

Echochange

Ethernet gateway for the connection
of different controllers



Version: E-21.03.2018

© Softing Industrial Automation GmbH 2018

Disclaimer of liability

We have checked the contents of the document for conformity with the hardware and software described. Nevertheless, we are unable to preclude the possibility of deviations so that we are unable to assume warranty for full compliance. The information given in the publication is, however, reviewed regularly. Necessary amendments are incorporated in the following editions. We would be pleased to receive any improvement proposals which you may have.

This document may not be passed on nor duplicated, nor may its contents be used or disclosed unless expressly permitted. Violations of this clause will necessarily lead to compensation in damages.

All rights reserved, in particular rights of granting of patents or registration of utility-model patents.

Softing Industrial Automation GmbH

Richard-Reitzner-Allee 6

DE-85540 Haar

Tel: +49 89 456 56-340

Fax: +49 89 456 56-488

Internet: <http://industrial.softing.com>

Email: info.automation@softing.com

Important notes

Read the manual before the start. For damages due to improper connection, implementation or operation Softing refuses any liability according to our existing guarantee obligations.

The recent version of this manual is available in the Download Area of the Softing at:
<http://industrial.softing.com>.

Table of Contents

Chapter 1 Help Overview	7
Chapter 2 echochange	9
2.1 Scope of Delivery	9
2.2 Features.....	10
2.3 Specifications.....	10
2.4 Hardware	11
2.5 Getting Started.....	12
2.6 Constraints of Protocol Conversion.....	16
Chapter 3 NetCon – General	18
3.1 Overview.....	18
3.2 System Requirements.....	19
3.3 License Conditions.....	19
Chapter 4 Basics	23
4.1 NetCon echo.....	23
4.2 Logger.....	23
4.3 ARP.....	24
4.4 PC-H1 Driver.....	24
Chapter 5 PLC Connections	26
5.1 S7 – General Information.....	26
5.2 S5 – General Information.....	26
5.3 Modbus – General Information.....	27
5.4 CLX – General Information	27
5.5 PLC-5 / SLC – General Information.....	27
5.6 MELSEC-Q – General Information.....	28
5.7 Send/Receive – General Information.....	28
5.8 OPCpipe – General Information.....	29
Chapter 6 Operation and Configuration	31
6.1 How to Proceed.....	31
6.2 Basic Configuration.....	31
6.3 Licensing.....	32
Chapter 7 Windows	34
7.1 Softing NetCon Configuration.....	34
7.1.1 Select a Station in Your Network	35
7.1.2 Edit Access to a Station in Your List	36

7.1.3	Station Not Found	37
7.1.4	Offline Configuration	37
7.2	NetCon Main Window	38
7.3	Connections List.....	39
7.4	Logger.....	40

Chapter 8 Connection 42

8.1	New Connection.....	42
8.1.1	New Connection – echochange	42
8.1.2	echochange Connection Network	43
8.2	Connection Settings.....	46
8.2.1	Network Protocol	46
8.2.2	Network PLC Protocol	47
8.2.3	TCP/IP Connect Parameters	47
8.2.3.1	TCP/IP Special Settings	48
8.2.3.2	IP Address.....	50
8.2.3.3	Port	51
8.2.3.4	TSAP.....	51
8.2.3.5	TSAP for S7 Connections.....	52
8.2.3.6	PLC Header.....	53
8.2.4	H1 Connect Parameters	54
8.2.5	S7 Protocol Settings	55
8.2.6	echocollect Connection: Modbus Protocol	55
8.2.7	echochange Connection: CLX Protocol	56
8.2.8	echochange Connection: SLC / PLC-5 Protocol	56
8.2.9	Melsec-Q Protocol	57
8.2.10	Mail Connect Parameters	57
8.3	Edit Connection.....	58
8.4	Copy Connection.....	58
8.5	Delete Connection.....	58
8.6	Disable Connection.....	58

Chapter 9 Main Menu 61

9.1	File.....	62
9.2	Connection.....	62
9.3	Diagnostics.....	63
9.3.1	echochange Connection Diagnostics	63
9.3.2	TCP/IP Stati	64
9.3.3	Logger	64
9.3.4	Logger Settings	65
9.3.5	Using the Diagnostic Text Output System	66
9.4	Station.....	66
9.4.1	Station Password	66
9.4.2	Station Parameters	67
9.4.3	Device SSH Settings	68
9.5	Settings.....	68
9.5.1	H1 System Settings	69
9.5.2	TCP/IP System Settings	70
9.5.3	Device System Settings	72

9.5.4	Diagnose of Default Connections	72
9.5.5	Clock Settings	72
9.5.6	PLC Conversion Table	73
9.5.7	Device Service Settings	74
9.5.8	Reboot	74
9.6	Help	74
9.6.1	Versions	75
9.6.1.1	Hardware Versions	75
9.6.2	About	75
9.6.3	License Overview	75
9.6.4	Licenses	75
	Index	77



Chapter 1

Help Overview

1 Help Overview

NetCon echo for echochange
echochange
NetCon - General
Basics
PLC Connections
Operation and Configuration
Windows
Connection
Main Menu



Chapter 2

echochange

2 echochange

This chapter covers the following topics:

- [Scope of Delivery](#)
- [Features](#)
- [Specifications](#)
- [Hardware](#)
- [Getting Started](#)
- [Constraints of Protocol Conversion](#)

2.1 Scope of Delivery

Before you commission the echo device, please make sure that the package contains the following elements:

- echochange device
- CD-ROM with configuration software
- Manuals
- echochange Quick Start

NOTE:

An AC adapter is not included in delivery. Please order it separately under the following order number:

AC adapter, 24V DC, 700-5596-04

Please also indicate the required plug type (Euro, UK, US) in your order.

If you want to use your own AC adapter, please observe the polarity of the 24V connector (positive pole at the top, negative pole at the bottom).

2.2 Features

echochange connects PLCs from different manufacturers by converting the Ethernet protocols in such a way that packets can be exchanged between previously incompatible protocols.

- Converts data from different Ethernet protocols
- Bridges two separate networks using different protocols
- Connects computers with standard TCP/IP to Industrial Ethernet
- Converts the following Ethernet protocols:

Supported transport protocols

- TCP
- UDP
- IP
- ISO (H1)
- ISO on TCP (RFC 1006)
- PLC Header
- EtherNet/IP

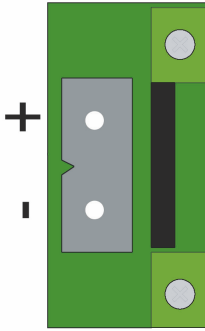
2.3 Specifications

Parameter	echochange
Network addressable PLCs	<ul style="list-style-type: none"> • Simatic S7 • Rockwell CLX • Rockwell SLC-500 • Simatic S5 • PLCs with Modbus over TCP • Wago, Phoenix, Beckhoff, etc.
Ethernet interface	2 x TP (RJ45), 10/100 MBit
Serial interfaces	
Power supply	24V DC, 0.3A
Storage temperature	-20°C .. 70°C
Operating temperature	5°C .. 55°C
Dimensions (in mm)	H = 131, W = 47, L = 111
Mounting	35mm top hat rail (DIN rail)
Protection class of housing	IP20
AC adapter	External

2.4 Hardware

Power supply

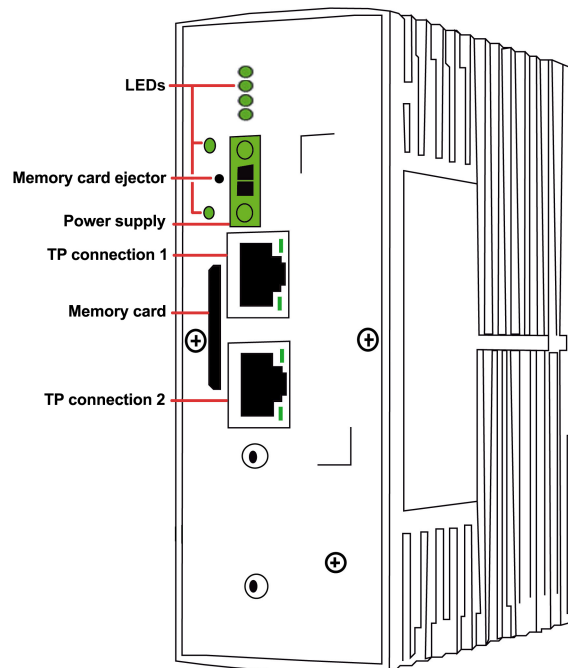
An AC adapter 230V / 24V is not included in delivery. Please order it separately. If you want to use your own AC adapter, please observe the polarity of the 24V DC connector (positive pole at the top, black wire of the cable, negative pole at the bottom, white wire of the cable).



Memory card

To eject the memory card, simply take the card out of the slot. Please do not insert any objects in the "SD eject" hole.

echochange device



LEDs

The 5 LEDs have the following meanings:

LED	Meaning
Power	echo device correctly connected to the power supply
SD	SD card inserted
Conn	Indicates that a configured connection has been established
Eth 1	IPv4 address configured for TP1
Eth 2	IPv4 address configured for TP2

2.5 Getting Started

Before working with the device, you need to carry out the following steps:

1. Mounting
2. Connection to the AC adapter
3. Connection to the Ethernet network
4. Installation of the NetCon configuration software
5. Connection of PC and device
6. Basic configuration

Mounting

- Install or remove the device only when it is switched off
- Horizontal mounting
- Keep the device away from heat and electrical interference
- Do not cover the cooling slots on the top and bottom
- Leave enough space for ventilation

The echo device can be mounted on a top hat rail. Additional accessories are not required for top hat rail mounting. The device is provided with a snap lock for easy mounting on a top hat rail (DIN rail).

Do the following:

1. Hang the rear panel of the device on the DIN rail.
2. Swivel the device down in the direction of the DIN rail. Make sure that the device properly snaps into place and is securely fastened to the rail.

Connection to the AC adapter

Connect the AC adapter with the device and then plug the adapter into the AC mains power supply.

The device has no ON/OFF switch. It switches on automatically when the AC adapter is plugged into the mains power supply.

Wait until only the green Power LED is on.

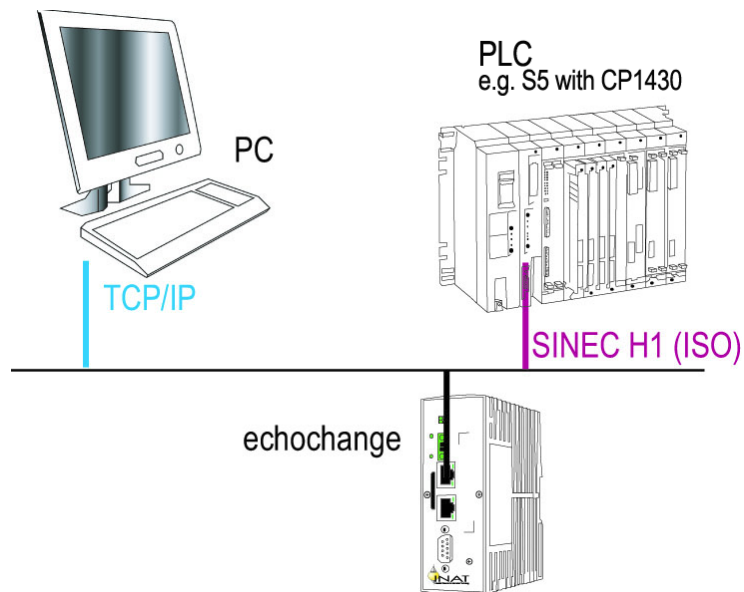
This means that the device is ready for operation.

Connection to the Ethernet network

The device has two RJ45 sockets for Ethernet connection.

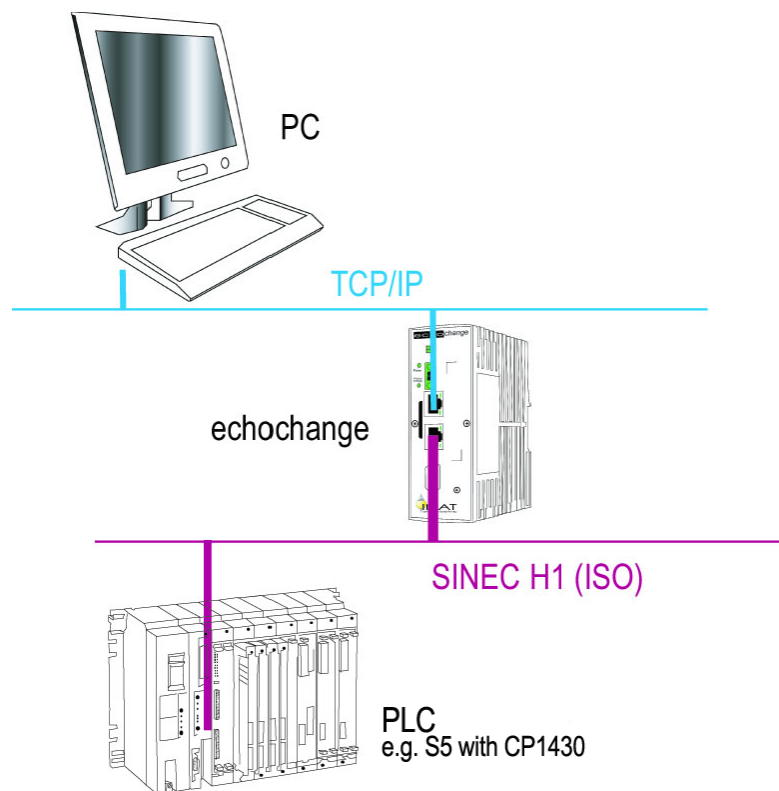
Use of 1 x RJ45

If you are using echochange in a heterogeneous network (i.e. the Ethernet protocols are running on one medium), you will only need one Ethernet connector.



Use of 2 x RJ45

If you are using the echochange as a bridge between two separate networks (i.e. the protocols are running on different media), you will need both Ethernet connectors.



- Connect one end of a TP cable with the TP socket (RJ45 socket) on the front panel of the device. Plug the other end into an Ethernet hub/switch connected to your network.
- The LEDs Eth 1 and/or Eth 2 should blink now. If they don't, please check the network connection and cabling.

Installation of the configuration software

Using the NetCon echo configuration software, you define the basic configuration of the device and set the parameters for your connections. The defined parameter settings are either transferred directly to the device or stored locally for later transmission. The configuration software allows you to monitor and diagnose configured connections. To configure the device, you will need a PC on which the NetCon echo configuration software is installed. PC and device have to be connected either directly or indirectly (see chapter 2.5). To install the configuration software, do the following:

1. Insert the CD-ROM in your CD drive.
2. Select the "echochange" installation.
3. You will be automatically guided through the installation process.

Connection of PC and device

A connection between PC and device is required for:

- Online configuration
- Transfer of a parameter file from PC to device and vice versa
- Diagnostic and test functions
- Programming of the S5 / S7 via network

The connection between PC and device can be established indirectly via bus.

Basic configuration

The echo device is configured with the NetCon software.

Resetting the device to default settings

- Start the configuration software.
- Select "Offline".
- Enter the file name "netfile.net". This file must be located in the main directory of the SD card.
- Set the Station Parameters to the desired values. For the MAC address, you can either leave 00 00 00 00 00 00 – in this case, the hardware address of the device will be used – or you can enter the desired MAC address.
- Exit the configuration software.
- Insert the card in the device.
- Restart the device.

The device has the specified parameters; all the connections have been removed. You can use any configuration file you have created.

Remove the card from the device. If you leave it inserted, all the parameter settings will be reset every time you switch on the device.

2.6 Constraints of Protocol Conversion

Protocol-specific conditions, such as physical memory, S7 SSLs, PLC diagnostics or PLC circuits, place constraints on protocol conversion. These elements are not supported and, consequently, errors cannot be evaluated. Therefore, visualizations that are based on these functions (WinCC with internal driver) cannot be used.

If requests do not match on both sides, no request is made on the destination side and an error is immediately returned to the requester. This is the case, for example, with byte requests via word protocols. Word/byte data is not converted. Byte swapping is processed, however.

Rockwell CLX uses little-endian, S7/S5 and Modbus usually use big-endian.

The S7 element types of the request are not evaluated because standard systems always request bytes. The setting of the allocation table is used here. The byte setting prevents any swapping from taking place. Bit requests are not possible. Bits are not included in any of the settings. If the destination does not reply to the request, the requester waits for the result. The requester must not make any further requests until it has received the response. To cancel a request, the connection has to be reset. Standard request systems such as the OPC server or Visu driver behave like this. PLC requesters sometimes do not know this behavior. They must wait or the PLC program must be capable of a timeout. S5 protocols are capable of requests of any length and requests with undefined lengths. The requests with undefined lengths (joker length) are not supported. Requests can have a maximum length of 750 bytes.

Many protocols recognize detailed data types, but standard systems do not use them (particularly with S7 and OPC servers). Applications' requests with variable offsets and lengths are combined into one long request by these systems. Multiple offsets in the allocation table cannot be used in that case. If necessary, the requester needs to adjust the optimization. Rockwell CLX is capable of arrays and structure arrays. Arrays can only be processed from the beginning. Structure arrays are not supported. When browsing, arrays and structure arrays are not resolved. For arrays, the browse window displays the array length. Browsing of large PLC symbol lists is slow. After a maximum of 10 seconds, a browse request is canceled. This happens, in particular, with slow or overloaded connections. Usually this behavior is caused by the short CLX frame lengths. The ping time has a greater effect than the actual line speed. CLX structures that are completely specified in Modbus register lists, for example, are not able to adapt the data individually.

When the source permits longer requests than the destination, the requests are processed by the destination one after the other. If this processing exceeds the target length in the destination, the transmission is aborted with an error message. During the write operation, part of the data has already been transferred to the destination, however. The possible error signaling varies from protocol to protocol. If an error occurs, protocol errors are converted although detail information may be lost. Examples: S5 only recognizes "Data block does not exist" and "Data block is too short", while S7 recognizes a large number of error codes. Rockwell CLX returns a general protocol error for non-existent symbols or deviating data types. If both protocol sides support multiple requests in one frame, the multiple requests are not always used on the destination side.



Chapter 3

NetCon – General

3 NetCon – General

This chapter provides general information about NetCon:

- [Overview](#)
- [System Requirements](#)
- [License Conditions](#)

3.1 Overview

echo

The devices of the **echo** product family allow you to exchange data between field devices (PLC) from many different manufacturers as well as communication servers, such as OPC servers or DDE servers, databases and other communication partners. The access path is routed via Ethernet TCP/IP, RFC 1006, ISO (H1), MPI, Profibus, RS232, RS485, RS422 or TTY (20mA).

NetCon echo

The user interface for device configuration and diagnostics is provided by the **NetCon** software application. The GUI connects to the devices via TCP/IP (port 982, 997) or via H1.

Access protection

A password can be set to prevent unauthorized modification of the configuration. Accessing devices with multiple NetCons at the same time is not recommended. Because it causes the danger of interfere with each other NetCon user.

Logger

The logger is integrated in the devices. The texts are logged in the device. Using NetCon, you can monitor and configure the logger.

See also [Logger](#).

Help

NetCon provides a context-sensitive help system. You can call the online help from any dialog box either by pressing the **F1 key** or clicking the **Help** button. This displays a help page with a detailed description of the elements and input options in that dialog box.

Manual

Every device comes with a manual in PDF format. It includes the chapters describing the hardware and commissioning, and the online help of the NetCon software. Free PDF readers are available on the Internet from <http://www.adobe.com> or <http://www.foxitsoftware.com>.

3.2 System Requirements

To use NetCon, the following minimum system requirements must be met:

Processor:	Intel Pentium II 200 MHz processor
RAM:	Minimum: 64 MB RAM
Hard disk capacity:	500 MB memory space on hard drive
Operating system:	Windows XP Windows Server 2003, 32 Bit Windows Server 2008, 32 Bit or 64 Bit Windows Server 2008 R2, 64 Bit Windows 7, 32 Bit or 64 Bit

3.3 License Conditions

Please read the following conditions carefully before you install the software product. You must declare that you accept the following conditions either when you buy the software product or, at the latest, when it is installed. If you do not accept these conditions, send the software and the manual back to us within 14 days starting with the date of the invoice. The purchase price can only be reimbursed within the specified time frame.

I. Preamble

The object of the contract is the computer program (called "SOFTWARE PRODUCT" hereafter) stored on the data medium. The LICENSER states that the state of technology makes it impossible to make computer software so that it will work correctly in all applications and combinations. Thus the object of the contract is only a piece of software which works correctly in the sense of the program description and user's guide. The SOFTWARE PRODUCT including all contents (e.g., figures, graphics, text and sample applications) is and will remain the property of the LICENSER and is thus protected by copyright.

The LICENSER is willing to give user's rights as defined in this contract in return for an appropriate licensing fee.

This license contract is concluded between LICENSEE and the LICENSER by the acceptance of the SOFTWARE PRODUCT by the LICENSEE.

II. Terms

LICENSER

Softing Industrial Automation GmbH
Richard-Reitzner-Allee 6
D-85540 Haar

LICENSEE

Natural or legal persons who purchase this license for the purpose of using the SOFTWARE PRODUCT.

THIRD PARTIES

Other natural or legal persons.

III. Scope

1. The SOFTWARE PRODUCT is exclusively licensed for use by the LICENSEE. The LICENSEE may sell the SOFTWARE PRODUCT to THIRD PARTIES under the condition that the THIRD PARTY agrees to this software licensing contract. In this case, the software license contract is invalid for the LICENSEE and the utilization rights to the SOFTWARE PRODUCT are cancelled for him since these rights have been passed on to a THIRD PARTY who has now become the LICENSEE him/herself.
2. The SOFTWARE PRODUCT may only be used on a single computer. The LICENSEE is obligated to purchase a separate license for every computer on which the SOFTWARE PRODUCT is used.

A different agreement between LICENSEE and LICENSER applies to the purchase of multiple and network licenses.

3. The duplication of the SOFTWARE PRODUCT and all related documentations is forbidden except for the creation of an archive copy for exclusive use by the LICENSEE.

If the LICENSEE's original data medium becomes defective, it can be exchanged at the LICENSER for a replacement data medium. The cost of the exchange will be carried by the LICENSEE.

4. The SOFTWARE PRODUCT is delivered on data medium as a demo version with restricted function scope.

The demo version may not be used for commercial purposes. After payment of the licensing fee for the particular desired version, the LICENSEE will receive a code number from the LICENSER for the release of the corresponding SOFTWARE PRODUCT.

5. If a new program version is given to the LICENSEE due to the purchase of an update or for any other reason, the user's rights for the earlier program versions become void. This means that you may only work with the latest version.

6. The LICENSEE and THIRD PARTIES are forbidden to modify the SOFTWARE PRODUCT or reverse engineer it (i.e., de-compile or disassemble it).

The LICENSEE is liable for all damages which occur because of the violation of these conditions.

IV. Limited Warranty

The data carriers on which the SOFTWARE PRODUCT was delivered are free from material and manufacturer's flaws during normal use during a period of time of 6 months starting on the delivery date. The data carriers are free of viruses according to the LICENSER. If, however hidden viruses have snuck in, the LICENSER will not be liable for any subsequent damages which may occur.

1. The preceding limited warranty does not cover data carriers which have been damaged by chance or misuse or manipulation of unauthorized parties (people other than employees of the LICENSER).
2. During the stated guarantee period, the LICENSER is obligated to replace a defective data carrier if this was sent to the LICENSER with a copy of the invoice. Other claims, in particular damage claims, will not be honored subject to para. 4 and Roman numeral V.
3. No further guarantee claims will be allowed. In particular, no guarantee claims will be accepted for program content and its freedom from errors or suitability for certain purposes. The responsibility for software and hardware selection, for installation, use, expected results and data protection and data backup with backup copies is the exclusive business of the LICENSEE.
4. Exceptions to the preceding warranty restrictions are promised characteristics. These promises must be in writing to be valid and accompanied by the signature of the authorized representative of the LICENSER. The LICENSER is only liable for damage claims in accordance with Roman numeral V.

V. RESTRICTION OF LIABILITY

1. The LICENSER is not liable for damages unless the damage is caused by intent or gross negligence of the LICENSER.
2. Liability due to any characteristics which may have been promised by the LICENSER is not affected by this. Liability for subsequent damages due to deficiencies which were not included in the promises of the LICENSER are excluded.
3. No liability is assumed for calculable damages, in particular lost profit.
4. Any damage claims are limited to the amount of the damage whose possible occurrence the LICENSER logically had to expect under the circumstances known at that time when the contract was concluded. In any case, liability is limited to the amount of twice the purchase price that was paid (license fee), regardless of whether claims pertaining to contract law, damage claims or other liability claims are concerned.

VI. Validity and Conclusion

1. The license given to the LICENSEE is valid until it is terminated by the licensee or the LICENSER.
2. The LICENSEE can terminate the license at all times by returning the SOFTWARE PRODUCT including the archivation copy and all related documentation to the LICENSER.

If the return is not due to a warranty claim, the license fee will not be reimbursed.

3. No liability is assumed for calculable damages, in particular lost profit.
4. The LICENSEE terminates the license by resale to a THIRD PARTY in accordance with III, para. 1.

VII. Applicable Laws

1. Regarding the laws which may apply, this license is subject to the laws of the Federal Republic of Germany and the exclusive adjudication of the German courts of law.
2. Court of jurisdiction for all legal disputes resulting from the contractual relationship and its creation and effectiveness for general merchants is Nuremberg. However, the LICENSER has the right to take the LICENSEE to court at his location.
3. Place of execution for all obligations from this contractual relationship is Nuremberg.



Chapter 4

Basics

4 Basics

This chapter covers the following topics:

- [NetCon echo](#)
- [PLC Connections](#)
- [Logger](#)
- [ARP](#)
- [PC-H1 Driver](#)

4.1 NetCon echo

This is the graphical user interface (GUI) used to configure and diagnose the echo devices. The GUI connects to the device via TCP/IP (port 982 or 997).

Starting the program

To start the program, proceed as follows:

- Select **Start - (All) Programs - Softing - NetCon echo - NetCon echo**.
The start window opens, allowing you to configure your echo device via TCP/IP or via H1 (provided the H1 protocol driver has been installed). Then, the [Select a Station in Your Network](#) window opens where you can establish a connection to the desired device. You can also perform the configuration **offline** and load the configuration data later into your echo device, but usually, the configuration is done online.

Password

To prevent parameters and settings from being changed, you can set a password. To do so, select **Station - Station Password**. If a password has been set, each user will be prompted for the password when trying to save or change parameters. Read-only access is not possible without entering the password.

If you forget the password, the only workaround is to transfer the parameters from the external SD card. In the root directory of the SD card, a file named `\netfile.net` is stored. This file contains either the known password or it is empty. Then, insert the card into the device and disconnect it from the power supply. Then, switch the device on again. While the device starts up, its parameters are overwritten with the ones from the card. There is no other remedy.

Operation and Configuration

For more information on the NetCon graphical inter user interface, see the [Operation and Configuration](#) section.

Logger

In NetCon, you can configure the [Logger](#) feature for the device. The Logger content is displayed in the [Logger](#) window.

4.2 Logger

The Logger feature allows you to log the device's communication over the configured connection. You can choose to keep the log data only temporarily in the RAM or save it to a log file. The Logger records the selected data traffic of a communication going over a particular connection. Such a log can be very useful, especially for troubleshooting. Each event is recorded with a timestamp, the name of the application and the actual message.

In NetCon, the [Logger](#) window displays the entries that have been recorded.

To set the parts of the communication to be logged, open the [Logger Settings](#) dialog box.

To specify whether to create the log in the RAM only or to also save it to a file, click [Settings](#) in the Logger dialog box.

4.3 ARP

The **Address Resolution Protocol (ARP)** is a network protocol which allows mapping network addresses to hardware addresses.

To map an IP address to a MAC address, an ARP request is used. After encapsulating this request in a frame, it is sent out as a broadcast. All stations in the network receive and evaluate this request. They compare the IP address submitted in the ARP request with their own IP address. The station whose the IP address matches the one in the request replies by sending an ARP response. The response is sent specifically to the station which had sent out the request, it contains the requested MAC address.

The MAC address is added to an ARP cache along with the associated IP address. The ARP cache is a temporary memory which is part of the respective station's RAM. Each time another IP address needs to be resolved to a MAC address, the station first checks whether it can do so using the ARP cache and thus without sending a new ARP request. If this is not possible, it sends an ARP request. Thus, ARP resolution is advantageous as it saves time and reduces the network load.

If an entry in the ARP cache is not accessed for a certain period of time, it will be removed. This behavior ensures that changes in the network can be detected and reflected by sending new ARP requests.

See also: ARP Cache Stati

4.4 PC-H1 Driver

To configure the echo devices via H1, you need the H1 driver (INAT H1 ISO protocol). This driver is installed with the software and is available for NetCon.

If the PC has multiple network adapters installed, the H1 driver should only be bound to the network adapter used for configuration.

A detailed description is included in the PC-H1 program folder.



Chapter 5

PLC Connections

5 PLC Connections

This chapter covers the following topics:

- [S7 – General Information](#)
- [S5 – General Information](#)
- [Modbus – General Information](#)
- [CLX – General Information](#)
- [PLC-5 / SLC – General Information](#)
- [MELSEC-Q – General Information](#)
- [Send / Receive – General Information](#)
- [OPCpipe – General Information](#)

5.1 S7 – General Information

The S7 protocol is used to communicate with S7 PLCs and with CPs capable of using the S7 protocol.

The S7 protocol can be used in conjunction with TCP/IP, H1, or MPI.

Read (Fetch active) and Write (Write active)

- When communicating with S7 PLCs, it is generally possible to both read and write data over a single connection.
- Usually, the parameterization of the S7 protocol is based on RFC 1006.
- Besides the S7 PLC address (IP address or MAC address), a read and write TSAP is required. When using MPI, enter the MPI address of the CPU.
- To read and write data from and to an S7 PLC (layer 7 communication), the following can be used:
 - non-parameterizable connections
 - parameterizable connections

Non-parameterizable connections

A connection will only be established on the echo side and NOT on the PLC side.

Default connections are required that are handled via standard TSAPs or default ports.

Only a limited number of default connections are available. If these are not sufficient, you need to use a "parameterizable connection".

Default connections with Siemens CPs are handled via RFC 1006 or H1 (see [Standard TSAPs](#) and [TSAP for S7 Connections](#)).

Parameterizable connections

The connection must be parameterized on both sides of the communication (one Fetch/Write active connection on the echo side AND one Fetch/Write passive connection in the S7 CP)

If you use echolink for the communication, parameterizable connections are required.

5.2 S5 – General Information

The S5 protocol is used to communicate with S5 PLCs (S5 AP headers) and with CPs capable of using the S5 protocol.

The S5 protocol can be used in conjunction with TCP/IP, H1 or for serial communication with AS511.

Read (Fetch active):

- To read data actively from an S5 PLC, you need to establish a read connection in the echo device.
- Besides the S5 PLC address (IP address or MAC address), a read port or a read TSAP must be specified.

- The read connection needs to be parameterized on both sides of the communication (Fetch active connection in the OPC server, Fetch passive connection in the S5).

Write (Write active):

- If you want to write data to the S5 PLC as well, a write connection needs to be established besides the read connection. When using S5 via TCP/IP or via AS511, a single connection may be used for this purpose.
- For the write connection, a write port or a write TSAP must be specified.
- The write connection needs to be parameterized on both sides of the communication (Write active connection in the echo device, Write / Receive passive connection in the S5).
- Newer S5 TCP/IP cards and echo devices support reading and writing over a single connection.

5.3 Modbus – General Information

The Modbus over TCP protocol is used for the communication with PLCs from Wago, Groupe Schneider, Beckhoff and all CPs capable of using the Modbus over TCP protocol (Modicon, Ethernet terminals from Phoenix, Wago, Beckhoff and many more). The Modbus protocol only works in conjunction with TCP/IP.

Read (Fetch active) and Write (Write active):

- When communicating with Modbus PLCs, it is generally possible to both read and write data over a single connection.
- If default port 502 is used, you only need to parameterize the connection on the echo device side. On the PLC side, no other settings are required.

5.4 CLX – General Information

The CLX protocol is used for the communication with ControlLogix / Compact Logix PLCs from Rockwell Automation. The CLX protocol only works in conjunction with TCP/IP.

Read (Fetch active) and Write (Write active):

- When communicating with CLX PLCs, it is generally possible to both read and write data over a single connection.
- If default port 44818 is used, you only need to parameterize the connection on the echo device side. On the PLC side, no other settings are required.

NOTE:

To address item IDs, you need to specify their symbolic names in the CLX.

Alias browsing:

Once the CLX connection has been established, symbol information will be read from the PLC and displayed for selection in the corresponding dialog boxes.

5.5 PLC-5 / SLC – General Information

This protocol is used for the communication with PLC-5 and SLC PLCs from Rockwell Automation Allen-Bradley.

The PLC-5 / SLC protocol only works in conjunction with TCP/IP.

We do not support the SLC firmware version which uses the function codes A2 and AA. In such cases a firmware update of the SLC is recommended.

Read (Fetch active) and Write (Write active):

- When communicating with SLC or PLC-5 PLCs, it is generally possible to both read and write over a single connection.

- If default port 2222 is used, you only need to parameterize the connection on the echo device side. On the PLC side, no other settings are required.

5.6 MELSEC-Q – General Information

The MELSEC-Q protocol is used for the communication with Mitsubishi PLCs from the MELSEC-Q series.

The MELSEC-Q protocol only works in conjunction with TCP/IP.

Read (Fetch active) and Write (Write active):

- When communicating with MELSEC-Q PLCs, it is generally possible to both read and write data over a single connection.
- The connection needs to be parameterized on both sides of the communication (one connection in the echo device and one connection in the MELSEC-Q PLC).
- By default, port 8192 is used. The same port number must be used on both sides of the connection.
- If the MELSEC-Q PLC uses non-parameterizable connections with fixed ports ("default connections"), you only need to parameterize the connection on the echo device side. On the PLC side, no other settings are required. Please make sure that the echo device uses the same ports as the MELSEC-Q PLC.

NOTE:

In Mitsubishi PLCs, addresses are often given in HEX notation (in this case, you need to convert the port numbers to decimal notation for the echo device side).

5.7 Send/Receive – General Information

In a Send / Receive communication, the data is transmitted without application headers, i.e. as raw data.

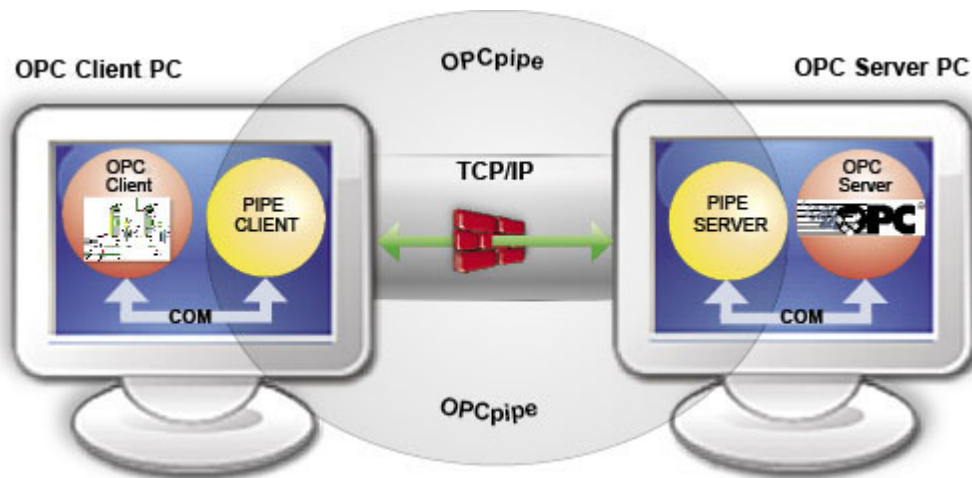
Any station that supports the Send / Receive direct interface can be used as the communication partner.

The Send / Receive protocol works both with TCP/IP and H1.

Receiving and sending data

- It is generally possible to both send and receive over a single connection.
- Besides the address of the Send / Receive PLC (IP address or MAC address), you need to specify a port or TSAP..

5.8 OPCpipe – General Information



OPCpipe is a tunnel protocol that tunnels the data exchanged in an OPC communication between a client and a server.

OPCpipe comprises two parts:

OPCpipe server: Runs on the same computer as the OPC server or on the echo device.

OPCpipe client: Runs on the same computer as the OPC client.

The OPCpipe client receives the request from the OPC client and converts the OPC communication to a “normal” TCP/IP communication. The data can thus be transmitted in a tunnel to the destination computer or echo device via the network by using a standard TCP/IP connection. There, the OPCpipe server receives the data, “decrypts” it by converting it back to OPC communication and forwards the data to the OPC server or the protocol logic of the echo device. The server or echo device performs the requested action and sends the data back to the OPC client. The tunnel mechanism works the same way in both directions.

Establishing an OPCpipe connection

The OPCpipe connection must be configured both on the server side (computer or echo device) and the client side (computer where the OPC client is running).

For this purpose, the OPC server with OPCpipe functionality must be installed on both sides of the communication. Usually, the OPCpipe client initiates the active connection. The default port number is 4444.



Chapter 6

Operation and Configuration

6 Operation and Configuration

This chapter covers the following topics:

- [How to Proceed](#)
- [Basic Configuration](#)
- [Licensing](#)

6.1 How to Proceed

The devices are very easy to parameterize in just a few steps. To set up communication, proceed as follows:

Basic Configuration

To be able to communicate with the echo device via TCP/IP, the device needs an IP address. How to assign the address is described in the [Basic Configuration](#) section.

Configuring the connection

For every hardware from which you want to read data or to which you want to write data, you create a connection to the echo device by using the NetCon software. This connection defines the access path to the hardware, i.e. the channel between the two communication partners. All the parameters needed for the communication between the echo device and the hardware are defined in the respective dialog boxes. The protocols that are supported by the communication partner (e.g. S7 protocol and RFC 1006) are provided for selection. To access specific hardware, you specify the destination addresses (e.g. IP address and port numbers, or MAC address and TSAP). You can also choose whether or not writes are basically allowed over this connection. See the [New Connection](#) section.

Logger

The [Logger](#) is provided for recording error events that have occurred in the device.

6.2 Basic Configuration

During the basic configuration, the device is provided with all the parameters needed for communication. The device is registered on the network.

- Start the NetCon configuration software.
- Select the [type of configuration](#) (usually IP).

NOTE:

The station you are configuring via H1 or IP has to be in the same network as the configuration computer. Stations connected behind a router cannot be discovered.

Configuration via H1 is only available if the INAT PC H1 protocol driver is installed.

Configuration via TCP/IP or H1

- The [Select a Station in Your Network](#) dialog box appears. The new echo device is displayed together with its MAC address.
- From the MAC address, you can determine the station to be configured. Double-click the station or select it and then click OK.
- The [Station Parameters](#) dialog box appears. Edit the settings and confirm your entries with

OK.

- The configuration is complete.

NOTE:

If you want to use both network connections provided by the echo device, both configurations should be configured.

6.3 Licensing

The echo devices are delivered with the functionality that was specified in the order. If, during commissioning or later when adding extensions, you find that you need to expand the functionality, you can do this by activating a license.

In the [License Overview](#) dialog box, you can see which functionalities are licensed and which not. The NetCon displays a License Request Code that you can send to Softing Industrial Networks GmbH. You will then receive an activation code that enables the desired functionality. How this is done is described in the [License Overview](#) and [Licenses](#) sections.

Please note the [license conditions](#).



Chapter 7

Windows

7 Windows

The program GUI basically consists of the following main windows:

- [Softing NetCon Configuration](#)
- [NetCon main window](#)
- [Connections list](#)
- [Logger](#)

Other functions are available from dialog boxes described in the [Connections List](#), [Main Menu](#) chapters.

7.1 Softing NetCon Configuration

The configuration window opens when you start NetCon by selecting **Start - (All) Programs - Softing - NetCon echo - NetCon echo**.

NetCon is required to configure the echo devices. The software is used to make basic settings, create and diagnose connections and display data recorded by the Logger feature. To configure NetCon for a device, use one of the following methods:

Configuration via TCP/IP

A socket connection to the device is established via TCP/IP. Any entries you make are transmitted directly to the device and stored there. This method allows you to configure the device from anywhere within the TCP/IP network.

Configuration via H1

A configuration via H1 is only possible if the H1 protocol driver is installed. An H1 connection is established to the device you want to configure. Any entries you make are transmitted directly to the station and stored there. This method allows you to configure the station from anywhere within the H1 network.

Offline configuration

You can create a configuration file offline on the PC and transfer it to the device. This is not the common way of configuration. It is recommended to configure the device online until everything works properly. Then, transfer the parameters from the device to the PC and save them there.

Language selection (buttons)

Use the buttons to select the desired user interface language. After a restart, NetCon will display all texts in the selected language. Please note that this does not toggle the texts displayed in the Logger.

7.1.1 Select a Station in Your Network

When you perform a **configuration via TCP/IP** or a **configuration via H1** the **Select a Station in Your Network** window opens.

All stations with an arrow (->) at the beginning of the row are currently online in the network. They are detected automatically by NetCon. The software displays all echo devices and PCs with servers.

NOTE:

Stations connected behind a router cannot be discovered automatically. For these, you need to define a direct connection using the [New](#) button.

Selecting the desired station

When you double-click the desired station (or click the OK button), NetCon will connect to the corresponding station. The connection attempt has a timeout of about 3 seconds.

Successful connection: the [Connections](#) main window opens.

Unsuccessful connection: If there is no reply from the station within 3 seconds, the connection attempt aborts.

New

If the station is not listed in the automatic online display (parameterization via IP) because it is located outside your network, you can click this button to configure a direct connection to this station in the [Edit Access to a Station in Your List](#).

Edit

Using this button, you can change the parameters for the station you created using the [Edit Access to a Station in Your List](#) dialog box.

Delete

Using this button, you can delete the parameters for the station. A prompt asks you to confirm that you really want to delete the parameters. **Deletions cannot be undone.**

Scan for stations

Starts the station scan and the automatic discovery of online stations and servers. This scan will only find stations that are accessible in the local network.

Execute station scan on start

Automatically starts the station scan when you open the dialog box. Since this may take a long time if many stations are online, you can disable this function.

Use Timeout

It is recommended to enable this option only if the default connection timeout is too short or the transmission is very slow. By default, this function is disabled.

Timeout

You can use the connection timeout option to change the default timeout (3 seconds) specifically for this connection. This is useful e.g. for Internet connections for which heartbeat monitoring (sending of life time acks) has been disabled. This also increases the response time in case of connection problems (such as a broken cable).

7.1.2 Edit Access to a Station in Your List

If a connection to the desired station was not possible and the [Station Not Found](#) dialog box appears, you can configure a direct connection to this station there. The entry will then be added to the list of available stations and displayed in the [Select a Station in Your Network](#) dialog box. After the station scan has been performed, an arrow symbol (->) preceding a station indicates that this station is available online.

Station Name

The name to be displayed in the list.

H1

Establishes a connection via the H1 protocol. Specify the MAC address and the TSAP.

TCP/IP

Establishes a connection via the TCP/IP protocol. Specify the IP address and the port number.

Extended

Extends the dialog box so that you can enter additional parameters.

H1 Settings

MAC address

The MAC address of the station to be configured and diagnosed.

Use Default TSAP / Special TSAP

Here, you can indicate the TSAP for H1 or RFC 1006 connections.

TCP/IP Settings

IP Address

Here, you can indicate the IP address or the DNS name of the station to be configured and diagnosed.

127.0.0.1 addresses the local device.

Use Default Port / Special Port

The OPC server uses port **982**.

The echo devices use port **997**, newer ones use **982**.

If you want to configure and diagnose the station using RFC 1006, you need to enter the TSAP.

Standard

Reduces the dialog box showing only a few parameters.

Optional Product Select

These entries will be ignored.

7.1.3 Station Not Found

The dialog box shows the message **A timeout occurred**.

If a station cannot be found, this can be due to the following reasons:

OPC server

- The server service has stopped.

Configuration via TCP/IP or Configuration via H1

- The selected station is switched off.
- A network cable is not properly connected or faulty.
- A switch, hub, router or gateway is switched off.
- The station is connected behind a router and therefore not accessible.
- On the operating PC, the protocol to be used for connecting to the station (H1 or TCP/IP) has not been installed or configured properly.
- The H1 or TCP/IP protocol on the remote network station has not been installed or configured properly.
- A station (e.g. a reference router) has disabled the forwarding of the frames.
- The firewall has not been configured properly.

NOTE:

Stations connected behind a router cannot be discovered automatically. For these, you need to define a direct connection using the New button (see [Edit Access to a Station in Your List](#)).

Serial connection

- The connection cable is not plugged in.
- The pins of the connection cable are not assigned correctly. The connection to the station only uses three wires: Send data, receive data, signal ground.
- The interface adapter installed in your PC is faulty.
- The interface of your PC is used by another task.

7.1.4 Offline Configuration

In the **Choose a Product** dialog box, you can select the device to be configured offline. The dialog boxes and menus may vary depending on the functionality of the device.

In an offline parameterization of a device, the parameter data is stored in a parameter file on the PC. The data can later be transferred to the device.

- After clicking the **Configuration Offline** button, the **Open File...** window opens. Here, you can either open an existing parameter file or enter a new file name.
- After you have entered a new file name, the following dialog box opens: **Choose a Product**.
- Here, select the device to be configured.
- Selecting the device closes the dialog and enables you to make further entries.

7.2 NetCon Main Window

The main window consists of two parts. The left panel shows all online stations. The right panel shows the parameterized connections of the station selected in the left panel, i.e. the [Connections](#) list.

When you select a station in the left panel, the right panel shows the associated connections.

Double-clicking a connection opens the dialog box where you can edit the connection.

Right-clicking opens a context menu that provides more functions.

The menu bar provides all functions required to parameterize the echo devices. The menus are described in the [Main Menu](#) chapters.

Frequently used functions are available on a toolbar where they can be accessed by a single click.

Press the **ESC** key to exit the window.

7.3 Connections List

The Connections list of the device is displayed in the main window. It shows an overview of the configured connections including their parameters. The connections are displayed in different colors to indicate their current status: active (**black**) or inactive (**gray**).

To edit a connection, double-click it. To do so, you need master access.

You can toggle the main window between the Connections list and Online Diagnostics by clicking the **Diagnosis - Show All Connections** menu item or the corresponding icon from the toolbar.

Clicking the table header sorts the table by this column in ascending order. Another click on the table header changes the sort order to descending.

The individual columns have the following meanings:

Column	Description
Type	Displays the transport protocol used: - TCP/IP - H1 - Iso TCP (RFC 1006) - Collect Type If the connection is inactive, its name is followed by (off) and grayed out.
Connection Name	The name of the connection.
Job	Shows the application protocol used.
NetProt	Shows the network protocol used and whether the connection has been established actively or passively: TCP/IP: Client [active] / Server [passive] H1: Act [active] / Pass [passive]
Dest. Address	Shows the address of the destination hardware (IP address , IP name or Ethernet address) which can be 0 if the connection has been established passively.
Parameters	This column displays some connection parameters: - Port number - Transport protocol TCP or UDP - Local TSAP , Dest TSAP for RFC 1006 and H1 connections
Parameter Details	Shows additional connection parameters and details, including: - OPCpipe access: Read and write: RW , read only: RO

7.4 Logger

A toolbar in the top part of the window provides the following functions:

Set Marker

Adds a marker text including the current timestamp to the list.

"-----"

Clear

Deletes the entries stored in the RAM. If you have selected to write the log data to a file, the RAM content will be saved to the file before deletion.

Settings

Opens the following dialog box: [Logger Settings](#)

Auto Scroll

Cyclically refreshes the window contents and automatically scrolls to the last line containing the most recent entry.

Suspend

Clicking this button suspends logging. This allows the user to diagnose the current content without overwriting older entries.

NOTE:

No more entries will be recorded.

Close

Closes the Logger dialog box. This does not affect the logging process. Logging continues even if the window is closed.

Master / Slave

Master / Slave shows the current mode of NetCon parameterization. In slave mode, it is not possible to make any settings in the Logger. The mode is selected automatically with the first NetCon instance always being the master; any other instances will run in Slave mode.

As a general rule, it is not recommended to access an echo device by more than one NetCon instance.

Operation

In this window, you can also select entries with the mouse or by pressing the space bar, and copy them to the clipboard. To access this function, master access is required.

Right-clicking then opens a **context menu** which provides the following functions:

Copy

The selected entries are copied to the clipboard and can be pasted into other programs.

Clear Logger

Deletes the entries stored in the RAM. If you have selected to write the log data to a file, the RAM content will be saved to the file before deletion.

Clear Selection

All selected entries are deselected.

To define which parts of the communication will be logged, open the [Logger Settings](#) dialog box. This function is only available in echocollect.

To specify whether to create the log in the RAM only or to also save it to a file, click the [Settings](#) button in the Logger window.

For more information on the logging function in the device, see the [Logger](#) section.



Chapter 8

Connection

8 Connection

This chapter describes the dialog boxes used to handle connections. Other dialog boxes are described in the [Windows](#), [Main Menu](#) chapters.

This chapter covers the following topics:

- [New Connection](#)
- [Connection Settings](#)
- [Edit Connection](#)
- [Copy Connection](#)
- [Delete Connection](#)
- [Disable Connection](#)

8.1 New Connection

New Connection

For each hardware system to be accessed (i.e. with which a communication needs to be established), you must create at least one connection in the device. This connection defines the access path to the hardware, i.e. the channel between the two communication partners. In this dialog box, you can specify the following:

Connection Name

You can choose any connection name you like. It may contain only letters and numbers. The connection name you specify here can be selected in other dialog boxes.

Connection Type

Here, you can select the type of the connection to be created. This is a cascading dialog box. When you select an image or a button, other options will appear. When you select one of those options, another level may be displayed.

8.1.1 New Connection – echochange

This dialog enables you to establish a new connection.

Each echochange connection actually consists of 2 individual connections that are coupled. One is displayed on the left side, the other on the right side. To facilitate the view on this connection pair with the expert mode disabled, the left side is considered to be the passive side, the right side the active side. Once the connection on the left (passive) side is up, the connection on the right (active) side will be established.

For each side, you can select the transport and application protocols individually.

To configure how data from the passive connection will be transmitted to the active connection, an allocation table in the [PLC Conversion Table](#) dialog box is used.

Name of the Connection

You can choose any connection name you like. All characters except brackets may be used.

Expert mode

Disables the simplified display defining the left side as passive and the right side as active. Displays the settings for Send/Receive (raw data) connections, for which the support is subject to a charge. With the Expert mode disabled, using the connection is free of charge.

Transport Protocol Passive / Active or Left / Right

You can select the TCP/IP or H1 transport protocol for the desired side.

Application Protocol Passive / Active or Left / Right

You can select the application protocol for the desired side. The available protocols are S5 and S7 (Siemens), ControlLogix and SLC / PLC-5 (Allen-Bradley) as well as MELSEC-Q (Mitsubishi Electric)

and Modbus over TCP. If you intend to transmit raw data without a PLC protocol, select the Send / Receive protocol.

Application Protocol

Here, you can select the application protocol.

Application Protocol	PLC
Send/Receive (only Expert mode)	Used for the communication with other PLCs or devices that do not support any of the protocols listed below. Only payload data (raw data) will be transmitted, but no protocol information.
Siemens S5 AP	Communication with Siemens S5 CPs or echo devices.
Siemens S7	S7 protocol used to connect to Siemens S7-400, S7-300 or S7-200 PLCs or echo devices.
Modbus TCP	Communication with PLCs or devices supporting the Modbus TCP protocol, such as Wago, Beckhoff, Groupe Schneider, Modicon ...
Rockwell CompactLogiX / ControlLogiX	Communication with Allen-Bradley ControlLogiX, CompactLogiX, SoftLogiX
Rockwell SLC / PLC-5	Communication with Allen-Bradley PLC-5 and SLC
Mitsubishi Melsec-Q	Communication with Mitsubishi Melsec-Q

8.1.2 echochange Connection Network

The editing window for echochange connections has a left and a right panel. Due to the 4 possible assignments of TCP/IP and H1, there are 4 different variants of this window. On the left and right, enter the TCP/IP or H1 parameters.

Editing a Connection – General Settings for All Connections

Name of the Connection

This field displays the connection name which can be changed here.

Connection is Active

Shows whether the connection is active or not. If not, you cannot register items and there will be no connection to the PLC. This feature allows you to disable a connection temporarily without deleting it so that you can re-enable it later without having to enter all parameters again.

Forward clock over TCP/IP

The purpose of this function is to forward clock master frames from an H1 network to a second H1 network. This requires that the two networks are linked by 2 echochange devices via TCP/IP.

If this setting is used, you should enable it on both sides.

When the first echochange device receives a clock master frame, its internal clock will be synchronized.

The device then sends a clock frame to the second echochange device using the TCP/IP protocol, UDP port 994.

The second echochange device receives the frame, synchronizes its internal clock and sends the corresponding clock master frame on the H1 side in order to synchronize the connected PLCs.

Number of the Adapter

Here, you can select network adapter 1 or 2. The selected adapter will be used for this connection.

Slave

Enable the Slave button for the side of the echochange connection that was parameterized as active. In the slave mode, a connection to the communication partner will only be established if a connection is already up on the master side (passive side). With the Slave option disabled, the side that was

defined as active always and immediately tries to connect, independently of whether the connection on the passive side is up or not.

Editing a Connection – TCP/IP Settings

Destination IP Address

When establishing an active connection, you must enter the destination IP address.

For passive connections, we recommend to enter the wildcard address (0.0.0.0).

With echochange, only IP-V4 addresses are allowed.

See also:

- [IP Address](#)

Port

Port numbers are addresses that are used on the transport layer in order to address applications.

Port numbers are required for TCP and UDP connections. Ports are similar to the TSAPs used for

RFC 1006 and H1 connections. Each port number is a 16-bit number in the range from 1 to 65535.

RFC 1006 uses the fixed port number 102. If you enable the RFC 1006 check box, the port number field is grayed out.

See also:

- [More detailed information on ports](#)

Type

Here, you can specify whether your own station will actively initiate the connection attempt or will wait passively for the destination station to establish the connection. Please make sure that different values are selected on both sides of the connection.

Client (Active)	The station will actively initiate the connection attempt.
Server (Passive)	The station will wait for the destination station to establish the connection.

For the side of the echochange connection which was parameterized as active, enable the **Slave** button.

TCP / UDP Protocol

The TCP (Transmission Control Protocol) is a secured protocol that uses checksums and acknowledgments. The UDP (User Datagram Protocol) is an unsecured protocol handled via datagram services.

Special Settings

Use PLC Header

The PLC header is used for the communication with echo devices. Use it if the data is to be transferred in blocks in the otherwise data stream-oriented TCP protocol.

Life Data Acks

If you enable this option, payload frames without content (only headers) are transmitted to keep a connection alive that is not used cyclically (heartbeat monitoring). Both communication partners must support this feature.

RFC1006

If you enable the RFC1006 option, H1 frames will be “wrapped” in a TCP/IP frame for transport. RFC 1006 is used for the communication with the Siemens S5 and S7 series communication processors. To set the TSAPs, click the **RFC1006 TSAPs** button that opens the [OSI TSAP Settings](#) dialog box.

Special Settings

This button gives access to special parameter settings for the TCP/IP connection. Usually, these parameter settings are not required. See also [Special TCP/IP Settings](#).

Editing a Connection – H1 Settings

Destination MAC

For active connections, you can enter the Ethernet address of the station in the H1 network to which you want to connect. For passive connections, you can enter 00 00 00 00 00 00 to accept any device or a specific MAC address that must match the station's address exactly. Otherwise, it will not be possible to establish a connection.

Own TSAP, Dest TSAP

The local TSAP (Transport Service Access Point) specified in the "Own TSAP" field indicates the connection address in your own system that will be used to exchange data. The remote TSAP specified in the "Dest TSAP" field indicates the connection address of the other system. In order to be able to establish the connection, the value in the "Own TSAP" field of one system must match the "Dest TSAP" value in the other system, i.e. they must match crosswise.

This condition can easily be met if you set the same value for the Own TSAP and Dest TSAP fields. TSAPs have a minimum length of 2 bytes and a maximum length of 16 bytes.

CR Parameters

For S5 PG connections to Siemens CPs (i.e. when programming an S5 PLC using a Siemens S5 CP in an H1 network via echochange), the following CR parameters must be specified:

53 35 10 01 03 0F 06 0A 20 20 20 20 20 20 20

Background information: With ISO (H1) connections, a transport connection is established. For this purpose, an active transport instance sends a CR TPDU (Connection Request Transport Protocol Data Unit) signaling that it wants to connect. This CR TPDU is used to send some parameters to the partner, such as the desired TPDU size, the TPDU format, and others. Since there is no standard CR parameter definition, please refer to the operating instructions of the destination system to find out which parameters you need to specify here, if any. If no information is available, do not enter any CR parameters.

Multicast

Multicast connections are connections that are not sent to all stations but to those that have the same multicast group (circle) number. The values range from 0 to 63. If you select a line type other than "Multicast", this value is not relevant.

Type

Here, you can specify whether your own station will actively initiate the connection attempt or will wait passively for the destination station to establish the connection. Please make sure that different values are selected on both sides of the connection.

Client (Active)	The station will actively initiate the connection attempt.
Server (Passive)	The station will wait for the destination station to establish the connection.

For the side of the echochange connection which was parameterized as active, enable the **Slave** button.

Line

In this option group, you can specify whether frames on this connection will go to all devices (Broadcast), whether a certain group of stations should be addressed (Multicast), whether a secured connection will be used (Normal) or whether the data will be transmitted over an unsecured connection (Datagram). The default setting for the line type is **Normal**. If you plan to use other line type settings, please get in touch with the network administrator.

Priority

The line priority can range from 0 (highest priority) to 4 (lowest priority). 0 and 1 are so-called express priorities, 2 and 3 are normal priorities. Priority 4 is only used on rare occasions because it causes the connection to be reestablished for each send transaction. On the other hand, if it is only used

intermittently, it puts less load on the network than the other priorities because the line will not be monitored as the connection is closed after each send transaction.

Please note that when using express priorities, the transmission will not be faster than with normal priorities. For some PLCs, however, the data will be transferred to the RAM using an interrupt if you select priority 0. This may result in a faster overall data transmission. For priorities 0 and 1, the maximum data length is 16 bytes. By default, the line priority is 3.

8.2 Connection Settings

This section describes all dialog boxes that open when you edit a connection. The number of dialog boxes varies depending on the echo device to be configured.

8.2.1 Network Protocol

Name of the Connection

Here, you can edit the connection name, if required. All characters except brackets may be used.

Expert mode

If the expert mode is disabled, the available settings that are typically not used, will be hidden. Only enable this mode if you want to make special settings. By default, this mode is off.

Transport Protocol

Here, you can select the transport protocol to be used when communicating via the Ethernet network.

Transport Protocol	
TCP/IP	The Transmission Control Protocol/Internet Protocol is capable of routing and is often used today for the communication with PLCs and field devices. For an RFC 1006 (ISO on TCP) communication, select TCP/IP.
H1	ISO H1 protocol to connect to Siemens S5 or S7 PLCs that do not support TCP/IP.

Application Protocol

Here, you can select the application protocol.

Application Protocol	PLC
Send/Receive	Used for the communication with other PLCs or devices that do not support any of the protocols listed below. Only payload data (raw data) will be transmitted, but no protocol information.
S5 AP	Communication with Siemens S5 CPs or echo devices.
S7	S7 protocol used to connect to Siemens S7-400, S7-300 or S7-200 PLCs or echo devices.
Modbus TCP	Communication with PLCs or devices supporting the Modbus TCP protocol, such as Wago, Beckhoff, Groupe Schneider, Modicon ...
CLX - Ethernet/IP	Communication with Allen-Bradley ControlLogix, CompactLogix, SoftLogix
Rockwell SLC / PLC5	Communication with Allen-Bradley PLC-5 and SLC
Melsec-Q	Communication with Mitsubishi Melsec-Q

OK

Click OK to apply your selection.

8.2.2 Network PLC Protocol

Name of the Connection

Here, you can edit the connection name, if required. All characters except brackets may be used.

Plc Protocol

Here, you can select the PLC application protocol.

Plc Protocol	PLC
Send/Receive	Used for the communication with other PLCs or devices that do not support any of the protocols listed below. Only payload data (raw data) will be transmitted, but no protocol information.
S5 AP	Communication with Siemens S5 CPs or echo devices.
S7	S7 protocol used to connect to Siemens S7-400, S7-300 or S7-200 PLCs, or echo devices
Modbus TCP	Communication with PLCs or devices supporting the Modbus TCP protocol, such as Wago, Beckhoff, Groupe Schneider, Modicon ...
CLX - Ethernet/IP	Communication with Allen-Bradley ControlLogiX, CompactLogiX, SoftLogiX
Rockwell Slc / Plc5	Communication with Allen-Bradley PLC-5 and SLC
Melsec-Q	Communication with Mitsubishi Melsec-Q

OK

Click OK to apply your selection.

8.2.3 TCP/IP Connect Parameters

In this dialog box, you can edit the TCP/IP parameters.

Name of the Connection

You can choose any connection name you like. All characters except brackets may be used.

Destination IP Address (or name)

Here, you can specify the IP address of the destination station (IP address of the PLC) or the DNS name of the destination station. If the device was configured for DNS and a DNS server is available in the network, you can also enter the symbolic name of the destination station.

For information on the structure of IP addresses, please refer to the [IP Address](#) section.

Port

Port numbers are addresses that are used on the transport layer in order to address applications. Port numbers are required for TCP connections. Ports are similar to the TSAPs used for RFC 1006 and H1 connections. Each port number is a 16-bit number in the range from 1 to 65535. To establish a connection, please note the following:

NOTE:

You can only establish a connection if the port number is identical on both sides.

[More detailed information on ports](#)

Type:

Here, you can specify whether your own station will actively initiate the connection attempt or will wait passively for the destination station to establish the connection. Please make sure that different

values are selected on both sides of the connection.

Client (Active)	The station will actively initiate the connection attempt.
Server (Passive)	The station will wait for the destination station to establish the connection.

Protocol

The TCP and UDP protocols are available for selection. TCP is a secured protocol.

PLC Header

Enable this option for the communication with echo devices.

For details on the structure of the PLC header, refer to the [PLC Header](#) section.

Life Data Acks

If you enable this option, payload frames without content (only headers) are transmitted to keep a connection alive that is not used cyclically (heartbeat monitoring). Both communication partners must support this feature. For the OPCpipe communication, it is recommended to enable this option.

RFC1006

If you enable the RFC1006 option, H1 frames will be "wrapped" in a TCP/IP frame for transport. To configure the TSAPs, click the **RFC1006 TSAPs** button.

Own TSAP, Dest TSAP

TSAPs (Transport Service Access Points) are addresses that are used on the transport layer in order to address applications. TSAPs are required for RFC 1006 connections. To connect, enter the local TSAP into the Own TSAP field and the TSAP of the communication partner into the Dest TSAP field. In this context, please note the following:

NOTE:

In order to be able to establish the connection, the value in the Own TSAP field of one system must match the Dest TSAP value in the other system, i.e. they must match crosswise.

[More detailed information on TSAPs](#)
[TSAPs for S7 Connections](#)

8.2.3.1 TCP/IP Special Settings

Use PLC Header

The PLC header can be used for communication with other Softing devices where the PLC header can also be enabled.

See also [PLC Header](#).

Life Data Acks

If you enable this option, payload frames without content are transmitted to keep a connection alive that is not used cyclically (heartbeat monitoring). Both communication partners must support this feature. For the communication with S7 PLCs, we recommend to disable this option.

Life Acks as TCP/IP Standard

By enabling this option, you can activate connection monitoring, a function that is poorly supported in many socket libraries. Life acks are frames that pass the connection status. It is recommended to enable this setting (default setting). If a WAN connection is used, you might want to disable this function for cost reasons.

Ignore TCP End Check

This setting only makes sense for Receive Direct connections.

Option enabled:

Reading in a TCP/IP frame disables its end tag. Thus, the reception buffer passes exactly the amount of data the PLC user program had requested. When data is read cyclically, this may cause problems if different data lengths were configured for the "Send Direct" and "Receive Direct" (user program) jobs.

Option disabled:

(default setting, recommended)

Excess data bytes will be ignored. This setting is only relevant to the currently edited connection (Receive Direct connection).

Life Acks with Previous Received Data

Same function as for "Life Acks as TCP/IP Standard"

If you enable this option, the data byte received last will be sent back, but with a wrong sequence number so that the other communication partner replies by sending a life ack with the correct sequence number.

Send an Ack Immediately after Received Data

It is recommended to enable this parameter if data is transmitted cyclically in a LAN. In most cases, the TCP/IP protocol collects multiple data blocks before sending an acknowledgment. If you enable this setting, the acknowledgment (ACK) is sent immediately. This increases the data rate when data blocks are sent cyclically in short intervals.

Send a Life Data Ack after the last Frame in a Sequence

This option is only available if PLC Header or RFC 1006 is used for communication.

Many socket implementations (socket libraries) do not send the IP acknowledgment frame. If you enable this function, a life data ack will be returned as an acknowledgment.

Do not Wait for Send Acknowledge

This option is only available if PLC Header or RFC 1006 is used for communication.

Option enabled:

The sending station initiates frames without waiting for the frame acknowledgment (ACK) relating to the previous frame.

Option disabled:

(default setting)

The sending station waits for the frame acknowledgment (ACK) relating to the previous frame before sending a new frame.

End Connection with FIN Instead of RST

Option enabled:

As a reply to the end connection frame (FIN), a corresponding end connection frame is sent.

Option disabled:

When a station receives an end connection frame, it resets the connection.

Use the same Port Number for both Ports

This setting sets both the source and the destination ports to the port selected in the parameterization. This disables the automatic setting of the source port to a value > 1024 in some devices (see also [TCP/IP System Settings](#)). This setting is required for the communication with CPs that do not correctly handle frame traffic via UDP.

Big Endian Format in the PLC Header

In the PLC header, the sequence number will be transmitted in the MOTOROLA format (big-endian). Usually (flag not set) the INTEL format (little-endian) is used to transmit the sequence number in the PLC header.

Change Connection Timeout

Using this setting, you can specifically change the timeout setting for connection monitoring that will end a connection when parameterizing a station remotely. This makes sense in cases where you disabled the transmission of life data acks for an Internet connection, for example. Please note that increasing this value will also increase the response time in case of connection problems (such as a broken cable).

Change Connection Memory

This setting allows you to change the memory size reserved for a connection. The minimum memory size for a connection is 1460 bytes (maximum number of payload for Ethernet connections). For a broadcast Receive connection (UDP), this setting might not be sufficient. If the partner station sends data faster than the PLC can accept it, the data will be buffered in this memory. The UDP data will only be discarded if this memory overflows.

8.2.3.2 IP Address

Basics

To establish the communication between two technical devices, each device must be capable of sending data to the other device. This data can only be received by the intended remote station if it has been addressed properly. In IP networks, this is ensured by specifying an IP address.

An OPC server is able to address a PLC directly by its IP address. Example: 192.168.1.20

It is also possible to address a PLC by its name. For this purpose, specify the name of the PLC and the corresponding IP address and enter the domain server in the TCP/IP settings of the server. For a domain name (e.g. "PLC1"), the server queries the name server to get the IP address and then addresses the PLC directly using its IP address (192.168.1.20).

IP Address

Each IP data packet starts with an IP header. This is an information section used for transmission on the IP layer. This header also includes two fields where the IP addresses of both the sender and the receiver are entered before transmitting the data packet. Routing is done on layer 3 of the OSI model, the network layer.

Structure

IPv4

The IPv4 addresses that have been used predominantly since the introduction of Internet Protocol Version 4 consist of 32 bits, i.e. 4 octets (bytes). This means that it is possible to represent $2^{32} = 4,294,967,296$ addresses. In dotted decimal notation, the four octets are written as four integers, from 0 to 255, in decimal format, separated by dots.

Example: 192.168.1.20.

IPv6 – new version with a bigger address space

Due to the rapidly increasing IP address demand, it was foreseeable that the usable address space provided by IPv4 would soon be exhausted. The IANA address pool was depleted on February 03, 2011. This was the main reason for developing the IPv6 protocol. IPv6 uses 128 bits to store addresses. This means that $2^{128} = 256^{16}$ (= 340,282,366,920,938,463,463,374,607,431,768,211,456 $\approx 3.4 \cdot 10^{38}$) addresses can be represented. This number is sufficient to provide each square millimeter of the surface of the earth with at least 665,570,793,348,866,944 (= $6.65 \cdot 10^{17}$) IP addresses.

Since a decimal representation with ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd would neither be very transparent nor handy, IPv6 addresses are usually represented in hexadecimal format. To further simplify this representation, every two address octets are grouped and separated by colons.

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7344

To further shorten the string, leading zeros in a block can be omitted.

A sequence of blocks consisting only of zeros can be replaced with :: but only once in each IPV6 address.

Example: 2001:db8:85a3::8a2e:370:7344

For IPV6, usually names are specified instead of the IP addresses.

8.2.3.3 Port

Port numbers are addresses that are used on the transport layer in order to address applications. Port numbers are required for TCP / UDP connections.

The port number is a 16 bit number from 0 to 65535.

Certain applications use fixed port numbers that have been assigned by the IANA and that are generally known. Usually, they are between 0 and 1023. They are referred to as well-known ports. The registered ports are between port 1024 and port 49151.

Application providers may register ports for their proprietary protocols.

The remaining ports (49152 through 65535) are referred to as dynamic and/or *private ports*. They can be used variably because they are not registered and do not belong to any application.

8.2.3.4 TSAP

TSAP = Transport **S**ervice **A**ccess **P**oint

On the transport layer, ISO (H1) uses so-called TSAPs to address applications. These connection endpoints are required both for ISO (H1) and RFC 1006 connections.

Parameters for ISO (H1) connections		Parameters for RFC 1006 connections	
Station A	Station B	Station A	Station B
Own TSAP A	Own TSAP B	Own TSAP A	Own TSAP B
Dest TSAP B	Dest TSAP A	Dest TSAP B	Dest TSAP A
MAC Address A	MAC Address B	IP Address A	IP Address B

In order to establish the connection, the value in the Own TSAP field of communication partner A must match the value in the Dest TSAP field of communication partner B, i.e. they must match crosswise. Accordingly, the Dest TSAP field of station A must match the Own TSAP field of station B.

Own TSAP (station A) = Dest TSAP (station B)

Dest TSAP (station A) = Own TSAP (station B)

This condition can easily be met if you set the same value for the Own TSAP and Dest TSAP fields. These values may be identical.

If multiple connections are to be established between 2 stations, the TSAPs for the individual connections be must different.

To exactly specify a connection, the combination of TSAP + MAC address (or IP address) must be unique.

Rules for entering TSAPs for S7 connections

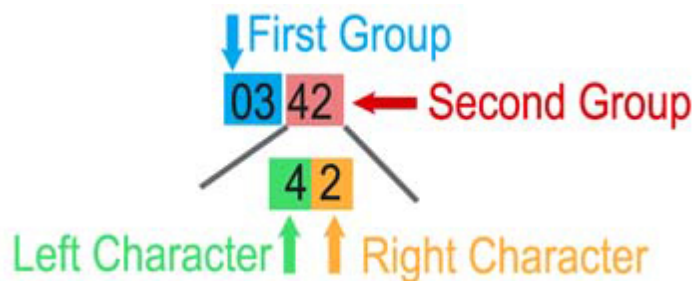
- TSAPs have a minimum length of 2 bytes and a maximum length of 8 bytes
- TSAPs can be entered as hex or ASCII characters.
- The TSAPs for S7 connections have a special meaning. See [TSAP for S7 Connections](#).

Rules for entering TSAPs for S5 connections

- TSAPs have a minimum length of 2 bytes and a maximum length of 8 bytes for TCP/IP, and 16 bytes for H1.
- TSAPs can be entered as hex or ASCII characters.
- The TSAPs for S5 connections do not have a special meaning. They are selected arbitrarily.

8.2.3.5 TSAP for S7 Connections

For non-parameterizable connections (= default connections), so-called standard TSAPs are used. For these, the following rules apply:



First group

contains device IDs for which resources are provided in the S7:

- 01: PG or PC
- 02: OS (operating or monitoring device)
- 03: Others, such as OPC server, Simatic S7 PLC...

Second group

contains the addresses of these components

Left character (bits 7....4):

Rack number multiplied by 2

Right character (bits 3...0):

CPU slot (< 16). S7-300 always uses slot 2

The standard TSAPs **MUST** be used on the PLC side (Dest TSAP field of the echo device).

The local TSAP of the echo device (Own TSAP field) may be selected freely, but should have the same format. We recommend to use 01 01 in the Own TSAP field.

Examples:

- 03 02 Communication with the S7 CPU in rack 0, slot 2
- 03 43 Communication with the S7 CPU in rack 2, slot 3
- 03 2E Communication with the S7 CPU in rack 1, slot 14

NOTE:

To enter the binary standard TSAPs, use the HEX field (left field).

S7-200

The S7-200 is usually addressed with the TSAP 10 00 (binary). The own TSAP is set to 10 00 by default.

S7-300, S7-400

The S7-300 and 400 is usually addressed with the TSAP 03 02 (binary). The own TSAP is set to 01 01 by default.

S7-1200, S7-1500

The S7-1200 and 1500 is usually addressed with the TSAP 02 01 (binary). The own TSAP is set to 01 01 by default.

8.2.3.6 PLC Header

The data-stream oriented TCP/IP protocol is capable of grouping multiple short data units into a larger unit. This increases the data throughput of the network. However, it requires a header for the protocol above TCP. This corresponds to the procedure common in other protocols (FTP, HTTP).

For this purpose, the 8-byte INAT PLC header was developed.

Only use the PLC header if the communication partner supports it. Otherwise, the connection will fail!

PLC Header Format

Byte no.	Meaning
Byte 0	0x4d 'M'
Byte 1	0x4b 'K'
Byte 2***	Number of payload bytes following the header (LSB*).
Byte 3***	Number of payload bytes following the header (MSB**).
Byte 4***	Bit 0 = 1, if other frames follow
Byte 5***	0
Byte 6***	SeqNo. LSB*
Byte 7***	SeqNo. MSB**
Datalen in bytes	Payload

*LSB: Least (Low er) significant byte

**MSB: Most significant byte

*** Bytes 2 / 3, bytes 4 / 5 and bytes 6 / 7 together form the "short" data value. They are represented in the INTEL format

Acknowledges

If DataLen equals 0, the frame does not contain payload, but a life data ack. Data acknowledgments allow connection monitoring, a feature that TCP/IP, as a wide area protocol, does not include inherently. The default times for connection monitoring are the same as for the H1 protocol. This makes the S5 TCP/IP system H1-compatible from the PLC or PC perspective.

Sequence Numbers

Bytes 6 and 7 contain a sequence number that is 0 when establishing the connection and will be incremented by 1 each time payload is sent. This frame counter additionally secures the data transmission. If live data acks are sent, the sequence numbers are not incremented and Datalen is 0.

Fetch and Write Connections

For Fetch and Write jobs, the first 16 data bytes at the start of a job correspond to the SINEC AP header. The SINEC AP header is also used for H1 communication.

Sending / Receiving Data

When sending data over the S5 TCP/IP, a frame can include a maximum payload of 512 bytes. This maximum value is preset by the default tile block size. Received data packets can contain up to 1460 bytes. These limits are monitored automatically by the TCP/IP protocol so that no monitoring is required on the user side.

Transmission without Frame Header

The header at the beginning of the frame may be disabled. In this case, the application programs on both sides are responsible for monitoring. In this context, please note the following:

1. In particular with Send Direct and Receive Direct jobs, certain time limits until frame receipt must not be exceeded. If these time limit were ignored, the internal buffers would be full, e.g. due to requests. Thus, it would be impossible to synchronize request and response.
2. A certain blocked data transmission mechanism must be used so that it is possible to recognize the end of payload.
3. On the recipient side, you need to make sure that the frames from the reception buffer have been read before the partner station sends the next frame.

It is mandatory to set up connection monitoring in the application program.

8.2.4 H1 Connect Parameters

In this dialog box, you can edit the H1 parameters.

Name of the Connection

You can choose any connection name you like. All characters except brackets may be used.

Adapter

Here, you can specify the number of the Ethernet adapter used to establish the H1 connection.

Destination MAC

Each Ethernet station is addressed using a unique MAC address (also referred to as Ethernet address or hardware address). Enter the Ethernet address of the destination station here. The destination address consists of 6 bytes (to be entered in hexadecimal notation).

NOTE:

In a single network, each station must have a unique Ethernet address.

Own TSAP, Dest TSAP

TSAPs (Transport Service Access Points) are addresses that are used on the transport layer in order to address applications. To connect, enter the local TSAP into the Own TSAP field and the TSAP of the communication partner into the Dest TSAP field. In this context, please note the following:

NOTE:

In order to be able to establish the connection, the value in the Own TSAP field of one system must match the Dest TSAP value in the other system, i.e. they must match crosswise.

[More detailed information on TSAPs
TSAPs for S7 Connections](#)

CR Parameters

With ISO (H1) connections, a transport connection is established. For this purpose, an active transport instance sends a CR TPDU (Connection Request Transport Protocol Data Unit) signaling that it wants to connect. This CR TPDU is used to send some parameters to the partner, such as the desired TPDU size, the TPDU format, and others. Since there is no standard CR parameter definition, please refer to the operating instructions of the destination system to find out which parameters you need to specify here, if any. If no information is available, do not enter any CR parameters.

Type (active / passive)

Here, you can specify whether your own station will actively initiate the connection attempt or wait passively for the partner station to establish the connection. Please make sure that different values are selected on both sides of the connection. Usually, the PC will be parameterized as active. This is the default.

Protocol

Using this option, you can specify whether frames on this connection will go to all devices (Broadcast), whether a certain group of stations should be addressed (Multicast), whether a secured connection will be used (Normal) or whether the data will be transmitted via an unsecured connection (Datagram). Usually, you select "Normal" here.

Priority

The line priority can range from 0 (highest priority) to 4 (lowest priority). 0 and 1 are so-called express priorities, 2 and 3 are normal priorities. Priority 4 is only used on rare occasions because it causes the connection to be reestablished for each send transaction. On the other hand, if it is only used intermittently, it puts less load on the network than the other priorities because the line will not be monitored (the connection is closed after each send transaction). Please note that when using express priorities, the transmission will not be faster than with normal priorities. For some PLCs, however, the data will be transferred to the RAM using an interrupt if you select priority 0. This may result in a faster overall data transmission. For priorities 0 and 1, the maximum data length is 16 bytes. Usually, Prio 3 is used here.

8.2.5 S7 Protocol Settings

Depending on the PLC family used, select **S7 1200/1500**, **S7 300/400** or **S7 200**.

Changing the PLC family updates the TSAP settings with default values, as described in [TSAP for S7 Connections](#).

The Use Short TPDU setting is required for some S7-compatible PLCs. Only use this option if the data exchange with the PLC does not work properly. This option may slow the communication.

8.2.6 echocollect Connection: Modbus Protocol

In this dialog box, you can edit the specific parameters for the connection to Modbus PLCs.

	Description	Default
Name of the Connection	This field displays the connection name which can be changed here.	
Slave address	The slave address entered here will be transmitted in the Modbus frame.	1
Start Address 0	The starting address in the frame will be transmitted as specified.	Yes
Start Address 1	Some Modbus devices expect a starting address in the frame that is 1 less than the one you entered. The first address is 1.	No
Use Byte Swap	Swaps the bytes within a word	Off
Use Word Swap	Swaps the words within a double word (32 bits)	Off
Use Write Single Coil (05)	For writes, the Modbus opcode "Write Single Coil 05" is used instead of "Write Multiple Coils 15".	Off
Use Write Single Register (06)	For writes, the Modbus opcode "Write Single Register 06" is used instead of "Write Multiple Registers 16".	Off
User Item Unit ID	The slave address will be indicated in the item syntax. Example: Id2.R2 For more details, see Modbus Item Syntax	1

8.2.7 echochange Connection: CLX Protocol

In this dialog box, you can edit the specific parameters for a connection to Allen-Bradley ControlLogiX PLCs.

Name of the Connection

Here, you can edit the connection name.

CPU Slot

Here, you can specify the ControlLogiX CPU slot.

8.2.8 echochange Connection: SLC / PLC-5 Protocol

In this dialog box, you can edit the specific parameters for a connection to Allen-Bradley PLC-5 and SLC PLCs.

Name of the Connection

Here, you can edit the connection name.

CPU Slot

Here, you can specify the PLC-5 or SLC CPU slot.

8.2.9 Melsec-Q Protocol

In this dialog box, you can edit the specific parameters for a connection to Mitsubishi Melsec-Q PLCs.

You need to set these parameters if a Mitsubishi Net has been set up and the hardware supports it.

	Description	Hex	Decimal
Destination Module	Network address	0x3FF	1023
Monitor Timer	Monitors the time within which the response should be received.	0x100	256
Network Number	Network ID in the hardware configuration of the programming software	0	0
PLC Number	Another intermediate PLC number	0xFF	255
PC Number	Only relevant if a permission management system has been set up, allowing or denying PC access.	0xFF	255
Destination Station	Module address of another module in a PLC.	0	0

The effect of these values depends on the hardware used.

8.2.10 Mail Connect Parameters

In this dialog box, you can edit the e-mail parameters.

For each e-mail connection, you need to specify the IP address or domain name of the mail server. For details on the parameters, please ask your mail operator or your e-mail provider or look them up in your e-mail contract.

Connection Name

You can choose any connection name you like. All characters except brackets may be used.

IP Settings

Destination IP Address (or name)

Here, you can specify the IP address of the destination station (IP address of the PLC) or the DNS name of the destination station, i.e. of the mail server. If the device was configured for DNS and a DNS server is available in the network, you can also enter the symbolic name of the destination station.

For information on the structure of IP addresses, please refer to the [IP Address](#) section.

Port

The default mail sending method (SMTP) often uses port 25.

Sender Address

Here, you can specify the address for replies.

Authentication

Depending on the mail server, login may be required.

Username and Password

These are the login data.

Login type

Select Auto Select or, if known, please specify.

The following protocols can be selected:

- PLAIN

- LOGIN
- CRAM-MD5

8.3 Edit Connection

Name of the Connection

This field displays the connection name which can be changed here.

Connection Active

Shows whether the connection is active or not. If not, you cannot register items and there will be no connection to the PLC. This feature allows you to disable a connection temporarily without deleting it so that you can re-enable it later without having to enter all parameters again.

Write allowed

For some connections, you can disable the Write function.

Poll interval ... ms

Here, you can specify the poll rate the device will use for reading data from the PLC.

Buttons

Depending on the connection type, you can edit further parameters.

Button	Dialog box that opens
Network Protocol	Network PLC Protocol
Network Parameters	TCP/IP Connect Parameters or H1 Connect Parameters or Mail Connect Parameters
Protocol Parameters	Opens the dialog box for protocol-specific parameters.
Save and Online Test	The data you have entered is saved in the device and then tested. For this purpose, the device will log on to the server.

The number of available options depends on the type of connection.

8.4 Copy Connection

It is possible to copy a connection. All parameters (except the connection name) of the highlighted connection will be copied. Make sure to specify the new connection name before saving the connection. Then, the connection will be displayed in the [Connections](#) list.

8.5 Delete Connection

The highlighted connection will be deleted. This process cannot be undone!
As an alternative to deleting, you can disable a connection using the [Switch on/off](#) option.

8.6 Disable Connection

To disable a connection, do one of the following:

- Menu: **Connection > Switch on/off**
- Highlight the connection, **right-click** and select **Switch on/off**

In the [Connections](#) list, the word (**off**) is displayed after the type.

You can disable a connection without losing the connection parameters. Later, you can re-enable the connection using the same parameters as before. By default, connections are enabled.



Chapter 9

Main Menu

9 Main Menu

The menu provides the following options:

- [File](#)
- [Connection](#)
- [Diagnostics](#)
- [Station](#)
- [Settings](#)
- [Help](#)

9.1 File

The File menu provides the following functions:

Load configuration from file

This menu item is used for loading the parameter file to the device.

- Click this menu item to open the Windows dialog box: Open File...
- Select the desired file and click the **Open** button.
- A new dialog box appears: Copy from File into the Device
- Here you can choose if you want to overwrite the MAC address, the IP address and the IP settings in the device.
- When you click the **OK** button, the parameters are irreversibly overwritten in the device.

Store configuration to file

Using this menu item, you can save all the device's parameters to a parameter file.

Store configuration to SD-Card

Using this menu item, you can save all the device's parameters to a sd-card in the device.

Attention: The configuration stored on the SD-card will replace the current configuration when the device restarts.

Refresh

Reestablishes the configuration connection to the device. If a password has been set, the password needs to be re-entered to allow editing.

This function is particularly useful for serial links. It allows rereading the list of connections from the module. This is necessary, for example, if the connection cable is plugged into a different module. The Connections list is cleared and rebuilt with the current connections.

Print

For documentation purposes, you can output a list of the connections.
The list is printed on the system's default printer.

Close Window

Closes the configuration of the device and switches to the [Configuration](#) window.

9.2 Connection

This menu provides the following options:

Switch on/off

You can disable a connection if it is not intended for communication. Thus, it is possible to disable it temporarily without having to delete and redefine it. See [Disable Connection](#).
To use this function, master access is required.

New Connection

Here you can enter a new connection. The [New Connection](#) dialog box appears. First, select the connection name and type. Then enter the required parameters.

When you save the connection, the connection parameters take effect immediately.

To use this function, master access is required.

Edit Connection

Here you can edit the parameters of the selected connection. The [Edit Connection](#) dialog box appears.

To use this function, master access is required.

Copy Connection

You can copy the connection. The [Copy Connection](#) dialog box appears. Before clicking Save, please keep in mind to rename the copied connection.

To use this function, master access is required.

Delete Connection

The connection is deleted after you confirm the prompt in the [Delete Connection](#) dialog box.

To use this function, master access is required.

9.3 Diagnostics

This menu provides the following options:

Show one Connection

The connection selected in the Connections list can be monitored. The [Connection Diagnostics](#) dialog box appears.

Signal Device

When you click this menu item, all the LEDs will blink for about 2-3 seconds. This shows you which device the NetCon is connected to.

IP/NetStat

Opens the [IP/NetStat](#) dialog box, which displays an overview of the connections entered in the runtime system.

Start Capture Network

If the device is equipped with a SD-card, then this menu entry starts the capture of the data traffic at both Ethernet interfaces. The capture ends after ca. 25 hours, the stop command or when the device restarts. If there is already one capture running, then no additional is started.

Stop Capture Network

This menu entry terminates a previously started capture of network traffic.

Logger

Opens the [Logger](#) window where the recorded messages are displayed.

This window can be opened in parallel to the software application. You can continue to configure and use the software while the Logger window is open.

Logger Settings

Opens the [Logger Settings](#) dialog box. There you can select the events that will be recorded by the Logger.

The file and memory settings for the Logger are made under Settings in the Logger window.

Free place on sd-card

If a memory card is inserted, the dialog box shows the size of the memory card and the free memory space (version 7.0 and higher).

9.3.1 echochange Connection Diagnostics

The dialog box shows the online diagnostics for an echochange connection.

The diagnostics window is divided into two parts:

- the left side or passive side
- the right side or active side

The number of transmitted frames and bytes as well as the number of received frames and bytes are

shown for each side.

In addition, the window shows you the number of disconnects and the connection status.

The PLC status indicates whether communication with the PLC is OK or whether problems have occurred.

The contents are cyclically refreshed.

9.3.2 TCP/IP Stati

The dialog box displays a list of the TCP/IP connections and provides diagnostics.

The individual columns show details about the configuration and status.

The contents are cyclically refreshed.

To scroll through the list, use the “**Page...**” buttons.

9.3.3 Logger

Here you can select different options to specify the information you want to log. The log data is displayed in the Logger window.

Error

Error	
Error	Log all types of errors in the Logger, except PLC errors.
PLC Element Error	If an area in the PLC does not exist or if a requested area is too small, a corresponding entry is made in the Logger. This also applies to all other errors generated by the PLC.
SQL Error	Logs all types of SQL connection errors in the Logger.
SQL Error Log File	The file name for logging SQL errors

Status

The reparameterization of connections and the login for reparameterization are recorded by the Logger.

Status	
Connection Parameterization	An entry is logged whenever connection parameters are changed and saved.
Connection Status Change	An entry is logged whenever the status of a connection changes.

PLC Data

The parameters of the respective PLC requests from the server to the PLC are recorded by the Logger.

PLC data	
Send	Content of the frames in write direction. The area that is written to is logged.
Send Data	The data content of the frames in write direction is logged.
Receive	Content of the frames in read direction. The area that is read is logged.
Receive Data	The data content of the frames in read direction is logged.

SQL Data

The requests and data of the Collect destination connection are recorded by the Logger. This can be

a SQL connection, but it can also be of any other type. The direction is selectable.

SQL data	
Send	Content of the frames in write direction. The area that is written to is logged.
Send Data	The data content of the frames in write direction is logged.
Receive	Content of the frames in read direction. The area that is read is logged.
Receive Data	The data content of the frames in read direction is logged.

9.3.4 Logger Settings

In the Logger Settings dialog box, you can choose to keep the log data only temporarily in the RAM or save it to a log file. For this, you can specify the logging intervals as well as the directory and the file to which the log data will be saved.

Cache Size

Specify how much RAM you want to allocate to data logging. The cache acts as a ring buffer. If you increase the cache size, more entries will be buffered in the RAM.

Use File Logging

Select this check box if you also want to save the data to a file.

File Settings

Maximum Disk Space

Specifies how much disk space may be occupied by log data. When the value you set here is reached, the old files are deleted. This setting serves to prevent the log files from taking up all the hard disk space.

NOTE:

When the selected setting is reached, the Logger will automatically delete files from the directory without a confirmation prompt.

Directory

Specifies the directory in which you want to save the log files.

File Prefix

The file name is made up of the prefix followed by a sequential number and the date and time.

Save Every ...

Specifies the interval at which the file will be saved if the cache in the RAM has not yet completed one loop. When the ring buffer is full and the write interval time has not been reached, the ring buffer loops around more quickly and the old data in the ring buffer is being overwritten.

NOTE:

When you save to a flash drive, the number of writes is limited. The fewer writes, the longer the lifetime of the flash drive will be.

New File Every ...

Specifies when a new file will be started. This facilitates the evaluation.

File Name Example

The display field shows an example of a file. Here you can see where the log files are located and what the file names look like.

9.3.5 Using the Diagnostic Text Output System

In the diagnostic text window, you can view and monitor the information you need for diagnostics. When you open the window, the system's diagnostics memory is read, displayed and deleted. To display more data, click **"New read"** repeatedly. This clears the old window contents.

For a continuous display, click **"Continuous Debug in Window"**. In this case, additional diagnostic data is appended to the existing contents.

To create a file, click **"In File"**. This writes the current window contents to a file.

The **"Cont. Debug in File"** button creates a plain text file that will grow in length.

Using the **"Cont. Color Debug in File"** button, you can create a special-format file that will grow in length. You can load these files again as you need them (the file icon opens the file selection). These files also contain the color information and the current timestamps for later evaluation.

You can filter individual contents during logging by selecting the relevant check boxes. The filter will only be enabled if the **"Direct"** check box is also selected.

To add timestamps to the files, select the **Timestamp** check box.

If you select the **Html** check box and write data to the file, the file is created in the format that can be viewed with a web browser. Please note that some web browsers may not be able to process very large HTML files.

9.4 Station

This menu provides the following options:

Station Password

Opens the [Change the Password](#) dialog box for creating, deleting or entering a password. Use this dialog box to specify whether a user is allowed to modify the parameters after the program start, or if the user has to log on with the password first.

Own Station 1

Opens the [Station Parameters](#) dialog box for displaying and entering the station parameters for the first network adapter.

Own Station 2

Opens the [Station Parameters](#) dialog box for displaying and entering the station parameters for the second network adapter.

SSH

Opens the [Device SSH Settings](#) dialog box for displaying and entering the SSH parameters (Secure Shell, network protocol for encrypted connections).

SSH allows you to establish an encrypted VPN connection to the device via the Internet. It also offers the possibility to reach the device through a firewall, usually via TCP/IP port 22.

Set Original MAC Addresses

Using this menu item, a MAC address that may have been changed can be reset to the hardware address. Please keep in mind, however, that in other devices communicating with this echo device the communication will be interrupted until the ARP cache is updated or manually deleted.

On a Windows PC, this is done with the command:

```
arp -d *
```

9.4.1 Station Password

In this dialog box, you can set or delete the password. It also appears when a user logs on. You can protect the configuration from modification by assigning a password.

To do this, open the dialog box by selecting the **Station** menu and clicking **Station Password**. Enter the password and repeat it in the Retype Password field. NetCon is now logged on and you can

modify the configuration.

9.4.2 Station Parameters

This dialog box shows details of the local station.

Some values cannot be changed. The dialog box displays the determined information.

Station Name

You can freely select a name for the device. This name will be displayed when you run a station scan in the [Select a Station in Your Network](#) dialog box.

Station Password

If this dialog has been opened from the station search, then the input field for the password input appears. If a password has been assigned to the station, then this password needs to be entered here. In order to change the ip-address , etc. Otherwise this field must remain empty.

MAC Address

The MAC address of the network adapter. Every station in the Ethernet network has a unique Ethernet address. This address can be changed. To restore the original setting after a change to the MAC address, select **Station – Set Original MAC Addresses**.

Use DHCP

Here you can enable automatic configuration via a DHCP server. This check box should only be selected if a DHCP server exists in the local network.

IP Address

This entry specifies the station's address when the TCP/IP protocol is used, see [IP Addresses](#).

Subnet Mask

This parameter determines which station requests to the active network are allowed to pass. Addresses in which the masked parts differ are transmitted to the routers.

Domain Name

The domain name is used for symbolic requests in which no domain has been explicitly specified. This is usually the case with names that have no dot.

DNS Addresses

These addresses specify the servers that resolve the symbolic Internet names to the IP number addresses in the network.

Router Addresses

Routers are used if the station should also communicate with stations located outside its own network. The IP-Address of the router must be within the own local network, because the router connects this local network with other networks or the internet.

We distinguish between dedicated routers and the default gateway:

- For dedicated routers the IP-address of the router within the local network, the net-address and subnet mask of the destination network needs to be provided.
- For the standard gateway only the IP-address needs to be provided. In the usual case, there should be only one default gateway.

Routing examples

Assume that the device has the following configuration:

- IPv4 Address of the 1st interface: 10.123.45.78
- Subnet mask of the 1st interface: 255.0.0.0
- Default gateway of the 1st interface: 10.0.0.1
- IPv4 Address of the 2nd interface: 192.168.1.2
- Subnet mask of the 2nd interface: 255.255.255.0
- Default gateway of the 2nd interface: not set
- Dedicated route at the 2nd interface: Address of the router: 192.168.1.1, net: 192.168.0.0, subnet mask: 255.255.0.0

And the device should reach the following destination addresses over IPv4: ntp.pool.org within the internet, 10.0.0.2, 192.168.1.3 und 192.168.47.11.

These destination could be reached as follows:

1. ntp.pool.org should be resolved to an address within the internet. The device attempts to reach this destination through the default gateway 10.0.0.1 at the 1st interface.
2. Destination 10.0.0.2 is within the local net of the 1st interface. Therefore it could be reached directly.
3. Destination 192.168.1.3 is within the local net of the 2nd interface. Therefore it could be reached directly.
4. Destination 192.168.47.11 is not within any of the two local networks. But it could be reached through the router 192.168.1.1 of the 2nd interface.

9.4.3 Device SSH Settings

The dialog box allows displaying and entering the SSH parameters (Secure Shell, network protocol for encrypted connections).

SSH allows you to establish an encrypted VPN connection to the device via the Internet. It also offers the possibility to reach the device through a firewall, usually via TCP/IP port 22.

In this way, you can access a connected PLC or parameterize the device.

SSH Base Settings

Use SSH

Enables access using SSH.

SSH Port

Port number at which the device is accessed via the SSH connection.

Encryption Bits

Specifies the number of bits used for encryption. Normally 1024 bits are used.

The following rule applies: The higher the number of bits, the more secure the connection – and the slower the line speed. The default value of 1024 suits most purposes.

SSH User Accounts

Displays a list of authorized users.

At least one user and one password have to be entered here. The minimum length of the password is 6 characters.

New User, Delete User

Allows managing the user entries.

Edit User

Opens the Edit User dialog box where you can enter the user data.

NOTE:

SSH encryption must be enabled by the database administrator.

SSH Certificates

Currently not used.

9.5 Settings

This menu provides the following options:

H1 System Values

Opens the [H1 System Settings](#) dialog box where you can edit the H1 settings.

IP System Values

Opens the [TCP/IP System Settings](#) dialog box where you can edit the TCP/IP settings.

Delete Connections and Tables

Deletes all user entries and settings except for the station parameters in the [Station Parameters](#) dialog box for the existing network adapters. The device is reset but remains accessible via NetCon.

PLC System Values

Opens the [Device System Settings](#) dialog box where you can edit the PLC system settings.

Clock Settings

Opens the [Clock Settings](#) dialog box where you can change the clock settings.

PLC Convert Table

Opens the [PLC Conversion Table](#) dialog box where you can display and modify the echochange data allocation table. This table describes how the protocol requests from one side are forwarded on the other side.

Service Settings

Opens the [Device Service Settings](#) dialog box where you can edit the services as well as the access permissions for the services.

Firmware Update

This menu item is used for loading a firmware file to the device. If an update is required, you will receive a new firmware version from Softing Industrial Networks GmbH. For compatibility the major and minor version number of the Firmware and the NetCon should match. See Firmwareupdate of echo devices.

Reboot

Use this menu item to reboot the device. All connections are closed.

Parameter in Flash

Here you can transfer the parameter settings to an external memory card inserted in the device. When the transfer is complete, the memory card should be removed and kept in a safe place. If necessary, you can then insert the card into the device and reboot it. The parameters are then loaded to the device.

9.5.1 H1 System Settings

The H1 system parameters represent the operating parameters of layer 4. The settings should only be changed in special cases. Please contact your system administrator before you make any changes to these settings.

The dialog box provides the following settings.

Connect Request Time Interval (fast)

This parameter specifies the time interval between two Connect Request attempts if the connection cannot be established. After the maximum number of fast CRs is reached, the slow CR time interval will be used.

Connect Request Time Interval (slow)

Here you specify the time interval between two Connect Request attempts if the connection cannot be established and the maximum number of fast CRs has been exceeded.

Number of Fast CRs

Here you define after how many failed Connect Request attempts the time interval between the attempts is increased so that the attempts are performed less frequently. This reduces the network load caused by unsuccessful attempts to establish connections. Whenever an established connection is closed, the system tries to reconnect.

Time Between Send Retries

Time interval after which a frame is retransmitted.

Time Until Connection Is Lost

Specifies the time after which a connection error is detected if the partner station no longer sends any frames. When this timeout expires, the connection has to be reestablished.

Timeout Between the Acknowledges

Specifies the time after which an acknowledgment is to be sent if no data traffic is taking place.

Maximum Credit

This parameter specifies how many frames the connection can buffer. With H1, this is usually 1.

Maximum Frame Length

Specifies the maximum length of a frame. The value is a power of two.

Class Options

The description for this parameter is provided in the OSI standard specification sheets.

Protocol Options

The description for this parameter is provided in the OSI standard specification sheets.

Timeout Wait

Not relevant for echo devices. (-1 is forever or until finished).

OK

The dialog box is closed and the data is applied.

Cancel

The dialog box is closed without applying the data.

Default

Resets all the input fields to the defaults.

9.5.2 TCP/IP System Settings

The TCP/IP system parameters represent the operating parameters in the TCP/IP core. The settings should only be changed in special cases. Please contact your system administrator before you make any changes to the settings.

Connect Request Time Interval (fast)

Short time interval between two CRs (Connect Requests).

The short time interval is used until the value set under Number of Fast CRs is reached.

Connect Request Time Interval (slow)

Long time interval between two CRs (Connect Requests). The long time interval is used after the value set under Number of Fast CRs was reached. This reduces the frequency of Connect Request attempts.

Number of Fast CRs

Specifies after how many failed Connect Request attempts the time interval between the attempts is increased so that the attempts are performed less frequently. As soon as the value specified here is reached, the Connect Request Time Interval (slow) is used between two Connect Request attempts. This allows reducing the network load.

Time Until Connection Is Lost

Time without data communication after which the connection is considered broken. Since TCP/IP as a WAN protocol normally does not use life acks, the connection is also broken if no data has been

transmitted during the specified time.

Timeout Between the Acknowledges

Specifies the time after which an acknowledgment (ACK) is to be sent if no data traffic is taking place. For TCP/IP this value can be 0, which disables the life acks.

Time of the Acknowledge After Received Data

Received data is acknowledged after this time if no data frame has been returned. The shorter the time, the faster the data traffic, which is only in one direction.

Number of Retries

Specifies the number of retransmissions if no acknowledgment arrives from the receiver (confirming receipt of the data). When the specified number is reached, the connection is considered broken.

Timeout of an ARP Entry

Specifies how long entries in the ARP cache are valid if they have not been accessed. If an entry in the ARP cache is not accessed for a certain period of time, it will be removed. This behavior ensures that changes in the network can be detected and reflected by sending new ARP requests.

Timeout for DNS

Specifies the maximum time for converting a name to an IP address. When the timeout expires, the DNS request is retransmitted.

Time Between Two Life Data Acks

Time without data communication after which the connection is considered broken. Since TCP/IP as a WAN protocol normally does not use life data acks, the connection is also broken if no data has been transmitted during the specified time.

Maximum Frame Length

TPDU = Transport Protocol Data Unit

Specifies the maximum number of bytes that can be transmitted in a frame.

Start Number of the TCP Port Pool

Used for TCP connections in which a port has not been specified. If a port is parameterized as 0, a port number is generated. The numbers that are used start at the value given here.

Start Number of the UDP Port Pool

Used for UDP connections in which a port has not been specified. If a port is parameterized as 0, a port number is generated. The numbers that are used start at the value given here.

Factor for Timeout If No Header Is Used

All the timeouts given above are multiplied by this factor if no PLC header has been selected.

Factor for Timeout If RFC1006 Is Used

All the timeouts given above are multiplied by this factor if the RFC 1006 header has been selected.

Allow ICMP Broadcast

By default, echo modules ignore smurph attacks from the Internet (in other words, they do not reply). If ICMP broadcast frames are to be used in the LAN of a plant, you can select this check box to cause the echo module to reply.

Default

Resets all the input fields to the defaults.

9.5.3 Device System Settings

Any changes to these parameters will take effect immediately.

Free bytes of the S5 AP Ack aren't mirrored

In the acknowledgment frame of the S5 AP header, not all the bytes are relevant. With this check box, you can choose whether you want these bytes to be filled with the bytes of the request, or set to 0.

Reset Diagnostics

Resets all internal diagnostic counters to 0.

9.5.4 Diagnose of Default Connections

If you are using default connections, you can diagnose them here. Up to 7 default connections can be used (2 x port 990, 5 x port 991). Each default connection is displayed with the following parameters:

Type

Always IP because default connections are only available for TCP/IP.

Name of the Connection

The connection name is numbered from Default 1 to Default 7.

Job

The job numbers are assigned automatically.

Anzw

The display word in hexadecimal code

Anzw Text

The display word in plain text

Network

Displays the current status of the connection. The following messages can be displayed: OK, Wait for ACK, No connection

Send + Rec

Here the number of transmitted and/or received frames is displayed.

9.5.5 Clock Settings

How to Set the Clock

To set the internal clock, enter the hour, minute, second, day, month and year. Then click the Set button to apply the displayed values to the echo device. The day of the week is then shown automatically. The clock continues to run as long as no entries are made. Entries stop the refreshing of the display. If NTP is selected, the clock is set automatically.

Time Location

Select the correct time zone.

NTP Settings

Use NTP Service

Select this check box to obtain the time settings over the Internet.

Many institutions provide master clocks based on UTC time (Coordinated Universal Time). To provide the local time, select the corresponding time zone. In this case, the clock will also be adjusted to daylight saving time and take into account the leap seconds that occur occasionally at the end of a year.

URL

Here you enter the address of the NTP server.

Poll Time in Minutes

The interval at which time will be synchronized. The clock is often synchronized once an hour – 60 minutes.

9.5.6 PLC Conversion Table

The PLC protocol assignment list defines how a PLC request is routed via the second connection to the destination connection.

The list box provides a list of all entries.

When you select an entry, the upper section of the dialog box automatically displays the associated information.

You can now edit the Source and Destination fields.

Then click the **Update ->** button to update the selected entry.

With **Add ->**, you can add a new entry with the specified settings to the list.

The **<- Delete** button deletes the selected entry.

If you click **Clear Table**, all entries will be deleted without confirmation prompt.

Any changes you make will only be applied after you close the dialog box with OK.

Procedure

If a request with a corresponding protocol arrives at a specified address, the data is routed over the second connection set to the respective protocol and forwarded to the destination address. Frames with requests that do not match the specified PLC protocol and the other settings are ignored.

If no matching entry is found, the PLC request is replied with **"Element not found"**.

If you set a **CLX** connection as the destination, use **Browse** to select the name online from the PLC. The associated data type is determined automatically. This procedure should be used for CLX in order to avoid incorrect settings.

The entries refer to the selected protocol and apply to all connections with that protocol.

Input Fields

The individual input fields have the following meanings:

Source	The parameters and the address of the passive source connection (left side).
Destination	The parameters and the address of the active destination connection (right side).
PLC Protocol	Specifies the PLC protocol of the connection.
Element	Specifies the data area of the connection. The list depends on the selected protocol.
Block	The data block number for S5 and S7.
Address	The starting address
Length	Number of elements of the selected type.
Typ	Data type; this parameter must be correctly set for CLX connections.
Destination Symbol	For CLX connections, a symbolic destination address must be entered. The -> Browse button allows browsing the online PLC
-> Browse	Browses a CLX PLC online

Only one DBx per Connection is allowed in the PLC conversion table.

9.5.7 Device Service Settings

In this dialog box, you can enable different services and edit the associated parameters.

Web Settings

Use Web Server

Enable or disable the web server in the device.

FTP Web User Name:/FTP Web Password:

This user account is only used for FTP access to the web pages of the web server in the echo device. Using this account, you can upload web pages and contents to the device for display in the web server. In addition, you can organize and delete web pages and contents. If no user and password is specified, FTP access to the web pages is denied.

Used Items

This counter shows the number of used and available items for visualization. The counter starts from zero at the boot of the device and counts every items that was in use on any website loaded since the start. If websites used identical items, those are only counted once. Click on update button to refresh the number; this will reset the counter to the number of items that are currently in use.

Memory Card FTP Account

To access the SD card in the device from an FTP client, you can enter the FTP user and password here. This account provides access to log files created by the Logger as well as to Collect frame tables.

9.5.8 Reboot

With the **Reboot** menu item you can reboot the device via software (warm start). When doing so, you may be prompted for a reboot password. The reboot password is determined in the following way:

- The station password defined in the [Station Password](#) dialog box.

In devices with a version earlier than V7.0, the reboot password is determined in the following way:

- Open the **Help** menu and select **Versions**.
- In the Versions dialog box, the value **Version Param Server** is used as the password in the following format: xyyzzz.
- Example: 3.08, Build 22 ==> the password is 308022

During rebooting, all connections are closed and then reestablished.

9.6 Help

This menu provides the following options:

Help

Starts the [Help Overview](#) of the online help.

Versions

Opens the [Versions](#) dialog box displaying the versions of all the program modules of the device.

Device Licenses

Opens the [License Overview](#) dialog box where you can view and edit the device licenses.

About

Opens the [About](#) dialog box displaying the manufacturer and the versions of the NetCon software.

9.6.1 Versions

The dialog box shows the software versions of the echo device and all of its individual components.

Using the -> **Clipboard** button, you can copy the content to the clipboard and paste it into an e-mail or word processing application for further processing.

You will need these version details if you have any **questions** or require **support** for the product. In addition, you will need the hardware versions from the [Hardware Versions](#) dialog box and the NetCon versions from the [About](#) dialog box.

9.6.1.1 Hardware Versions

The dialog box shows the hardware versions of the echo device and all of its individual components.

Using the -> **Clipboard** button, you can copy the content to the clipboard and paste it into an e-mail or word processing application for further processing.

You will need these version details if you have any **questions** or require **support** for the product. In addition, you will need the software versions from the [Versions](#) dialog box and the NetCon versions from the [About](#) dialog box.

9.6.2 About

The dialog box shows the copyright, the versions of the NetCon configuration software, and the contact details for questions, suggestions or support.

You will need these version details if you have any **questions** or require **support** for the product. In addition, you will need the hardware versions from the [Hardware Versions](#) dialog box and the software versions from the [Versions](#) dialog box.

[License Conditions](#)

9.6.3 License Overview

Displays a list of the available modules with order number and license status. A function can be enabled by entering an activation code. This allows adding functionality to the device without having to return it to the manufacturer.

Show License

To edit an entry, double-click it or use the button. The [Licenses](#) dialog box appears. To edit licenses, master access is required.

Refresh List

This button reads the license status from the device and refreshes the displayed status.

9.6.4 Licenses

In the dialog box, you can enable the functionality of a software component provided in the device.

Please follow the steps below to license the product:

- Enter the **Company Name** and the **Customer Name** to make the license unique.
- The **Authorisation Code** is not relevant to echo devices. For OPC servers, please enter the authorization code that is given in the delivery note.
- Then click the -> **Clipboard** button. The data needed for requesting the license is copied to the clipboard and can be pasted into an e-mail or word processing application. For example:

```
-----  
Product      : COM5 MPI  
Order No     : 200-7120-01  
Customer     : Softing Industrial Networks GmbH  
User         : Dipl. Inform. Thomas Muster  
Authorization :  
Request      : 2E2380H0CH8SFMH  
Confirm      :  
=====
```

NOTE:

The License Request Code is unique for the device!

- Please send this data by fax to +49 911 54427-27 or e-mail it to info-in@softing.com.
- Softing Industrial Networks GmbH will send you a **License Confirm Code** for product activation.
- Enter the received code in the **License Confirm Code** field.
- The **License Status** field indicates whether the input is OK and the function is enabled.
- The device will only accept valid **License Confirm Codes**.

Index

- A -

A timeout occurred. 37
About 75
Access Path 42, 46, 58, 62
Additional features 23
Allen Bradley 27, 56
ARP 24

- B -

Basic Configuration 31
Basics 23

- C -

Change the Password 66
Clock Settings 72
CLX 27, 46, 56
Configuration 34, 42
Connection 42, 46, 58
Connection diagnostics for echochange 63
Connection menu 62
ControlLogiX 27, 56
Copy Connection 58
CR Parameters 54

- D -

Default connections, monitoring 72
Delete 58
Delete Connection 58
Destination MAC 54
Device SSH Settings 68
Device System Settings 72
Diagnose of Default Connections 72
Diagnostics menu 63
Dialog boxes 34, 42
Disable connection 58

- E -

echochange connection diagnostics 63
echochange Connection Network 43
echochange connection to SLC / PLC-5 56
echochange Connection: Clx Protocol 56

echocollect Connection: Modbus Protocol 55
Edit Access to a Station in Your List 36
Edit Connection 58
Edit H1 parameters 54

- F -

F\$\$\$Connection not found 37
File menu 62

- H -

H1 Connect Parameters 54
H1 System Settings 69
Help menu 74
Hilfeüberblick 7
How to Proceed 31

- I -

INAT OPC-Server – General 18
IP address 50, 67
IP address syntax 50
IP System Settings 70

- L -

License 75
License conditions 75
License Overview 75
Licenses 75
Licensing 32
Line 54
Lizenzbedingungen 19
Logger 18, 23, 40, 64, 65
Logger configuration 64
Logger Settings 65

- M -

MAC address 67
Mail connection 57
Master/Slave 23
MELSEC-Q 28, 46, 57
Melsec-Q Protocol 57
Menu 61, 62, 63, 66, 68, 74
Mitsubishi 28, 57
Modbus 27, 46, 55
Multicast 54

- N -

NetCon configuration 34
 NetCon OPC 23
 netLINK 46
 Network Parameters 58
 Network PLC Protocol 47
 Network Protocol 46
 New Access Path 42
 New Connection 42, 46
 New Connection – echochange 42
 New station 36

- O -

Offline parameterization 37
 On/Off.connection 58
 OPCpipe 29, 42, 46
 OPCpipe Client 42
 OPCpipe Server 42
 Operation and Configuration 31
 Overview 18

- P -

Password 23, 66
 PLC connections 26
 PLC Header 53
 PLC-5 27, 46
 Port 51
 Port number 51
 Priority 54
 Protocol selection 46
 Protocol settings 55, 56, 57

- R -

Reboot 74
 Reboot password 74
 Restart 74
 Rockwell 27, 56

- S -

S5 26, 46
 S7 26, 46, 52
 Select a connection 38
 Select a Station in Your Network 35
 Select station 35

Send / Receive 28, 46
 Settings menu 68
 Simulation 58
 SLC 27, 46
 Specific settings for TCP/IP 48
 Starting the program 23
 Station menu 66
 Station not found 37
 Station parameters 67
 Station Password 66
 Station selection in the network 35
 Switch off 58
 Switch off (connection) 58
 System requirements 19

- T -

TCP/IP Stati 64
 TCP/IP System Settings 70
 TSAP 51, 52
 Type 54

- V -

Versions 75

- W -

Warm start 74
 Windows 34, 42