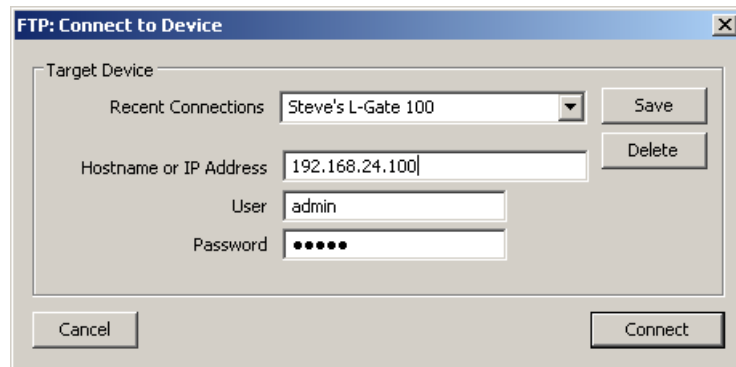


Figure 86: FTP connection dialog.

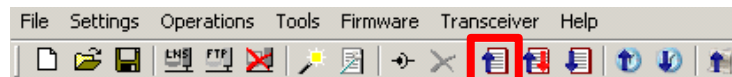
2. Enter the IP address of the L-Gate, the user and password. The default user is “admin” and the default password is “admin”.
3. Optionally, click into the **Recent Connections** field and enter a user-defined name for this connection. That name can be selected later to connect. Click on **Save** to store that connection.
4. Click on **Connect**. This established the connection to the device.

Uploading the Configuration

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

To Upload a Configuration

1. Click on the upload button



in the tool bar of the main connections window. The configuration upload dialog opens up as shown in Figure 87.

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 L-Gate is on-line, also the current connection information and manually created dynamic NVs and schedules are uploaded.

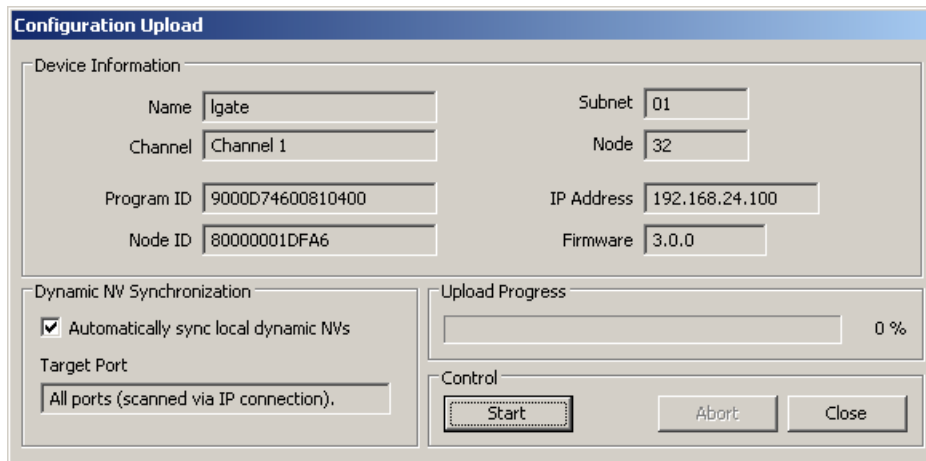


Figure 87: Configuration upload dialog.

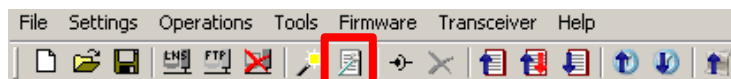
3. When asked, if schedules shall be uploaded also, click **Yes**, if you want the current schedule configuration be extracted from the device. Note, that when doing so, the original schedules in the project are replaced by the uploaded schedules.
4. If dynamic NVs were synchronized, click on **Finish**.

Scanning for Network Variables


When the L-Gateway configuration software 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. In the main connections window, click on the **Open Datapoint Manager** speed button



in the tool bar of the main connections window. The **Datapoint Manager** dialog opens.

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

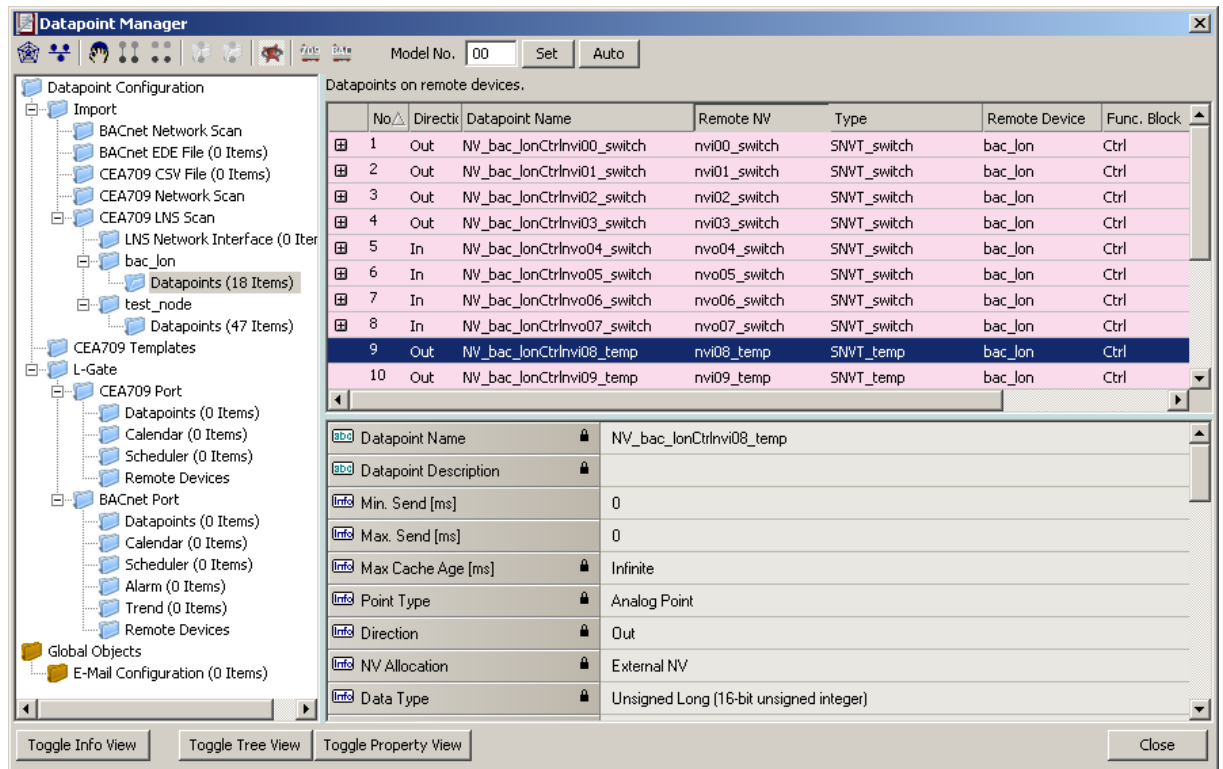


Figure 88: Scanned NVs in the LNS Database Scan Folder

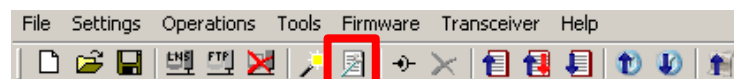
Figure 88 shows an example result of the database scan. The list can be sorted by each column. Selecting a line will display a number of associated properties in the property view below. Multiple items can be selected by using the <Ctrl> key and clicking with the mouse. All items can be selected by pressing <Ctrl-A>.

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 the L-Gate 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 0.

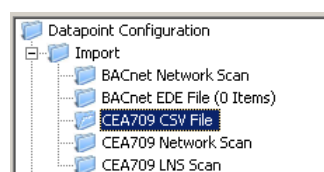
To Import NVs from a File

1. In the main connections window, click on the **Open Datapoint Manager** speed button



in the tool bar of the main connections window. The **Datapoint Manager** dialog opens.

2. Select the folder **CEA709 CSV File**



3. Right-click and select **Import File**. In the following file selector dialog, choose the CSV import file and click **Ok**.

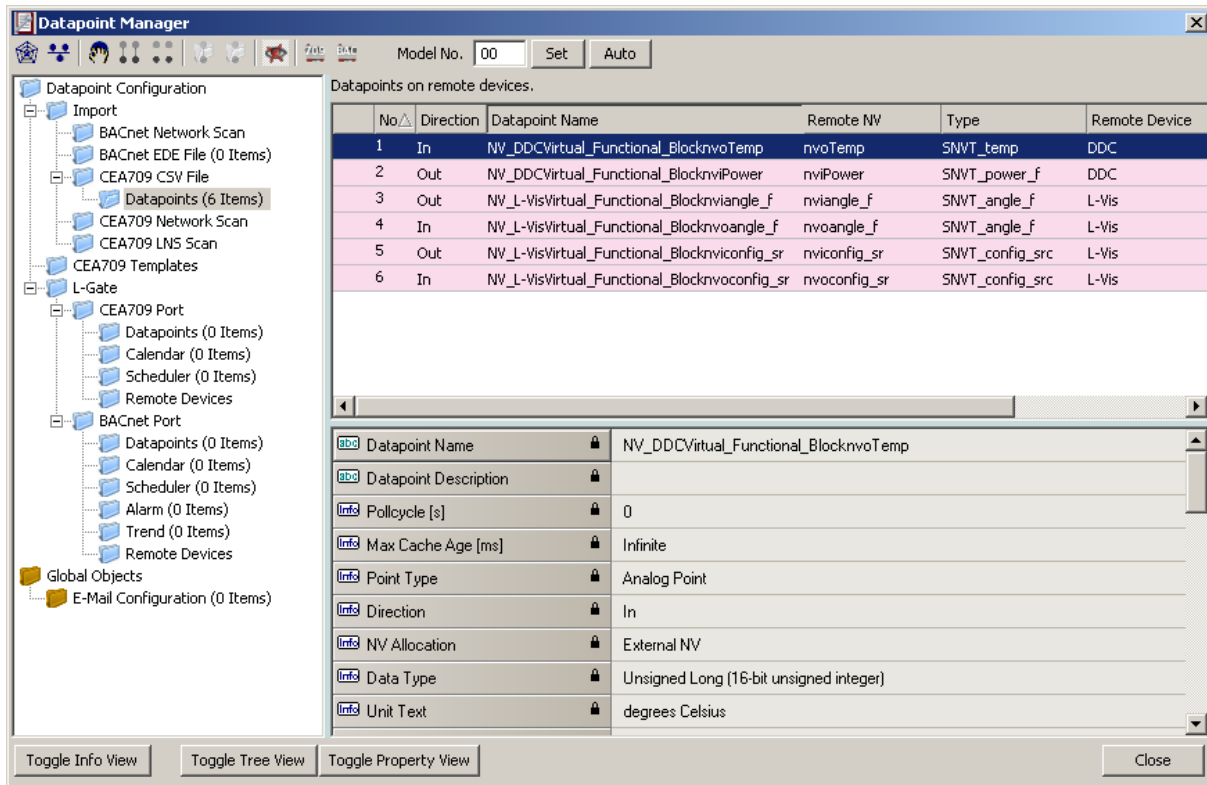


Figure 89: Imported NVs

4. Now the CSV File folder is populated with the imported NVs as shown in Figure 89.

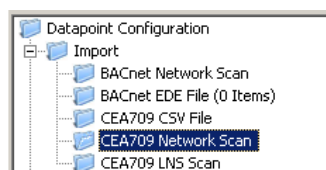
The list can be sorted by each column. Selecting a line will display a number of associated properties in the property view below. Multiple items can be selected by using the <Ctrl> key and clicking with the mouse. All items can be selected by pressing <Ctrl-A>.

Scanning NVs online from the Network

LOYTEC gateway 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. Open the data point manager dialog.
2. Select the folder CEA709 Network Scan



3. Right-click on that folder and select **Scan CEA709/852 Network...**. This opens the CEA709/852 Network Scan dialog as shown in Figure 90.

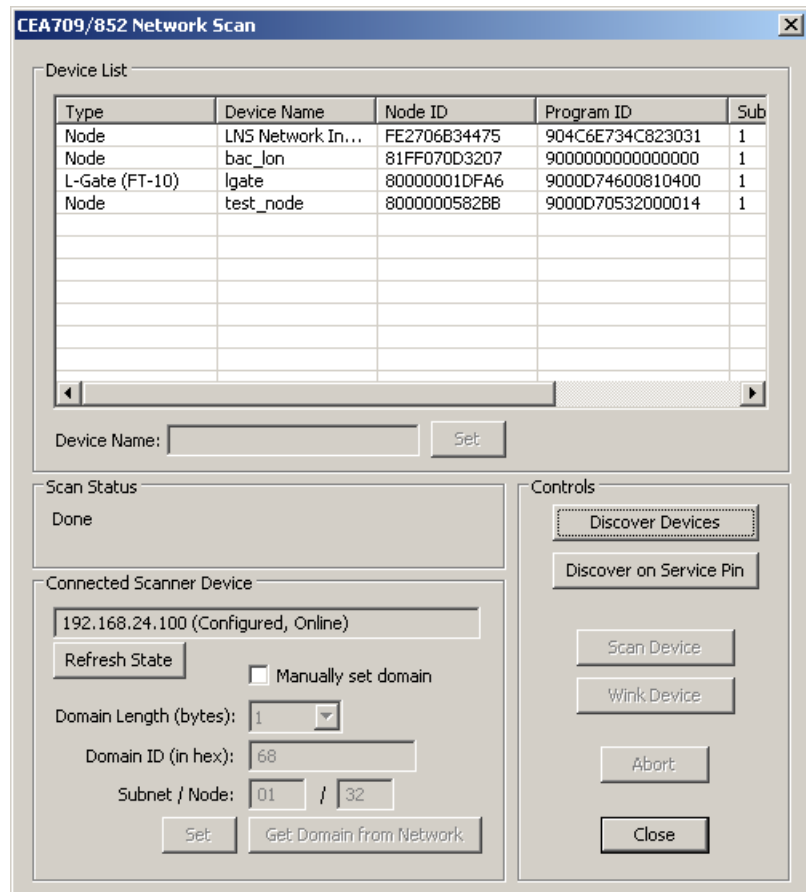


Figure 90: CEA-709 network scan dialog.

4. Click on the button **Discover Devices**. This starts a network scan. The results are put in the device list box.
5. Alternatively, click the button **Discover on Service Pin**. Then press the service pin of a particular device on the network. This device will be added to the device list.
6. Select a device in the device list and click the button **Scan Device**. This scans the NVs on the selected device and adds them to the CEA709/852 Network Scan folder as a separate sub-folder for the device as shown in Figure 91.

Tip!

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

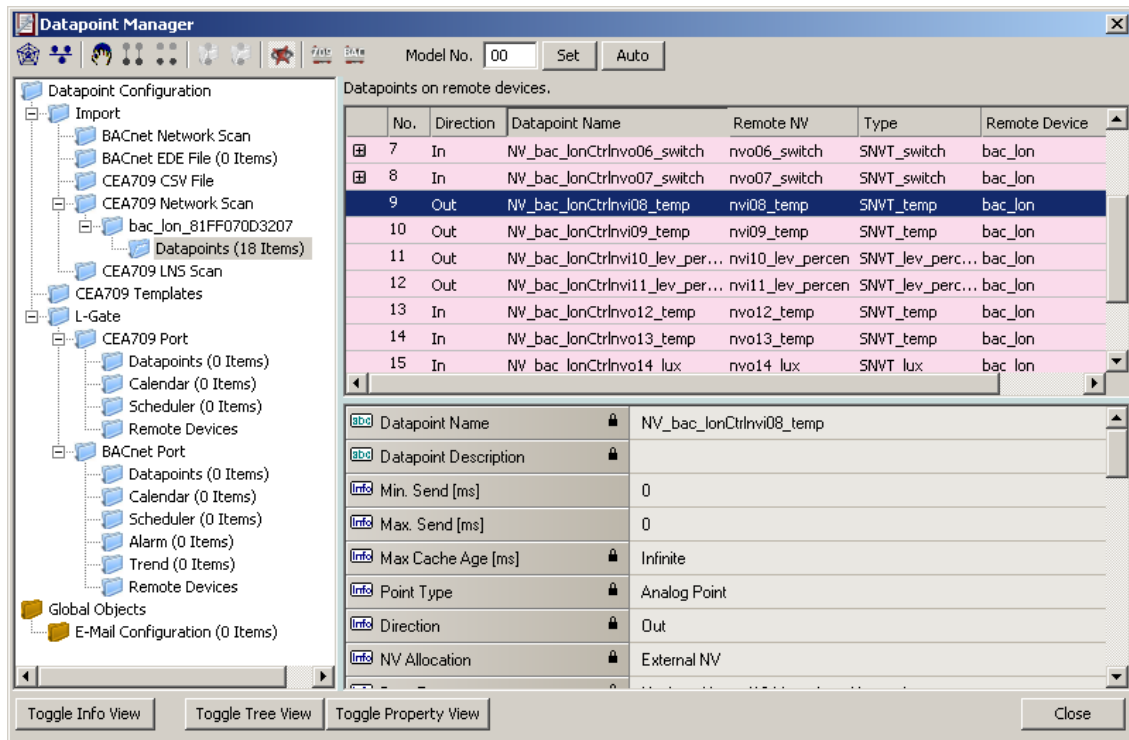



Figure 91: CEA-709 network scan results.

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

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 L-Gate. Select those NVs, which shall be exposed to BACnet objects.

To Use NVs on the L-Gate

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

Tip!

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

Change the NV Allocation

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

To Change the NV Allocation Type

1. In the data point view select the NVs in the L-Gate/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 92.
3. To make the data points static NVs on the L-Gate, select **Static NV**.

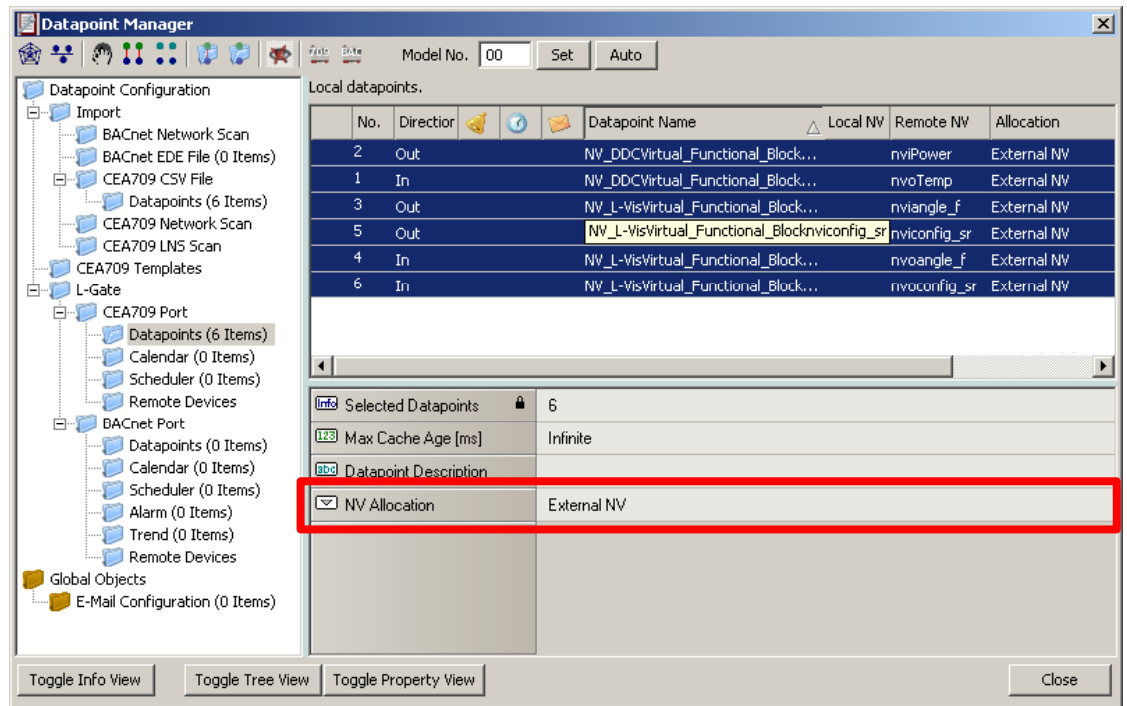


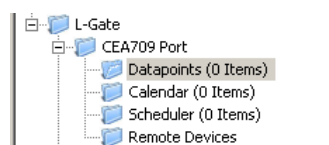
Figure 92: Change the NV allocation type.

Create Static NVs

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

To Create Static NVs Manually

1. Select the L-Gate/CEA-709 Port/Datapoint folder



2. Right-click in the data point list and select **New Datapoint...** in the context menu. This opens the NV creation dialog as shown in Figure 93.

Figure 93: 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, while the data point name is used for exposing the NV as a BACnet object.
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.

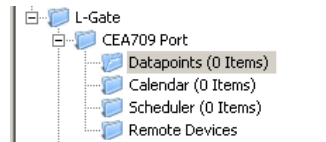
Note, that the static interface of the L-Gate will change as soon as static NVs are added or modified in the data point manager. This change is reflected in a new model number, which the L-Gate will have after the configuration download (see Section 0). Also note that the manually created static NVs are not bound automatically by the L-Gateway configuration software. They simply appear on the device and need to be bound in the network management tool.

Create External NVs

External NVs are not actually allocated NVs on the L-Gate. Instead, the L-Gate 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 L-Gate, they can be used to extend an L-Gate's interface configuration at run-time, when no LNS with dynamic NVs is available.

To Create an external NV manually

1. Select the L-Gate/CEA-709 Port/Datapoints folder



2. Right-click in the data point list and select **New Datapoint...** in the context menu. This opens the NV creation dialog.
3. Click on the tab **External** as shown in Figure 94.

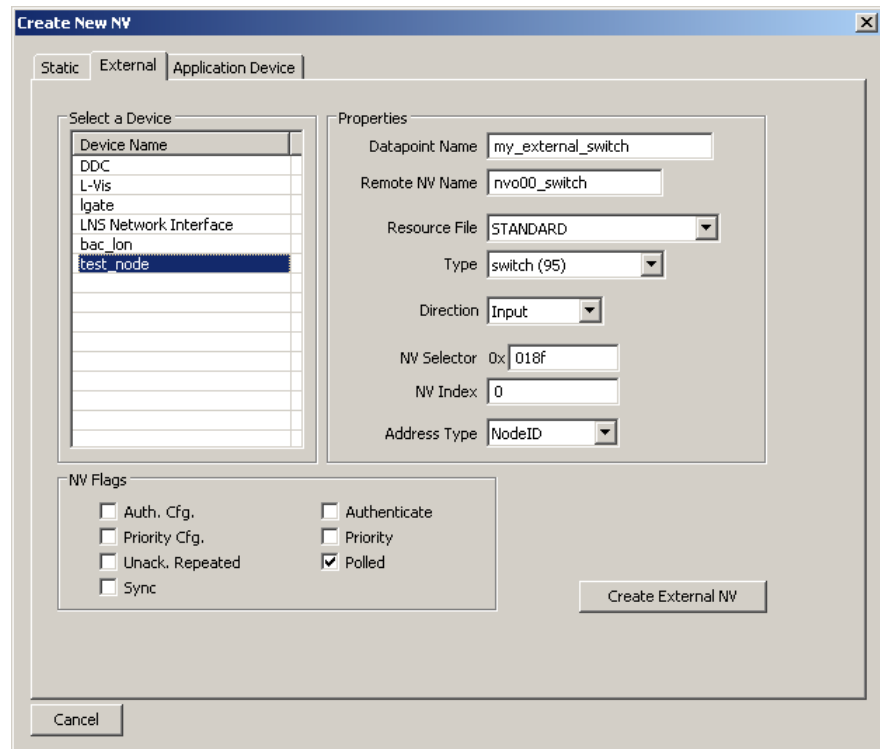


Figure 94: Create a new external NV.

4. Select the device in the box **Select a Device** on the left-hand side.
5. Enter the properties of the external NV on that device, starting with the local data point name, the remote programmatic NV name, the NV type (SNVT) and direction. Note, that the direction is the direction of the external NV on the L-Gate. Therefore, the remote output NV nvo00_switch becomes an input on the L-Gate. 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 95. For external NVs, which are inputs to the L-Gate, adapt the poll cycle property to your needs.

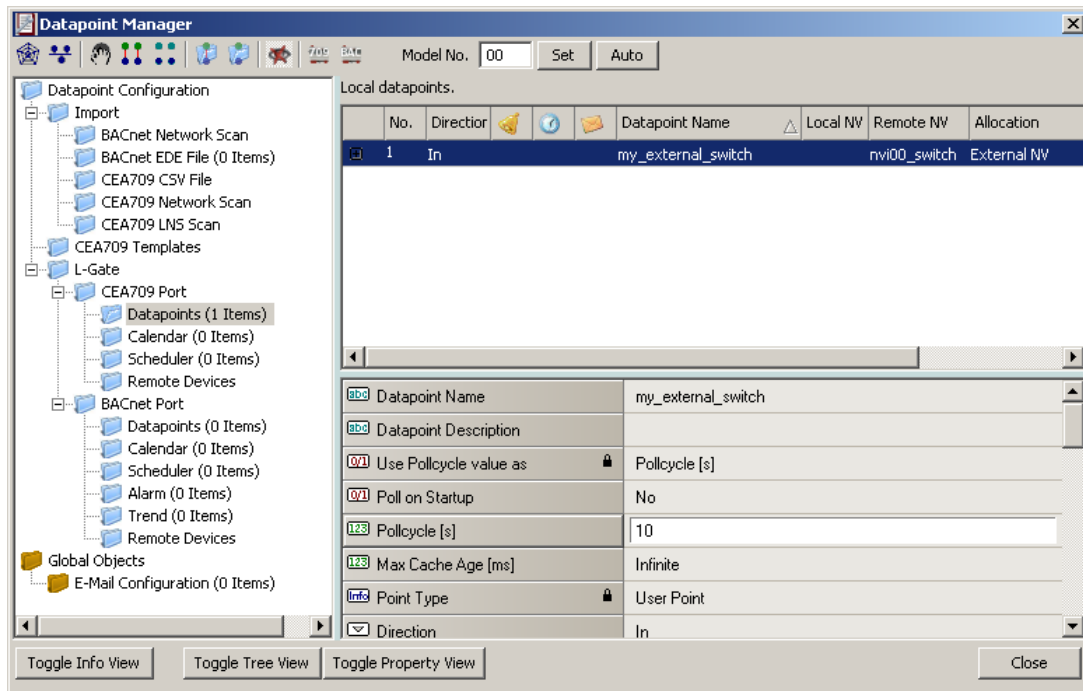




Figure 95: Manually created external NV in the port interface definition.

Generate BACnet Objects

To actually create BACnet mappings from the used NVs on the L-Gate, use the “Datapoint Manager” dialog. This section describes how to automatically generate BACnet objects from NVs. The auto-generation method also adds the NV and the BACnet object to a new connection.

To generate BACnet objects and connections from NVs on the L-Gate

1. Open the data point manager dialog.
2. In the L-Gate/CEA-709 folder select all the NVs, which shall be mapped. The multi-select feature or <Ctrl-A> may be used for doing this.
3. Click on the speed button  **Generate Points and auto-connect** in the tool bar.
4. Alternatively, you can select the L-Gate/CEA-709 Port folder and click the speed button  **Folder-wide Generate points and auto-connect** in the tool bar. This generate BACnet objects and connections for all NVs in the folder.
5. When the generation is complete, a dialog reports how many connections have been created. Click **Ok**.



6. The generated BACnet objects appear in the L-Gate/BACnet Port/Datapoints folder as shown in Figure 96.

- Click **Close** in the data point manager dialog to view the created connections in the main connections window.

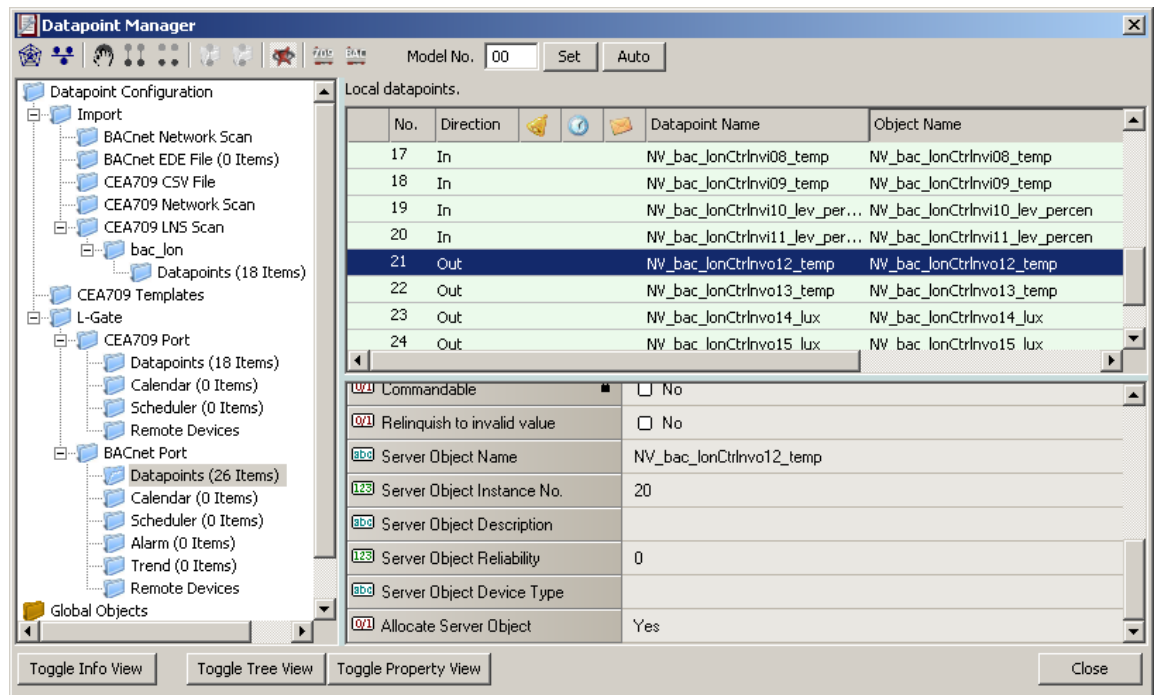


Figure 96: Auto-created BACnet Points in the BACnet Folder

Note, when auto-creating the BACnet objects, the L-Gateway configuration software initializes the BACnet properties with default values derived from the properties of the CEA-709 NVs. In particular, the object name, description, minimum and maximum present value, and engineering units are generated. If the default properties do not have the desired values, the user can edit them in the BACnet folder.

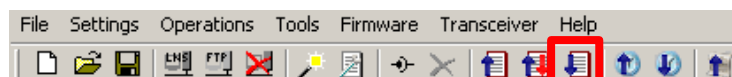
Configuration Download

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

If connected via LNS, and the NVs on the L-Gate are “Static NV” or “Dynamic NV”, the L-Gateway configuration software 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

- 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 97.

- If no bindings shall be generated, deselect the **Automatically create bindings** checkbox indicated by the red circle in Figure 97.

3. If the static NV interface has been changed, a new model number for the L-Gate needs to be selected. This is necessary, as the static network interface of the L-Gate changes on the CEA-709 network. The L-Gateway configuration software automatically selects a usable value, which can be overridden in the field **Model Number** marked by the blue rectangle in Figure 97.
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.

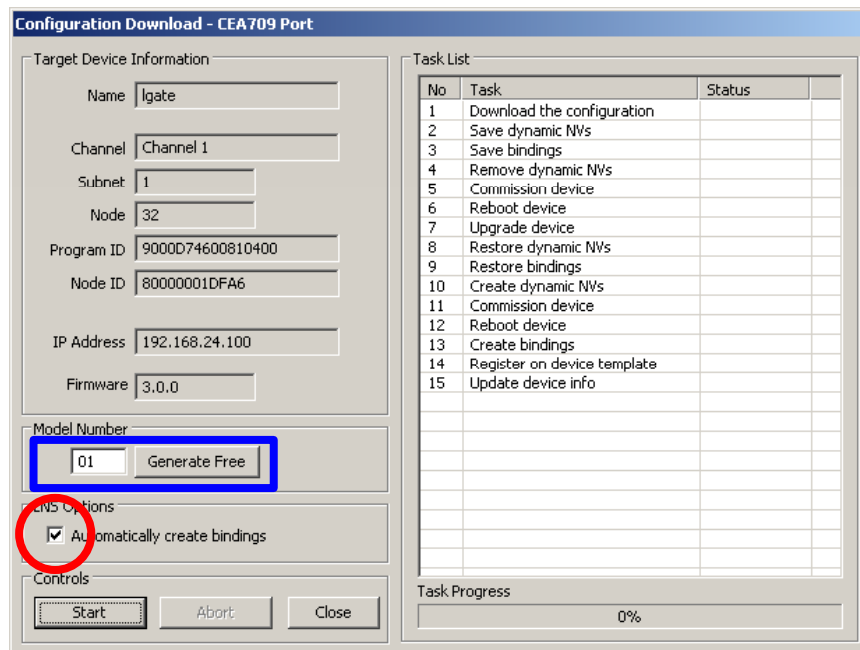


Figure 97: Configuration Download Dialog

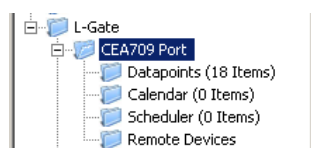
Note, that after the download is complete, the interface changes become active on the L-Gate (i.e., the static NV interface has changed). Refresh the network management tool to synchronize the tool with the changes to the LNS database made by the L-Gateway configuration software (e.g., use the menu “LonMaker|Refresh”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

Build XIF for Port Interface

When using static NVs on the L-Gate, the L-Gateway configuration software can export a new XIF file for the changed static interface.

To Create a XIF File

1. Select the L-Gate/CEA-709 Port folder



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 L-Gate, e.g. as "lgate1.xif".

Enable Legacy NM Mode

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

To Enable Legacy NM Mode

1. In the L-Gateway configuration software menu go to "Settings|Project settings ...". This opens the project settings dialog as shown in Figure 98.
2. Click on the tab CEA709/852.
3. Put a check mark in the Enable Legacy Network Management Mode group box on Port 1 as indicated by the red rectangle.
4. Click **Ok**.
5. Download the configuration to activate the change.

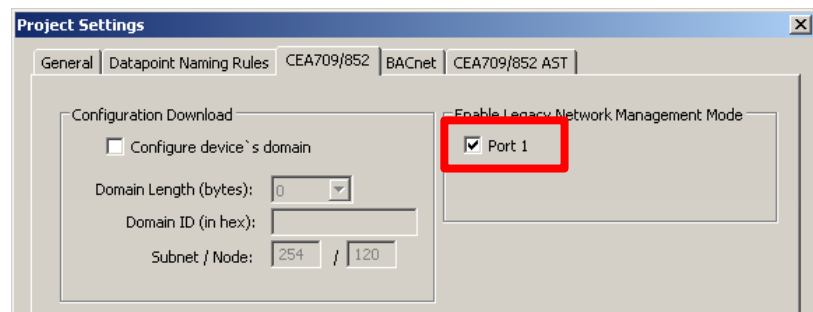


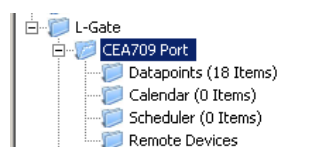
Figure 98: CEA709/852 Project Settings.

Upload Dynamic NVs from Device

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

To Upload Dynamic NVs

1. Select the CEA-709 Port folder.



2. Right-click and select **Sync Dynamic NVs** in the context menu. The L-Gateway configuration software 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 99 appears.

Note: This option upload dynamic NVs from all CEA-709 ports, if the device has an IP connection. If no IP connection is available, only dynamic NVs from the port are loaded, which is connected via LNS.

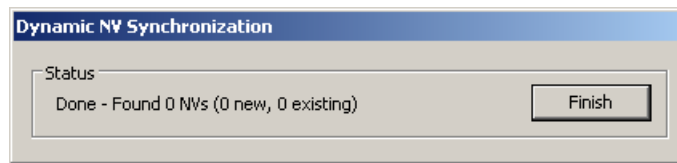


Figure 99: Synchronizing dynamic NVs from the device.

3. Click on Finish. The new dynamic NVs now appear in the data point list and can be edited and used for creating BACnet objects and connections.

Working with Configuration Properties

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

The L-Gate 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 100.

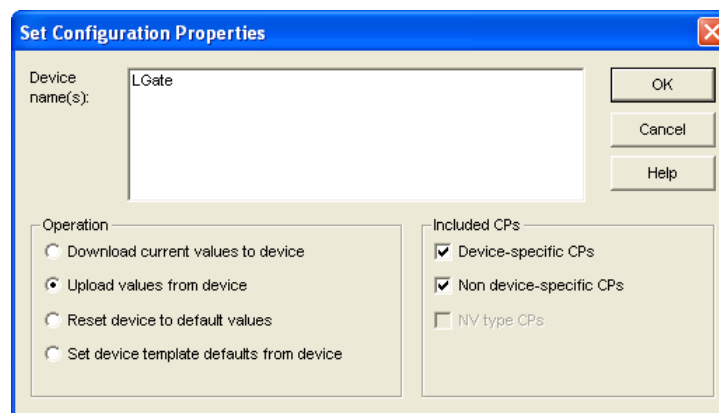


Figure 100: Set Configuration Properties in LonMaker TE.

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 101).

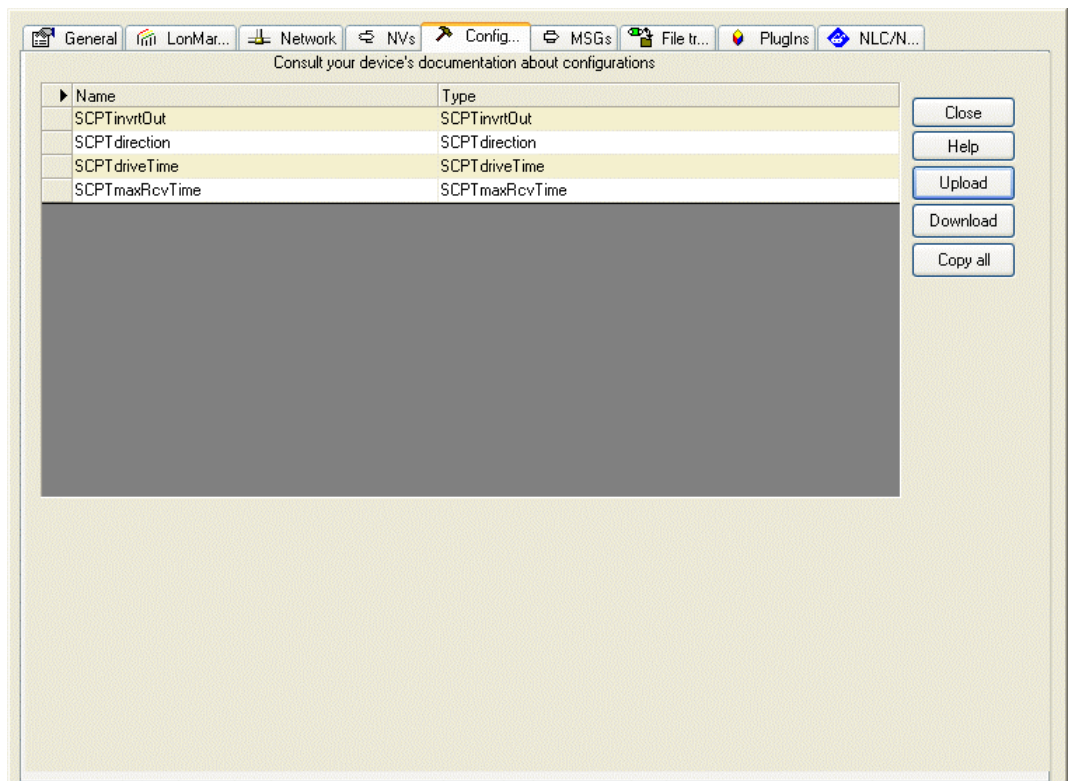


Figure 101: Configuration Tab for Configuration Properties in NL220.

Connections

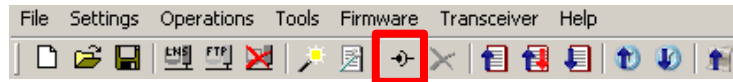
Create a New Connection

After having configured the device's network ports with data points, internal connections between those data points of different inputs and outputs can be created. Usually, the manual method to create a connection is used to create n-way connections or connections for data points, where the generate-and-auto-connect method cannot be applied.

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

To manually create a new connection

1. Click on the **Create a new connection** button



in the tool bar of the main connections window. This will bring up the connection dialog as shown in Figure 102.

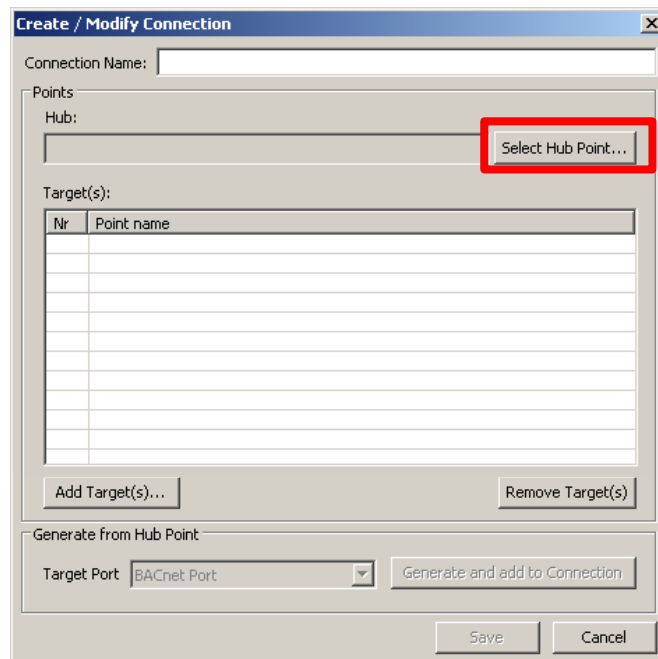


Figure 102: Connection Dialog: Select Hub.

2. Click on **Select Hub Point ...** to select the hub point. This opens the Datapoint Manager dialog. Select the data point in that dialog and click on **Add selected points**.
3. Then click on **Add Target(s)...** in the connection dialog as shown in Figure 103.

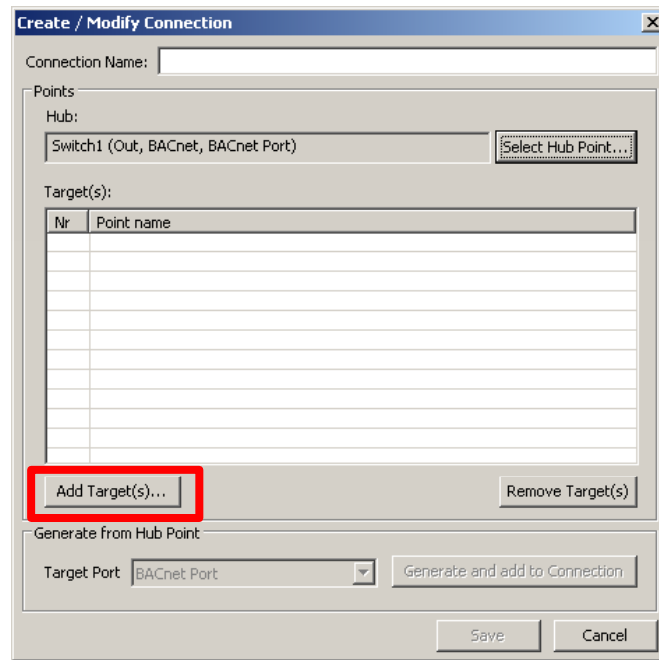



Figure 103: Connection Dialog: Select Target.

- This opens a Datapoint selector dialog again. Select the target points in that dialog. You may use multi-select to select more than one data point at a time. Then click on Add selected Points.

Note:

By default only compatible data points are displayed. Data points already in a connection are displayed in red. Sometimes compatible data points are available as member points (e.g., a SNVT structure member). Click on  to expand the data point and select the desired member point.

- Now the connection dialog contains a hub and one target data point as shown in Figure 104. Optionally, you may enter a connection name with a user-friendly text. By default, the name of the hub point is used. Then click on **Save** to save the created connection.

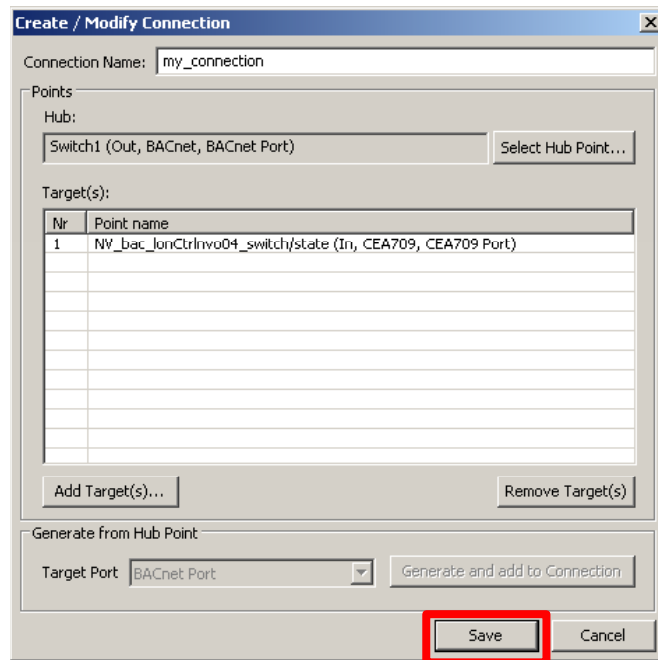


Figure 104: Connection dialog with hub and target points.

- The main window of the L-Gateway configuration software shows the list of connections as shown in Figure 105.

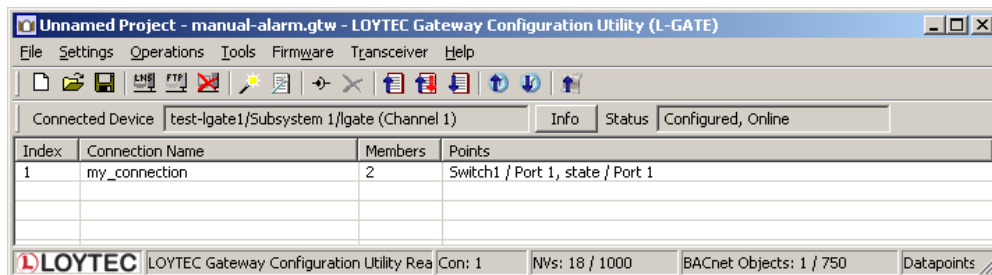
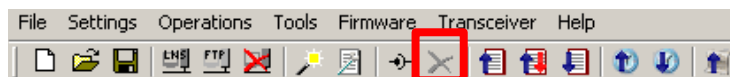


Figure 105: We have created a new connection.

Delete a Connection

To delete a connection select the connection in the main window and select the Delete connection button



in the tool bar. Optionally, you may select the connection and hit the *Del* key on the keyboard. To delete multiple connections you can use the multi-select feature.

Edit a Connection

To edit a connection double-click on the connection in the main window. This opens the **Create/Modify Connection** dialog as shown in Figure 106. When editing the connection, the user can select a different hub data point, add or delete target data points. To delete a target, select the target and click on **Remove Target(s)**.

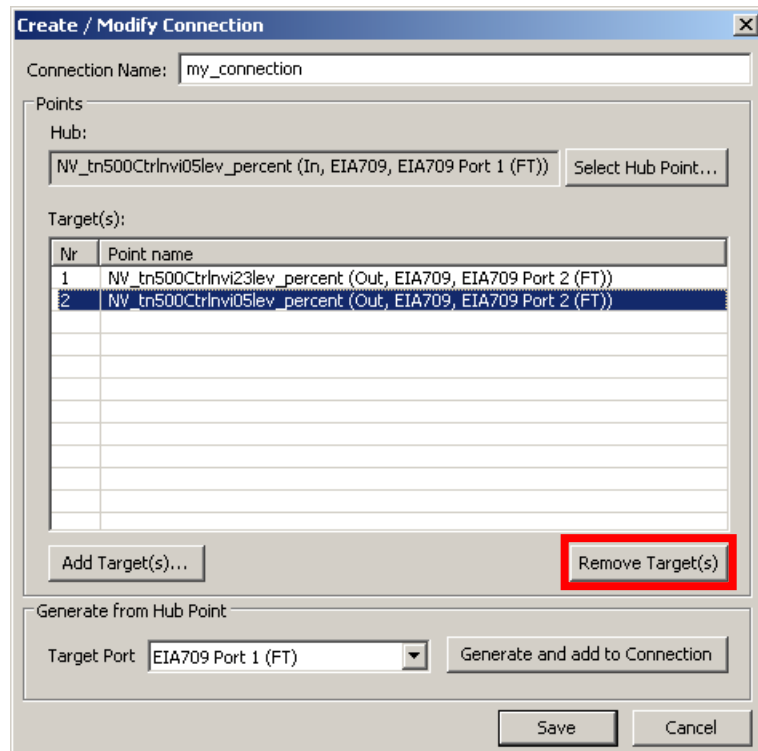


Figure 106: Delete a target from a connection.

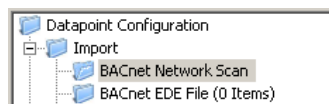
BACnet Configuration

Scan for BACnet Objects

LOYTEC gateway devices also support an online network scan on the BACnet network. In this scan the device searches for other devices on the BACnet network and pulls in the BACnet object information of these devices. These BACnet objects can then be used on the device as the basis for client mapping.

To Scan for BACnet Objects

1. Open the data point manager dialog.
2. Select the folder BACnet Network Scan



3. Right-click on that folder and select **Scan BACnet Network...**. This opens the BACnet Network Scan dialog as shown in Figure 107.

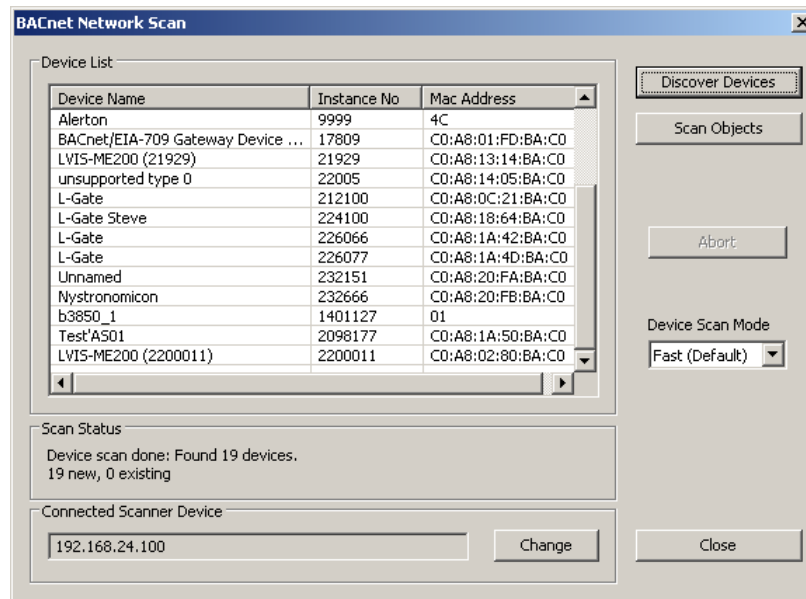


Figure 107: BACnet network scan dialog.

4. Click on the button Discover Devices. This starts a network scan. The results are put in the device list box.
5. Select a device in the device list and click the button Scan Objects. This scans the BACnet objects on the selected device and adds them to the BACnet Network Scan folder as a separate sub-folder for the device as shown in Figure 108.

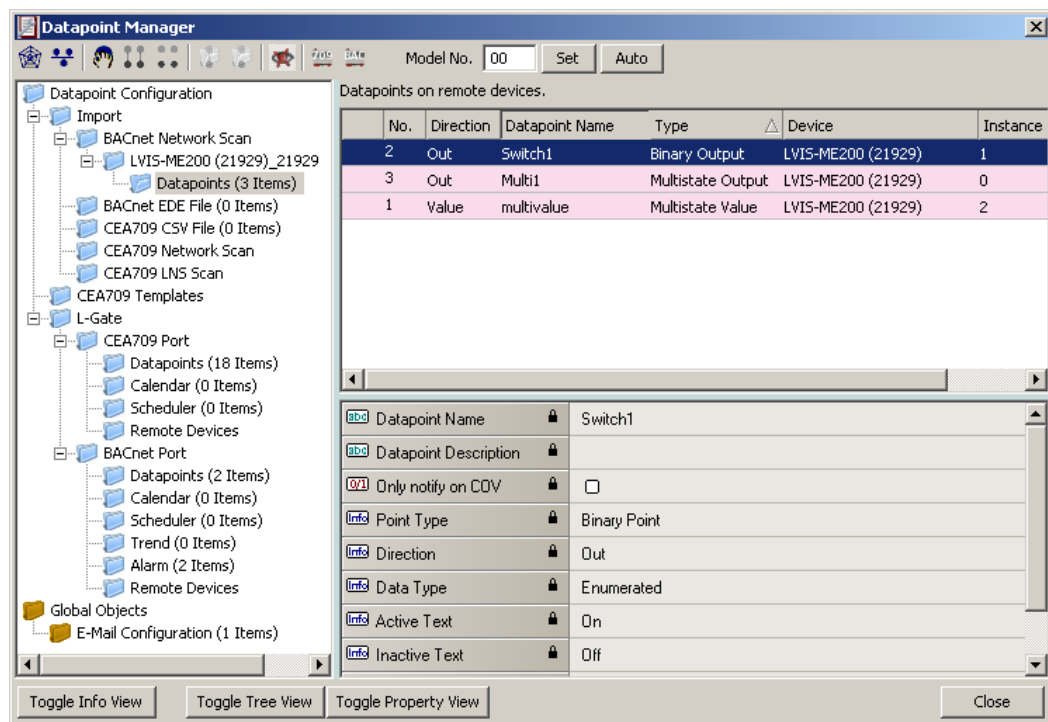


Figure 108: BACnet network scan results.

6. Click Close when all devices needed have been scanned.

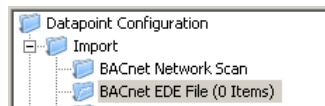
Import from EDE File

If the device is engineered offline or some of the required BACnet devices are not yet online in the network, the engineering process can be done by importing a device and object list from a set of EDE files. These objects also appear in the import folder and can be later used on the device.

There are a set of EDE files. Select the main EDE file, e.g. *device.csv*. The EDE import will also search for the other components, which must be named *device-states.csv*. Which components are expected, please refer to Section 0. Example EDE files can be found in the 'examples' directory of the LOYTEC Gateway Configuration software installation directory.

To Import BACnet Objects from an EDE File

1. Open the data point manager dialog.
2. Select the folder **BACnet EDE File**




3. Right-click and select **Import File**. In the following file selector dialog, choose the EDE import file and click **Ok**.
4. Now the BACnet EDE File folder is populated with the imported BACnet objects.

Use Imported BACnet Objects

After BACnet objects have been imported (with a network scan or by importing from an EDE file) the user can select the BACnet objects that the L-Gate shall access. When executing the "Use on device" the configuration software allocates client mappings on the device. These client mappings will read or write values from the BACnet objects in the network.

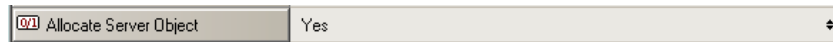
In an additional step, there can be also server objects allocated on the device. These server objects can be created automatically from converting a client mapping to a server object. This is usually done, if the imported BACnet objects shall also be directly modified over the BACnet network on the device itself.

To Use Imported BACnet Objects on the Device

1. Open the data point manager dialog and select the desired BACnet objects in one of the import folders.
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 BACnet Port/Datapoints folder. All data points in that folder will be created as client mappings. No server object is created automatically in this case.

Client Map Count	1
Client Map [0]	(17800), AI 0, Present_Value, Auto, Expiry 90 sec / Poll 10 sec
Allocate Server Object	No
Allocate Client Mapping	Yes

- To also create server objects select the data points in question using the multi-select feature. Then edit the property **Allocate Server Object** and set it to **Yes**.

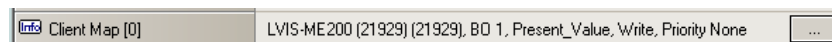


Edit a Client Mapping

The client mapping information in BACnet data points can be edited after they have been created. Usually, this is done to correct the remote BACnet object instance number.

To Edit a Client Mapping

- Select the BACnet data point that has the client mapping to be edited.
- On the **Client Map** property click the **...** button



- This opens the **Modify Client Mapping** dialog as shown in Figure 109.

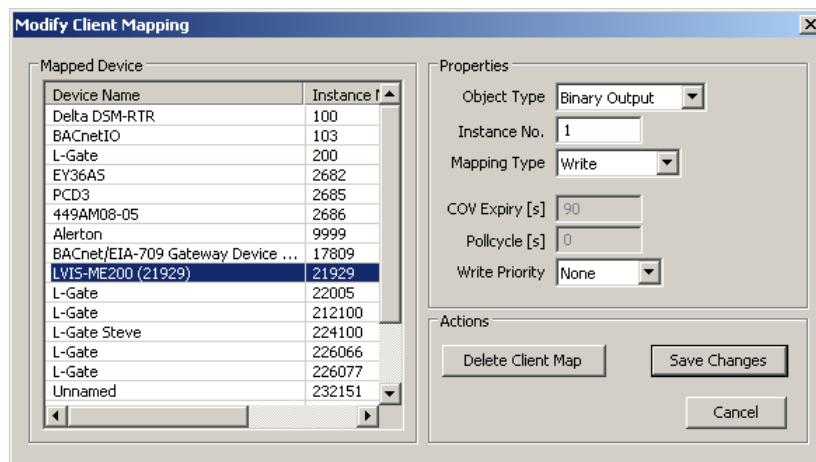


Figure 109: Modify Client Mapping Dialog.

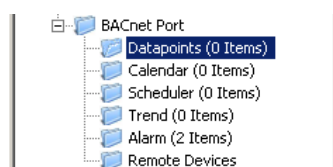
- Edit the target device by selecting a different device in the **Mapped Device** list. Edit the target object instance number. For read client mappings edit the **COV expiry** or **Polcycle** setting. For write client maps edit the **Write Priority**. When finished click **Save Changes**.

Create Server Object

On the BACnet port server objects can also be created manually. These BACnet objects are visible on the BACnet network and can be modified by other devices. They appear as data points in the BACnet/Datapoints folder.

To Create Server Objects Manually

- Select the BACnet Port/Datapoints folder



2. Right-click in the data point list and select **New Datapoint...** in the context menu. This opens the **Create New BACnet Point** dialog as shown in Figure 110.

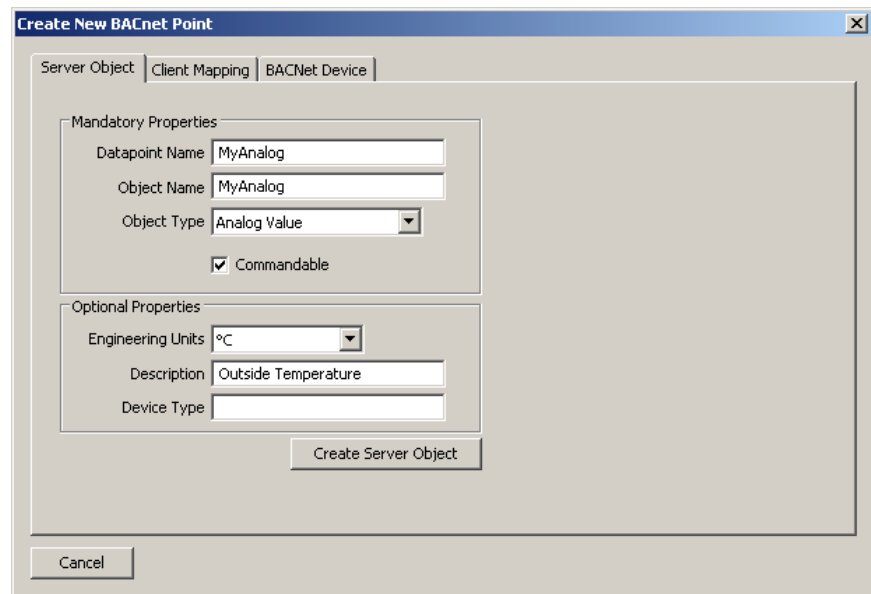


Figure 110: Create a Server Object manually.

3. In the **Mandatory Properties** enter a **Datapoint Name** and an **Object Type**. Optionally, select the **Commandable** check box for value objects, if the value object shall be commandable from the network.
4. In the **Optional Properties** you may select **Engineering Units** for analog objects. For all object types you can enter the **Description**. The **Device Type** can be left empty.
5. Click **Create Server Object**. The BACnet data point is created and appears in the data point list.

Enable International Character Support

By default BACnet objects on the device contain ASCII strings in properties such as object name, description, active/inactive text, state texts. This is the setting most third-party tools are interoperable with. To support international character sets, the device can be configured to expose strings as ISO-8859-1 (for most Western European languages) or UCS-2 (for Unicode character sets such as Japanese).

To Enable International Character Support

1. In the L-Gateway configuration software menu go to “Settings|Project settings ...”. This opens the project settings dialog.
2. Click on the tab **BACnet**.
3. Put a check mark either on ASCII (default), UCS-2 (Unicode, e.g., for Japanese), or ISO-8859-1 (for Western European languages), as indicated by the red rectangle in Figure 111.
4. Click **Ok**.
5. Download the configuration to activate the change.

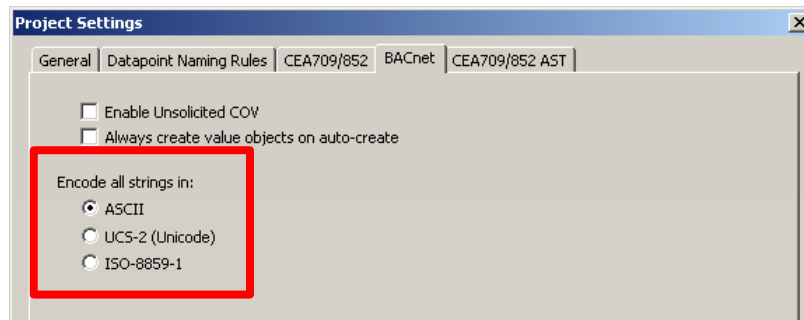


Figure 111: BACnet Project settings dialog.

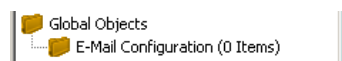
E-Mail Templates

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 0).

To Create an E-Mail Template

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



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 112 enter the **To** address and **Subject**. Optionally, **Cc** and **Bcc** addresses can be specified.

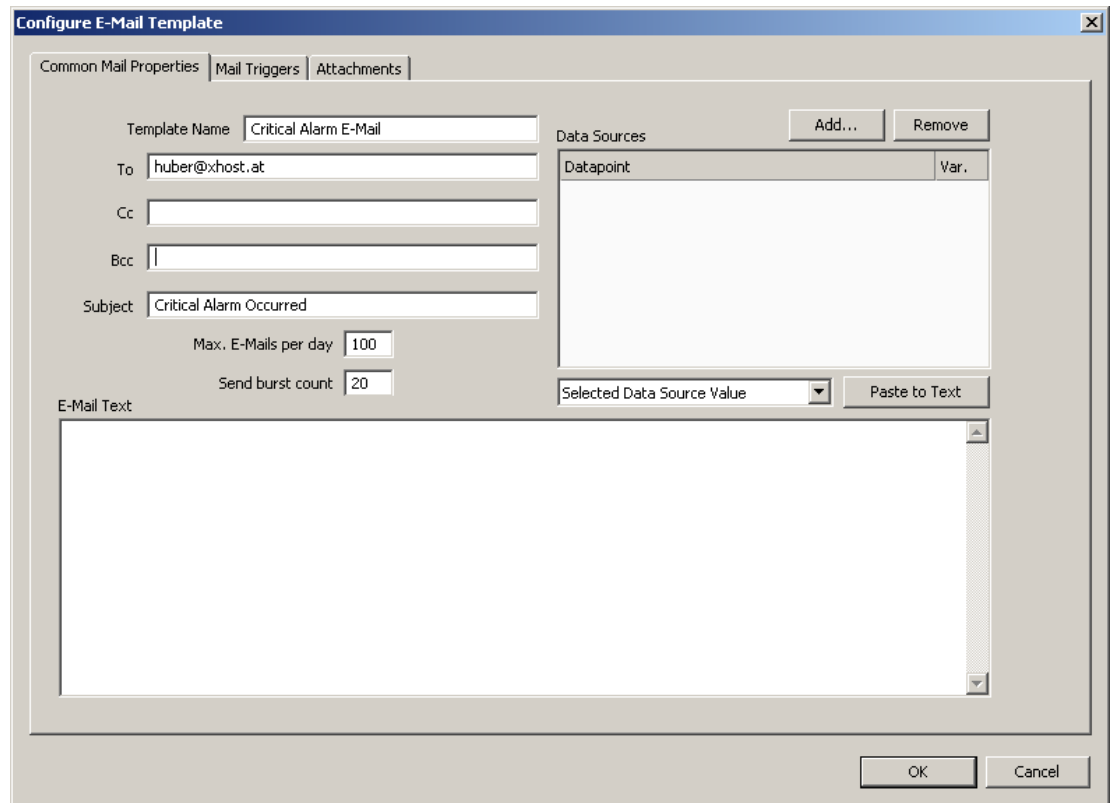
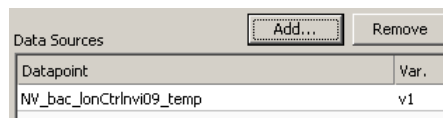


Figure 112: Configure E-Mail Template Dialog.

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.



7. 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.
8. 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.



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

Trigger E-Mails

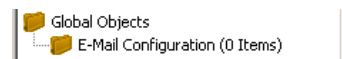
E-Mail templates are used to assemble and transmit E-Mails when certain trigger conditions occur. For an E-Mail template, one or more trigger conditions can be defined. The E-Mail will be sent, when one of the trigger conditions is activated. Depending of the trigger data point type, the trigger conditions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



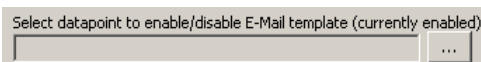
2. Right-click and select **Configure E-Mail Template ...** from the context menu.
3. Change to the **Mail Triggers** tab.

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.

Mail Triggers		
Datapoint	Type	Condition
Critical	Alarm	-

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.



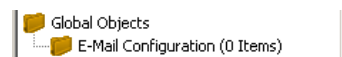
9. To remove such a trigger enable, click the **Remove Enable Trigger** button.

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.



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**.

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.

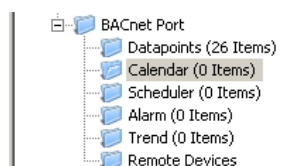
Local Schedule and Calendar

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. On each port, one calendar can be created.

To Create a Calendar

1. Under the port folder, select the Calendar sub-folder, e.g., BACnet port to create a BACnet calendar.



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

3. In the Create New Calendar dialog box (as shown in Figure 113) enter Name and Description of the calendar.

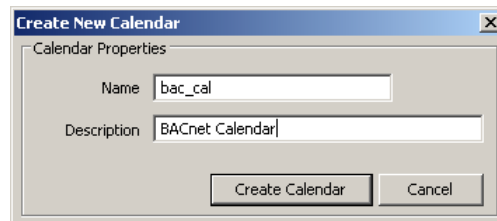


Figure 113: Create New Calendar dialog box.

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

Create Calendar Pattern

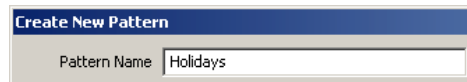
When a local calendar is used, it needs to be configured with calendar patterns. A calendar pattern represents a class of days such as “Holidays”. The calendar patterns can then be used in a schedule to define daily schedules for exception days. The available calendar patterns should be created when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

2. Right-click and select **Create Calendar Pattern...**
3. Enter a Pattern Name in the **Create Calendar Pattern** dialog



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

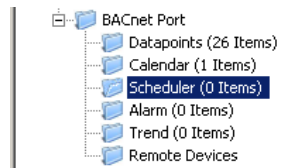
No.	Direction	Calendar Name	Object Name	Obj Type	Instance
1	In	bac_cal			
1.1		Holidays	Holidays	Calendar Object	26

Create a Local Scheduler

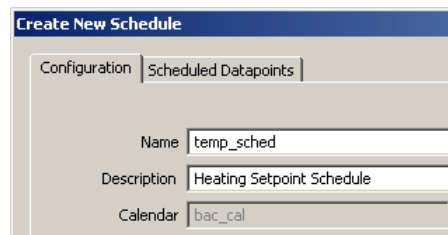
For scheduling data points, a scheduler object must be created. On each port, multiple local scheduler objects can be created. These local schedulers can then be configured to schedule data points.

To Create a Local Scheduler

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



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



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

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 0).

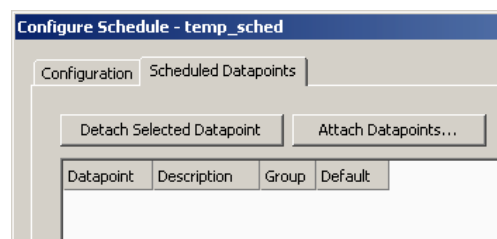
This configuration must be done as an initial setup. Which data points are scheduled cannot be changed at run-time. The daily schedules, however, can be changed later in the Web UI or over the network.

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.

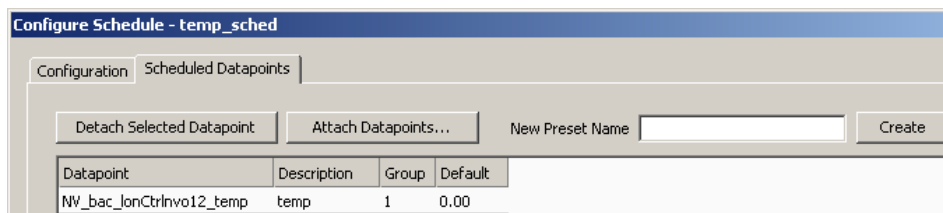


4. Click the button **Attach Datapoints** . This opens another data point selector window.
5. Select the data points to attach and click **Ok**. For each of the attached data points, one or more lines appear in the list below the attach button. If the attached point is a structure, there will be one 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.



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	Group	Default	day	night
NW_bac_IonCtrlInvo12_temp	temp	1	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	Group	Default	day	night
NW_bac_IonCtrlInvo12_temp	temp	1	0.00	21.00	16.00
NW_bac_IonCtrlInvo13_temp	temp	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.

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 0).
2. Select the day for which to configure a daily schedule.

Weekday / Exception	Priority	Events	Use
Mon	-	0	<input checked="" type="checkbox"/>
Tue	-	0	<input checked="" type="checkbox"/>
Wed	-	0	<input checked="" type="checkbox"/>
Thu	-	0	<input checked="" type="checkbox"/>
Fri	-	0	<input checked="" type="checkbox"/>
Sat	-	0	<input checked="" type="checkbox"/>
Sun	-	0	<input checked="" type="checkbox"/>
Holidays	1 (highest)	0	<input type="checkbox"/>

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.

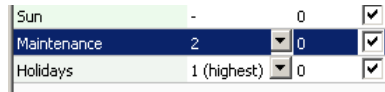
Time	Value
00:00	00:00:00 - Default
01:00	
02:00	
03:00	
04:00	
05:00	
06:00	
07:00	
08:00	06:00:00 - day
09:00	
10:00	
11:00	

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**.

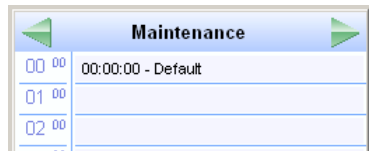
Source	Monday
Select Targets	<ul style="list-style-type: none"> Daily Schedule Tuesday Wednesday Thursday Friday Saturday Sunday Holidays
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

To Use Exception Days

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



2. Edit the daily schedule.



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 0).

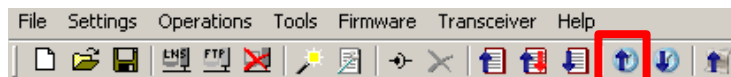
Important! *Choose different priorities for different exceptions. If two exceptions are valid for a given day and their priorities are equal, it is not determined, which exception is in effect.*

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 L-Gateway 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	Object Name	Obj Type	Instance
1	In	bac_cal			
1.1		Holidays	Holidays	Calendar Object	26

3. Right-click and select Configure Pattern ... in the context menu.
4. The Configure Pattern dialog appears as shown in Figure 114. 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.

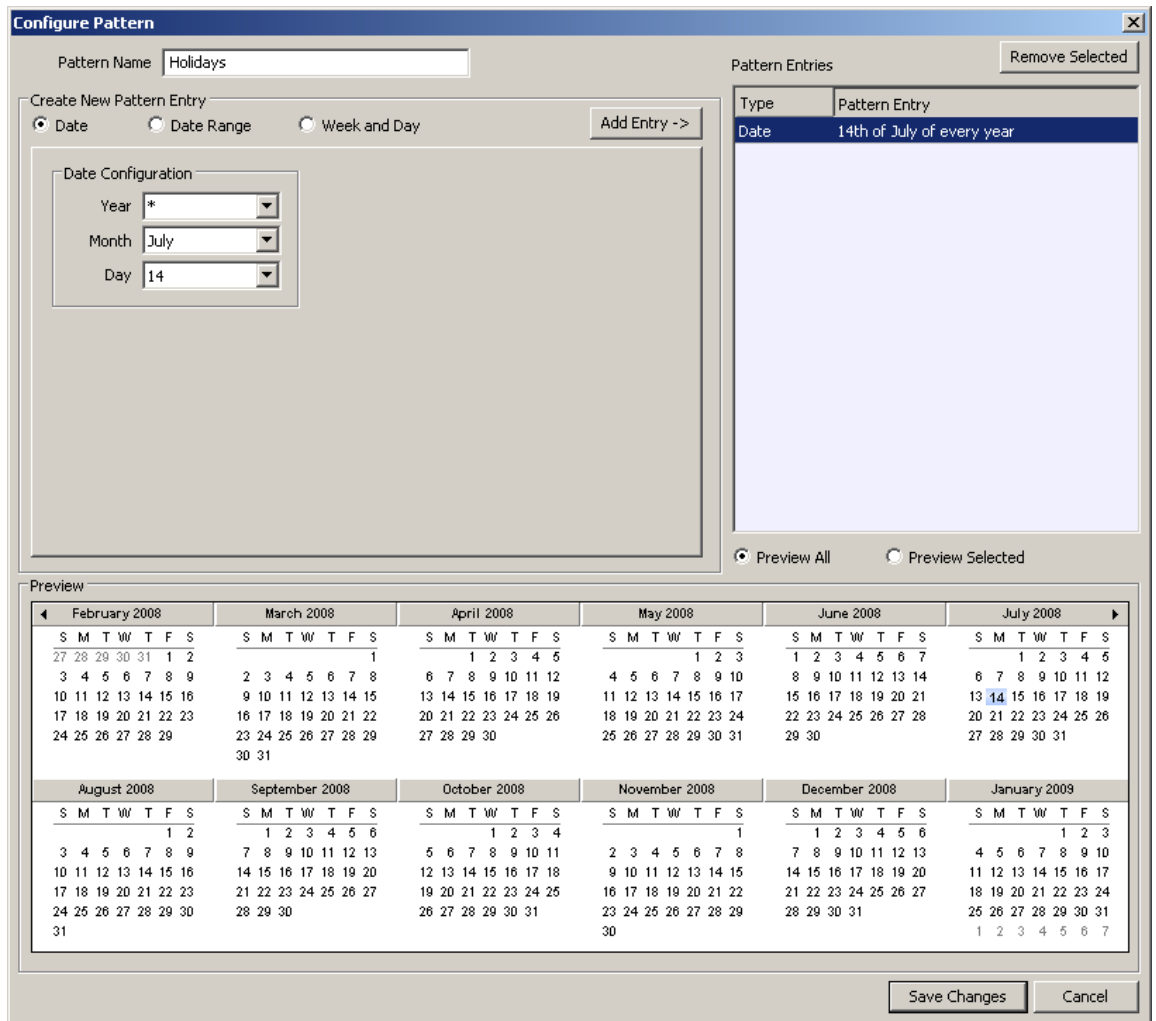


Figure 114: Configure Calendar Pattern Dialog.

- 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**.*

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 0). The local schedule can be altered over the Web UI or using the network technology of the port, where the scheduler has been created.

Limitations

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 115.

Datapoint	Description	Group	Default	day	night
NV_bac_lonCtrlInvo08_temp	temp	-	0.00	20.00	16.00
NV_bac_lonCtrlInvo07_switch.value	dimlevel	-	0.00	0.00	50.00
NV_bac_lonCtrlInvo07_switch.state	state	-	0.00	0.00	1.00

Figure 115: 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. When 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 0). 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.

Local BACnet Schedulers

BACnet schedulers and the BACnet calendar adhere to the standard schedule and calendar object in BACnet. For each scheduler a BACnet Schedule object is created. The calendar deserves a closer look. For each calendar pattern a BACnet Calendar object is created. The visible calendar on the Web UI is therefore a collection of BACnet calendar objects. Each calendar pattern therefore is associated with a BACnet object instance number. The calendar pattern "Holdidays" is for example visible as CAL,1 on the BACnet port.

The BACnet schedule object allows only objects of one selected data type to be scheduled. Therefore, schedulers on BACnet can only schedule one class of data points (e.g., only one group of analog data points). As a consequence, the value preset in BACnet always has only one element. The name of the value preset is not stored in BACnet. Therefore, a default name is created, such as "Value(22)" for an analog value. An example of two scheduled BACnet objects is shown in Figure 116

Datapoint	Description	Group	Default	Value(21)	Value(16)
NV_bac_lonCtrlInvo12_temp	temp	1	0.00	21.00	16.00
NV_bac_lonCtrlInvo13_temp	temp	1	0.00	21.00	16.00

Figure 116: Example value presets in BACnet schedulers.

Priorities of exception days in a BACnet scheduler range from 1 (the highest) to 16 (the lowest). Weekdays in BACnet have no priority.

Changing the number of calendar patterns in a BACnet calendar can only be done through the configuration software and not during run-time. The individual calendar pattern entries in the calendar patterns can be changed at run-time. Therefore, it is advisable to reserve a suitable number of calendar patterns in a BACnet calendar and leave them empty if not needed immediately.

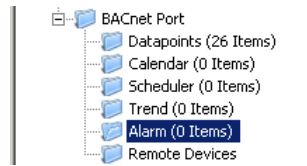
Local Alarming

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, e.g., under the BACnet port to create a BACnet alarm server.



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 117) enter Name and Description of the alarm server.

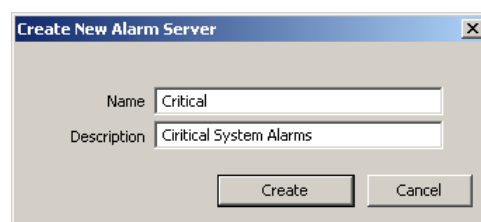


Figure 117: Create New Alarm Server dialog box.

4. Click **Ok**. The alarm server appears now in the data point list view.
5. For a BACnet alarm server, select the created object and edit the properties for transition priorities (To-Normal, To-Fault, To-Offnormal) and the corresponding check boxes, which define whether acknowledgements are required. These are the standard BACnet settings in a Notification Class object.

128	To-Normal Priority	127
128	To-Fault Priority	127
128	To-Offnormal Priority	127
071	Ack To-Normal	<input type="checkbox"/>
071	Ack To-Fault	<input checked="" type="checkbox"/>
071	Ack To-Offnormal	<input checked="" type="checkbox"/>

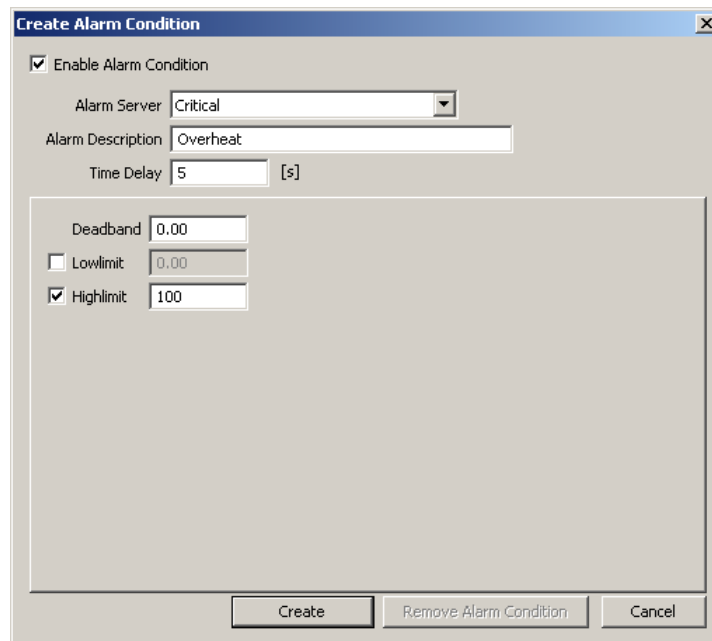
Create an Alarm Condition

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. Currently, only BACnet data points can be configured with intrinsic alarm conditions.

To Create an Intrinsic Alarm Condition

1. Select an analog BACnet 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 117 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.



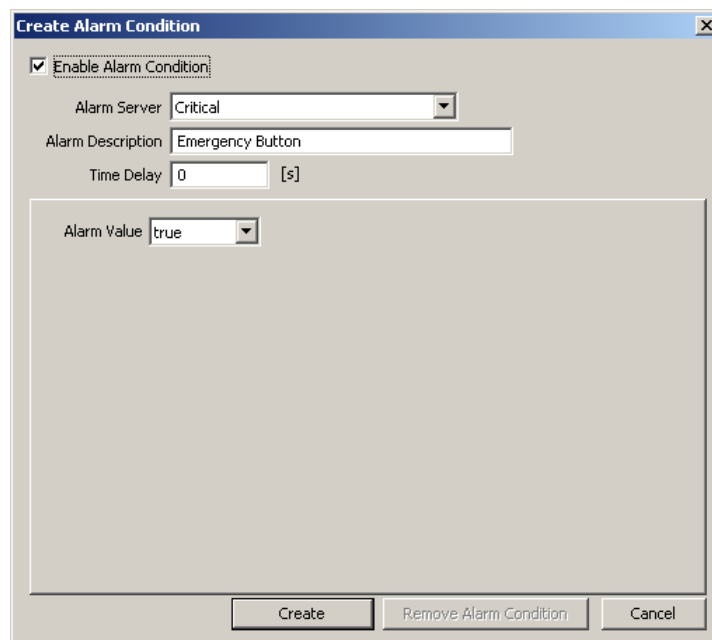
The screenshot shows the 'Create Alarm Condition' dialog box. It has a title bar with a close button. The main area contains the following fields and controls:

- Enable Alarm Condition
- Alarm Server: Critical (dropdown menu)
- Alarm Description: Overheat (text input)
- Time Delay: 5 [s] (text input)
- Deadband: 0.00 (text input)
- Lowlimit: 0.00 (text input)
- Highlimit: 100 (text input)

At the bottom, there are three buttons: 'Create', 'Remove Alarm Condition', and 'Cancel'.

Figure 118: Alarm Condition for an Analog Data Point.

4. For a binary data point the dialog as shown in Figure 119 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.



The screenshot shows the 'Create Alarm Condition' dialog box. It has a title bar with a close button. The main area contains the following fields and controls:


- Enable Alarm Condition
- Alarm Server: Critical (dropdown menu)
- Alarm Description: Emergency Button (text input)
- Time Delay: 0 [s] (text input)
- Alarm Value: true (dropdown menu)

At the bottom, there are three buttons: 'Create', 'Remove Alarm Condition', and 'Cancel'.

Figure 119: Alarm Condition for a Binary Data Point.

5. For a multi-state data point the dialog as shown in Figure 120 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 trigger the alarm, and click the arrow button.

Figure 120: Alarm Condition for a Multi-State Data Point.

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

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 0). Then an E-Mail template can be created and the alarm point attached as a trigger.

To Create an E-Mail Template for Alarms

- Create or configure an E-Mail template as described in Section 0.
- Change to the Mail Triggers tab.
- Click the Add... button and select an alarm data point.
- In the Mail Triggers list select the added trigger data point.

Mail Triggers		
Datapoint	Type	Condition
Critical	Alarm	-

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

- 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 0.

Generate Alarms from NVs

Since alarm conditions can only be defined for BACnet data points, NVs cannot be monitored directly. To generate alarms from NVs, first create a BACnet object for that NV and create a connection. Then define the alarm condition on the mapped BACnet object.

Local Trending

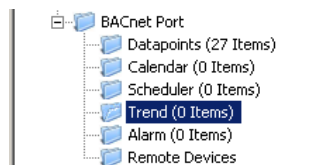
Create a Local Trend

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 0).

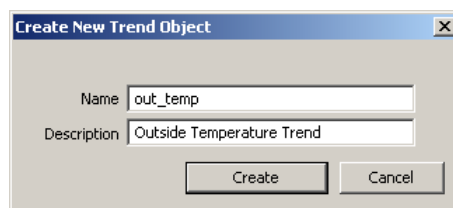
Trending on the L-Gate is based on the BACnet TrendLog object. This object has to be created first. Then the BACnet operator workstation (OWS) can configure the TrendLog object over BACnet, which BACnet object shall be trended. The OWS can then also access the trend data via BACnet.

To Create a Trend Object

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



2. Right-click and select New Trend ... from the context menu.
3. In the Create New Trend Object dialog enter a name and optionally a description for the trend log object.



4. Click Ok. The new trend log object appears in the data point list of the Trend folder.

Trend NVs

Trending on the L-Gate is based solely on the BACnet TrendLog object. Consequently, only BACnet objects can be trended. NVs cannot be trended directly. To trend data of an NV, first generate a BACnet object from the NV and auto-connect it. In the operator workstation (OWS) choose that BACnet object and configure the TrendLog object.

Download Trend Data in CSV Format

Trend logs can be downloaded from the device via FTP in CSV format (see Section 0). 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 121. 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	50	0	107C

Figure 121: 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 0) of the L-Gate. 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.

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 on a timely basis. For doing that, an E-Mail template has to be set up for the trend log to be transmitted. To trigger the transmission on a timely basis, a binary data point must be scheduled. That binary data point then is used as an E-Mail trigger to send the trend log E-Mail template. For setting up E-Mails, the account information has to be configured on the device, e.g. on the Web UI (see Section 0).

Of course, the scheduled binary point can be used as a trigger for more than one trend E-Mail. The binary data point can also be written from the network to explicitly trigger the transmission of E-Mails.

To Create an E-Mail Template for Trend Data

1. Create a binary data point as described in Section 0. As an example create a commandable BACnet BV object that will serve as a trigger for sending trend log E-Mails. Two data points are created: *trend_trigger_in* and *trend_trigger_out*.

The screenshot shows a web-based configuration window titled "Create New BACnet Point". It has three tabs: "Server Object", "Client Mapping", and "BACNet Device", with "BACNet Device" being the active tab. Below the tabs, there is a section for "Mandatory Properties" containing three input fields: "Datapoint Name" with the value "trend_trigger", "Object Name" which is empty, and "Object Type" which is a dropdown menu set to "Binary Value". At the bottom of this section, there is a checked checkbox labeled "Commandable".

2. Create a schedule for the binary data point *trend_trigger_out* (see Section 0).
3. Create or configure an E-Mail template as described in Section 0.

4. Change to the Mail Triggers tab.
5. Click the Add... button and select the binary data point, which is scheduled.
6. In the Mail Triggers list select the added trigger data point.

Mail Triggers		
Datapoint	Type	Condition
trend_trigger_out	Value Update	True (!= 0)

7. In the Manage Trigger Conditions list put a check mark on the True condition. This will trigger the E-Mail transmission every time the value of the binary data point changes to TRUE.

Manage Trigger Conditions	
Enabled Conditions	
<input checked="" type="checkbox"/>	True (!= 0)
<input type="checkbox"/>	False (== 0)
<input type="checkbox"/>	Invalid
<input type="checkbox"/>	Offline

8. Change to the Attachments tab.
9. In the Attach File drop-down box select the trend log file to be transmitted and click the Add button.

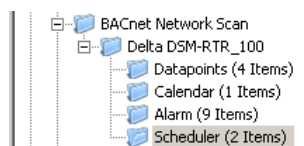
Remote AST Objects


Remote Scheduler and Calendar

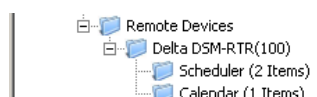
Adding remote access to the configuration of a scheduler and calendar, which is located on another device, is done by creating remote scheduler and calendar objects. These objects can be created from data obtained by a network scan or LNS scan.

To Create a Remote Scheduler

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



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.



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. For BACnet, also adjust the poll cycle, which will be used to periodically fetch the current configuration in case the remote device does not support COV subscriptions.
5. For CEA709, 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.

On BACnet devices, the new data points can be used right away to exchange configuration data with the scheduler on the remote device. Just connect the new scheduler data point to a schedule control to view and edit the configuration of the remote devices scheduler.

On CEA709 devices, there is one extra step to take before the new data points will be operational: 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.

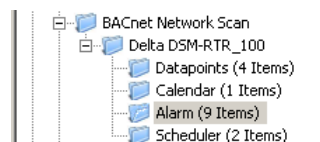
Note: If connected via LNS, the bindings to the `nvoCalLink` and `nvoSchedLink` NVs are made automatically by the configuration software in the download process.


Alarm Clients

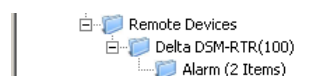
Accessing alarm server objects on remote devices is done by creating remote alarm data points. These points may be created from data obtained by a network scan. The local device is configured as an alarm client and subscribes to alarm updates from the remote alarm server. The alarm client can also be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



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.



3. For CEA709, 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.

On BACnet devices, the new data points can be used right away to exchange alarm information with the alarm server on the remote device. Just connect the new alarm client data point to an alarm list control to view and acknowledge alarms reported by the associated alarm server.

On CEA-709 devices, there is one extra step to take before the new data points will be operational: 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.

Mapping CEA-709 and BACnet Schedules

Mapping and Limitations

Mapping schedulers and calendars is realized by creating connections between schedulers, and connections between corresponding calendars. The information in a scheduler connection is synchronized between its participants. When starting up, however, it is important to define where the source of the information is located, i.e., the actual execution of the schedule takes place. If the schedules and calendars are out-of-sync when the system starts, the information from the source schedule/calendar is distributed in the system. The hub of a connection is always the source of the information. The targets receive the initial schedules/calendars.

In the configuration software, only local schedulers and calendars that are hub in a connection can be configured. The target schedules are synchronized automatically on the device. Changing schedules or calendars on the Web UI or over the network automatically synchronize the change with all members of the connection.

Since schedules and calendars in the two technologies have their own restrictions, the mapping underlies a number of restrictions as well:

- Only schedules that schedule a single value can be mapped. In practice, all schedules can be mapped where one only value can be defined per value preset, e.g., one analog value.
- The target schedule, which is used to expose the actual scheduler to a different technology, must not itself have data points attached, that are scheduled. The target scheduler only acts as a shell that stores the daily schedules.
- CEA-709 schedulers, which schedule only one NV, but that NV is a structure (e.g., *SNVT_switch*) cannot be mapped to a BACnet scheduler. This is because the value preset on the CEA-709 scheduler has two values to configure. This violates the one-value rule.
- All calendars referred to by mapped schedulers must be added to a calendar connection.
- On one port, only one calendar can exist. Therefore, all exposed calendars must be added to a single connection. As a consequence all calendars are synchronized in the

system. There can exist only one calendar connection on a device, that contains all exposed calendars.

- Once a scheduler is in a connection, do not change its scheduled data points. Doing so after creating may violate the connection rules and result in a non-functioning connection.

Figure 122 shows an example, how two remote CEA-709 schedulers are exposed to BACnet schedulers. There are three connections involved. One connection *sched_1_conn* is created for *lon_sched_1* and *bac_sched_1*. A second connection *sched_2_conn* is created for *lon_sched_2* and *bac_sched_2*. Since there is only one BACnet calendar, all calendar objects must be put into a single connection *cal_conn*, containing *lon_cal_1*, *lon_cal_2*, and *bac_cal*.

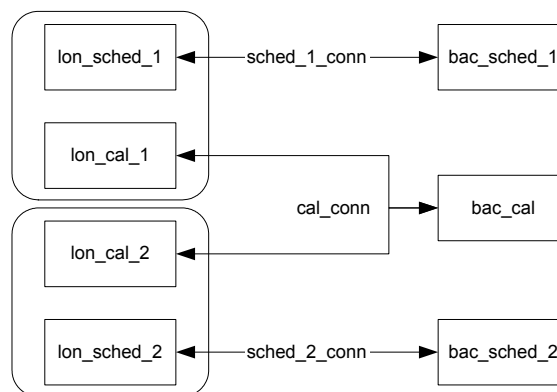


Figure 122: Example for schedule and calendar connections.

Map from CEA-709 to BACnet

This section describes how to expose a CEA-709 scheduler and calendar to a BACnet operator workstation (OWS). It is assumed that the CEA-709 scheduler is either a local or a remote scheduler on the L-Gate and schedules only one value. That CEA-709 scheduler must be the hub.

To Expose a CEA-709 Schedule to BACnet

1. Prepare a CEA-709 schedule object to be exposed (local as in Section 0 or a remote scheduler as in Section 0 from the Remote Devices folder)
2. Create a local BACnet scheduler as in Section 0. Do not attach data points to that scheduler.
3. Create a new connection (see Section 0). Give it a descriptive name, e.g. *sched_conn*.
4. Select the CEA-709 schedule object as the hub.
5. Select the BACnet scheduler as the target.
6. Click **Save**. Now a scheduler connection appears in the connections list.

Important: *Once a scheduler is in a connection, do not change the scheduled data points!*

7. Create a local BACnet calendar object, if not existing yet. Add the required number of calendar patterns, i.e., the number of calendar patterns used in the CEA-709 calendar. It is recommended to allocate a number of spare calendar patterns, too. This can be

handy, because BACnet calendars cannot dynamically add calendar patterns at run-time, while CEA-709 calendars can. Do not specify names for the calendar patterns.

8. Create a second new connection. Give it a descriptive name, e.g., cal_conn.

Important: *If there already exists a calendar connection, don't create a new connection and add the exposed calendar as a target to the existing connection! There can only be one calendar connection that contains all exposed calendars.*

9. Select the CEA-709 calendar as the hub. When exposing a remote schedule, select the calendar from the same remote device folder where the schedule was selected from.
10. Select the created BACnet calendar as the target.
11. Click **Save**. Now a calendar connection appears in the connections list.

Index	Connection Name	Members	Points
1	cal_conn	2	lon_cal / Port 1, bac_cal / Port 1
2	sched_conn	2	lon_sched / Port 1, bac_sched / Port 1

Map from BACnet to CEA-709

This section describes how to expose a BACnet scheduler and calendar to a CEA-709 network. It is assumed that the BACnet scheduler is either local or remote. That BACnet scheduler must be the hub.

To Expose a BACnet Schedule to CEA-709

1. Prepare a BACnet schedule object to be exposed (local as in Section 0 or a remote scheduler as in Section 0 from the Remote Devices folder)
2. Create a local CEA-709 scheduler as in Section 0. Do not attach data points to that scheduler.
3. Create a new connection (see Section 0). Give it a descriptive name, e.g. sched_conn.
4. Select the BACnet schedule object as the hub.
5. Select the CEA-709 scheduler as the target.
6. Click **Save**. Now a scheduler connection appears in the connections list.

Important: *Once a scheduler is in a connection, do not change the scheduled data points!*

7. Create a local CEA-709 calendar object, if not existing yet. Do not add any calendar patterns.

Important: *If there already exists a calendar connection, don't create a new connection and add the exposed calendar as a target to the existing connection! There can only be one calendar connection that contains all exposed calendars.*

8. Create a second new connection. Give it a descriptive name, e.g., cal_conn.
9. Select the BACnet calendar as the hub. When exposing a remote schedule, select the calendar from the same remote device folder where the schedule was selected from.
10. Select the created CEA-709 calendar as the target.
11. Click **Save**. Now a calendar connection appears in the connections list.

Index	Connection Name	Members	Points
1	sched_conn	2	bac_sched / Port 1, lon_sched / Port 1
2	cal_conn	2	bac_cal / Port 1, lon_cal / Port 1

Operating Interfaces

Common Interface

Schedule and Calendar XML Files

The daily schedule and calendar pattern configuration can be changed 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 121. 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/`.

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 121. 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 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 and the 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. 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;LGATE-900;3.0.0;IP (192.168.24.100)
#log_info;47110;Log Name
#log_create;2007-11-02;16:00:00
#log_capacity;700;2000
#log_item;0;UID;data point name
```

After those lines any number of comment lines starting with a hash character '#' are allowed. The column format is defined in Table 8. 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 ';'.

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.

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 <code>log_item</code> of the CSV header.
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/time 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 $n - 1$	1	Logged value from source $n - 1$ or empty

Table 8: Columns of the Trend Log CSV File

CEA-709 Interface

Resource Limits

The CEA-709 interface has the following resource limits. These limits are per CEA-709 interface.

- 1000 NVs per interface (static, dynamic, external)
- 1000 alias NVs (both in ECS and legacy network management mode)
- 512 address table entries (15 in legacy network management mode)
- 100 LONMARK scheduler objects

NV Import File

Network variables can be imported to the Gateway configuration software 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 a hash character '#' are allowed. Lines that are not comments specify one NV per line, using the column information as described in Table 9. The columns are separated by commas ',' or semi-colons ';'. Which separator is used can be configured in the Web UI (see Section 0).

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 9: CSV Columns of the NV Import File

Node Object

The L-Gate provides a node object conforming to the LONMARK guidelines. A diagram of the node object is depicted in Figure 123.

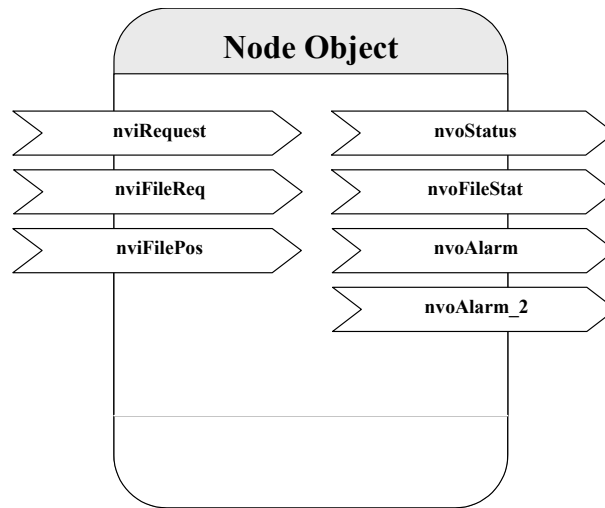


Figure 123: Node Object

- 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 L-Gate 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.

Extended Node Object Interface

When any of the AST features is enabled in the project settings, the node object contains some extensions.

- *nviDateEvent* (SNVT_time_stamp), *nvoDateResync* (SNVT_switch): These NVs are part of the standard LONMARK node object, if schedulers are used.
- *nvoSystemTemp* (SNVT_temp): This NV can be used to poll the system temperature of the L-Gate. It does not send updates.
- *nvoSupplyVolt* (SNVT_volt): This NV can be used to poll the supply voltage of the L-Gate. It does not send updates.
- *nvoIpAddress* (SNVT_str_asc): This NV can be used to poll the IP address of the L-Gate. It does not send updates.
- *nciEarthPos* (SNVT_earth_pos): This configuration property can be used to set the earth position of the L-Gate. It has been implemented as an NV to make other devices send that configuration to the L-Gate over the network (e.g., from a GPS device).

Real-Time Keeper Object

When the scheduler objects are enabled in the project settings, the L-Gate includes the standard LONMARK real-time keeper object.

Calendar Object

When the scheduler objects are enabled in the project settings, the L-Gate includes the standard LONMARK calendar object.

Scheduler Object

When the scheduler objects are enabled in the project settings, the L-Gate includes the configured number of standard LONMARK scheduler objects.

Clients Object

When the remote AST object feature is enabled in the project settings, the L-Gate 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.

Gateway Objects

The L-Gate contains eight proprietary Gateway objects. These are containers for all NVs, which are configured on the L-Gate'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.

BACnet Interface

Resource Limits

The BACnet interface has the following resource limits. These limits are per BACnet interface.

- 750 regular data BACnet objects (analog, binary, multi-state)
- 100 BACnet scheduler objects
- 100 BACnet calendar objects
- 32 BACnet notification class objects
- 100 BACnet trend log objects. For the aggregated size over all trend logs on the device there is a limit of 130000 log records or roughly 2MB.

Device Object

The BACnet interface provides one device object as shown in Table 10.

Property Identifier	Property Datatype	Conformance Code
Object_Identifier	BACnetObjectIdentifier	R
Object_Name	CharacterString	R
Object_Type	BACnetObjectType	R
System_Status	BACnetDeviceStatus	R
Vendor_Name	CharacterString	R
Vendor_Identifier	Unsigned16	R
Model_Name	CharacterString	R
Firmware_Revision	CharacterString	R
Application_Software_Version	CharacterString	R
Location	CharacterString	R
Description	CharacterString	R
Protocol_Version	Unsigned	R
Protocol_Revision	Unsigned	R
Protocol_Services_Supported	BACnetServicesSupported	R
Protocol_Object_Types_Supported	BACnetObjectTypesSupported	R
Object_List	BACnetARRAY[N]of BACnetObjectIdentifier	R
Max_APDU_Length_Accepted	Unsigned	R
Segmentation_Supported	BACnetSegmentation	R
Max_Segments_Accepted	Unsigned	R
APDU_Segment_Timeout	Unsigned	R
APDU_Timeout	Unsigned	R
Number_Of_APDU_Retries	Unsigned	R
Max_Master	Unsigned(1..127)	R
Max_Info_Frames	Unsigned	R
Device_Address_Binding	List of BACnetAddressBinding	R
Database_Revision	Unsigned	R
Active_COV_Subscriptions	List of BACnetCOVSubscription	R
Profile_Name	CharacterString	R

Table 10: Properties of the Device Object

Object_Identifier (Read-Only)

This property, of type “BACnetObjectIdentifier”, is a numeric code that is used to identify the object. For the Device object, the object identifier is unique internetwork-wide.

The “Object Type” part of the “Object_Identifier” is 8 (=device). The “Instance” part of this property is configurable via the configuration UI (see Section 0 and 0). The default value for the “Instance” part is 17800.

Object_Name (Read-Only)

The value of this property is configurable via the configuration UI (see Section 0 and 0). The default value is “L-Gate”. Note that this name must be unique in the BACnet internetwork.

Object_Type (Read-Only)

The value of this property is DEVICE (8).

System_Status (Read-Only)

The value of this property is always OPERATIONAL.

Vendor_Name (Read-Only)

The value of this property is "LOYTEC electronics GmbH".

Vendor_Identifier (Read-Only)

The value of this property is 178.

Model_Name (Read-Only)

The value of this property is equal to the product code of the device ("LGATE-900").

Firmware_Revision (Read-Only)

The value of this property gives the current firmware version of the device.

Application_Software_Version (Read-Only)

The value of this property gives the build date and the version of the current firmware.

Location (Read-Only)

This property is configurable via the configuration UI (see Section 0 and 0). The default value is "unknown".

Description (Read-Only)

This property is configurable via the configuration UI (see Section 0 and 0). The default value is "L-Gate".

Protocol_Version (Read-Only)

The value of this property is 1.

Protocol_Revision (Read-Only)

The value of this property is 4.

Protocol_Services_Supported (Read-Only)

For the services supported please refer to the LGATE-900 PICS document.

Protocol_Object_Types_Supported (Read-Only)

For the supported object types please refer to the LGATE-900 PICS document.

Object_List (Read-Only)

This read only property is a BACnetARRAY of "Object_Identifier", one "Object_Identifier" for each object within the device that is accessible through BACnet services (see below).

Max_APDU_Length_Accepted (Read-Only)

The value of this property is 487 if BACnet MS/TP is used and 1473 if BACnet/IP is used.

Segmentation_Supported (Read-Only)

The value of this property is SEGMENTED_BOTH.

Max_Segments_Accepted (Read-Only)

The value of this property is 16.

APDU_Segment_Timeout (Read-Only)

The value of this property is 2000 milliseconds.

APDU_Timeout (Read-Only)

The value of this property is 3000 milliseconds.

Number_Of_APDU_Retries (Read-Only)

The value of this property is 3.

Max_Master (Read/Write)

This property is only present in case BACnet MS/TP is used. The value of this property is configurable via the configuration UI (see Section 0 and 0). The default value of this property is 127.

Max_Info_Frames (Read/Write)

This property is only present in case BACnet MS/TP is used. The value of this property is configurable via the configuration UI (see Section 0 and 0). The default value of this property is 1.

Device_Address_Binding (Read-Only)

The "Device_Address_Binding property" is a List of "BACnetAddressBinding" each of which consists of a BACnet "Object_Identifier" of a BACnet Device object and a BACnet device address in the form of a "BACnetAddress". Entries in the list identify the actual device addresses that will be used when the remote device must be accessed via a BACnet service request.

Database_Revision (Read-Only)

This property, of type Unsigned, is a logical revision number for the device's database. It is incremented when an object is created, an object is deleted, an object's name is changed, an object's Object_Identifier property is changed, or a restore is performed.

Active_COV_Subscriptions (Read-Only)

The Active_COV_Subscriptions property is a List of BACnetCOVSubscription, each of which consists of a Recipient, a Monitored Property Reference, an Issue Confirmed Notifications flag, a Time Remaining value and an optional COV Increment. This property provides a network-visible indication of those COV subscriptions that are active at any given time. Whenever a COV Subscription is created with the SubscribeCOV or SubscribeCOVProperty service, a new entry is added to the Active_COV_Subscriptions list. Similarly, whenever a COV Subscription is terminated, the corresponding entry is removed from the Active_COV_Subscriptions list.

Profile_Name

The value of this property is "178-LGATE".

Client Mapping CSV File

Client functionality for the BACnet server objects can be defined by so-called "client mappings". These mappings basically specify whether present value properties shall be written to or polled from the BACnet network, and what the destination address and objects are. These definitions can be downloaded as a CSV file onto the L-Gate using FTP.

The CSV file must be named “bacclnt.csv” and stored in the directory “/var/lib/bacnet” on the L-Gate. The file is read when the L-Gate boots. If any errors occur they are reported in “/tmp/bacclnt.err”.

The column format is shown in Table 11. Lines beginning with a hash (“#”) sign are comment lines. The example values in Table 11 setup a client mapping named “Lamp Room 302”, which writes (mapping type 2) the present value of the local object AI,4 to the remote object AO,1 on the device with the instance number 17801.

Column	Field	Example	Description
A	Description	Lamp Room 302	User-defined description of this client mapping. Can be left empty. Don't use commas or semi-colons in the text!
B	Local Object-Type	AI	The BACnet object type of the local server object (AI, AO, AV, BI, BO, BV, MI, MO, MV)
C	Local Object Instance Number	4	The object instance number of the above object.
D	Remote Device Instance	17801	The device object instance number of the remote BACnet device
E	Remote Object-Type	AO	The BACnet object type of the remote server object (AI, AO, AV, BI, BO, BV, MI, MO, MV)
F	Remote Object Instance Number	1	The object instance number of the above object.
G	Map Type	2	Defines the type of the mapping: 0=Poll, 1=COV, 2=Write
H	Interval/ Priority	8	Defines the poll interval in seconds for poll mappings and the COV lifetime in seconds for COV mappings. For write mappings this defines the write priority (1..16). Omit this field or set it to '-1' to write w/o priority.

Table 11: CSV Columns of the BACnet Client Mappings File

EDE Export of BACnet Objects

The BACnet server object configuration of the L-Gate is accessible as a set of CSV files following the EDE format convention. They can be downloaded via FTP from the directory ‘/data/ede’ on the L-Gate. The files are

- lgate.csv: This is the main EDE sheet with the list of BACnet objects.
- lgate-states.csv: This is the state text sheet. For each state text reference in the main sheet, a line contains the state texts for this multi-state object.
- lgate-types.csv: This is the object types text sheet. The file contains a line for each object type number. Note, that lines for standard object types can be omitted.
- lgate-units.csv: This is the unit text sheet. The file contains a line for each engineering unit enumerator value. Note that lines for standard units can be omitted.

Network Media

FT

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

When using the Free Topology Segment feature of the FT, only one termination (Figure 124) 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.

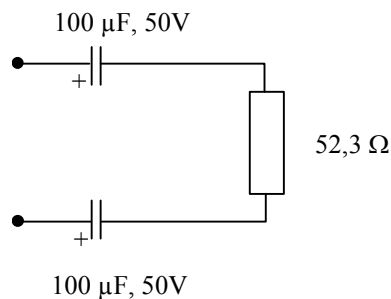


Figure 124: FT Free Topology Termination

In a double terminated bus topology, two terminations are required (Figure 125). These terminations need to be placed at each end of the bus. Here, also L-Term modules can be used at either end.

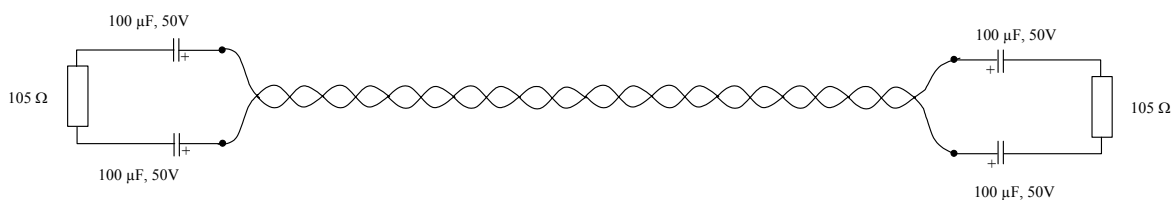


Figure 125: Termination in an FT Bus Topology

L-Gate Firmware Update

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

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

- L-Gate fallback image,
- L-Gate primary image.

The L-Gate 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 to reinstall a valid primary image.

When the L-Gate boots up with the fallback image, the CEA-709 port LED and the STATUS LED are flashing red.

Firmware Update via FTP

The L-Gate primary image can be updated using any FTP client. For convenience, it is recommended to use the L-Gateway configuration software to perform this upgrade. For this purpose, the L-Gate must be connected to the Ethernet and must have a valid IP configuration (see Section 0 and 0). The L-Gateway configuration software must be installed (see Section 0).

To Update the Firmware using the L-Gateway Configuration Software

1. Start the L-Gateway configuration software from the Windows Start menu: Start → Programs → LOYTEC Gateway Configuration → Configure L-Gate.
2. Select the menu: Operations → Connect to Gateway Device → FTP. This opens the FTP connection dialog as shown in Figure 126.

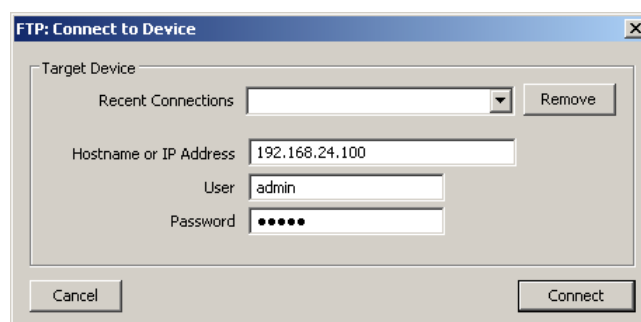


Figure 126: FTP connection dialog.

3. In the FTP connection dialog enter the IP address of the L-Gate 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 0) and reset via the console UI (see Section 0).
4. Click on **Connect**.
5. Select the menu: Firmware → Update ...
6. This opens the Firmware Update dialog as shown in Figure 127. Click on the button “...” and select the firmware image (“lgate_lc3k_primary.dl”).

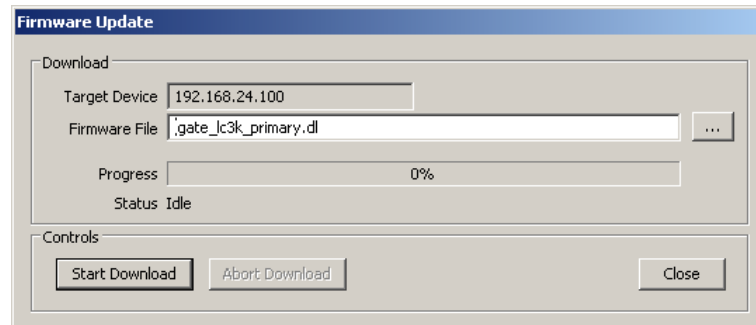


Figure 127: Firmware Update dialog of the L-Gateway configuration software.

7. Click on Start Download.
8. Observe the download progress. When the download is complete the dialog shown in Figure 128 appears.



Figure 128: 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.

Firmware Update via the Console

To download the firmware via the console interface, the L-Gate must be connected to the RS-232 port of a PC via its console interface as described in Section 0. You will need the LOYTEC serial upgrade tool (LSU Tool), which can be downloaded from our homepage at www.loytec.com.

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

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 129.

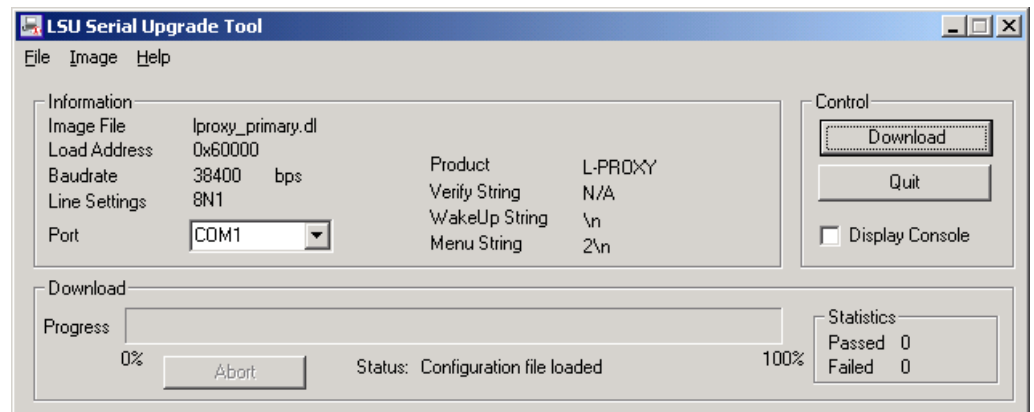


Figure 129: LSU Serial Upgrade Tool in Idle Mode

2. If the L-Gate 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 130 can be seen.

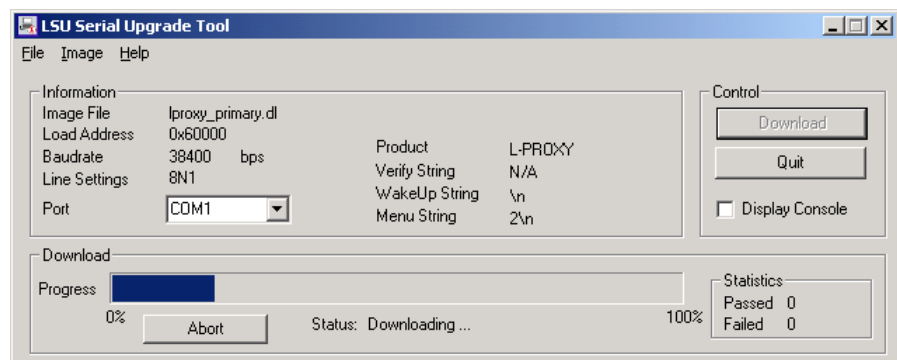


Figure 130: Progress Bar during Firmware Download.

3. If the upgrade is successful, the following window appears (Figure 131).

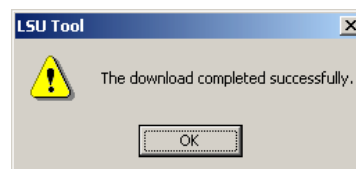


Figure 131: Successful Firmware Upgrade

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.

Troubleshooting

Technical Support

LOYTEC offers free telephone and e-mail support for our L-Gate 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.
583 Union Chapel Road
Cedar Creek, TX 78612
USA*

*Email: support@loytec-americas.com
web: http://www.loytec-americas.com
tel: +1/512/332 2445
fax: +1/512/332 2445*

Application Notes

The LSD Tool

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

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.

Firmware Versions

Table 12 shows the most important features available only in certain firmware versions.

Firmware Version/ Features	1.0.0	1.1.0	1.2.0	3.0.0
CEA-709/BACnet gateway	√	√	√	√
BACnet Network Scan	-	√	√	√
CEA-709 Network Scan	-	√	√	√
UNVTs, SCPTs	-	-	√	√
XML configuration	-	-	-	√
Scheduler	-	-	-	√
Trendlog	-	-	-	√
Alarming (Intrinsic Reporting)	-	-	-	√
E-Mail	-	-	-	√
L-Gate Backup/Restore configuration	-	-	-	-

Table 12: Available Features depending on Firmware Version

Specifications

LGATE-900

Operating Voltage	12-35 VDC or 12-24 VAC \pm 10%
Power Consumption	typ. 3 W
In rush current	up to 950 mA @ 24 VAC
Operating Temperature (ambient)	0°C to + 50°C
Storage Temperature	10°C to +85°C
Humidity (non condensing) operating	10 to 90% RH @ 50°C
Humidity (non condensing) storage	90% RH @ 50°C
Enclosure	Installation enclosure 6 TE, DIN 43 880
Environmental Protection	IP 40 (enclosure); IP 20 (screw terminals)
Installation	DIN rail mounting (EN 50 022) or wall mounting

Revision History

Date	Version	Author	Description
29-09-06	1.0	STS	Initial revision V1.0
11-01-07	1.0.1	STS	Corrected Table 4, 7. Updated Section 2.3, 6.2, 6.3, and 6.4 for L-Gateway configuration software 2.0.
16-03-07	1.1	STS	Updated Section 4.9.3, added Section 4.11, added Section 5.2.6 on the data point Web UI, rewrote Chapter 6 to cover more use cases, added Chapter 7 on using the L-Gateway configuration software, updated firmware update Section 10.1.
08-02-08	3.0	STS	Major revision to cover L-Gate 3.0 and L-Gateway configuration software 3.0.
04-04-08	3.0.1	STS	Updated Section 8.1.2 with new data logger CSV format version 2.