Description Data transmission:

Modbus TCP

Single Smart Controller - SSC

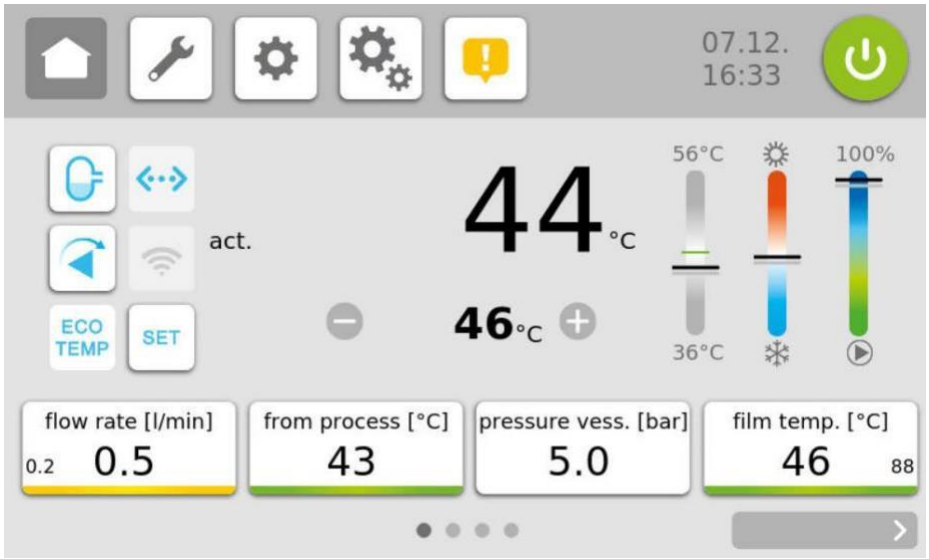


Table of contents

SINGLE Temperature Control
Technology GmbH Ostring 17-19
D - 73269 Hochdorf
PHONE: +49 7153 3009 0FAX : +49 7153 3009 50
www.single-temp.de

Foreword

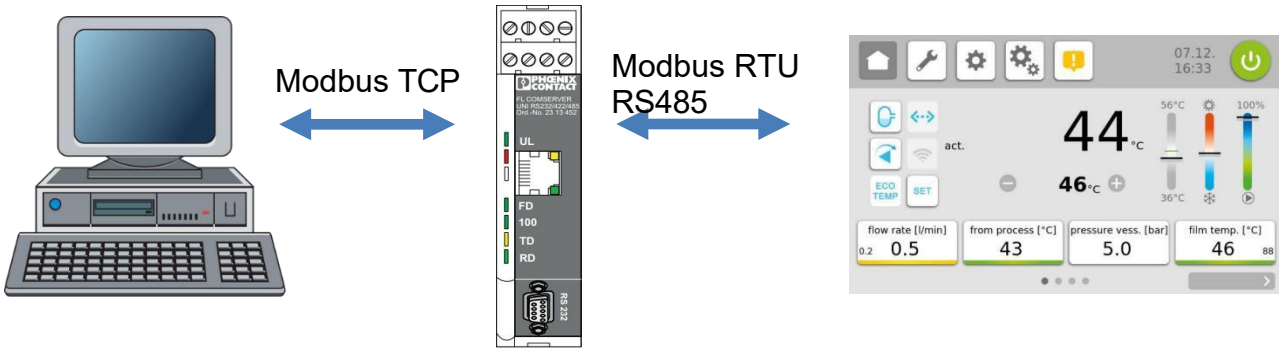
This description was created with the greatest possible care.
However, the information provided herein does not constitute a warranty of product characteristics. SINGLE Temperiertechnik GmbH assumes no liability for errors.
SINGLE Temperiertechnik GmbH reserves the right to make changes at any time in the interest of technical progress.

1 Interface, general description

The Modbus TCP protocol is a further development of the Modbus protocol for serial interfaces. Here the data of the Modbus protocol, the serial interface, are "packed" into a TCP-IP frame, and can be transported so over the Ethernet.
The application range of the Modbus protocol TCP-IP is not only limited to a local network, but can be applied with appropriate hardware to other networks such as the Internet.

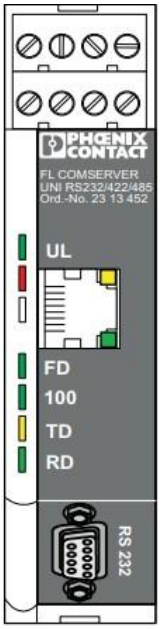
With the help of a gateway, devices with a serial interface and Modbus RTU protocol can be connected to an Ethernet network relatively easily.
A Modbus master with Modbus TCP protocol then communicates with a Modbus RTU slave (here a temperature control unit) via the gateway.
The gateway extracts the Modbus data from the TCP-IP frame of the master and forwards it on the serial interface to the temperature control unit(s).
Conversely, the responses of the temperature control unit are packed into a TCP-IP frame with the help of the gateway and forwarded to the Modbus master via the Ethernet.
Figure 1 shows a possible structure of a master/slave system via Modbus TCP and gateway.

The gateway is already installed in the temperature control unit.



1.1 Commissioning

1.1.1 Gateway settings



Settings at delivery:

IP address: 192.168.0.254
Subnet mask: 255.255.252.0

Settings can be changed via web server in the gateway.

Do not enter anything in the Remote IP Address field!

Application Settings for Modbus

Protocol settings	
Operation Mode	○ UDP ○ TCP ◉ MODBUS/TCP ○ PPP
IP and port address	
Remote TCP port	0
Remote IP address	0 . 0 . 0 . 0
Set the Remote port or IP Address if it is required to check these values when the Master requests a Session	
Channel settings	
Device type	◉ Slave ○ Master
Protocol	◉ RTU ○ ASCII
Disconnect with Inactivity timeout	0 minutes 0 seconds
Valid range: 0...255. If unused set to 0,0.	
TCP Flush Mode	Clear Input Buffer ○ Off ◉ On Clear Output Buffer ◉ Off ○ On
Idle Force Timeout Characters	10
Serial Response Time Out	100 milliseconds
Session profiles	
Max Sessions, Port	8 502
A maximum of 8 sessions may be configured. The MODBUS port for the Slave to Listen on is usually 502.	
Advanced Settings	
Fixed Slave Address	0
May be used if the Master can only send a slave address of 0. In which case the 0 will be converted to this value when the data is transmitted on the serial line.	

Confirm

Note: To switch operation modes press the button and then Confirm.
*You have to **save and reboot** to activate the new configuration (and Firmware). Current Firmware Image loaded: **PC***
PC=UDP and TCP, PM=MODBUS/TCP, PP=PPP.

1.1.2 Settings control unit

Set the following parameters on the controller:
Parameter "Address" to "1" (delivery state) Parameter "Protocol" to "Modbus" (delivery state) Parameter "Baud rate" to 9.6 kbaud (delivery state) Parameter "File format" to "8N1" (delivery state)
Parameter "Switchover" to "RS232 / RS485" (delivery state)

2 Protocol

4 Modbus services are supported from the temperature control unit side. **Function code**	**Meaning**
0x03	READ (n WORDs)
0x06	WRITE (1 WORD)
0x08	LOOPBACK TEST
0x10	WRITE (n WORDs)

The detailed description of the Modbus protocol (both on TCP-IP and for serial transmission) including all public function codes can be taken from the Modbus protocol specification.

See the documents at http://www.modbus.org

• Modbus Application Protocol Specification
• Modbus Messaging Implementation Guide

2.1 Response times and timeouts

Response times of the slave: is approx. 20-60 ms

2.2 Transmission format of the numerical values

The pure numerical value is always transmitted as INTEGER16 number via the protocol.

Example without decimal place: the value 25 is transmitted as 25 (0x0019)

Example with one decimal place: the value 12.4 is transmitted as 124 (0x007C)

Temperature values are ALWAYS transmitted in °C with one decimal place, regardless of the controller setting.

2.3 Data layout

Address	Parameter	Attribute	Meaning	Number range
1	Set point 1	RW	Control set point in 1/10 degree C	MB start ... MB end with one decimal place
2	Operating mode	RW	Rules, Heating/cooling on, Pump on Pump off, Heating/cooling off Cooling to Security-temperature, then switch-off Tempering medium suction	'r' (0x72, 114) 'p' (0x70, 112) 'k' (0x6B, 107) 'a' (0x61, 97)
10	act. Actual value	RO	act. Actual control value in 1/10 degree C	MB start ... MB end with one decimal place
11	act. Manipulated variable	RO	Act. Output ratio in %	-100%(cooling) ... +100%(heating)
12	Operating mode (high byte) ---------- -- general r status (low byte)	RO	akt. Operating mode (Bit 8-15) ---------- Bit 0 Bit 1 Bit 2 Bit 3 Bit 4 Bit 5-7	'r' Rules 'p' pump off 'k' Cooling to safety temperature 'a' Suck off tempering medium ---------- 1 = manual operation, 0 = remote operation 1 = internal sensor, 0 = ext. sensor 1 = impermissible setpoint value received Reserve Collective alarm (details see address 13) Reserve
13	Alarms	RO	Alarms (bit coded) Bit 0 Bit 1 Bit 2 Bit 3 Bit 4 Bit 5 Bit 6-7 Bit 8 Bit 9 Bit 10 Bit 11-15	 1 = Sensor error of the current control sensor always 0, heating defective always 0, cooling defective 1 = low level (ext. contact S5) 1 = too low flow (S7,AFL) 1 = alarm limit has triggered (AL) Reserve Pump error (ext. Contact S9) Phase or direction of rotation error System error (err8 or err0) Reserve

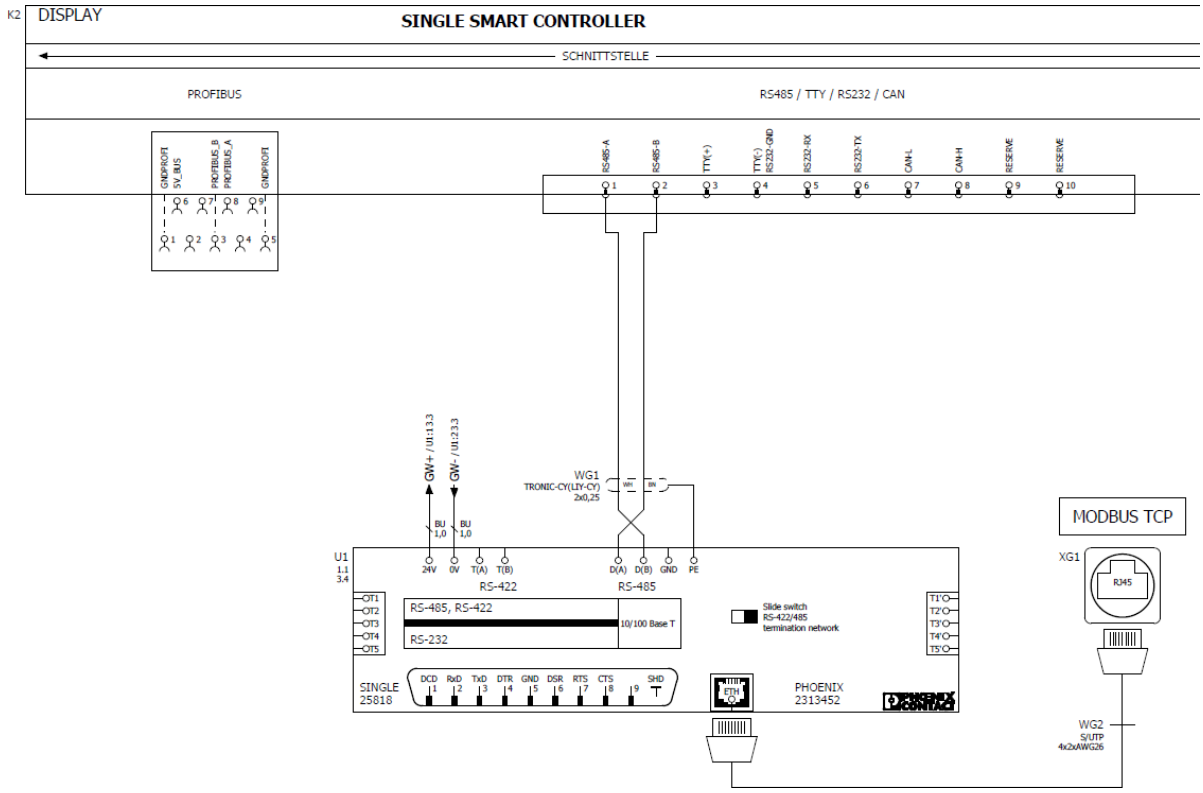
Address	Parameter	Attribute	Meaning	Number range
20	act. Actual value	RO	act. Actual control value in 1/10 degree C	MB start ... MB end with one decimal place
21	act. Set point	RO	Set point in 1/10 degree C	MB start ... MB end with one decimal place
22	act. Manipulated variable	RO	Act. Output ratio in %	-100%(cooling) ... +100%(heating)
23	Fast forward	RO	Flow temperature in 1/10 degree C	MB start ... MB end with one decimal place
24	Return	RO	Return temperature in 1/10 degree C	MB start ... MB end with one decimal place
25	ext. Sensor	RO	Temperature of the ext. probe in 1/10 degree C	MB start ... MB end with one decimal place
26	Flow rate	RO	Flow rate in 0.1 l/min	
27	Print	RO	Pressure in 1/10 bar	
28 1) SBC-T only	Desired flow rate value as of V15/18	RW	Flow rate in 0.1 l/min or 0.1 gal/min or 0.1 m^3 /h	0,0 .. 2000.0 l/min 0,0 .. 528.3 gal/h 0,0 .. 120.0 m^3 /h

2.4 Error messages (Exception codes)

Code	Name	possible causes
01	ILLEGAL FUNCTION	-The selected function code is invalid. -A write command to a read-only parameter was attempted. -controller is not switched to REMOTE mode.
02	ILLEGAL DATA ADDRESS	-The selected address is invalid.
03	ILLEGAL DATA VALUE	-Checksum incorrect -Data lengths incorrect -range limits were exceeded

3 Connection example

3.1 Gateway TCP via RS485



INTERFACE

User manual

UM DE FL COMSERVER ... 232/422/485

Item no.: -

Installation and commissioning of the
FL COMSERVER BASIC 232/422/485- and
FL COMSERVER UNI 232/422/485 hard- and
Software

PHOENIX CONTACT
INSPIRING INNOVATIONS

INTERFACE

User manual

Installation and commissioning of the FL COMSERVER BASIC 232/422/485- and FL COMSERVER UNI 232/422/485 hardware and software

10/2009

Designation: UM DE FL COMSERVER ... 232/422/485

Revision: 01

Item no: -

This manual is valid for:

Designation	Item no.
FL COMSERVER BASIC 232/422/485	2313478
FL COMSERVER UNI 232/422/485	2313452

Please note the following

In order to use the product described in this manual safely, you must have read and understood this manual. The following notes provide you with an initial orientation for using the manual.

Target group of the manual

The product use described in this manual is intended exclusively for qualified electricians or persons instructed by qualified electricians who are familiar with the applicable standards and other regulations on electrical engineering and in particular with the relevant safety concepts.

Phoenix Contact accepts no liability for incorrect actions and damage to Phoenix Contact products and third-party products caused by disregarding the information in this manual.

Explanations of the symbols and signal words used

This symbol indicates dangers that can lead to personal injury. Observe all instructions marked with this symbol to avoid possible personal injury.

DANGER

Indicates a hazardous situation which, if not avoided, will result in personal injury or death.

WARNING

Indicates a hazardous situation which, if not avoided, may result in personal injury or death.

The following symbols indicate hazards that can lead to property damage or stand in front

CAUTION

Indicates a hazardous situation which, if not avoided, may result in injury.

of tips.

ATTENTION

This symbol and the associated text warn of actions that may result in damage to or malfunction of the device, the device environment or the hardware or software.

This symbol and the associated text convey additional information, such as tips and advice for efficient device use or software optimization. It is also used to refer you to additional sources of information (such as manuals or data sheets).

General Terms of Use for Technical Documentation

Phoenix Contact reserves the right to change, correct and/or improve the technical documentation and the products described in the technical documentation at any time without prior notice, provided this is reasonable for the user. This also applies to changes that serve technical progress.

The receipt of technical documentation (in particular data sheets, assembly instructions, manuals, etc.) does not constitute any further obligation to inform Phoenix Contact about any changes to the products and/or technical documentation. Agreements to the contrary shall only apply if they have been expressly approved by Phoenix Contact.
Phoenix Contact in written form. Please note that the documentation provided is exclusively product-related documentation and that you are therefore responsible for checking the suitability and intended use of the products in the specific application, in particular with regard to compliance with the applicable standards and laws. Although Phoenix Contact always takes the necessary care to ensure that the information and contents are correct and state of the art, the information may contain technical inaccuracies and/or typographical errors. Phoenix Contact gives no guarantees with regard to the accuracy and correctness of the information. All information to be taken from the technical documentation is provided without any express, implied or tacit warranty. It does not contain any agreements on quality, does not describe any quality customary in the trade and does not represent any assurance of properties or assurance with regard to suitability for a specific purpose.

Phoenix Contact assumes no liability or responsibility for errors or omissions in the content of the technical documentation (in particular data sheets, assembly instructions, manuals, etc.).

The above limitations and exclusions of liability shall not apply in cases of mandatory liability, e.g. under the German Product Liability Act, in cases of intent, gross negligence, injury to life, body or health, or breach of a condition which goes to the root of the contract. However, the claim for damages for breach of material contractual obligations shall be limited to the foreseeable damage typical for the contract, unless caused by intent or gross negligence or based on liability for injury to life, body or health. A change of the burden of proof to the disadvantage of the user is not connected with this regulation.

Explanations of the legal basis

How to reach us

Internet

Current information on Phoenix Contact products and on our General Terms and Conditions of Business and Warranty can be found on the Internet at:
www.phoenixcontact.com.

Make sure that you always work with the current documentation. This is available for download at the following address:

www.phoenixcontact.de/download.

Country representatives

If you have problems that cannot be solved with the help of this documentation, please contact your respective country representative.
For the address, visit www.phoenixcontact.com.

Publisher

PHOENIX CONTACT GmbH & Co. KG
Flax Market Road 8
32825 Blomberg
GERMANY
Phone+49 - (0) 52 35 - 3-00
Fax+49 - (0) 52 35 - 3-4 12 00

If you have any suggestions or ideas for improving the content and design of our manual, we would be pleased if you would send us your suggestions to: tecdoc@phoenixcontact.com

Table of contents

1 Foreword

1.1 Description

Ethernet is now widely accepted in industrial applications. However, automation devices are often not network-compatible. The new "Serial De- vice Server" FL COMSERVER ... It allows easy integration of serial RS-232, RS-422 and RS-485 interfaces into industrial 10/100 Base-T(X) networks.

Theoretically, this can be used from any point in the world over Ethernet networks to

– the system status is queried
– Transfer visualization data
– a program or firmware download is initiated
– or remote maintenance can be performed for service purposes.

Network integration eliminates the need for costly cable installations. Serial connections are converted to Ethernet and optionally tunneled through the network with TCP or UDP protocol. Modbus gateways and the establishment of PPP connections can also be implemented.

Depending on the device type used, the following data protocols are supported:

Table 1 Supported data protocols

	Data logs			
FL COMSERVER ...	**TCP/IP**	**UDP**	**Modbus/ TCP**	**PPP with CHAP**
... UNI 232/422/485 Item no. 2313452	x	x	x	x
... BASIC 232/422/485 Item no. 2313478	x	x	-	-

Existing application software that only supports serial communication can be redirected to the network card of a Windows PC with the free COM port redirector software using virtual COM ports.

Simple configuration and diagnostics

Configuration and diagnostics can be performed without additional software via web-based ma- nagement using standard browsers. The menu structures are clearly structured according to topics for intuitive configuration and the web pages adapt dynamically to the desired applications. If, on the other hand, configuration and diagnostics are to be performed directly with a process visualization, corresponding SNMP objects are available for integration in OPC databases.

Performance for industrial requirements

For safe and permanent operation under industrial environmental conditions, the **FL COMSERVER ... 232/422/485 offers** a high-quality 3-way potential isolation (VCC // RS-232, RS-422, RS-485 // Ethernet) as well as a redundant feed-in option for the 24 V voltage supply. High availability is also ensured by the

high EMC compatibility of the devices. In addition to the hardware, the software also takes into account the special industrial requirements. The 3964R protocol is supported as well as the various Modbus protocols or status messages via SNMP objects.

The **FL COMSERVER ... 232/422/485** is specially designed for industrial applications in the control cabinet. It is characterized by the following features:

– Mounting on EN mounting rail,
– extended temperature range,
– 22.5 mm narrow width,
– 10/100 BASE-T(X) autonegotiation,
– 24 V AC/DC ± 20% power supply,
– redundant power supply and modular station design with T-bus connectors possible,
– High quality 3-way isolation (VCC // RS-232, RS-422, RS-485 // Ethernet),
– comprehensive diagnostic displays,
– Integration with network management tools and visualization systems by supporting SNMP services,
– Configuration with web-based management, including password protection,
– Support of all common network protocols,
– PPP protocol with CHAP (128 bit password encryption),
– Modbus TCP support,
– COM Redirector software included.

1.2 Content

This manual describes the simple commissioning of a **FL COMSERVER ... 232/ 422/485** in the following sequence:

1. Mounting the **FL COMSERVER ... 232/422/485**
2. Selection and configuration of application options
3. Checking the settings
4. Commissioning

1.3 Hardware and software requirements

A PC with the following equipment is required for configuration and commissioning:

– Ethernet network connection
– HTML browser, e.g. Internet Explorer as of 5.0 or Netscape Navigator as of 4.6

1.4 Trademark

Windows® is a registered trademark of Microsoft Corp.

2 Mounting the FL COMSERVER ... 232/422/485

2.1 Unpacking the FL COMSERVER ... 232/422/485

The FL COMSERVER ... 232/422/485 is supplied together with a CD and a package insert with installation instructions. Please read the package insert carefully before unpacking the FL COMSERVER ... 232/422/485 carefully before fitting it out.

2.1.1 Scope of delivery

The following items are in the package

- FL COMSERVER BASIC 232/422/485 Part no.: 2313478 resp.
  FL COMSERVER UNI 232/422/485 Item no.: 2313452
- Multilingual package insert
- CD with manual in PDF format, COM redirection software and MIB files.

2.2 Connection and operating elements

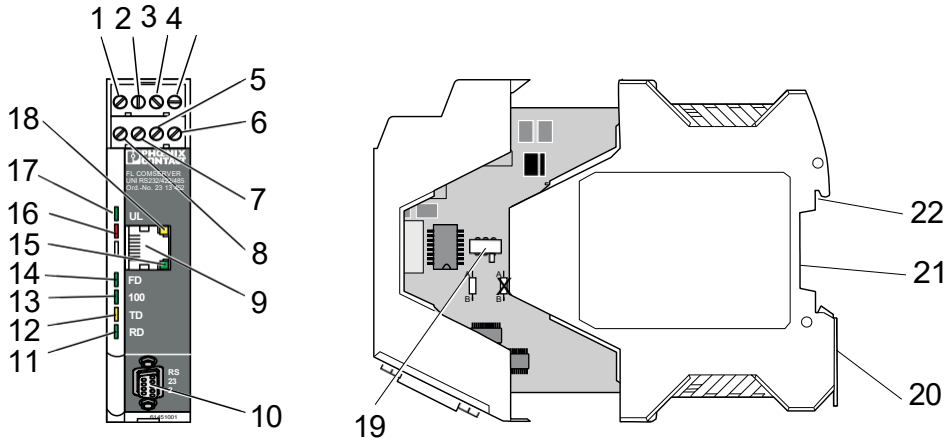


Fig. 2-1 Structure of the FL COMSERVER ... 232/422/485

1. Connection Voltage supply 24 V AC/DC ±20 %.
2. Connection voltage supply 0 V
3. T(A), RS-422 port
4. T(B), RS-422 port
5. D(A), RS-422/485 connection
6. D(B), RS-422/485 connection
7. GND
8. 5 Screen, same potential as FE
9. Ethernet connection, RJ45
10. RS-232 connector, SUB-D-9 male connector
11. LED green, RD, receive data
12. LED yellow, TD, transmit data
13. LED green, 100, transmission speed 100 MBit/s
14. LED green, FD, operating mode full duplex active
15. LED green, LINK status TP port
16. LED red, error display
17. LED green, UL, power supply
18. LED yellow, ACT data transmission TP port, dynamic
19. Slide switch for RS-422/485 termination network (390 180 390
20. Snap-in foot for mounting rail installation
21. Bus connector for redundant power supply (concealed)
22. FE, functional earth contact (concealed)

2.3 Configuration

2.3.1 Enable/disable termination network

The FL COMSERVER ... 232/422/485 is optionally operated on a 2-wire or 4-wire bus line. For proper operation of the bus system, termination networks are always required for the RS-422/485 bus connection.

The FL COMSERVER ... 232/422/485 is equipped with a switchable termination network. Depending on the position used on the RS-485 bus line, the termination network must be activated or deactivated.

2.3.2 Open/close housing

To set the required operating mode via the termination network, it is necessary to open the housing of the FL COMSERVER ... 232/422/485 to be opened.

To do this, proceed as follows:

1. Open the housing head with a suitable screwdriver (see Fig. 2-2, 1).
2. Carefully pull out the printed circuit board as far as it will go (see Fig. 2-2, 2).
3. Depending on the position on the bus system, activate/deactivate the termination network (see chapter 2.3)
4. Carefully push the printed circuit board back as far as it will go.
5. Snap housing head into place

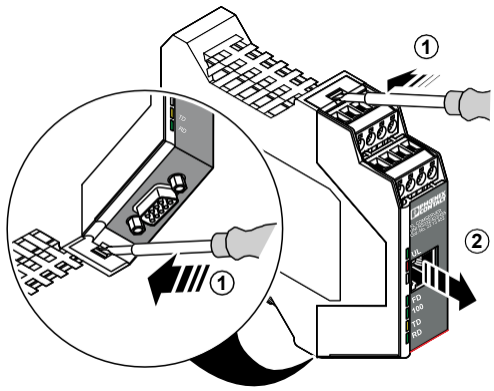


Figure 2-2 Open/close housing

2.3.3 Set operating mode

The operating mode of the FL COMSERVER ... 232/422/485 is set depending on the position on the bus system by means of termination networks. Select the required operating mode and set it using the slide switch.

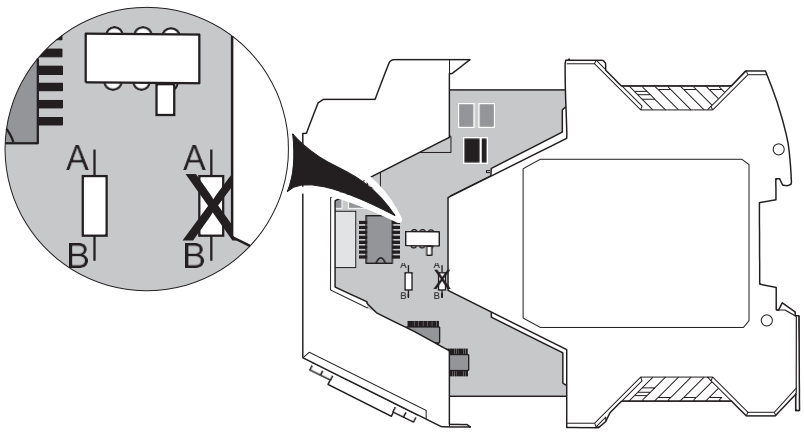


Fig. 2-3Location of the slide switch

Operating mode/participant	Switch position	Resistor network
RS-422	left	activates
RS-485 end user	left	activates
RS-485 Participant*	right	deactivated

* factory default

2.4 Mounting the FL COMSERVER ... 232/422/485 on the mounting rail profile

ATTENTION:
Only mount the FL COMSERVER ... 232/422/485 only in a de-energized state.

2.4.1 Mounting rail (single device)

Proceed as follows for mounting on the mounting rail:

1. Place the device on the mounting rail from above so that the upper housing groove hooks onto the upper edge of the mounting rail (see Fig. 2-4 A).
2. Carefully push the device by the housing head in the direction of the mounting surface.
3. After the snap-in foot has audibly engaged on the mounting rail, check that it is firmly seated

To disassemble, proceed as follows:

1. Use a suitable screwdriver to loosen the locking mechanism on the snap-in foot of the device (see Fig. 2-4 B).
2. Grasp the device by the housing head and carefully turn it upwards.
3. Carefully lift the device off the mounting rail bus connector and the mounting rail.

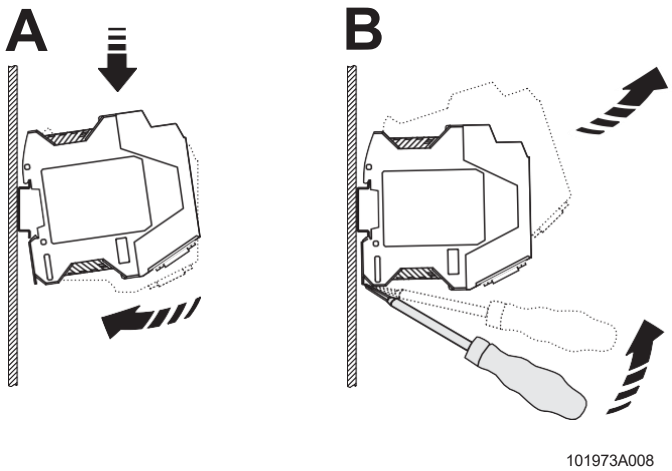


Figure 2-4 Mounting and dismounting single unit

2.4.2 Carrier rail bus connector (composite station)

For the modular electronic housings of the ME.../TBUS series, DIN rail bus connectors of different widths are required in an interconnection.

By plugging together the mounting rail bus connectors (see Figure 2-5 A) and inserting them into the 35 mm wide mounting rail (see Figure 2-5 B/C), the power supply is continued on the backplane (see Figure 2-5).

By using an additional system power supply, a redundant power supply is provided for other connected devices in the compound station.

CAUTION: Damage to equipment or property if the current load is too high!

Due to the current load, a composite station with FL COMSERVER ... 232/422/ 485 may consist of a maximum of 20 devices.

The maximum current load of 2 A must not be exceeded.

For mounting on the carrier rail bus connector, proceed as follows:

When using the FL COMSERVER ... 232/422/485 in a composite station, provide for a 22.5 mm wide mounting rail bus connector (article no. 2707437).

Configure two 17.5 mm mounting rail bus connectors (article no. 2709561) for the system power supply (e.g., MINI SYS PS 100-240AC/24DC/1.5, article No.: 2866983).

Ensure exact alignment between the mounting rail bus connector and the device.

- Carrier rail bus connector (connector part) left and
- Device (snap-in foot) bottom

1. Place the device on the mounting rail from above so that the upper housing groove hooks onto the upper edge of the mounting rail (see Fig. 2-5, part D).
2. Carefully press the device at the housing head in the direction of the mounting surface so that the device bus connector is securely seated on the mounting rail bus connector.
3. After the snap-in foot has audibly engaged on the mounting rail, check that it is firmly seated.

The device is mechanically fixed only by the mounting rail.

To disassemble, proceed as follows:

1. Use a suitable screwdriver to loosen the locking mechanism on the snap-in foot of the device (see Fig. 2-5 E).
2. Grasp the device by the housing head and carefully turn it upwards.
3. Carefully lift the device off the mounting rail bus connector and the mounting rail (see Fig. 2-5 E).

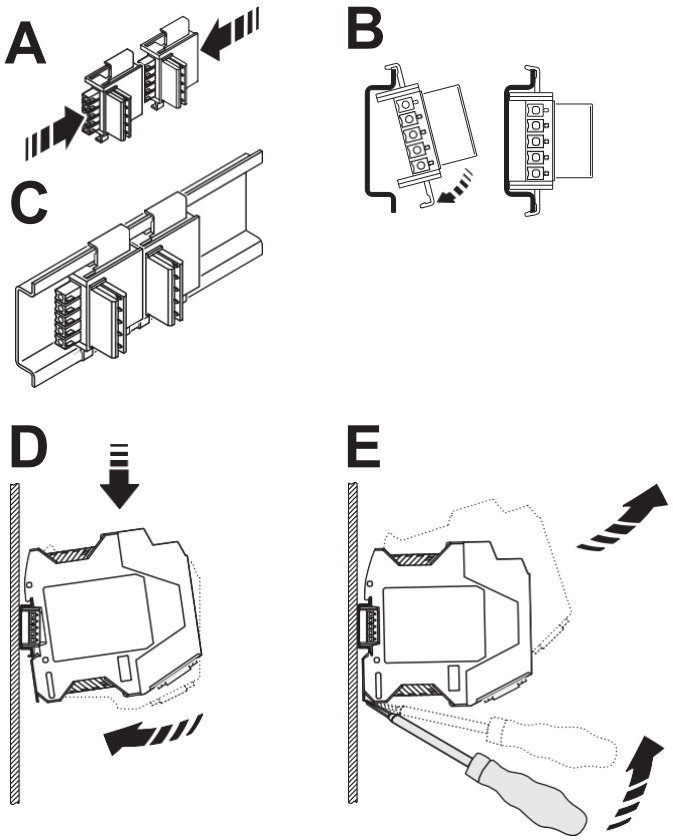


Figure 2-5 Assembly and disassembly of compound station

2.5 Connection of the RS-232 connection cable

Connect the FL COMSERVER ... 232/422/485 with the RS-232 device to be connected, e.g. a PC, using the RS-232 cable PSM-KA-9SUB 9/BB/2 METER (Part No. 2799474). This is an interface cable with 1:1 connected contacts.

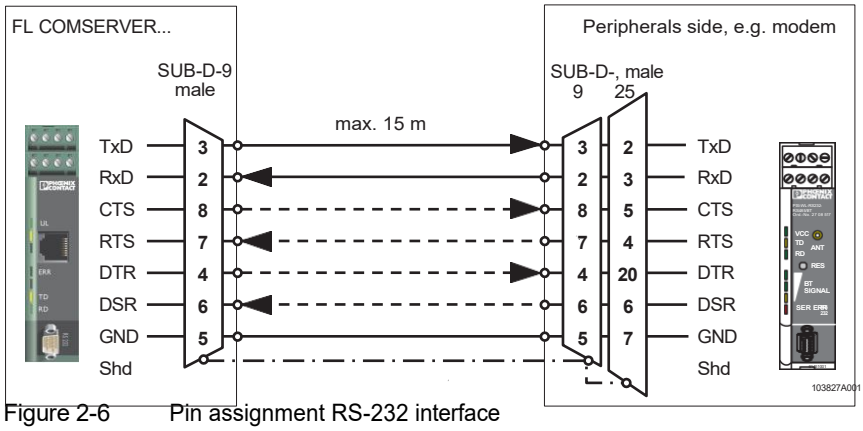


Figure 2-6 Pin assignment RS-232 interface

The RS-232 interface of the FL COMSERVER ... 232/422/485 can be switched via WBM between DTE (Data Terminal Equipment) / DCE (Data Communication Equipment) assignment.

In the delivery state (DTE), the interface behaves like a PC.

When changing devices from a FL COM SERVER... (previous variant) to FL COM SERVER ... 232/422/485, please also observe this modified interface configuration when reusing the existing RS-232 cable.

	Setting the FL COMSERVER ... 232/422/485 via Web-Based Management (WBM) to DTE or DCE
PC (DTE)	DCE
Modem (DCE)	DTE (delivery state)
Interbus Controller (DCE)	DTE (delivery state)
Siemens S7 with MPI- Adapter (DTE)	DCE

ATTENTION:

The FL COM SERVER RS... may only be connected to devices that meet the requirements of EN 60950 (Safety of Information Technology Equipment).

2.6 Connection of the RS-422 connection cable

RS-422 pin assignment

In the RS-422 operating mode, it is possible to establish a point-to-point connection.

Use a twisted pair, jointly shielded bus cable to connect the peripheral device.

Connect the individual wires of the data line to the pluggable COMBICON screw terminal.

Check the correct signal assignment!

In this operating mode, the full duplex transmission mode is supported.

FL COMSERVER ... RS232/422/485

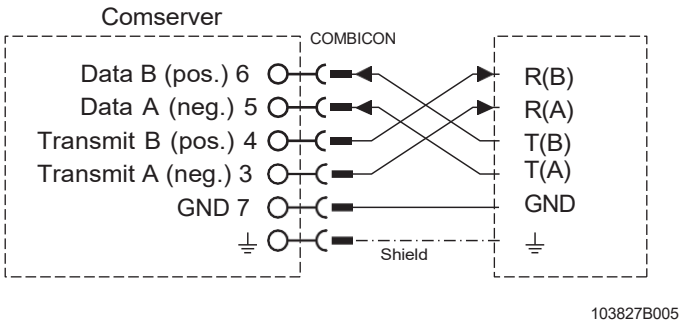


Figure 2-7 Pin assignment RS-485

Provide this bus line at each peripheral device with a termination network.

To do this, activate the termination network integrated in the FL COMSERVER ... 232/422/485 integrated termination network (see chapter 2.3).

ATTENTION:

The FL COM SERVER RS... may only be connected to devices that meet the requirements of EN 60950 (Safety of Information Technology Equipment).

The shield connection of the RS-422 bus line may only be connected at one end to the FL COMSERVER ... 232/ 422/485 on one side only.

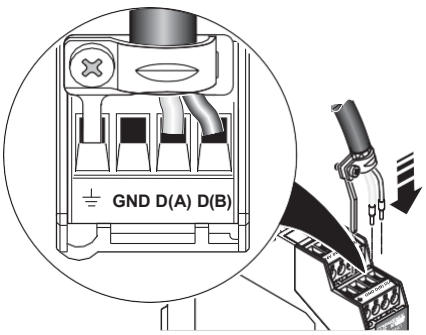


Figure 2-8 Shield connection

2.7 Connection of the RS-485 connection cable

In the RS-485 operating mode, an RS-485 network with several peripheral devices can be set up. Use a twisted-pair, jointly shielded bus cable to connect the peripheral devices.

Connect the individual wires of the data line to the pluggable screw terminal COMBI-CON...

ATTENTION: Pay attention to the polarity of the RS-485 line.

Provide this bus line with a termination network at the two most distant points of the RS-485 network.

FL COMSERVER ... 232/422/485

To do this, activate the termination network integrated in the FL COMSERVER ... 232/422/485 integrated termination network (see chapter 2.3).

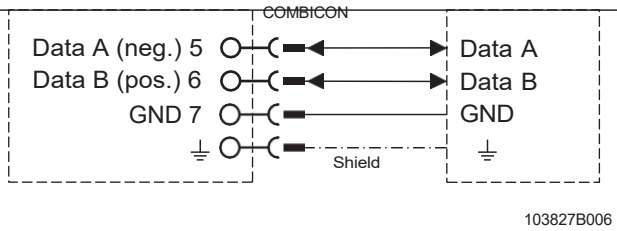


Figure 2-9 Pin assignment RS-485

Provide this bus line at each peripheral device with a termination network.

To do this, activate the termination network integrated in the FL COMSERVER ... 232/422/485 integrated termination network (see chapter 2.3).

The shield connection of the RS-422 bus line may only be connected at one end to the FL

ATTENTION:

The FL COM SERVER RS... may only be connected to devices that meet the requirements of EN 60950 (Safety of Information Technology Equipment).

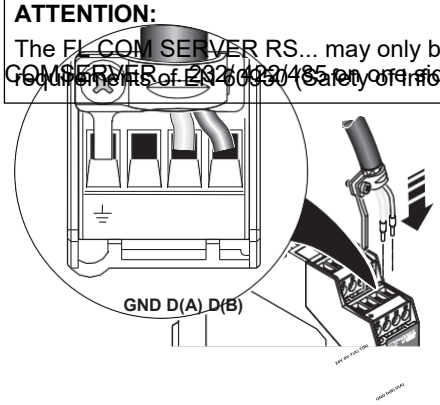


Figure 2-10 Shield connection

2.8 Ethernet network connection

2.8.1 Twisted pair interface (TP)

The FL COMSERVER ... 232/422/485 has a front Ethernet interface in RJ45 format to which only twisted pair cables with an impedance of 100 can be connected. The data transmission rate is optionally 10 or 100 MBit/s. For the selection of the transmission rate, the FL COMSERVER ... 232/422/485 supports the autonegotiation function.

2.8.2 Connection

Insert the Ethernet cable with the crimped RJ45 plug into the TP interface until it audibly locks into place.

CAUTION: Possible malfunction of device, device environment and hardware or software.

Only use shielded twisted pair cables and suitable shielded RJ45 plugs.

Pay attention to the correct signal assignment of the connector.

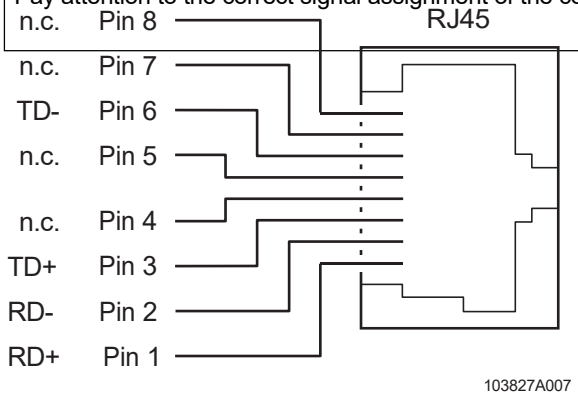


Figure 2-11 Pin assignment RJ45

2.8.3 Selection of suitable connecting cables

To connect Ethernet components, you need either lines with crossed line pairs (**CROSS OVER**) or straight line pairs (**LINE**,1:1). In general, straight wired lines are required between structural components and end devices; the CROSS OVER lines are used for connections between two structural components and for connections between two end devices. The following table can be used to select the appropriate line. For a better differentiation of the respective cable types, you should use green bend protection sleeves (protective caps) for the CROSS-OVER cables and gray for the straight-wired cables (LINE, 1:1).

Table 2-1 Connection types of different Ethernet components

• Line 1:1 = gray protective caps • CROSS OVER = green protective caps	PC/ RFC	IBS Gateway	I/O bus terminal	COM Server	Switch	Hub	Media converter
PC / RFC	Cross	Cross	Cross	Cross	Line	Line	Line
IBS Gateway	Cross	Cross	Cross	Cross	Line	Line	Line
I/O bus terminal	Cross	Cross	Cross	Cross	Line	Line	Line
FL COMSERVER ... 232/422/485	Cross	Cross	Cross	Cross	Line	Line	Line
Switch	Line	Line	Line	Line	Cross	Cross	Cross
Hub	Line	Line	Line	Line	Cross	Cross	Cross
Media converter	Line	Line	Line	Line	Cross	Cross	Cross

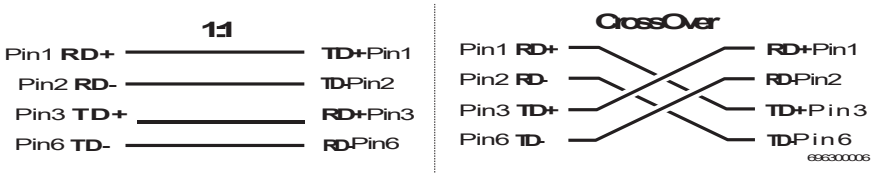


Figure 2-12 Pin assignment Ethernet connection lines

2.8.4 Ethernet operating displays

The FL COMSERVER ... 232/422/485 is equipped with extensive operating displays for diagnostics at the twisted pair port.

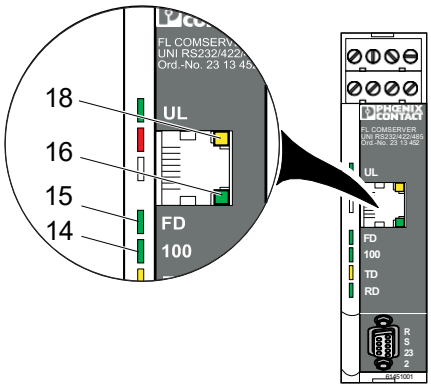


Figure 2-13 Diagnostic displays for the TP port

No.	Ref.	Function
14	100	The 100 LED (green) lights up when the data is transmitted at 100 Mbps.
15	FD	The FD LED (green) lights up when the data is transmitted in full duplex mode.
16	LINK	Line monitoring checks the line segment for interruptions. For this purpose, the remote station must send link or data signals. The LINK LED (green) lights up if no error has occurred. An unused interface or a terminal device that has been switched off is indicated as an error and the LED goes out.
18	Activity	The Activity LED (yellow) flashes depending on the amount of data currently sent or received on the TP port.

2.9 Connection of the power supply

CAUTION: Severe personal injury and/or damage to property due to improper connection!

The electrical connection, commissioning and operation of this device may only be performed by qualified persons. Qualified persons with a 24 V DC safety-low voltage (SELV).

The persons in this document are persons who are authorized to commission, ground and mark devices, systems and plants in accordance with the standards of safety engineering. In addition, the persons are familiar with all warnings and maintenance measures of this document.

Failure to observe the instructions may result in serious bodily injury and/or damage to property.

The power supply is connected via the plug-in COMBICON screw terminals (24 V and 0 V).

Alternatively, the devices in a composite station are supplied with redundant voltage via the carrier rail bus connector (see chapter 2.4.2).

Both voltages US1/US2 are continued on the backplane and are thus available to other connected modules.

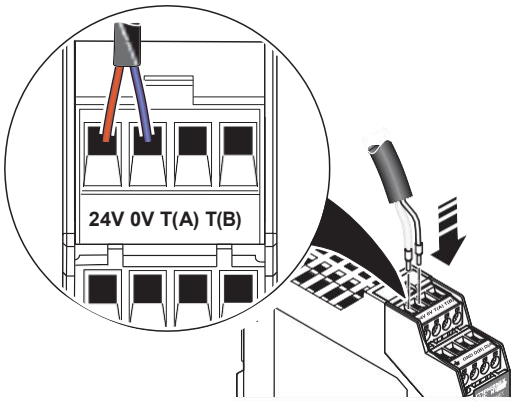


Fig. 2-14 Connection of the supply voltage without T-bus connector

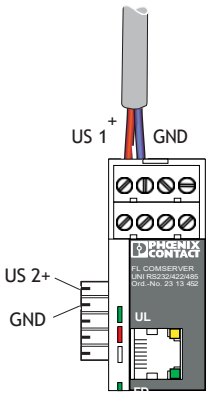


Figure 2-15 Connection of the power supply, module snapped onto T-bus connector

3 Configuration and commissioning

3.1 Delivery state / factory settings

The following functions and properties are available in the delivery state or after a later reset to the factory settings (with the exception of the IP parameters):

- The FL COMSERVER ... 232/422/485 has a valid private IP address.
  IP address: 192.168.0.254
  Subnet mask: 255.255.255.0
  Gateway: 0.0.0.0

The IP parameters are retained in the event of a subsequent reset to the factory settings. This gives you immediate access to the web-based management again.

- BootP and DHCP is enabled as addressing mechanism.
- There is no password set for read access.
- The password for write access is "**private**".
- The WBM (Web Based Management) can be accessed from any IP address.
- The serial interface is configured:
  Interface Type: Port 0 RS-232
  Transmission rate: 9600 bit/s
  Data bit: 8
  Parity: none
  Stop bit: 1
  Flow control: No
  RS.232 Interface Type: DTE

In the delivery state (DTE), the interface behaves like a PC.

The RS-232 interface of the FL COMSERVER ... 232/422/485 can be switched via WBM between DTE (Data Terminal Equipment) / DCE (Data Communication Equipment) assignment.

When changing devices from a FL COM SERVER... (previous variant) to FL COM SERVER ... 232/422/485, please also note this changed interface configuration if you reuse the existing RS-232 cable.

- The application settings are configured for a "COM port redirector" application
  Operation Mode: TCP
  Own TCP Port: 3001
  Remote TCP Port: 0
  Remote IP address: 0
  Device Type: Server (Responder)

- All collected information of the SNMP agent is deleted.
- There is no trap receiver entered.

3.2 IP address configuration

Each device in an Ethernet network must have a unique address with which communication and data exchange is controlled, cf. telephone number with country and area code. This Internet Protocol address (IP address) is a numerical code of four numbers between 0 and 255 separated by a dot (Decimal Dot- ted Notation). The IP address is assigned by the network administrator.

When delivered, the FL COMSERVER ... 232/422/485 is set to a private IP address (IP=192.168.0.254, subnet= 255.255.255.0). In addition, BootP and DHCP operation is activated.

The assignment of valid IP parameters is mandatory for the management function and further configuration.

For more information and background about IP address assignment, refer to the chapter "Assigning IP addresses" on page A-1.

3.2.1 Configuration via WBM

1. Set the IP address of your PC to the subnet of the COM server. (e.g. IP= 192.168.0.10, Subnet= 255.255.255.0).
2. Change to your WEB browser and type the IP address of the COM server into the address line (default=192**.168.0.254**).
3. The WBM will get back to you immediately.

If no response is received from the WBM of the FL COMSERVER ... 232/422/485, first check the IP parameters of your PC.
If everything is set properly, check in the WEB browser if any PROXY settings are loaded. For a function, the settings must be set to "automatically load" or "deactivated".

4. Switch to the "General Configuration".
5. Complete the following query with the password "**private**". It is not necessary to enter the user name.

Figure 3-1 Password query

6. The "IP configuration" menu opens:

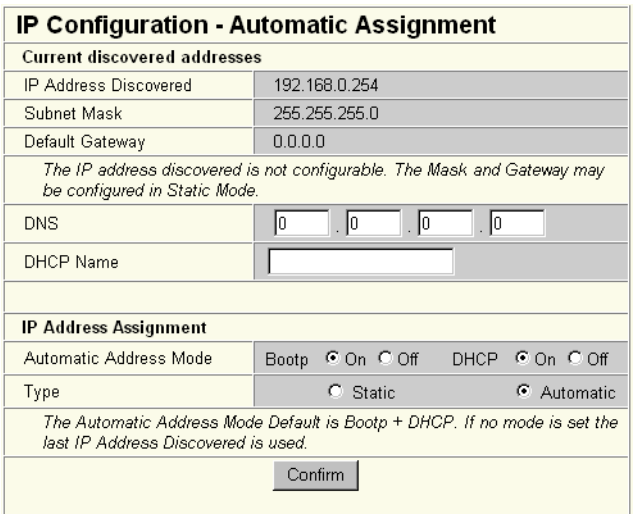


Figure 3-2 IP Configuration" menu

7. To make changes to the IP address or subnet mask, activate "Static✂ under "Type" and confirm with "Confirm".
   The input fields for IP address, subnet mask and gateway open.
8. Change the settings and confirm with "Confirm".
9. To permanently save and activate the new configuration, switch to the "Save and Reboot" menu.

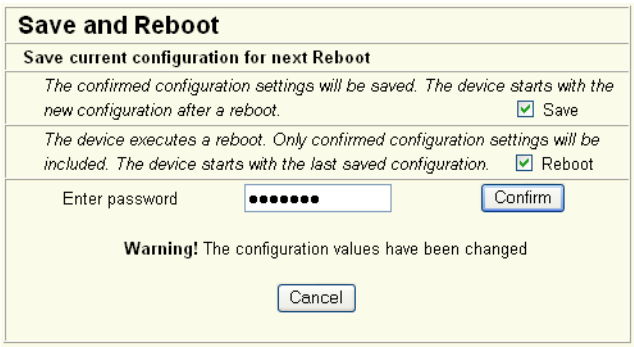


Figure 3-3 IP Configuration" menu

10. Type "**private**" as password and accept / activate the new confi- guration.

3.2.2 Configuration via the RS-232 interface

1. Connect the FL COMSERVER ... 232/422/485 to a serial COM port of a PC (1:1 cable).
2. Open a terminal program, e.g. Hyperterminal in the Windows start menu under "Programs... Accessories... Communication... Hyperterminal".
3. Configure the interface (e.g. COM 1) under "File... Properties" to 9600 bit/s; 8 data bits; No parity; 1 stop bit; No flow control.

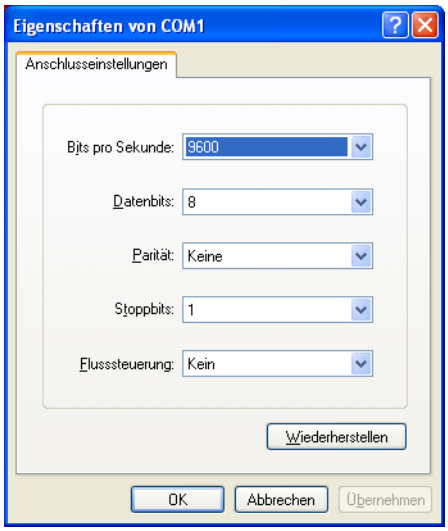


Figure 3-4 Properties menu in Windows Hyperterminal

4. Confirm the settings with "OK" and close the menu.
5. Check the correct settings in the status bar of Hyperterminal.

Figure 3-5 Status bar in Windows hyperterminal

6. Now perform a voltage reset on the FL COMSERVER ... 232/422/485 and simultaneously hold down the X key on your keyboard.
7. As soon as a response from the FL COMSERVER ... 232/422/485 appears on the screen, press the ENTER key within three seconds.

The following display appears:

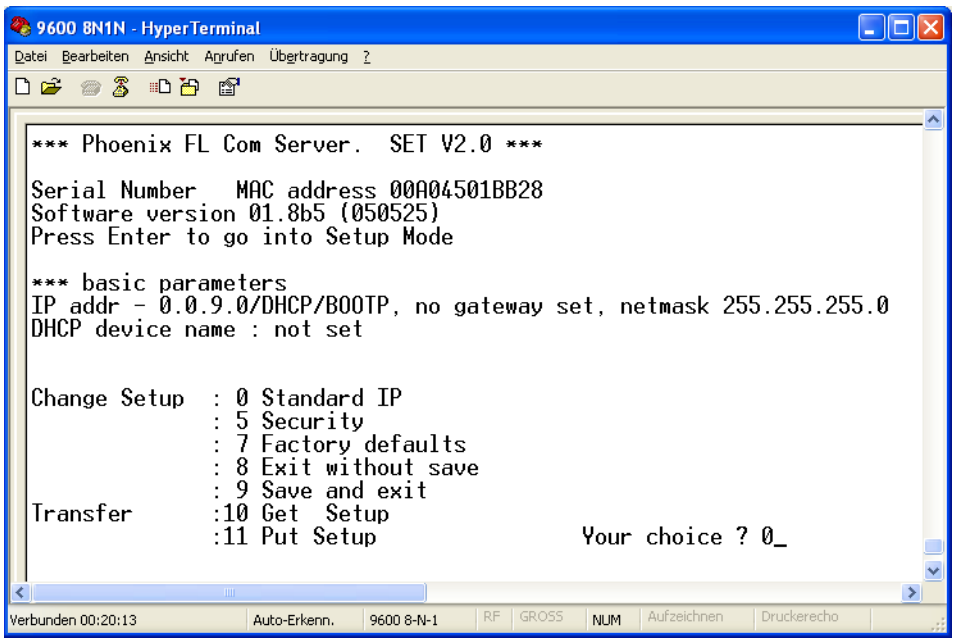


Figure 3-6 Serial setup menu

8. Press "0" and confirm with "ENTER".
9. Enter the IP address in dotted notation and confirm each entry with "ENTER".
10. Enter the network mask and gateway address accordingly.

The subnet mask is set in Telnet and Serial Setup by entering the computer bits (host bits).

	Network Bits	Calculator bits	Subnet mask
Class A	8	24	255.0.0.0
Class B	16	16	255.255.0.0
Class C	24	8	255.255.255.0

For more examples, see the "Subnet masks" chapter on page A-4.

11. Press "9". You save and end the input with this.

The other device settings can now be made with a browser via the Web Based Management. To do this, the IP address just entered is entered in the address line of the web browser in dotted notation.

3.2.3 Configuration via BootP

1. Make a note of the MAC address printed on the FL COMSERVER ... 232/422/485 is printed on. For Phoenix Contact Factory Line products, this always starts with 00.A0.45.xx.xx
2. Enter the MAC address and the desired IP address, subnet mask and gateway address for the BootP server.
3. At the next BootP request of the FL COMSERVER ... 232/422/485 the Boot-P-Server answers the request with the desired IP address.
4. The FL COMSERVER ... 232/422/485 is now accessible via the assigned IP address.

3.2.4 Configuration via ARP command and Telnet

3.2.4.1 Assign temporary IP address

1. Switch to the DOS command window. It is located in the Windows Start menu under "Start... Programs... Accessories... Command Prompt".

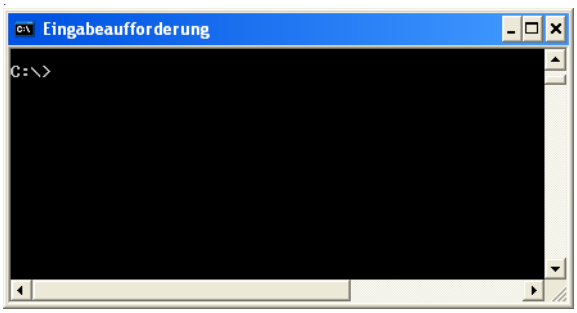


Figure 3-7 DOS command window

2. Enter the ARP command followed by the desired IP address and the MAC address of the device.

```
z. e.g. arp -s 192.168.0.17 00-A0-45-21-BE-61
```

The MAC address is sticked on the side of the device and always starts with 00-A0-45...

Note that you use hyphens when entering the MAC address in the arp command!

3. Now try to establish a Telnet connection to the IP address and port 1.

```
z. e.g. telnet 192.168.0.17 1
```

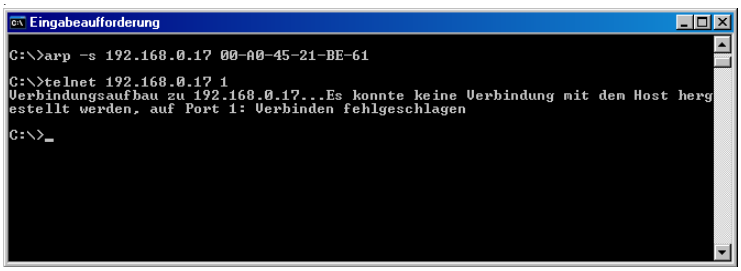


Figure 3-8 DOS command window

A message appears that the connection cannot be established.

The FL COMSERVER ... 232/422/485 now has a temporary IP address and can be configured with a browser and WBM or via Telnet.

3.2.4.2 Call Telnet configuration menu

1. Establish a Telnet connection to port 9999 of the FL COMSERVER ... 232/422/485.

```
e.g. telnet 192.168.0.17 9999.
```

Figure 3-9arp command and telnet configuration

2. Type the system password in the following password prompt (default= private).

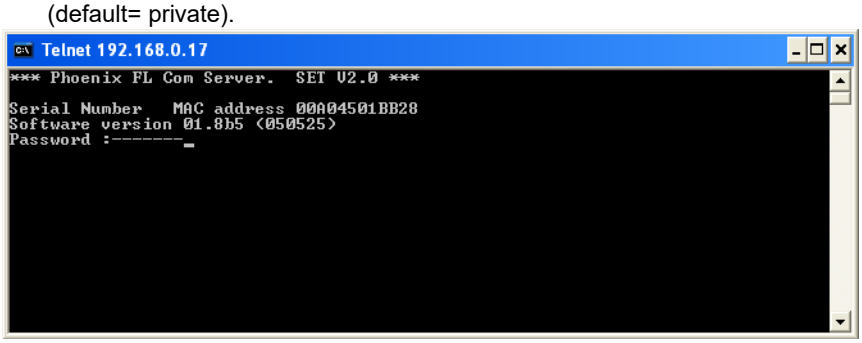


Figure 3-10 Password entry

3. Confirm the entry by pressing the "ENTER" key twice.

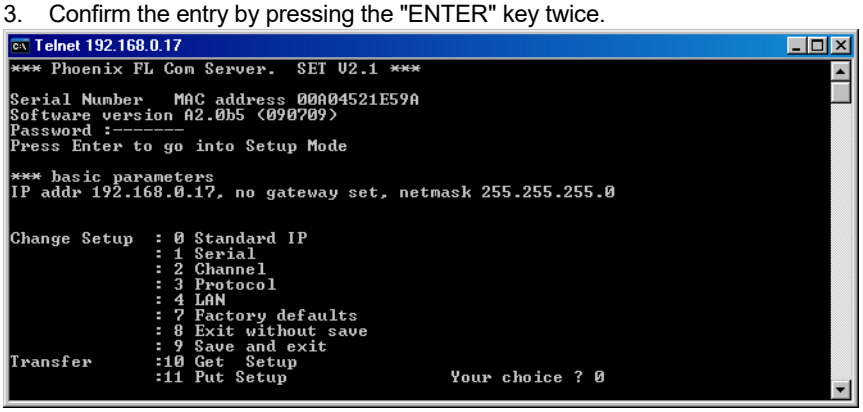


Figure 3-11 Telnet configuration menu

You can now configure a new IP address via "Change Setup" or reset the device to the delivery state (all passwords and application settings are reset). Please refer to the chapter "Delivery state / Factory settings" on page 3-1.

Setup 0 - STANDARD IP

```
                                                    Your choice ? 0
IP Address : (192) .(168) .(  0) .(104)
Set Gateway IP Address (N) N
Netmask: Number of Bits for Host Part (0=default) (8)
Last Auto IP address: 192.168.0.254
```

Fig. 3-12 Delivery state / factory settings

1. Change IP address
2. Gateway settings selection
3. Setting the Subnet Mask

.

The subnet mask is set in Telnet and serial setup by entering the computer bits (host bits).

	Network bits	Calculator Bits	Subnet mask
Class A	8	24	255.0.0.0
Class B	16	16	255.255.0.0
Class C	24	8	255.255.255.0

Example:

Subnet Mask	PC Bits
255.255.255.252	2
255.255.255.248	3
255.255.255.240	4
255.255.255.224	5
255.255.255.192	6
255.255.255.128	7
255.255.255.0	8
255.255.254.0	9
255.255.252.0	10
255.255.248.0	11
...	
...	
255.128.0.0	23
255.0.0.0	24

For more examples, see the "Subnet masks" chapter on page A-4.

Setup 1 - SERIAL Settings

```
Line Speed 0-11 (2):
Mode: Bits 7¦6       Bits 5¦4          Bits 3¦2     Bits 1¦0
      01=1SB 11=2SB  00=NP 01=OP 11=EP  10=7B 11=8B  00=RS232 01=422 11=485
 (4C):
```

Figure 3-13 Serial settings

1. Select your serial transmission speed

Serial Speed (Bit/s)	Setup No.	
300	7	
600	6	
1 200	5	
2 400	4	
4 800	3	
7 000	11	
9 600	**2**	**(default)**
19 200	1	
38 400	0	
57 600	9	
115 200	8	
187 500	10	

2. Select your serial parameters

Interface Mode Options	7	6	5	4	3	2	1	0
RS-232							0	0
RS-422							0	1
RS-485, 2-wire							1	1
7 bit					1	0		
8 bit					1	1		
No Parity			0	0				
Even Parity			1	1				
Odd Parity			0	1				
1 Stop bit	0	1						
2 stop bits	1	1						

List of possible I/F mode settings

Interface	Bits	Parity	Stop Bits	Binary	Hex	
RS-232	7	No	1	01001000	48	
	7	No	2	11001000	C8	
	7	Even	1	01111000	78	
	7	Even	2	11111000	F8	
	7	Odd	1	01011000	58	
	7	Odd	2	11011000	D8	
	8	**No**	**1**	**01001100**	**4C**	**(default)**
	8	No	2	11001100	CC	
	8	Even	1	01111100	7C	
	8	Even	2	11111100	FC	
	8	Odd	1	01011100	5C	
	8	Odd	2	11011100	DC	
RS-422	7	No	1	01001001	49	
	7	No	2	11001001	C9	
	7	Even	1	01111001	79	
	7	Even	2	11111001	F9	
	7	Odd	1	01011001	59	
	7	Odd	2	11011001	D9	
	8	No	1	01001101	4D	
	8	No	2	11001101	CD	
	8	Even	1	01111101	7D	
	8	Even	2	11111101	FD	
	8	Odd	1	01011101	5D	
	8	Odd	2	11011101	DD	
RS-485	7	No	1	01001011	4B	
	7	No	2	11001011	CB	
	7	Even	1	01111011	7B	
	7	Even	2	11111011	FB	
	7	Odd	1	01011011	5B	
	7	Odd	2	11011011	DB	
	8	No	1	01001111	4F	
	8	No	2	11001111	CF	
	8	Even	1	01111111	7F	
	8	Even	2	11111111	FF	
	8	Odd	1	01011111	5F	
	8	Odd	2	11011111	DF	

Setup 2 - CHANNEL settings

```
                                                Your choice ? 2
Own Port (3001):
Partner IP(  0) .(  0) .(  0) .(  0)
Partner Port (0):
Idle Force T.O. chars(Max 255): (10):
```

Figure 3-14 Port settings

1. Setting of the own port through which the application communicates
2. Setting the IP address of the remote terminal
3. Setting the port number of the remote terminal

Setup 3 - PROTOCOL settings

```
                                                Your choice ? 3
Mode: UDP:0 TCP:1 MODBUS_TCP:3 PPP:4 (1):
Type: Server:0 Client:1  (0):
```

Figure 3-15Mode settings

1. Setting of the communication protocol (default: TCP)
2. Setting the device type (default: Server)

Setup 7 - FACTORY defaults

This option can be used to reset the configurations (all passwords and application settings) of the device to the factory settings.

The IP address cannot be reset in this case.

Setup 8 - Exit without save

With this option the Telnet session can be left without saving the changed parameters.

Setup 9 - Save and Exit

This option saves all changed parameters and exits the Telnet menu.

Setup 10 and 11 - Get/Put Setup

With these options, device configurations can be uploaded or downloaded externally.

Please request separate instructions for this.

3.3 Sending a ping

You can use the PING command to check whether a connection to the desired device is possible.

1. Open the command prompt (DOS box) in the Windows Start menu under "Programs... Accessories... Command Prompt".
2. Type the following command: ***PING <IP address>*** , e.g.:

   ```
   PING 192.168.0.162
   ```
3. The participant reports back in the standard with three responses:

   ```
   Reply from 192.168.0.162: bytes=32 time=10ms TTL=32
   ```
4. If the feedback is not received, the system reports a timeout:

   ```
   Request timed out
   ```

Additional parameters can be used to send multiple ping commands in sequence with a specific size, etc.

-tRepeats the ping command until the user responds with	<STRG> C aborts.
-n"count"	Repeatsthe ping command as often as entered in "count".
-l "size"	The packet is padded by the "size" number of bytes.
-w "timeout"	The "timeout" time (in milliseconds) on a return message is set. ding serviced.

3.4 Web Based Management - WBM

3.4.1 General function

Online diagnosis

The convenient web-based management interface allows you to manage the FL COMSERVER ... 232/422/485 from anywhere in the network using a standard browser. Extensive configuration and diagnostic functions are clearly displayed on a graphical user interface. Any user can access the device via a browser - assuming a network connection to the device and a known password. In accordance with the physical structure of the FL COMSERVER ... 232/422/485, a wide range of information about the device itself, the set parameters and the operating status can be viewed.

Accesses can only be made in connection with the valid password. In the delivery state, it is "**private**" for write accesses.

For security reasons, it is recommended that you change to a new password known only to you.

3.4.2 Requirements for the use of the WBM

Since the web server works via the Hyper Text Transfer Protocol (http), the use of a standard browser is sufficient. The call is made via the URL "http://<IP address of the device>". Beispiel: „http://192.168.0.112“.
Cascading Style Sheets Level 1 support is required to fully operate the web pages. The use of Microsoft Internet Explo- rer 5.5 or higher is recommended.

The WBM can only be called via a valid IP address. The FL COMSERVER ... is delivered with the IP address 192.168.0.254. 232/422/485 has the IP address 192.168.0.254. Refer to the section "Configuring the IP address" on page 3-2.

3.4.2.1 Structure of the web pages

The web pages are divided into four sections:

– Device type and device logo,
– Device name (assigned by the user) and loading time to avoid confusion,
– Navigation tree on the left side,
– Information tables that are filled with the current device information at runtime.

3.4.2.2 Procedure for applying configuration changes

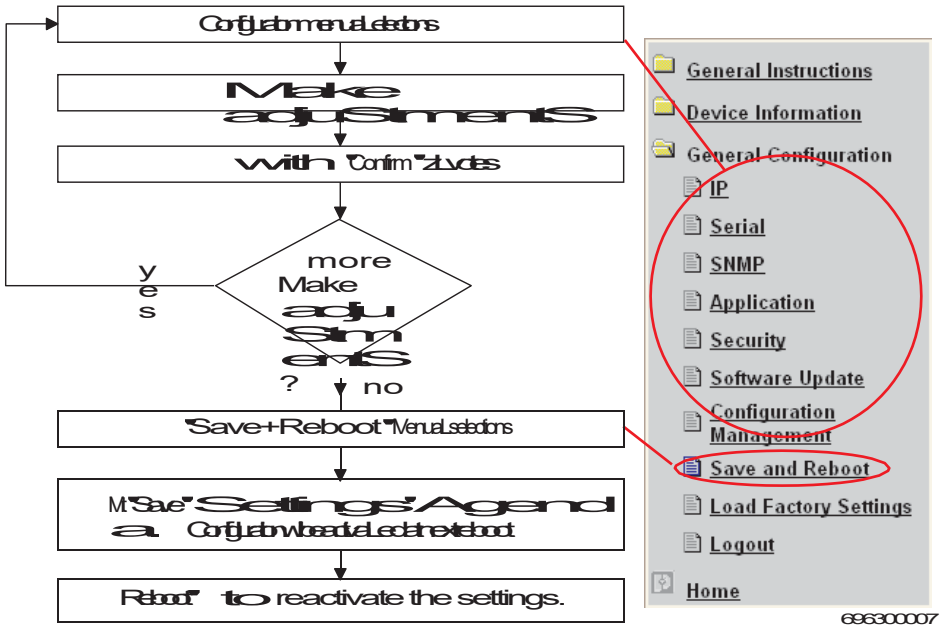


Fig. 3-16 Procedure for configuration changes with WBM

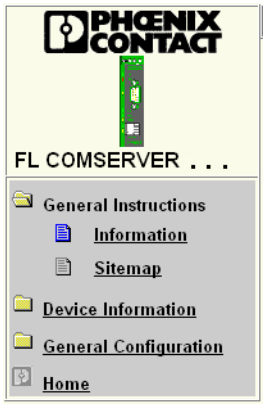
Settings made must first be confirmed by clicking "Confirm" and then permanently saved by clicking "Save current configuration for next reboot" on the "Save and Re-boot" web page.

3.4.3 Functions and information in the WBM

The navigation tree provides direct access to the following three areas:

- **General Instructions**
  Basic information about the WBM.
- **Device Information**
  Static information about the device.
- **General Information**
  Configuration and parameterization of the FL COMSERVER ... 232/422/485 .

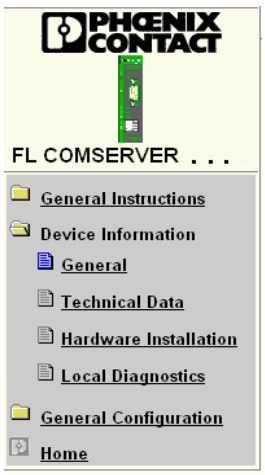
3.4.3.1 General Instructions



"Information" Menu
Here you will find a brief description of the WBM.

Sitemap" menu
Here you will find a complete navigation tree (sitemap) from which each page of the WBM is linked.

3.4.3.2 Device Information



"General" Menu
Here you will find information about the device and the manufacturer (e.g. address, designation, serial and version numbers, etc.).

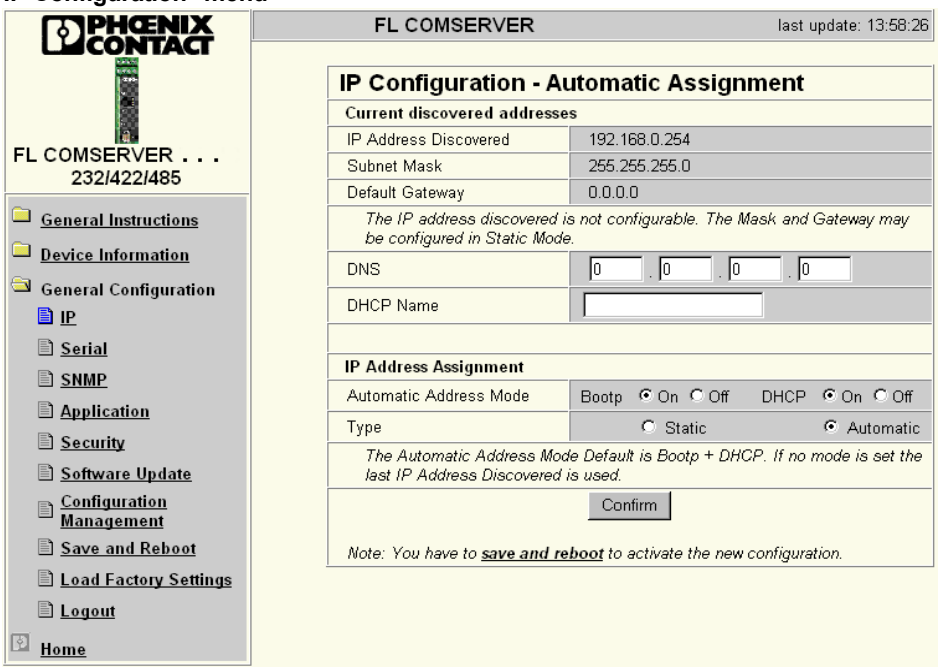
Technical Data Menu
Here you will find a compilation of the most important technical data.

Hardware Installation Menu
Here you will find a diagram for connecting the redundant power supply as well as a connection diagram for the RS-232/485 interface.

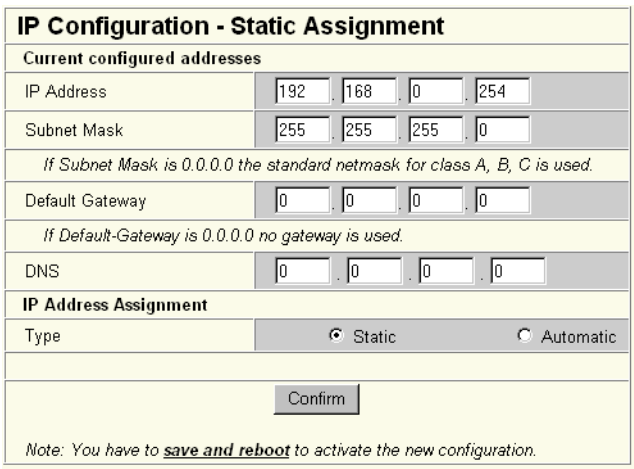
Local Diagnostics Menu
Here you will find a description of the integrated diagnostic LEDs and the current status of the displays.

3.4.4 Changing the IP settings

IP Configuration" menu

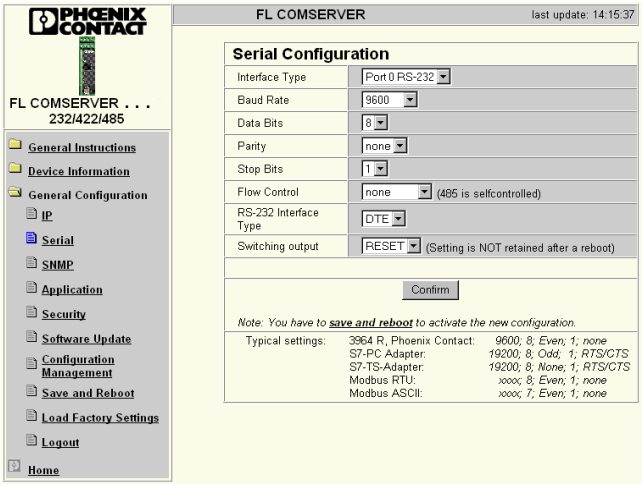


The current IP parameters and the addressing mechanism are displayed in this menu. To change the IP parameters via the WBM, the "Static" selection must be active.



3.4.5 Configuration of the serial interface

3.4.5.1 RS-232 device



In this menu, set the serial interface of the FL COMSERVER ... 232/422/485 to the requirements of the application.

Interface Type	Select the serial interface to be used for communication. The following settings are possible: - RS-232 - RS-422 - RS-485
RS-232 Interface Type	Switching between DTE and DCE. When delivered, the FL COMSERVER ... 232/422/485 is set to DTE.

3.4.5.2 Switching Output - Switching Output

The FL COMSERVER ... 232/422/485 has a transistor switching output for connecting accessories such as the PSI MODEM SPLITTER (article no. 2708766), (see chapter "Point-to-point / PSI MODEM SPLITTER" on page 4-1).

The transistor - switching output is located on the backplane and is to be used in a composite station with T-Bus connectors (see chapter 2.4.2).

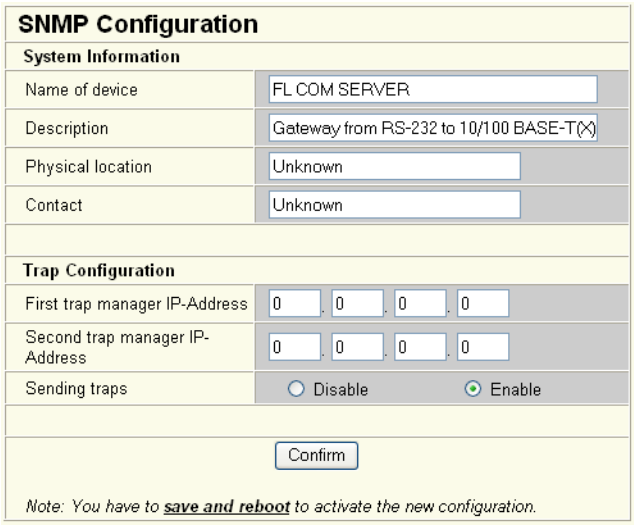
To switch the output, set the setting under "Switching output" to SET.
The output is reset with the Reset setting.
After a power failure or a reboot of the device, the output is also reset.

3.4.6 Configuration of the SNMP traps

SNMP Configuration Menu

System InformationIn this part of the table, user-specific device data, e.g. location, device name or function, can be displayed or changed.

Trap ConfigurationIn this area of the table you can read or change the IP addresses of the two trap receivers. You can also activate or deactivate the sending of traps here.



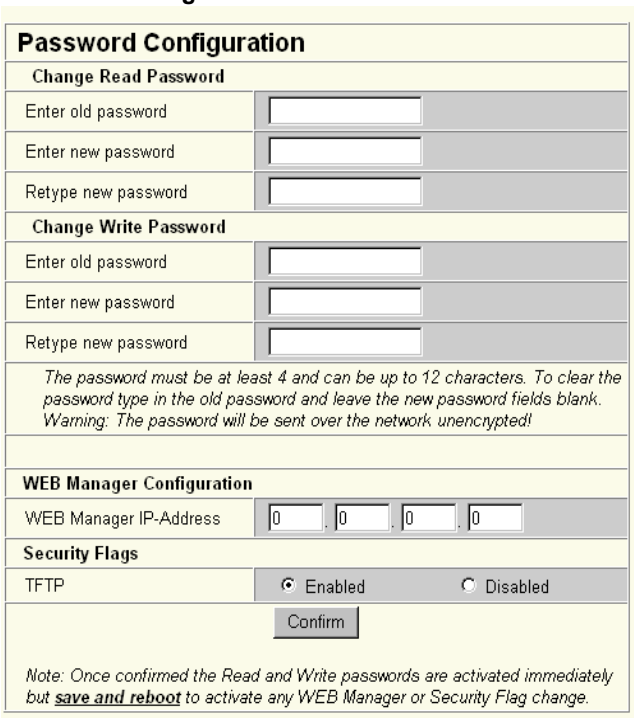
3.4.7 Application settings

Application settings" menu

Here you can make the settings for the desired application. These are
z. e.g. protocol used, port number, destination IP, etc. This menu is described separately in the chapter "Applications" on page 4-1.

3.4.8 Change the password

Password Configuration Menu



Enter a new password here that is known only to you, specifying the current password. The default password for write access is "private" (upper case).
/(case sensitive). A password for read access is not stored in the delivery state.

The password must be between four and twelve characters long. Note that the password is always transmitted unencrypted over the network.

Password forgotten?
An emergency access is available via the serial interface. You can use this to reset the device to the delivery state with the aid of Hyperterminal, for example (see Chapter 3.2.4.2).

WEB Manager IP address

Here you can enter the IP address of a PC in the network.
Only via this PC (IP address) is it then possible to access the FL COMSERVER ... 232/422/485 is possible.

Security Flags - TFTP

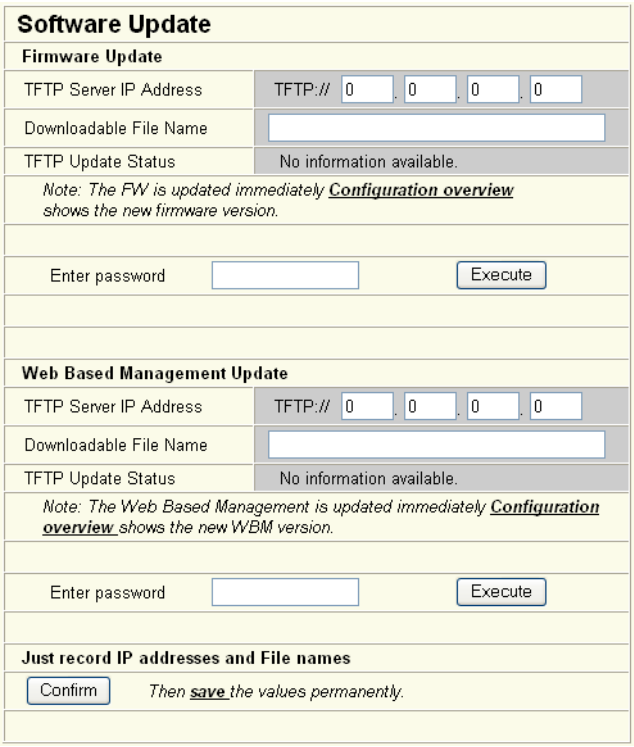
Here you can enable or disable the transfer of configuration files via a TFTP server (see chapter 6.2.2 and chapter 6.2.3).

3.4.9 Update the software and firmware

Software Update" menu

Firmware UpdateHere you can read or change the parameters for a firmware update and trigger the update.

Web Based Management Update Here you can read or change the parameters for a WBM update and trigger the update.



After a firmware or WBM update, a reset is required to activate the new ver- sion.

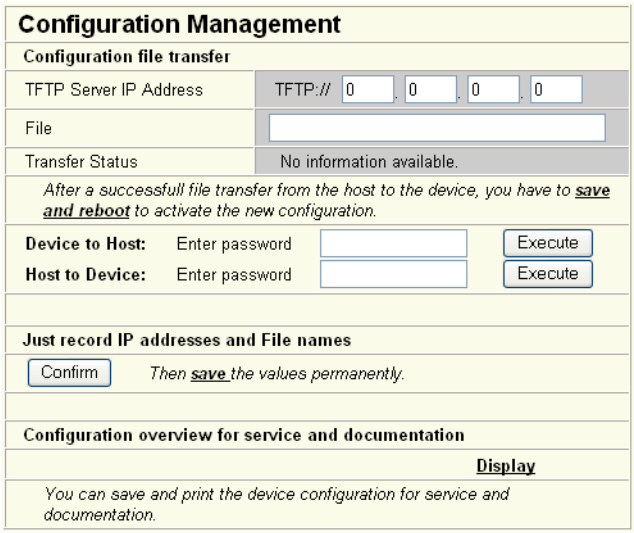
Just Record IP addresses and File names With this item you can enter the IP address of the TFTP server and the stored file name of the firmware file.

3.4.10 Save and load the device configuration

Configuration Management Menu

Configuration file transfer

Here you can save the current configuration of the FL COMSERVER ... 232/422/485 in a backup file (direction: Device to Host). Conversely, you can restore a backup file to the FL COMSERVER .... 232/422/485 (direction: host to device). This function can be used in particular in series production.



During a configuration upload from the FL COMSERVER ... 232/422/485 to a PC, the last saved version is transferred. To transfer the current configuration, it is recommended to save it again beforehand ("Save + Reboot" menu).

When downloading a configuration from a PC to a FL COMSERVER ... 232/422/ 485, the new configuration is only activated after a reset of the FL COMSERVER ... 232/422/ 485 is activated.

Configuration via a configuration file is used for device replacement. If devices are to be duplicated via configuration file, the following details must be observed:

– Establishing a connection from the FL COMSERVER ... 232/422/485 to an FTP ser- ver or local connection via the RS-232 interface of the FL COMSERVER ... 232/422/485.
– Load the configuration file onto the FL COMSERVER ... 232/422/485.
– Reset the FL COMSERVER ... 232/422/485.
– Adjust IP parameters.
– Save current configuration.

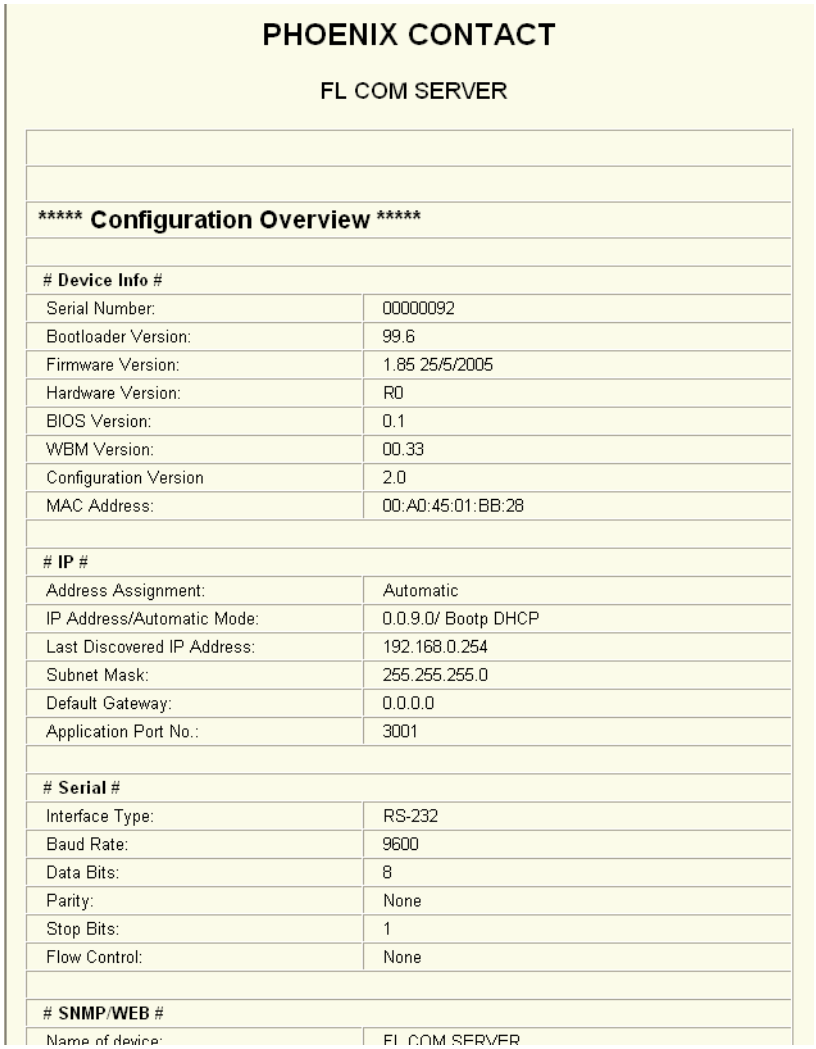
The duplicated FL COMSERVER ... 232/422/485 can now be operated in the network with the adapted IP parameters.

Just record IP addresses and File names

With this item you can fix the IP address of the TFTP server and the file name of the saved configuration file.

Configuration overview ...

This item opens a new window in the browser. The current values of all variable settings are clearly displayed in an HTML file. You can now easily print out this configuration overview for plant documentation. Alternatively, you can save this information as an HTML or TXT file on a data carrier using the browser's "Save as" menu.



PHOENIX CONTACT

FL COM SERVER

***** Configuration Overview *****

# Device Info #	
Serial Number:	00000092
Bootloader Version:	99.6
Firmware Version:	1.85 25/5/2005
Hardware Version:	R0
BIOS Version:	0.1
WBM Version:	00.33
Configuration Version	2.0
MAC Address:	00:A0:45:01:BB:28
# IP #	
Address Assignment:	Automatic
IP Address/Automatic Mode:	0.0.9.0/ Bootp DHCP
Last Discovered IP Address:	192.168.0.254
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
Application Port No.:	3001
# Serial #	
Interface Type:	RS-232
Baud Rate:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None
# SNMP/WEB #	
Name of device:	FL COM SERVER

This function is only used for the plain text display of the settings. Automatic configuration of the device by file download is only possible with the "Configuration file transfer" function on page 3-23.

For more information on the Configuration Management menu, see Chapter 6.2.

3.4.11 Acceptance of the configuration changes and restart of the device

Save and Reboot Menu

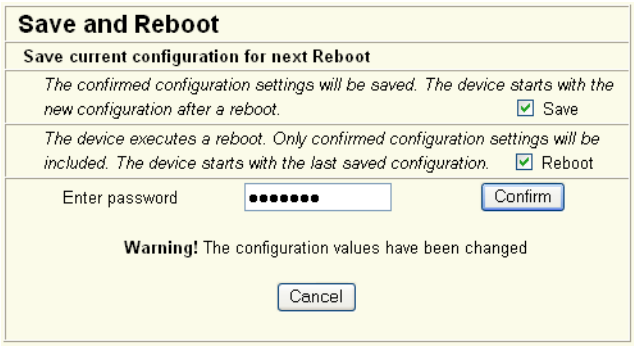


Figure 3-17Save and Reboot menu with present changes

Save current configuration for next Reboot

Here you can save the current configuration perma- nently by entering the valid password and/or initiate a restart of the device.

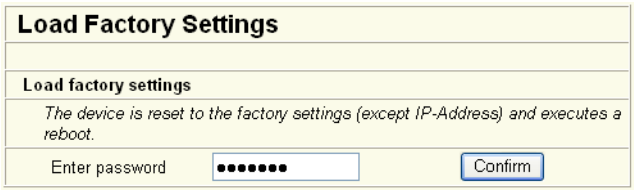
As soon as configuration changes have been confirmed, the "Save" checkbox is activated and a warning message appears (see Fig. 3-17).

The new configuration will not be active until the next reboot. To do this, activate the "Reboot" checkbox.

Configuration changes that have only been agreed to and are not yet permanently saved can be discarded by deactivating the "Save" checkbox and activating the "Reboot" checkbox.

3.4.12 Reset to factory settings

Load Factory Settings Menu



Load factory settingsHere you can reset the configuration of the FL COMSER- VER ... 232/422/485 to the factory settings.

The IP settings are excluded so that the FL COMSERVER ... 232/422/485 can still be configured via the WBM.

3.4.13 End configuration session

Logging out" menu

Logging outHere you can terminate the configuration session definitively and immediately. If the configuration is to be continued afterwards, the password will be requested again. It is not possible to resume via the browser's "Back" button.

For security reasons, always end the configuration via this menu item.

4 Applications

4.1 Overview and selection

Thanks to its wide range of integrated functions, the device can be used variably for a wide variety of applications. The user is comfortably supported during configuration by the web-based management. The following applications are supported by the FL COMSERVER ... 232/422/485 are supported.

Point to point / tunnel
(see "Cable replacement with peer-to-peer connection" on page 4-10)

A common application is the simple point-to-point connection of two serial devices via an existing network. For this cable replacement, the data is tunneled through the network with two FL COMSERVER ... 232/422/485 tunnel the data through the network and any range restrictions, e.g. max. 15 m for RS-232, are thus eliminated.

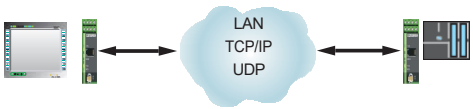


Fig. 4-1 Point-to-point connection / tunnel

Point-to-Point / PSI MODEM PLITTER

In another application, the additional device PSI-MODEM-SPLITTER (article no. 2708766) enables interface switching between two RS-232 channels or ports.

The optional switching of the point-to-point coupling is performed via the WBM of the FL COMSERVER ... 232/422/485 or via the switch on the front of the splitter (see chapter 3.4.5.2).

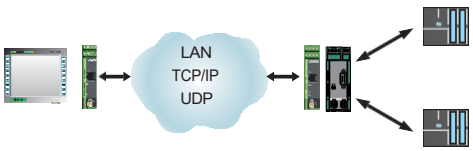


Fig. 4-2 Point-to-point coupling (two controllers)

Client-server operation
(see "Application Settings menu description" on page 4-6)

If, on the other hand, the serial data of an application software is to be available in the network, only a FL COMSERVER ... 232/422/485 is installed on the serial device. The FL COMSERVER ... 232/422/485 can then make the data available as a client or server and transmit it in TCP/IP or UDP. The so-called sockets of the application software can thus directly access the serial data in the field.

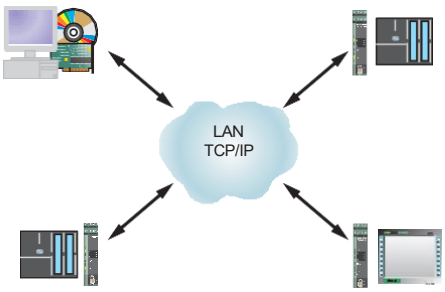


Figure 4-3 Client-server operation

Redirector / Virtual COM ports
(see "COM port redirector" on page 4-12)

Often, the existing application software does not support Ethernet communication. In contrast, local connections, e.g. to programming interfaces, should often be implemented via the existing network card of the PC and the connected network against the background of progressive networking. The COM port redirector software included in the scope of delivery provides a remedy for this. It creates virtual COM ports on the PC that are used by the existing application software. The application software does not have to be changed, so that the connection to programming interfaces with all the advantages of networking can be realized in a simple way.

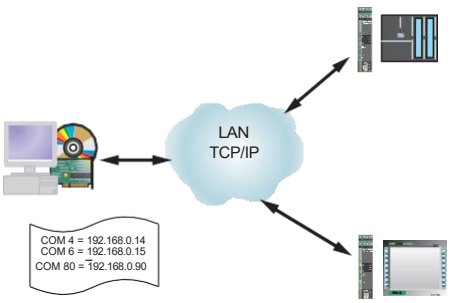


Figure 4-4 Redirector / Virtual COM ports

Modbus gateway / multidrop networks (see "Modbus gateway" on page 4-27)

Classic RS-485 multidrop networks can also be supplemented or replaced by modern network technology with the FL COMSERVER UNI 232/ 422/485. Modbus is the best known representative of this technology. The FL COMSERVER UNI 232/422/485 supports both the serial Modbus ASCII and RTU protocols as well as the Ethernet-based Modbus TCP protocol. The full-fledged gateway function allows the use at Modbus masters and slaves and thus the integration of any serial Modbus participants into Modbus TCP networks.

Other multidrop networks can be addressed by simple broadcast addressing to all network nodes or by means of intelligent mechanisms. For this purpose, the necessary target address is read directly from the serial data stream and used for addressing.

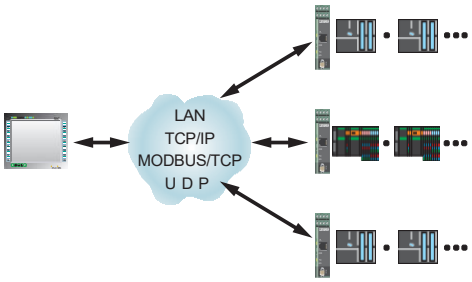


Figure 4-5 Modbus gateway and other multidrop networks

Remote access to remote networks (see "PPP applications" on page 4-31)

Dial-up to remote networks that are otherwise difficult to reach (e.g. wind farms) can be ensured in a simple way via a modem connection (dial-up) in combination with the FL COMSERVER ... 232/422/485. The FL COMSERVER ... 232/422/485 supports the PPP protocol with CHAP authentication (Challenge Authentication Protocol). This secures unauthorized access to the network by means of 128-bit password encryption. This makes remote maintenance and remote diagnostics of remote network users as easy as private dial-up to the Internet.

Furthermore, by combining the new PSI WL BLUETOOTH converter with the FL COMSERVER ... 232/422/485 a Bluetooth access point can be realized. This enables the wireless integration of serial nodes into an Ethernet network with a range of up to 150 m.

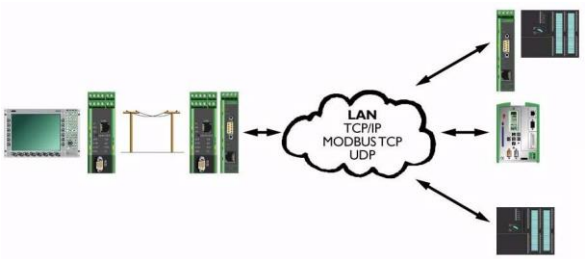


Figure 4-6 Dial-up to remote networks with RAS server

4.2 General operation

The FL COMSERVER UNI 232/422/485 supports the UDP, TCP and Modbus TCP protocols for data transmission, each with client and server accesses. Applications can therefore often be implemented in different ways. The main differences between the protocols are shown in the following table.

Table 4-1 Differences in Ethernet protocols

Feature	UDP	TCP
Unique connection	no	yes
Connection control through targeted opening and closing of the connection	no	yes
Correct packet order guaranteed	no	yes
Timeout possible	no	yes
Acknowledgement of data transmission	no	yes
Data transmission secured by checksum	yes	yes

In UDP mode, the pending data is sent immediately. However, the communication partner does not send any feedback about the correct transmission. Destroyed or lost packets must either be requested again by the connected application software or the application allows such transmission errors, e.g. for temperature values.

In TCP/IP or Modbus TCP operation, there is a fixed connection between two participants. The communication partner confirms the correct data transmission. The participant that initiates the connection is referred to as the client. The participant that accepts the connection is referred to as the server.

UDP: For frequently changing communication partners or if data security is guaranteed by the connected application software.
TCP: For large data volumes, continuous data traffic, and a high level of data security.

The data transfer takes place in several individual steps.

– The FL COMSERVER ... 232/422/485 unpacks the serial data from the serial packet and puts it back into a TCP/IP packet.
– The FL COMSERVER ... 232/422/485 sends the data via the LAN network.
– Data is transmitted through infrastructure components such as hubs, switches, etc.
– The FL COMSERVER ... 232/422/485 receives the data and unpacks it from the TCP/IP packet and then puts it back into serial data packets.
– The FL COMSERVER ... 232/422/485 transmits the data to the serial device.

This mode of operation leads to delays that can additionally fluctuate strongly due to the existing network load.

4.3 Menu description "Application Settings

The "Application Settings" menu dynamically changes the menu structure depending on the settings made. The user is shown the menu items that are relevant for the application.

The menu adjusts dynamically for the items "Operation Mode" and "Multi Device Setting" after confirmation with "Confirm". This results in three possible menu structures.

Confirm each time after selecting the "Operation Mode" and the "Multi Device Settings" with "Confirm" so that the menu structure is updated.

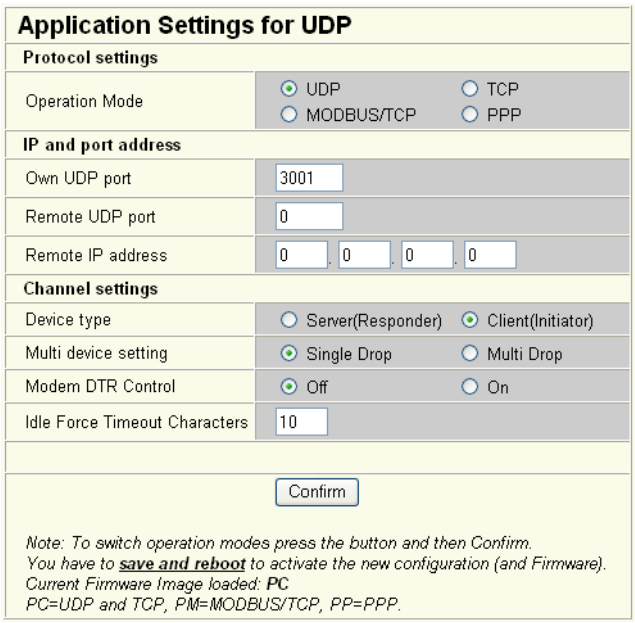


Figure 4-7 Application Settings menu for UDP, single-drop operation

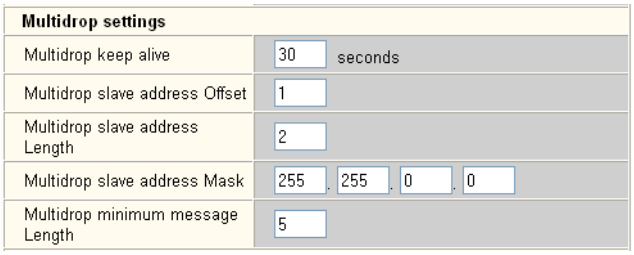


Image 4-8 Menu extensions for multi-drop operation

Table 4-2 Description of the "Application Settings" menu items

Menu heading	Menu selection	Explanation
Protocol settings		
Operation Mode	UDP	User Datagram Protocol
	TCP	Transport Control Protocol
	MODBUS TCP	Modbus Transport Control Protocol
	PPP	Point to Point Protocol (RAS Server)
IP and port address		
Own UDP port	3001	Own communication port
Remote UDP port	3001	Port of the communication partner
Remote IP address	0.0.0.0	IP address of the communication partner
Channel settings		
Device type	Server (Responder)	The device accepts connections
	Client (Initiator)	The device initiates the communication
Multi device setting	Single drop	Point to point connection
	Multi drop	Multipoint connection
Modem DTR control	OFF	The DTR control signal is ignored
	ON	The DTR control signal is taken into account / controlled
Idle Force Timeout Characters	10	Number of characters that are collected before a data packet is sent. A small number increases the speed, but also the network load, since a data packet is transmitted for a small number of characters.

Table 4-2 Description of the "Application Settings" menu items (continued)

Menu heading	Menu selection	Explanation
Options for multi-drop operation		
Multidrop settings		
Multidrop keep alive	30 seconds	Time interval in seconds in which the FL COMSERVER ... 232/422/485 reports back to the bus slaves with a sign of life or in which the FL COMSERVER ... 232/422/485 expects a sign of life at the bus master.
Multidrop slave address offset	1	Position of the slave address in the data telegram
Multidrop slave address Length	2	Length of the slave address in the data telegram (max. 4 bytes)
Multidrop slave address Mask	255.255.0.0	Mask with which individual bits can be masked out of the first 4 bytes of the data telegram in order to extract the slave address.
Multidrop minimum message Length	5	Minimum telegram length in bytes. Shorter telegrams (e.g. acknowledge) are handled specially and forwarded directly to the last sender address.
Options for TCP operation		
Remote domain name		As an alternative to the static IP address, the name of a network subscriber can be entered here.
Modem mode	OFF	Modem operation is deactivated
	ON without echo	The TCP connection setup is controlled by AT commands.
	ON with echo	The TCP connection setup is controlled by AT commands. The AT commands sent are echoed back to the sender for evaluation.
Disconnect with inactivity timeout	0 minutes 0 seconds	As soon as no data is transferred for the set time (IDLE), the TCP connection is closed. Special case: 0 minutes : 0 seconds, the connection is never closed.
PC Flush Mode	Clear Input Buffer	**ON:** When a connection is established, the input buffer is cleared.
		OFF: When a connection is established, the input buffer is not cleared.
	Clear Output Buffer	**ON:** When a connection is established, the output buffer is cleared.
		OFF: When a connection is established, the output buffer is not cleared.

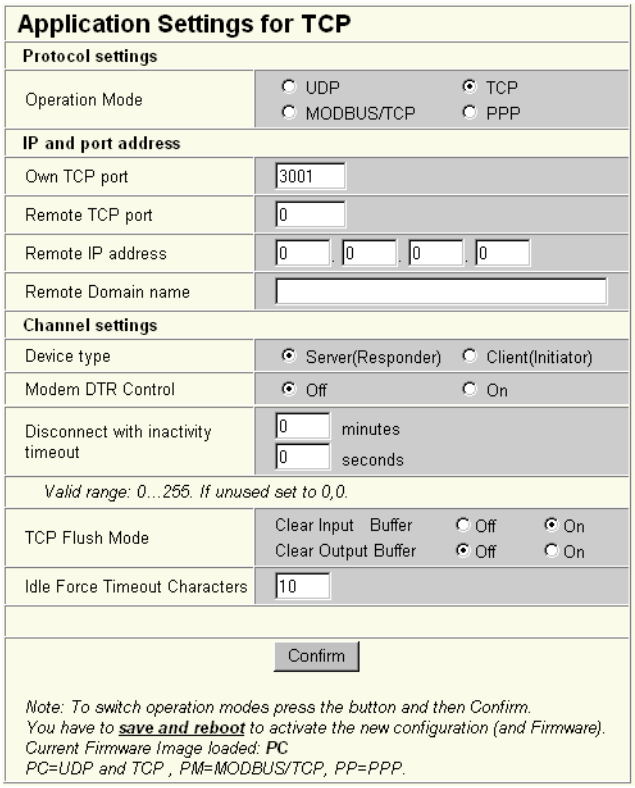


Figure 4-9 Application Settings menu for TCP operation

4.4 Cable replacement with peer-to-peer connection

The peer-to-peer connection (tunneling) is a simple way to connect two RS-232-ba- sing end devices in a point-to-point connection via an existing network. This also works across subnets and gateways. Both FL COMSERVER ... 232/422/485 are logically linked to each other via the destination and source IP.

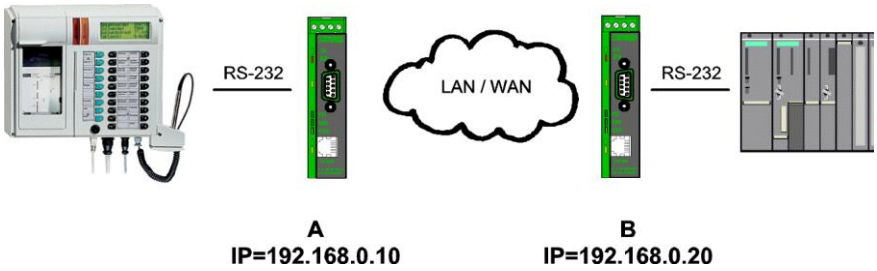


Figure 4-10 Application example peer-to-peer connection

The application can be implemented either with UDP or TCP-IP protocol.

The UDP protocol is connectionless. Transmission takes place as soon as data is available at the RS- 232 interface.

The TCP/IP protocol is connection-oriented. The connection establishment can be controlled by different conditions.

Connection establishment:

– permanent network connection after power-up
– When DTR active
– when a character is received on the serial port.

Disconnection:

– if serial communication was "Idle" (adjustable from 0 to 255 min:255 sec.)
– when DTR signal becomes inactive.

4.4.1 Settings in the UDP operating mode

Table 4-3 Application Settings in UDP mode

Parameter	Device A	Device B	Explanation
Operation Mode	UDP	UDP	User Datagram Protocol
Own UDP port	3001	3001	Communication port
Remote UDP port	3001	3001	Communication port
Remote IP address	192.168.0.20	192.168.0.10	IP address of the communication partner
Device type	Client (Initiator)	Client (Initiator)	Active communication can be started equally from both sides as soon as a pointer is received at the serial port.
Multi device setting	Single drop	Single drop	Point-to-point connection
Modem DTR control	OFF	OFF	DTR signal is ignored
IDLE FORCE Timeout Character	10	10	

4.4.2 Settings in the TCP/IP or Modbus operating mode

Table 4-4 Application Settings in the TCP/IP operating mode

Parameter	Device A	Device B	Explanation
Operation Mode	TCP/IP	TCP/IP	Transport Control Protocol / Internet Protocol
Own TCP port	3001	3001	Communication port
Remote TCP port	3001	3001	Communication port
Remote IP address	192.168.0.20	192.168.0.10	IP address of the communication partner
Device type	Client (Initiator)	Server (Responder)	The client establishes the active communication
Modem DTR control	OFF	OFF	OFF = DTR signal is ignored ON = The DTR signal is evaluated. The client establishes or terminates the TCP connection
Modem mode	OFF	OFF	Disabled, since it is a point-to-point connection.
Disconnect with inactivity timeout	0:0	0:0	TCP connection termination after xx minutes and zz seconds without data transmission. 0:0 if the TCP connection should never be closed.
TCP Responder Flush Mode	Clear input buffer	Clear Input Buffer	RS-232/485 data that was written to the FL COMSERVER ... before the TCP/IP connection was established is deleted. 232/422/ 485 are deleted.
Idle Force Timeout Characters	10	10	

Finish the configuration settings each time with "Confirm".

The new configuration will only become active at the next reboot. Activate and start the reboot in the "Save and Reboot" menu by entering the valid password.

4.5 COM Port Redirector

4.5.1 Application

The Redirector application is a special case of the peer-to-peer connection.

This allows existing application software that communicates exclusively via serial COM ports to be redirected to remote COM ports.

The COM port redirector creates virtual COM ports on the PC, which are available to the software for communication. Physically, the virtual COM ports are redirected to the network card and a target IP in the network. The receiver in the network for each COM port is **a** FL COMSERVER ... 232/422/485 with the corresponding IP address is configured as the receiver in the network for each COM port.

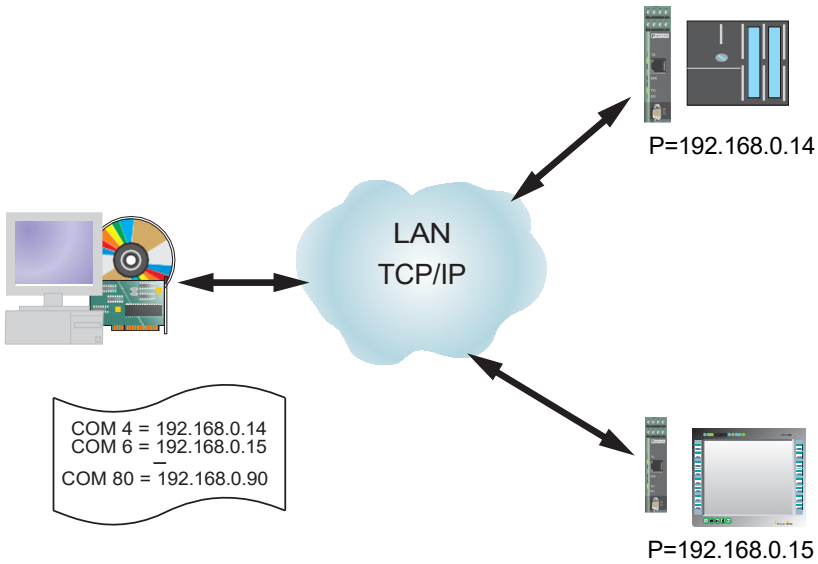


Figure 4-11 Application example COM port redirector

The communication takes place exclusively with the TCP/IP protocol.

4.5.1.1 Boundary conditions

Most software applications that require the COM port redirector were originally created for direct connection of serial devices. The direct cable connection does not cause any delays in the communication. When using the COM port redirector, the same software application is no longer directly connected to the serial device. The serial data is transferred as follows:

- The COM port redirector unpacks the serial data from the serial packet and puts it back into a TCP/IP packet.
- Then the COM port redirector sends the data via the network card to the LAN.
- Data is transmitted through infrastructure components such as hubs, switches, etc.
- The FL COMSERVER ... 232/422/485 receives the data and unpacks it from the TCP/IP packet and then puts it back into serial data packets.

– The FL COMSERVER ... 232/422/485 transmits the data to the serial device.

This path leads to delays in communication, which can also fluctuate greatly due to the existing load on the Ethernet network.

Some software applications react to these system-related transmission delays with a timeout, because the software thinks that the opposite device is not responding.

Communication via COM port redirector leads to delays, which some software applications acknowledge with a timeout.

Activate the "No Net Close" option if timeout problems occur. The option maintains the TCP/IP connection when the COM port is closed by the software application. This eliminates the need to re-establish a TCP/IP connection, which causes additional delays.

Other boundary conditions

– the COM port redirector is always the client and establishes the connection
– communication is performed exclusively via TCP/IP protocol
– up to 80 virtual COM ports can be set up.

4.5.2 Configuration of the FL COMSERVER ... 232/422/485

1. Assign an IP address to the FL COMSERVER ... 232/422/485
2. Set the serial interface in the Web Based Management under "General Configuration... Serial", set the serial interface according to the requirements of the connected device.

The settings of the serial interfaces must be identical in the software application, in the FL COMSERVER ... 232/422/485 and in the connected serial device must be identical.

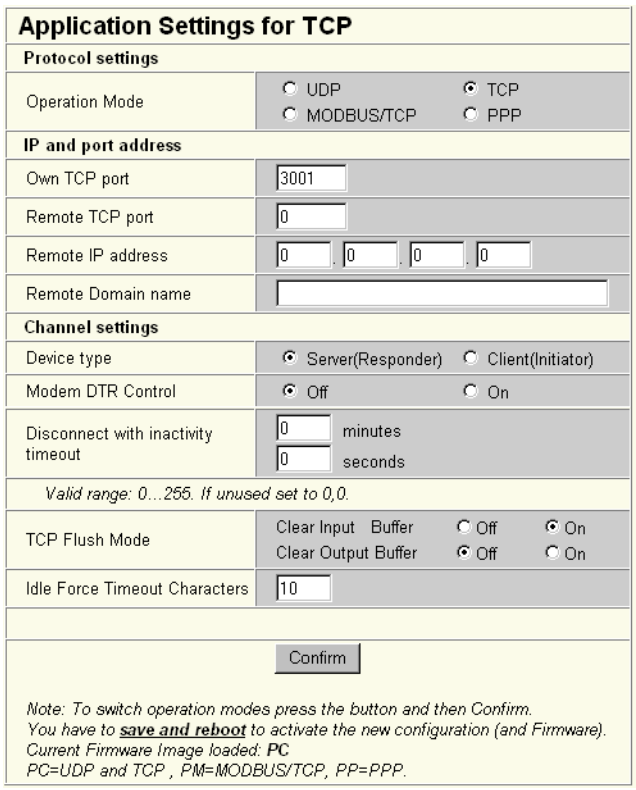


Figure 4-12 Application settings for Redirector connection

Table 4-5 Application Settings for a Redirector Application

Parameter	Device	Explanation
Operation Mode	TCP/IP	Transport Control Protocol / Internet Protocol
Own TCP port	3001	Communication port
Remote TCP port	0	Communication port
Remote IP address	0.0.0.0	Default value
Device type	Server (Responder)	The server accepts the connection. The connection is established by the Redirector software
Modem DTR control	OFF	OFF = DTR signal is ignored
Modem mode	OFF	Disabled, since it is a point-to-point connection.
Disconnect with inactivity timeout	0:0	TCP connection termination after xx minu- tes and zz seconds without data transfer. 0:0 if the TCP connection should never be closed.
TCP Responder Flush Mode	Clear Input Buffer	RS-232/485 data that was written to the FL COM- SERVER ... before the TCP/IP connection was established is deleted. 232/422/485 are deleted.
Idle Force Timeout Characters	10	The number of characters that are collected before a data packet is sent. A small number increases the speed, but also the network load, since a data packet is transmitted for a small number of characters.

Finish the configuration settings each time with "Confirm".

The new configuration will only become active at the next reboot. Activate and start the reboot in the "Save and Reboot" menu by entering the valid password.

4.5.3 Installing the Redirector software

The COM port redirector software can be found on the supplied CD.

1. Insert the CD into the CD drive. The CD will start automatically.
2. If the autostart mechanism is deactivated, change to the CD drive with the explorer and start the CD with a double click on the file "start.html".
3. Select the desired language.
4. Start the software installation by double-clicking the file "red32bit.exe".

An automatic installation routine appears.

Figure 4-13 Welcome screen

5. Click on "NEXT

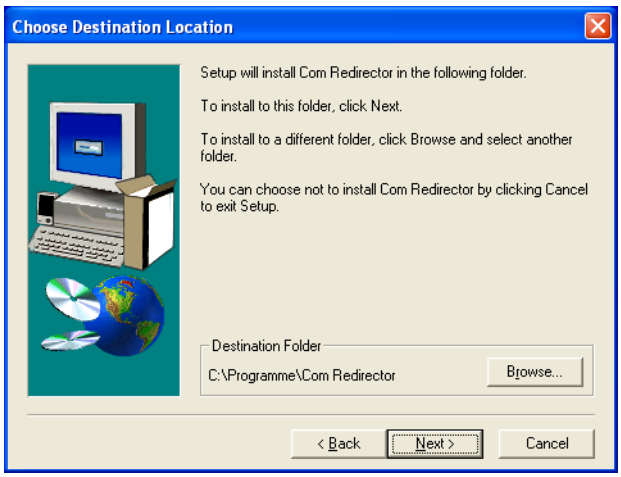


Figure 4-14Selecting the installation path

6. If necessary, select a different installation path. Close the selection by clicking on "Next".

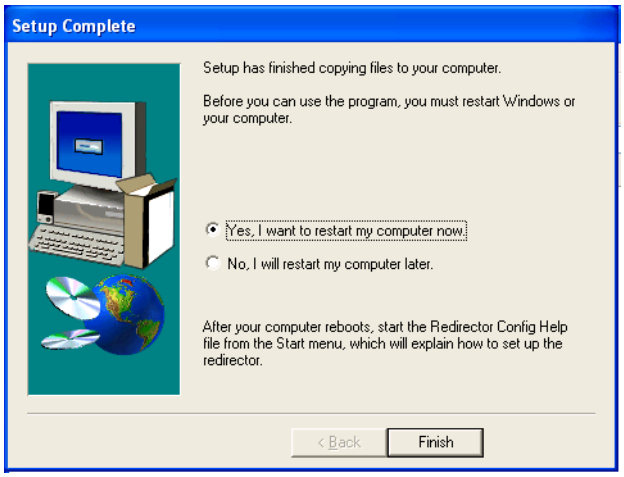


Figure 4-15 Finalize installation

7. Restart the computer.

The software is now successfully installed.

4.5.4 Selection and configuration of the virtual COM port

After installation, the program can be started from the menu "Start... Programs... Redirector... Configuration" menu. The main menu window will open.

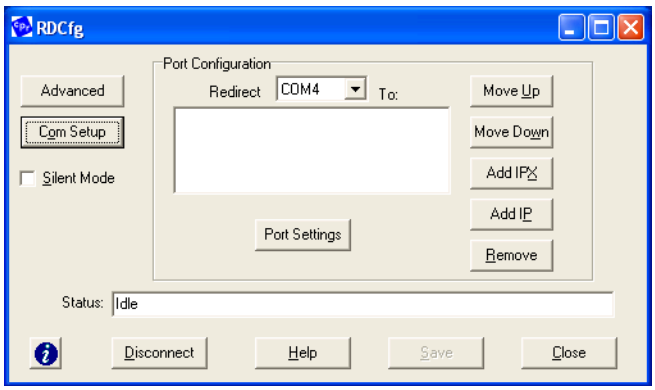


Figure 4-16 Redirector main menu

1. In the Port Setup menu, enable the port numbers to be supported.

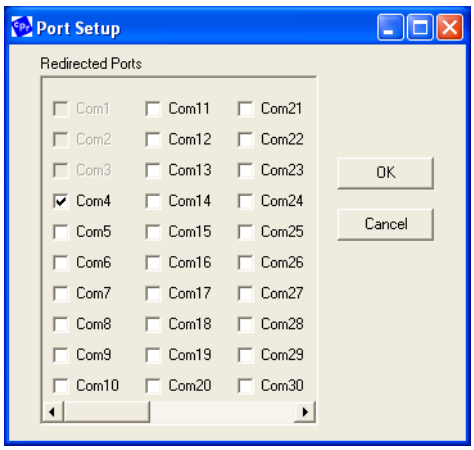


Figure 4-17 Port Setup Menu

2. Confirm the selection with "OK" and return to the main menu.
3. Select a previously enabled COM port from the pull-down menu.
4. Then click on the "Add IP" button.

The "IP Service Setup" window opens.

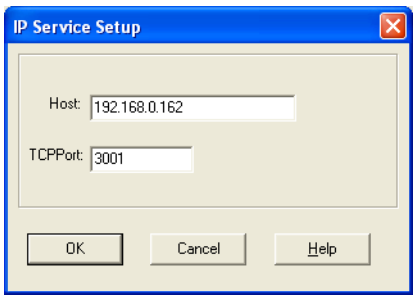


Figure 4-18 IP Service Setup Menu

5. In the "Host" field, enter the IP address of the target FL COMSERVER ... 232/422/485 to which the activated COM port is to be redirected (e.g. 192.168.0.162).
6. In the "TCP port" field, enter the port number "3001" via which the communication will be carried out.
7. Confirm your entries with "OK" and return to the main menu.
8. Then click on the "Port Settings" button. The "Port

Settings" window opens.

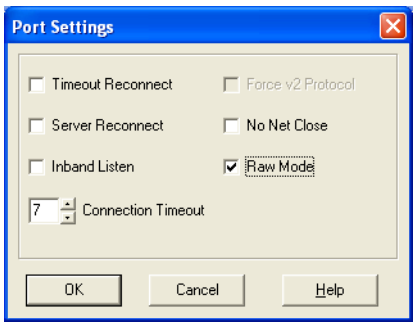


Fig. 4-19 Port Settings menu

9. Activate the "RAW mode" option.

RAW mode must **always be** enabled for Redirector applications.

10. Depending on the application, select other options for establishing and terminating connections.

Table 4-6 Options in the "Port Settings" menu

Function	Description
Timeout reconnect	With this option the COM port redirector re-establishes the TCP connection if the connection has not been established yet, the connection was interrupted by a timeout (TCP keepalive) or if the "Can- cel" button was pressed. The mechanism is terminated when the software application closes the COM port or when the "Disconnect" button is pressed.
Server reconnect	With this option the COM port redirector re-establishes the TCP connection if the FL COMSERVER ... 232/ 422/485 has interrupted the connection, the connection has not yet been established or if the "Cancel" button has been pressed. The mechanism is terminated when the software application closes the COM port or when the "Disconnect" button is pressed.
Inband lists	Without use. The FL COMSERVER ... 232/422/485 does not support "Inband Listen" operation.
Connection timeout	Specifies the maximum time in seconds until the COM port redirector aborts the connection setup. If the "Timeout Reconnect" option is also activated, each connection setup takes the set time. Without the "Timeout Re- connect" option, the connection setup is aborted after the set time.
Force v2 Protocol	Without use. The FL COMSERVER ... 232/422/485 does not support V2 protocol.
No Net Close	With this option the TCP/IP connection is not disconnected when the COM port is closed by the software application. This allows a faster communication, because there is no time delay for the Ethernet connection establishment.
Raw Mode	Must always be activated. The FL COMSERVER ... 232/ 422/485 only uses the RAW protocol.

In the "No Net Close" function, the connection can only be disconnected via the "Disconnect" button in the Redirector software.

11. Confirm your entries with "OK" and return to the main menu.

12. The "TCP KeepAlive" time is set to 7,200,000 ms (2 hours) as default. This parameter is typically not changed.

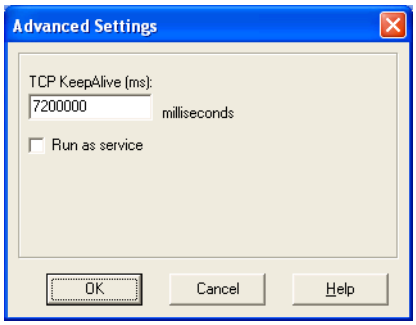


Figure 4-20Advanced Settings menu

All parameters for the selected COM port are now set. If necessary, repeat the settings for further COM ports.

CAUTION: Possible malfunction of device, device environment and hardware or software.
Restart the PC so that the virtual COM ports are safely available in the operating system.

4.5.5 Checking the connection

When all settings have been made, you can check the connection. The easiest way to do this is to use Windows Hyperterminal.

1. Open the program in the Windows Start menu under "Programs... Accessories... Communication... Hyperterminal".
2. Configure a connection with the new virtual COM port.
3. Confirm with OK.
4. Hyperterminal opens the COM port and a pop-up window appears.

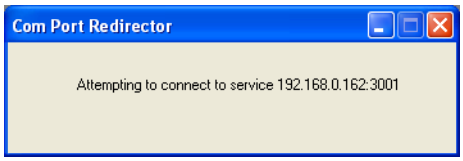


Figure 4-21 COM port redirector connection setup

5. The successful or failed connection establishment is displayed accordingly in the pop-up window.

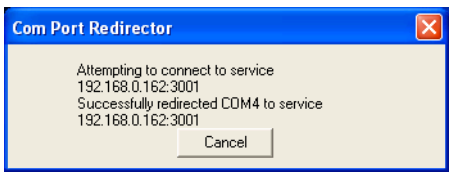


Figure 4-22 Successful connection establishment

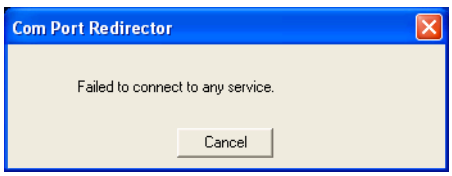


Fig. 4-23 Failed connection establishment

In the "No Net Close" function, the connection can only be disconnected via the "Disconnect" but- ton in the Redirector software.

4.6 Modem operation

In modem mode, the FL COMSERVER ... 232/422/485 behaves like a dial-up modem. The connection establishment and termination is controlled via AT commands. This allows costly modem connections to be easily replaced by an inexpensive network connection.

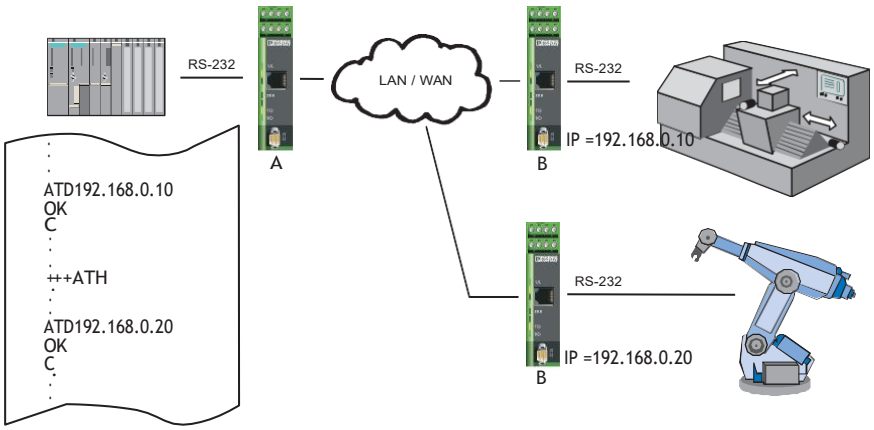


Fig. 4-24Modem operating mode

Communication can be implemented using TCP/IP protocol only. Connection establishment:

– Dialing with AT command, followed by IP address and port number.

Disconnection:

– AT command +++ATH or
– DTR control signal or
– Closing of the TCP connection by the communication partner.

4.6.1 Settings in the modem operating mode

Table 4-7 Application settings in modem operating mode

Parameter	Device A	Device B	Explanation
Operation Mode	TCP/IP	TCP/IP	Transport Control Protocol / Internet Protocol
Own TCP port	3001	3001	Communication port
Remote TCP port	0 or 3001	0	Communication port
Remote IP address	0.0.0.0 or 192.168.0.10	0.0.0.0	IP address of the communication partner
Device type	Client (Initiator)	Server (Responder)	The client establishes the active communication
Modem DTR control	ON	OFF	OFF = DTR signal is ignored ON = The DTR signal is evaluated. The client establishes or terminates the TCP connection
Modem mode	ON	OFF	The FL COMSERVER ... 232/422/485 sends the AT commands back to the sender in the operating mode "On with echo
Disconnect with inactivity timeout	0:0	0:0	TCP connection termination after xx minutes and zz seconds without data transmission. 0:0 if the TCP connection should never be closed.
TCP Responder Flush Mode	Clear Input Buffer	Clear Input Buffer	RS-232/485 data that was written to the FL COMSERVER ... before the TCP/IP connection was established is deleted. 232/422/ 485 are deleted.
Idle Force Timeout Characters	10	10	Number of characters that are collected before a data packet is sent. A small number increases the speed, but also the network load, since a data packet is transmitted for a small number of characters.

Finish the configuration settings each time with "Confirm".

The new configuration will only become active at the next reboot. Activate and start the reboot in the "Save and Reboot" menu by entering the valid password.

The FL COMSERVER ... 232/422/485 only accepts uppercase letters when entering AT commands.

Table 4-8 AT command set

AT command	Function
AT	Attention string with which each modem command starts
ATS?	The set values of the remote IP and the remote port number from the FL COMSERVER ... 232/422/485 are displayed
Optional ATD<IP address>,<port number> ATD<IP address>/<port number> ATD<IP address>:<port number> ATDT<IP address>,<port number> ATDT<IP address>/<port number> ATDT<IP address>:<port number>	Connection setup to <IP address> and <port number>.
Optional ATD<IP address> ATDT<IP address>	Connection setup to <IP address> . The communication port used is the remote port number set in the FL COMSERVER ... 232/422/485 is used as the communication port.
Optional ATD ATDT	Establishing a connection to the communication partner that is permanently set as the remote IP and remote port number in the FL COMSERVER ... 232/422/485 is permanently set.
C	Connected, the TCP connection to the communication partner is established. The FL COMSERVER ... 232/422/485 has changed from the "Command mode" to the "Data mode" status.
D	Disconnect, the TCP connection was interrupted or could not be established at all. The FL COMSERVER ... 232/422/485 has changed from the status "Data mode" to the status "Command Mode" changed.
E	Error, an error has occurred
OK	The FL COMSERVER ... 232/422/485 has executed a modem command
+++	Abort sequence to change from data to command mode
ATH	Terminates the connection and switches back to command mode

All other AT commands have no function and are acknowledged in command mode by the FL COMSERVER ... 232/422/485 with **Not Accepted**, followed by the indication of the possible AT commands.

4.6.2 Change from data mode to command mode

To terminate a connection with AT commands, the following conditions must be observed:

- The data traffic must be idle for at least 1 second before the abort sequence **+++** may be sent
- The time between the input of each plus sign must not be greater than one second
- After the abort sequence **+++** a pause of 1 second must follow again
- When the FL COMSERVER ... 232/422/485 has changed to command mode, it returns an **OK.**
- Type **ATH** and press the **ENTER key**. If the modem operating mode "On with echo" is activated you will get another **OK.**

4.7 Modbus gateway

The Modbus gateway application is only supported by the FL COMSERVER UNI 232/422/485!

The master-slave mode is based on RS-485 networking. Here, a bus master sends an addressed call and receives the response from the addressed slave. By using the FL COMSERVER UNI 232/422/485, the RS-485 network is simply replaced by an existing Ethernet network.

The operating mode enables simple integration of serial Modbus stations into a Modbus TCP network. Entire bus systems can also be operated on the FL COMSER- VER UNI 232/422/485. The FL COMSERVER UNI 232/422/485 supports both Modbus RTU and Modbus ASCII. However, the entire system can only be operated in one operating mode at a time (RTU or ASCII). Of course, the Modbus TCP master can also control the network directly, i.e. without FL COMSERVER UNI 232/422/485.

Depending on whether the FL COMSERVER UNI 232/422/485 are connected to the bus master or to one of the bus slaves, they receive different configurations. Two mechanisms are available for configuring the bus masters:

– The FL COMSERVER UNI 232/422/485 on the Modbus master receives a list of which slave addresses can be addressed via which IP address. An entire bus system can be connected to the FL COMSERVER UNI 232/422/485.
– The FL COMSERVER UNI 232/422/485 on the Modbus master extracts the called slave address from the serial data stream and thus completes the last octet of the target IP address. In this operating mode, only individual Modbus stations can be connected to a FL COMSERVER UNI 232/422/485.

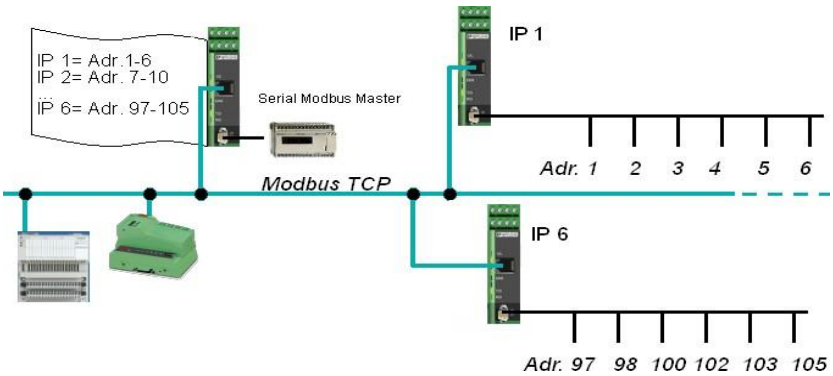


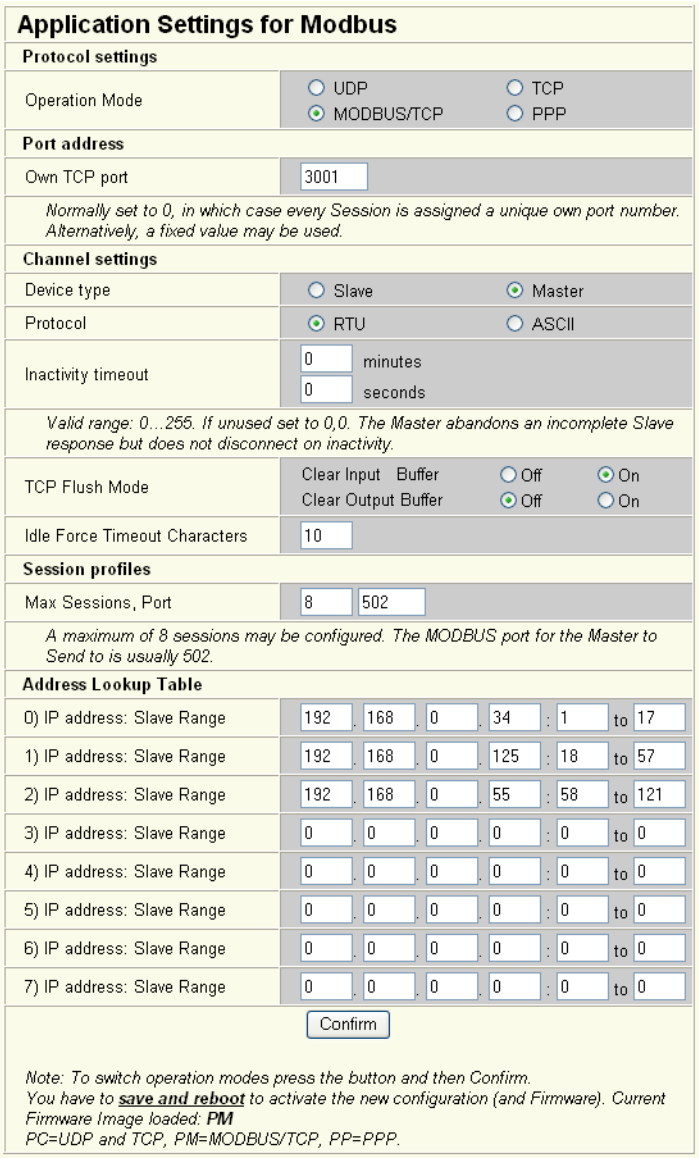
Fig. 4-25Modbus application

4.7.1 Master configuration

Either a PC with network card and Soft-PLC can be used as Modbus-TCP master or a serial master can be converted to a Modbus-TCP master by means of a FL COMSERVER UNI 232/422/485 (see Fig. 4-26).

Configuration for FL COMSERVER UNI 232/422/485 operation with slave list

1. First switch in the WBM to the menu "General Configuration... Application" menu.
2. Activate the operation mode "MODBUS/TCP".
3. Confirm the selection with the "Confirm" button at the end of the menu. The menu adapts dynamically.
4. Activate under "Channel Settings... Device Type... Master".
5. Enter the IP addresses of the FL COMSER- VER UNI 232/422/485 to which the bus slaves are connected under "Master Address Lookup Table".
6. After the colon enter the address range of the Modbus slaves that are accessible via this IP address.



Application Settings for Modbus

Protocol settings

Operation Mode	○ UDP ○ TCP ◉ MODBUS/TCP ○ PPP

Port address

Own TCP port	3001

Normally set to 0, in which case every Session is assigned a unique own port number. Alternatively, a fixed value may be used.

Channel settings

Device type	○ Slave ◉ Master
Protocol	◉ RTU ○ ASCII
Inactivity timeout	0 minutes 0 seconds

Valid range: 0…255. If unused set to 0,0. The Master abandons an incomplete Slave response but does not disconnect on inactivity.

TCP Flush Mode	Clear Input Buffer ○ Off ◉ On Clear Output Buffer ◉ Off ○ On
Idle Force Timeout Characters	10

Session profiles

Max Sessions, Port	8 502

A maximum of 8 sessions may be configured. The MODBUS port for the Master to Send to is usually 502.

Address Lookup Table

0) IP address: Slave Range	192 . 168 . 0 . 34 : 1 to 17
1) IP address: Slave Range	192 . 168 . 0 . 125 : 18 to 57
2) IP address: Slave Range	192 . 168 . 0 . 55 : 58 to 121
3) IP address: Slave Range	0 . 0 . 0 . 0 : 0 to 0
4) IP address: Slave Range	0 . 0 . 0 . 0 : 0 to 0
5) IP address: Slave Range	0 . 0 . 0 . 0 : 0 to 0
6) IP address: Slave Range	0 . 0 . 0 . 0 : 0 to 0
7) IP address: Slave Range	0 . 0 . 0 . 0 : 0 to 0

Confirm

Note: To switch operation modes press the button and then Confirm.
*You have to **save and reboot** to activate the new configuration (and Firmware). Current Firmware Image loaded: **PM***
PC=UDP and TCP, PM=MODBUS/TCP, PP=PPP.

Figure 4-26 Settings at the Modbus master with slave list

4.7.2 Slave configuration

The setting of the FL COMSERVER UNI 232/422/485 on the bus slaves is identical for both variants and must be carried out as follows (see Fig. 4-27):

1. First switch in the WBM to the menu "General Configuration... Application".
2. Activate the operation mode "MODBUS/TCP".
3. Confirm the selection with the "Confirm" button at the end of the menu. The menu adapts dynamically.
4. Activate under "Channel Settings... Device Type... Slave".
5. Enter under "Slave Remote TCP Port= 502".
6. Enter under "Slave Remote IP address" the IP address under which the Modbus master can be reached.

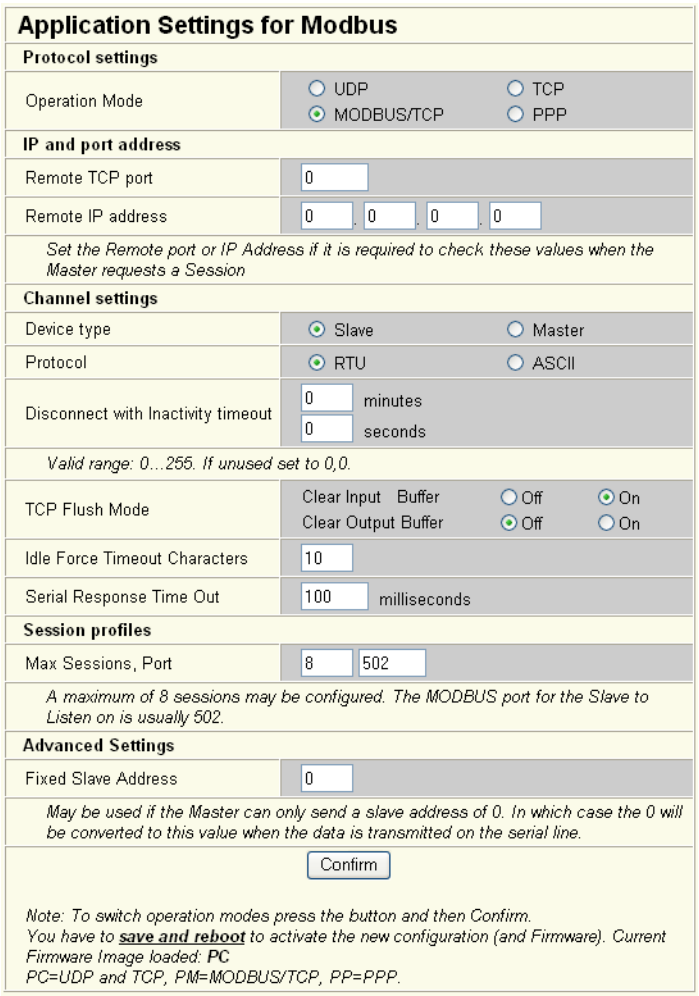


Fig. 4-27 Settings at the slaves

4.8 PPP applications

The PPP applications are only supported by the FL COMSERVER UNI 232/422/485!

4.8.1 Possible applications

The firmware and thus the range of functions of the new FL COMSERVER UNI 232/422/ 485 has been extended, which now enables a large number of new PPP applications.

4.8.1.1 Leased line connection between two Ethernet networks

This application can be realized via different physical transmission paths: - Direct connection between two comservers over up to 1000m using
the integrated RS-422 interface (see Fig. 4-28)

– Bridging of up to 20 km via simple two-wire lines with additional leased line modems, e.g. PSI-DATA/FAX-MODEM/RS232, Part No.: 2708203 (see Fig. 4-29)

– Radio connection over up to 2000 m using radio modems, e.g. RAD-ISM-2400-DATA-BD-BUS, part no. 2867872 (see Fig. 4-30)

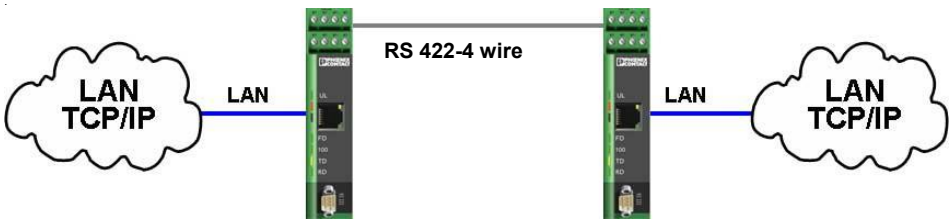


Figure 4-28 Direct RS422 connection

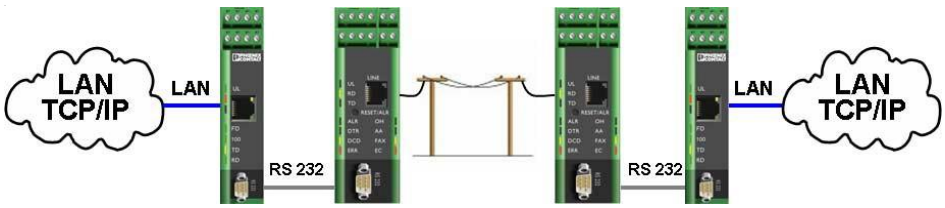


Fig. 4-29 Two-wire leased line connection

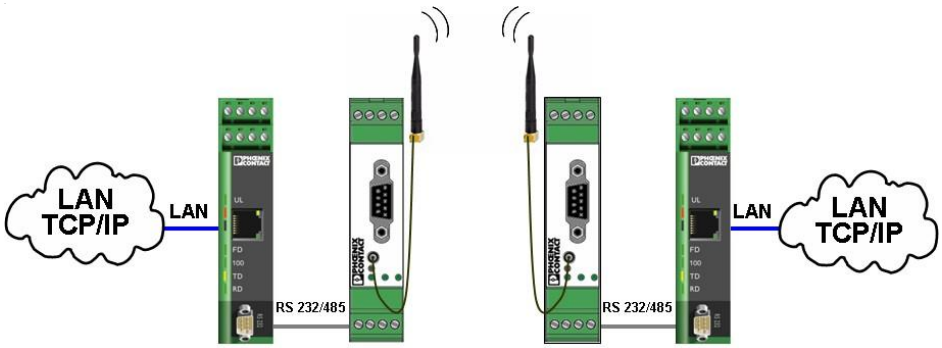


Fig. 4-30 Radio connection

For configuration please refer to chapter 4.8.2 "Configuration of a leased line connection".

4.8.1.2 Dial-up connection between two Ethernet networks

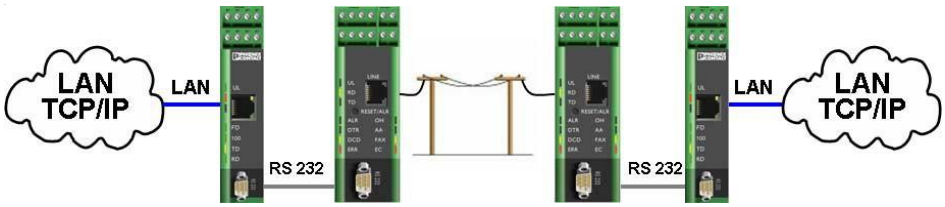


Figure 4-31 Dial-up connection

For the realization of this application the integrated variant PSI-MODEM/ETH, article no.: 2313300 can be used alternatively.

For configuration please refer to chapter 4.8.3 "Configuration of a dial-up connection".

4.8.1.3 Remote maintenance of a remote network via a modem connection

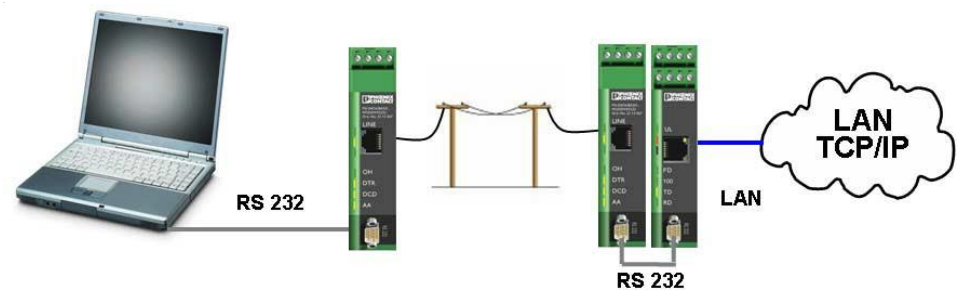


Figure 4-32 Modem connection

Phoenix Contact offers an integrated, preconfigured solution for this application. This considerably reduces the installation effort. The product is available under the designation PSI-MODEM/ETH, article no. 2313300.

For configuration, please refer to 4.8.4 "Configuring a remote maintenance connection".

4.8.1.4 Combined operation of dial-up connection and remote maintenance

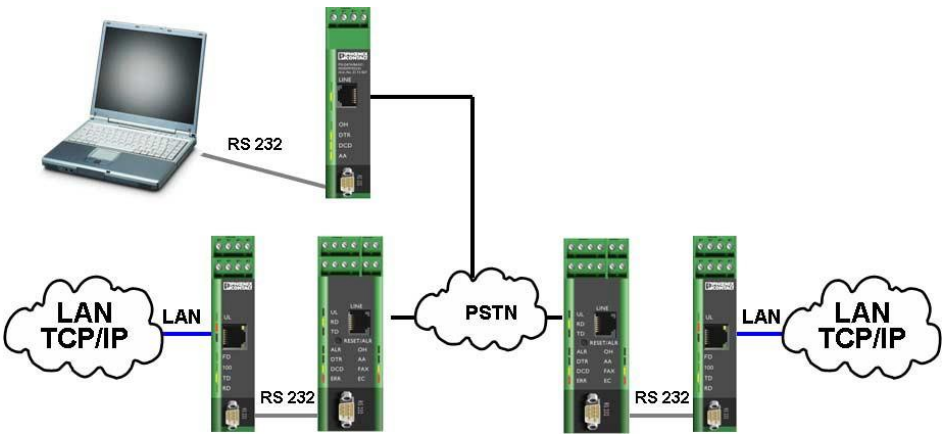


Fig. 4-33 Dial-up connection and remote maintenance

This configuration enables both the establishment of a connection from a remote network to a superordinate network (e.g. in the event of a fault in an otherwise autonomous system) and the dial-up into the network of this remote system, e.g. for a software update.

For configuration, please refer to 4.8.3.3 "Special case: Combined dial-up connection and remote access".

4.8.2 Configuration of a leased line connection

The configuration is described as an example for a direct RS-422 connection. Configure the serial interface to RS-232 operation when using additional modems as an alternative.

4.8.2.1 FL COMSERVER UNI 232/422/485 set up

1. Configure under "General Configuration... Serial", set the serial interface of the FL COMSERVER UNI 232/422/485 to RS-422, 8 data, no parity, one stop bit.

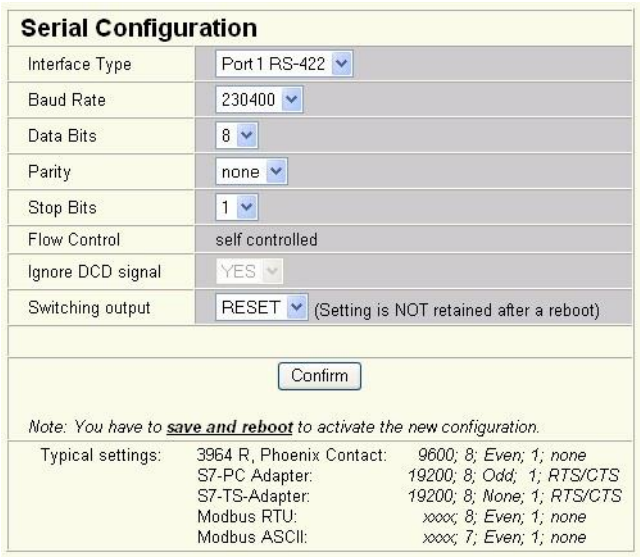


Figure 4-34 Configuring the serial interface

2. Configure the application to PPP operation under "General Configuration... Application Settings", configure the application for PPP operation.
3. Confirm the entry with "Confirm". The Web Based Management now shows the relevant PPP parameters.
4. Then save and activate the new settings under "General Configuration... Save and Reboot" by selecting the "Save" and "Reboot" items and finally entering the system password (default = private).
5. Repeat steps 1-4 for the second FL COMSERVER UNI 232/422/485.

Configure comserver 1 (server) in the main network

The FL COMSERVER UNI 232/422/485 integrates remote subnets into a main network. In the example, the subnet with subnet mask 255.255.255.192 (Comserver 2) is coupled to the main network with subnet mask 255.255.255.0 (Comserver 1).

6. Switch to the "General Configuration ... IP" menu. Set a valid IP address from the main network.

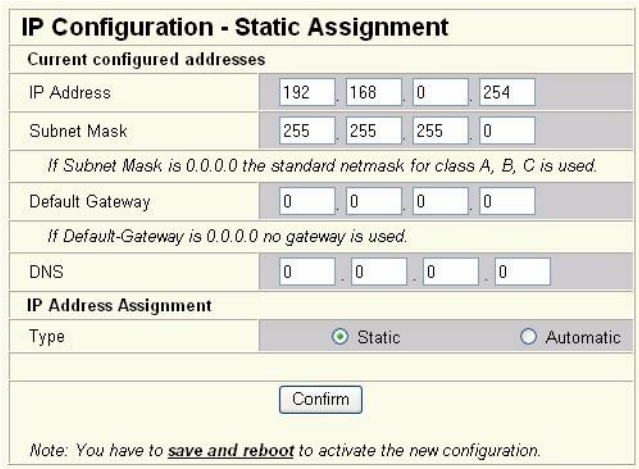


Figure 4-35 Setting the IP address (server)

7. Confirm the setting with "Confirm".
8. Switch to the "General Configuration ... Application" menu. Make the following configuration:

PPP Link Type =	Dedicated
Device Type =	Server (Router)
Assign Client IP Address =	Set here the IP address of the second Comservers one
Assign Client Subnetmask =	Set the subnet mask of the remote client here. Subnet on
User Name =	This specification is optional
Password =	Enter a password of at least four digits here

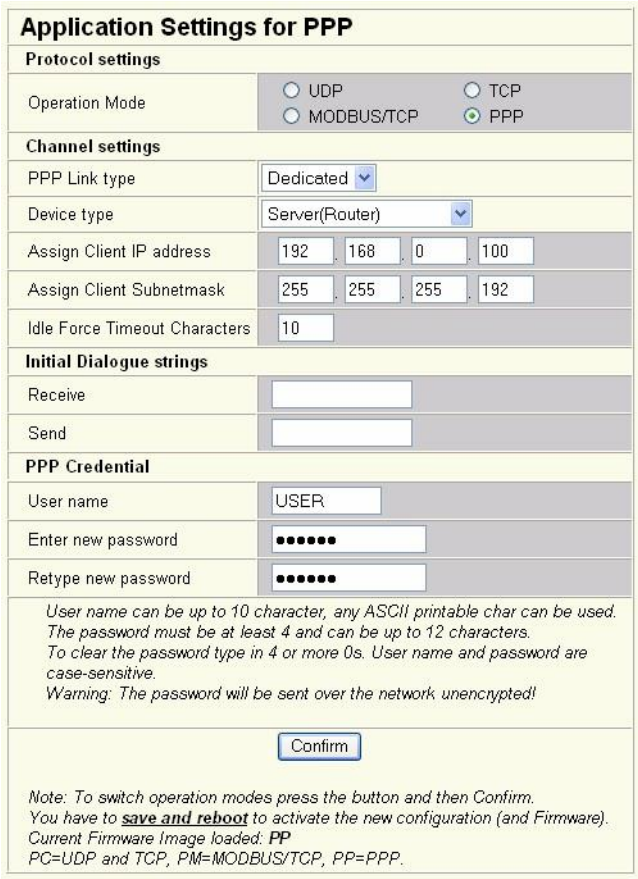


Fig. 4-36 Application settings leased line connection (server)

9. Confirm the configuration with "Confirm".
10. Then save and activate the new settings under "General Configuration... Save and Reboot" by selecting the "Save" and "Reboot" items and finally entering the system password (default = private).

The configuration of the first device (server) is now complete.

Configure Comserver 2 (client) in the subnet

11. Switch to the "General Configuration ... IP" menu. Set a valid IP address from the subnet.

The configured IP address and subnet mask must be identical to the Assign IP and Assign Subnetmask values in the server.

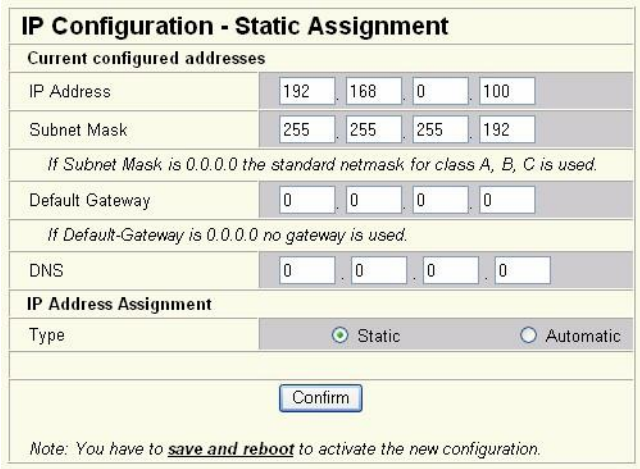


Fig. 4-37 Setting the IP address (client)

12. Confirm the setting with "Confirm".
13. Switch to the "General Configuration ... Application" menu. Make the following configuration:

PPP Link Type =	Dedicated
Device Type =	Client (Gateway
Filter IP Address =	Optional input to filter the data traffic via the slower serial modem connection. Allowed IP address(-space) to communicate over the modem link. Data packets from other IP addresses are discarded. The address space is de- fined together with the filter subnetmask. An entry of 0.0.0.0 deactivates the filter and allows all nodes to communicate.
Filter Subnetmask =	Subnet mask that is specified together with the filter IP-. address defines an address space that is allowed to communicate via the modem link. Special case: Sub-netmask = 0.0.0.0, only the entered IP address is legitimate

User Name =This specification is optional

Password =Enter a password of at least four digits here

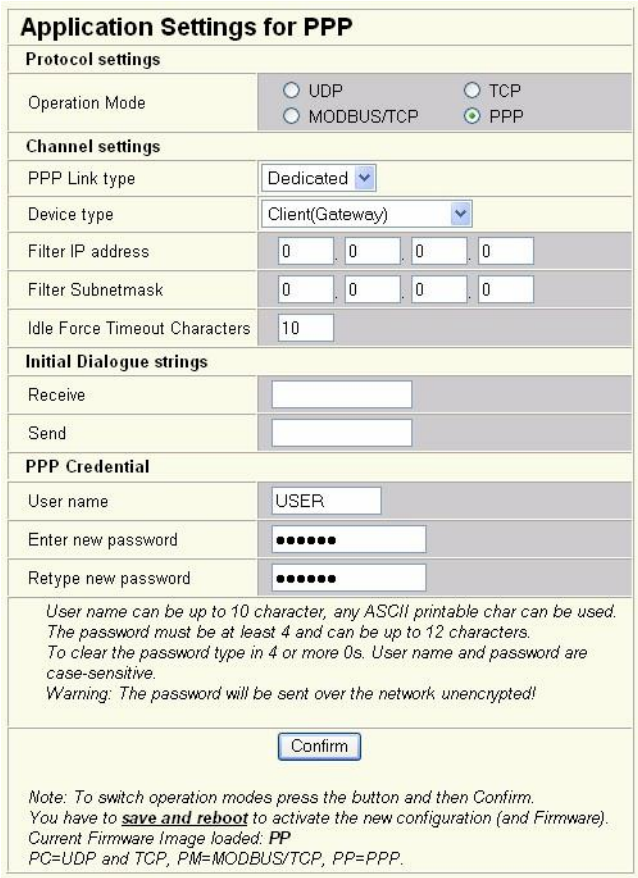


Fig. 4-38 Application settings leased line connection (client)

14. Confirm the configuration with "Confirm".
15. Then save and activate the new settings under "General Configuration ... Save and Reboot" by marking the items "Save" and "Reboot" and finally entering the system password (default = private).

This also completes the configuration of the second device (client).

For operation, the IP address of the second com server (client) must be configured as the gateway address for all subscribers of the subnet.

4.8.3 Configuration of a dial-up connection

4.8.3.1 Functional description

The connection of remote subnetworks to superordinate networks via dial-up modems is particularly suitable if the decentralized system operates autonomously and only needs to connect to superordinate nodes in the event of a fault. In this case, a telegram to the configured gateway address (comserver) starts the connection setup. The FL COMSERVER UNI 232/422/485 controls the connected modem with AT commands.
During the establishment of the connection, packets received by the FL COMSERVER UNI 232/422/485 are discarded. As soon as the connection has been successfully established, bidirectional data exchange takes place.

In the event that the connection could not be established, a second phone number can be configured alternatively, which is used after a timeout period that can also be set.

4.8.3.2 Set up comserver

The configuration differs only in the "Application" menu compared to the leased line connection.

Therefore, please observe steps 1-6 as well as 10-11 from chapter 4.8.2 "Configuration of a leased line connection".

1. In addition, monitoring of the DTR signal can be activated in dial-up connection mode in the serial setup.

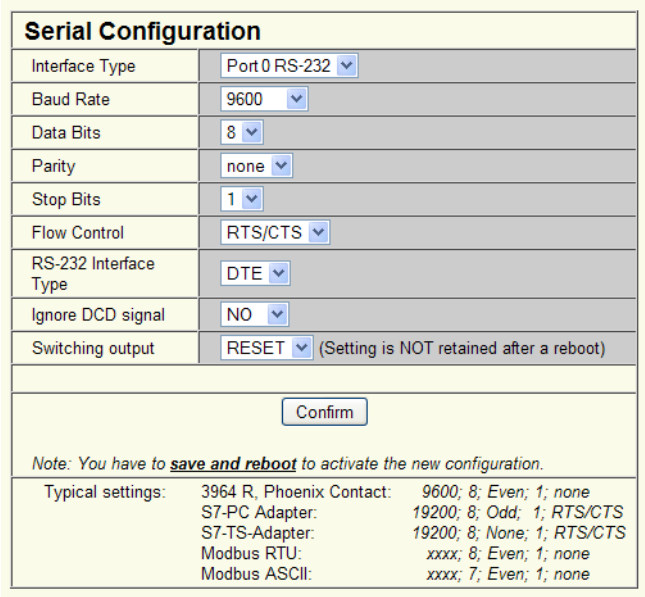


Figure 4-39 Configuring the serial interface

Configure comserver 1 (server) in the main network

2. Switch to the "General Configuration ... Application" menu. Make the following configuration:

   PPP Link Type =Dial Up

   Device Type = Server (Router)

   Assign Client IP Address = Set here the IP address of the second Comservers one

   Assign Client Subnetmask = Set the subnet mask of the remote client here. Subnet on

   User Name =This specification is optional

   Password =Enter at least a four-digit password here

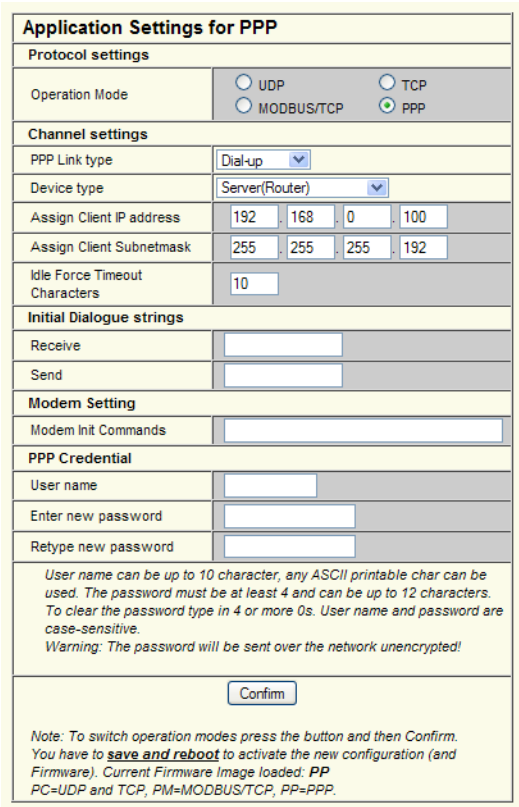


Figure 4-40 Application settings Dial-up connection (server)

3. Confirm the configuration with "Confirm".
4. Then save and activate the new settings under "General Configuration ... Save and Reboot" by marking the items "Save" and "Reboot" and finally entering the system password (default = private).

The configuration of the first device (server) is now complete.

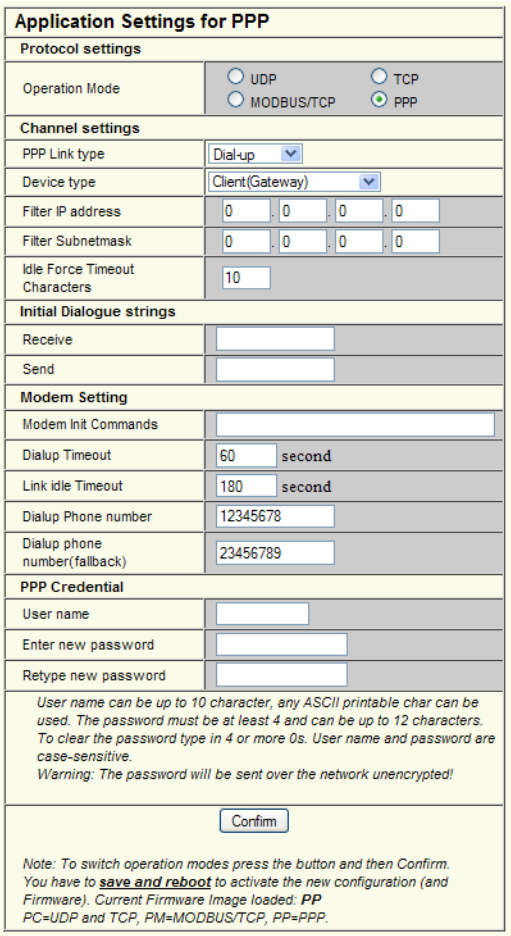
Configure Comserver 2 (client) in the subnet

5. Switch to the "General Configuration ... Application" menu. Make the following configuration:

PPP Link Type =	Dial-Up
Device Type =	Client (Gateway
Filter IP Address =	Optional input to filter the data traffic via the slower serial modem connection. Allowed IP address(-space) to communicate over the modem link. Data packets from other IP addresses are discarded. The address space is de- fined together with the filter subnetmask. An entry of 0.0.0.0 deactivates the filter and allows all nodes to communicate.
Filter Subnetmask =	Subnet mask that is specified together with the filter IP-. address defines an address space that is allowed to communicate via the modem link. Special case: Sub-netmask = 0.0.0.0, only the entered IP address is legitimate
Dialup Timeout = established	Waiting time during which the connection was successfully must be. After the time has elapsed, an attempt is made to establish a connection with the backup number. If no backup number is configured, the connection is aborted after the waiting time.
Link idle Timeout =	When no more data is transferred after the set waiting time, the connection is disconnected.
Dialup Phone number =	Phone number of the overlaid network
Dialup Phone number (backup)=	Alternative phone number to be used in case of failed connection setup.

User Name =This specification is optional

Password =Enter a password of at least four digits here



Application Settings for PPP

Protocol settings	
Operation Mode	○ UDP ○ TCP ○ MODBUS/TCP ◉ PPP
Channel settings	
PPP Link type	Dial-up
Device type	Client(Gateway)
Filter IP address	0 . 0 . 0 . 0
Filter Subnetmask	0 . 0 . 0 . 0
Idle Force Timeout Characters	10
Initial Dialogue strings	
Receive	
Send	
Modem Setting	
Modem Init Commands	
Dialup Timeout	60 second
Link idle Timeout	180 second
Dialup Phone number	12345678
Dialup phone number(fallback)	23456789
PPP Credential	
User name	
Enter new password	
Retype new password	

User name can be up to 10 character, any ASCII printable char can be used. The password must be at least 4 and can be up to 12 characters. To clear the password type in 4 or more 0s. User name and password are case-sensitive.
Warning: The password will be sent over the network unencrypted!

Confirm

*Note: To switch operation modes press the button and then Confirm. You have to **save and reboot** to activate the new configuration (and Firmware). Current Firmware Image loaded: **PP***
PC=UDP and TCP, PM=MODBUS/TCP, PP=PPP.

Fig. 4-41 Application settings Dial-up connection (client)

6. Confirm the configuration with "Confirm".
7. Then save and activate the new settings under "General Configuration... Save and Reboot" by selecting the "Save" and "Reboot" items and finally entering the system password (default = private).

This also completes the configuration of the second device (client).

The IP address of the second com server (client) must be configured as the gateway address for all subscribers of the subnet.

Now configure the connected modems if necessary.

4.8.3.3 Special case: Combined dial-up connection and remote access

If the remote network is to be connected to a superimposed network via a dial-up connection as well as being accessible for configuration purposes by means of a dial-up connection, the FL COMSERVER UNI 232/422/485 can be configured accordingly.

Additional settings on Comserver 2 (client)

Device Type =	Client/Server(Gateway)
Receive Initial dialogue strings =	CLIENT
Send Initial dialogue strings =	CLIENTSERVER

The initial dialogue strings must be entered in CAPITAL LETTERS.

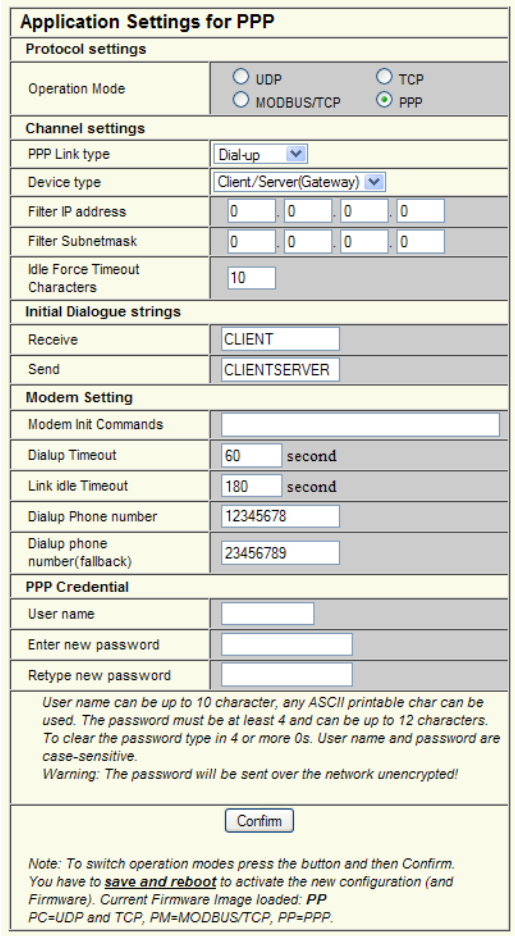


Figure 4-42Application settings combined dial-up connection and remote access (client)

4.8.4 Configuration of a remote maintenance connection

4.8.4.1 Set up COMSERVER

1. Under "General Configuration ... Serial", configure the serial RS-232 interface of the FL COMSERVER UNI 232/422/485 to 8 data, no parity, a stop bit and hardware handshake (RTS/CTS).
2. Configure the application to PPP operation under "General Configuration ... Application Settings".
3. Confirm the entry with "Confirm".
4. Then save and activate the new settings under "General Configuration ... Save and Reboot" by marking the items "Save" and "Reboot" and finally entering the system password (default = private).
5. Switch to the "General Configuration ... Application" menu, Make the following configuration:

PPP Link Type =	Dial Up
Device Type =	Server (Router)
Assign Client IP Address =	Set here a free IP address from the remov-. subnet a
Assign Client Subnetmask =	Set the subnet mask of the remote client here. Subnet on
User Name =	This specification is optional
Password =	Enter at least a four-digit password here

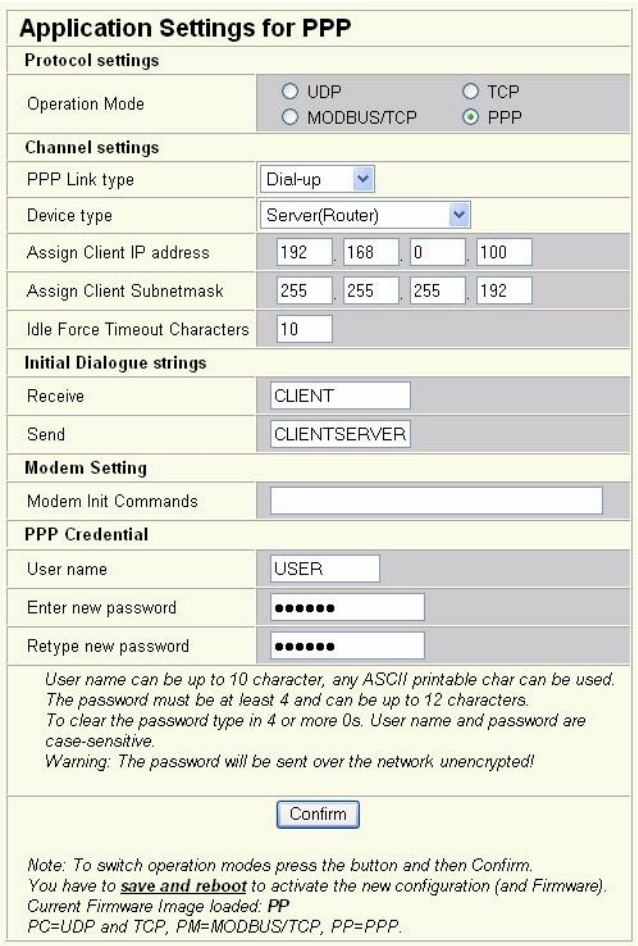


Fig. 4-43 Application settings Remote maintenance connection

6. Confirm the entries with "Confirm".
7. Then save and activate the new settings under "General Configuration ... Save and Reboot" by marking the items "Save" and "Reboot" and finally entering the system password (default = private).
8. Configure the serial interface of the modem also to
   8 data, no parity, one stop bit and hardware handshake (RTS/CTS).
9. In addition, configure the modem to "Automatic Answer mode".
10. Connect the two serial interfaces from the FL COMSERVER UNI 232/422/ 485 and modem.

4.8.5 Set up dial-up connection under Windows XP

1. Install a new network connection under "Start... Settings... Network connections... New connection".

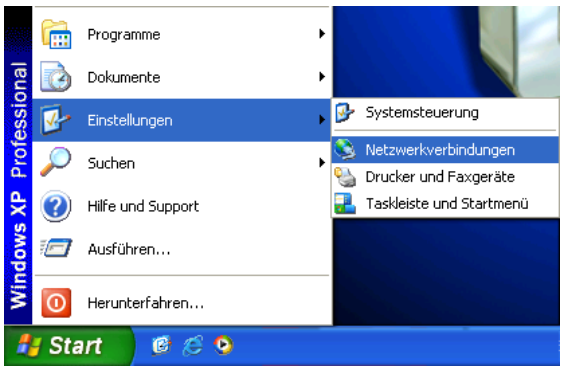


Fig. 4-44 Network connections

2. An assistant welcomes you

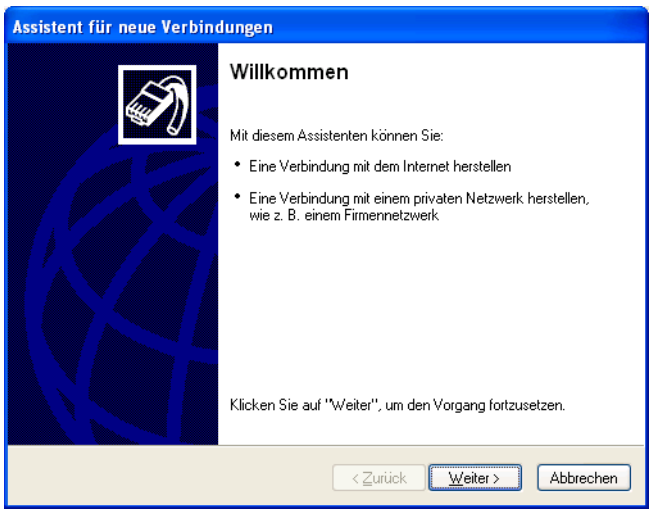


Fig. 4-45 Wizard for new connections

3. Select "Connect to network".

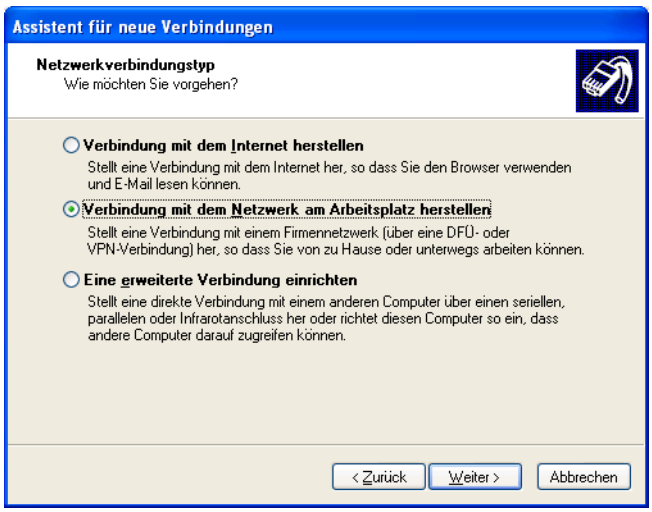


Fig. 4-46 Network connections

4. Select "Dial-up connection".

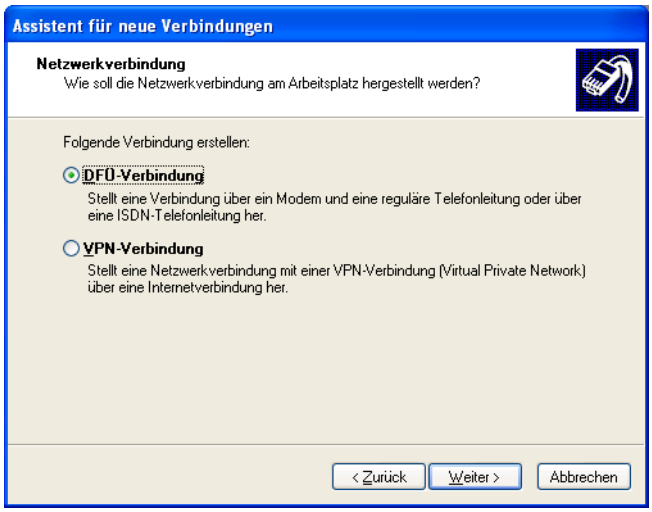


Figure 4-47 Dial-up connection

5. Assign a connection name.

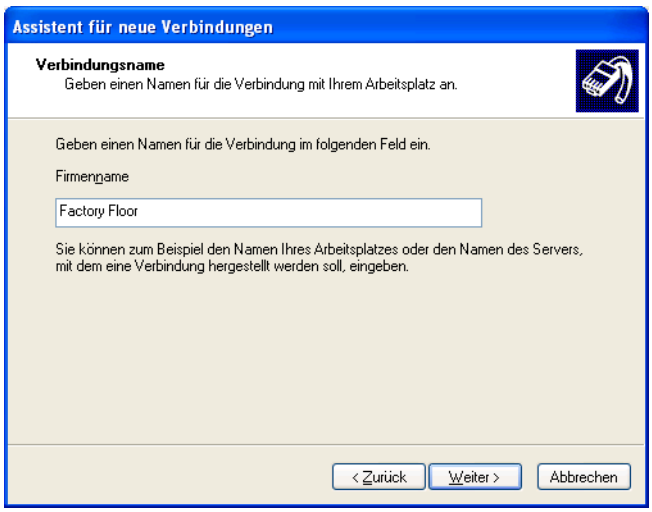


Figure 4-48 Connection name

6. Enter the phone number.

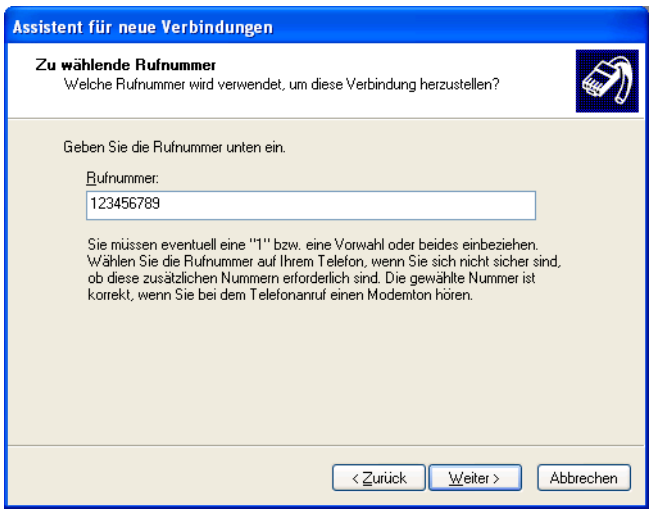


Fig. 4-49 Phone number

7. Select whether the connection is available only in your user profile or to all users of the computer.

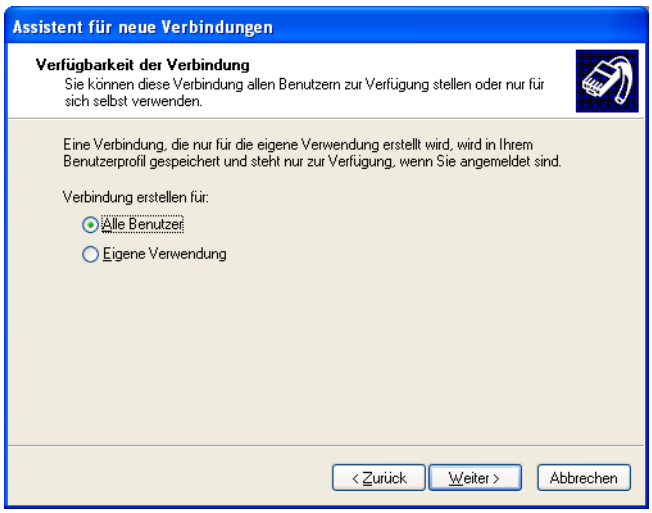


Figure 4-50 Availability of the connection

8. A shortcut on the desktop facilitates the later start of the connection setup.

Figure 4-51 Exit wizards

9. Double-click to start the dial-up connection setup.
10. The "Connect to <connection name>" window appears. Select the "Properties" item.

11. Under "Properties" a window with five tabs appears.

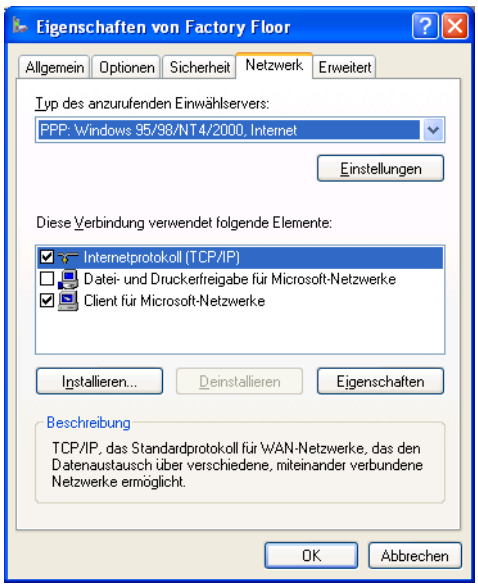


Fig. 4-52Overview of the connection properties

12. Select the "Network... Settings" and disable the software compression.

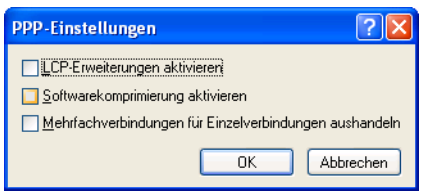


Figure 4-53 PPP settings

13. Select the item "Network... Properties" and then the item "Advanced".

Figure 4-54 Properties IP configuration

14. Disable IP header compression

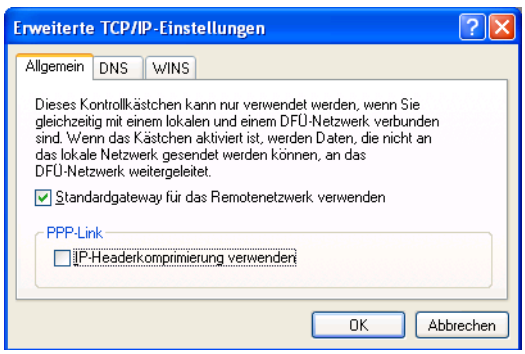


Figure 4-55 Advanced IP configuration

15. Select the "Security" item and then activate the "Advanced" item and click on the "Settings" item.

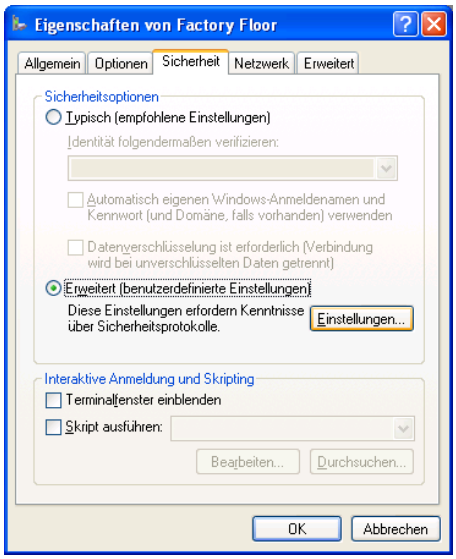


Figure 4-56 User-defined security settings

16. Disable all "unsafe" protocols and enable only the "Challenge Authentication Protocol (CHAP)".

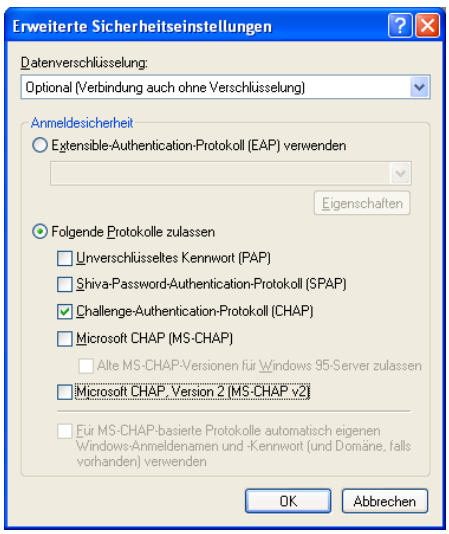


Figure 4-57 Activation CHAP protocol

17. Under "Start... Control Panel... Network Connections" the new dial-up connection is now available.

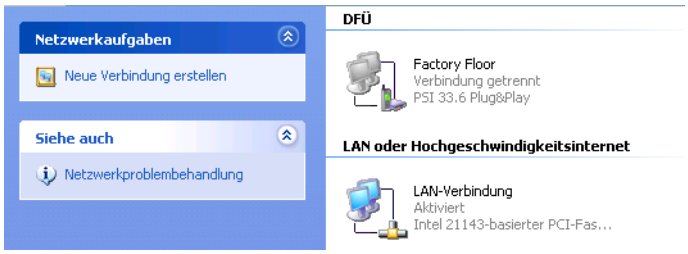


Figure 4-58 Network connections

18. Check the entered password and the entered phone number before you start the connection setup by clicking on the "Dial" button.

Figure 4-59 Connection setup

19. As soon as the modem connection is successfully established, the computer is registered in the network and the password is checked. After this process is successfully completed, the window is reduced to an icon in the status display.

Figure 4-60 Network registration

5 SNMP management

5.1 General function

SNMP (Simple Network Management Protocol) is a vendor-neutral standard for Ethernet management and defines commands for reading and writing information and formats of error and status messages. SNMP also provides a structured model consisting of agents with their respective MIB (Management Information Base) and a manager. The manager is software that runs on a network management station. The agents reside within switches, bus terminals, routers and other devices that support SNMP. The task of the agents is to collect and provide data in the MIB. The manager periodically requests and presents this infor- mation. With data written from the manager to the MIB, configuration of the devices is possible. In urgent cases, the agents can also send messages (traps) directly to the manager.

SNMP interface

The manageable components of the Factory Line product series each have an SNMP agent. This agent manages the Management Information Base II (MIB 2) according to RFC1213, RMON-MIB, Bridge-MIB, If-MIB, Etherlike-MIB and the private SNMP objects of Phoenix Contact.

Via the Simple Network Management Protocol, network management statio- ns, such as a PC with the Factory Manager, are given the possibility to read and modify configuration and diagnostic data of the network nodes. It is also possible to use any SNMP tools or network management tools to access Factory Line products via SNMP. For this purpose, the MIBs supported by the respective device must be made available to the SNMP management tools.

On the one hand, these are globally valid MIBs that are defined and described in RFCs (request for comments). These include, for example, the MIB2 according to RFC1213, which is supported by every SNMP-capable network subscriber. On the other hand, each manufacturer can define its own private SNMP objects, which are then classified in the large SNMP object tree in a private manufacturer area. Each manufacturer is then responsible for this private (enterprise) area, i.e. an object ID may only be assigned (object name and parameters) and published once, for example. If this object is then no longer required, it is marked as expiring, but is not reused under any circumstances, for example with different parameters.

The ASN1-SNMP objects are announced by Phoenix Contact by publishing the description on the Internet pages.

The reading of SNMP objects is not protected by a password. Although a password must be specified in the SNMP for read access, this is set to "public", as is usual for network users, and cannot be changed. The password for write access is "private" in the delivery state and can be changed by the user.

SNMP, web interface and serial terminal use the same user changeable password.

Another benefit for the user is offered by Simple Network Management through the possibility to send traps.

Management Information Base

Database in which all data (objects and variables) required for network management are entered.

Agent

An agent is a software that collects the data of the network subscriber on which it is installed and sends it on demand. Agents reside in all manageable components of a network and transmit the values of specific settings and pa- rameters to the management station. When requested by a manager or when an event occurs, the agent transmits the previously collected information to the management station.

Traps

Traps are spontaneous SNMP alarm or information messages that an SNMP-capable device sends on its own in response to special events. The traps are transmitted with the highest priority, if necessary to different addresses, and can then be displayed in plain text by the management station. The recipient IP addresses (trap targets/receivers) of these traps must be set by the user on the respective device.

5.2 Supported MIBs

The FL COMSERVER ... 232/422/485 supports the MIB2 according to RFC 1213 and the private FL-COM-SERVER.mib. The MIB files can be found on the supplied CD and on the Inter- net at www.factoryline.de.

5.2.1 Schematic representation of SNMP management

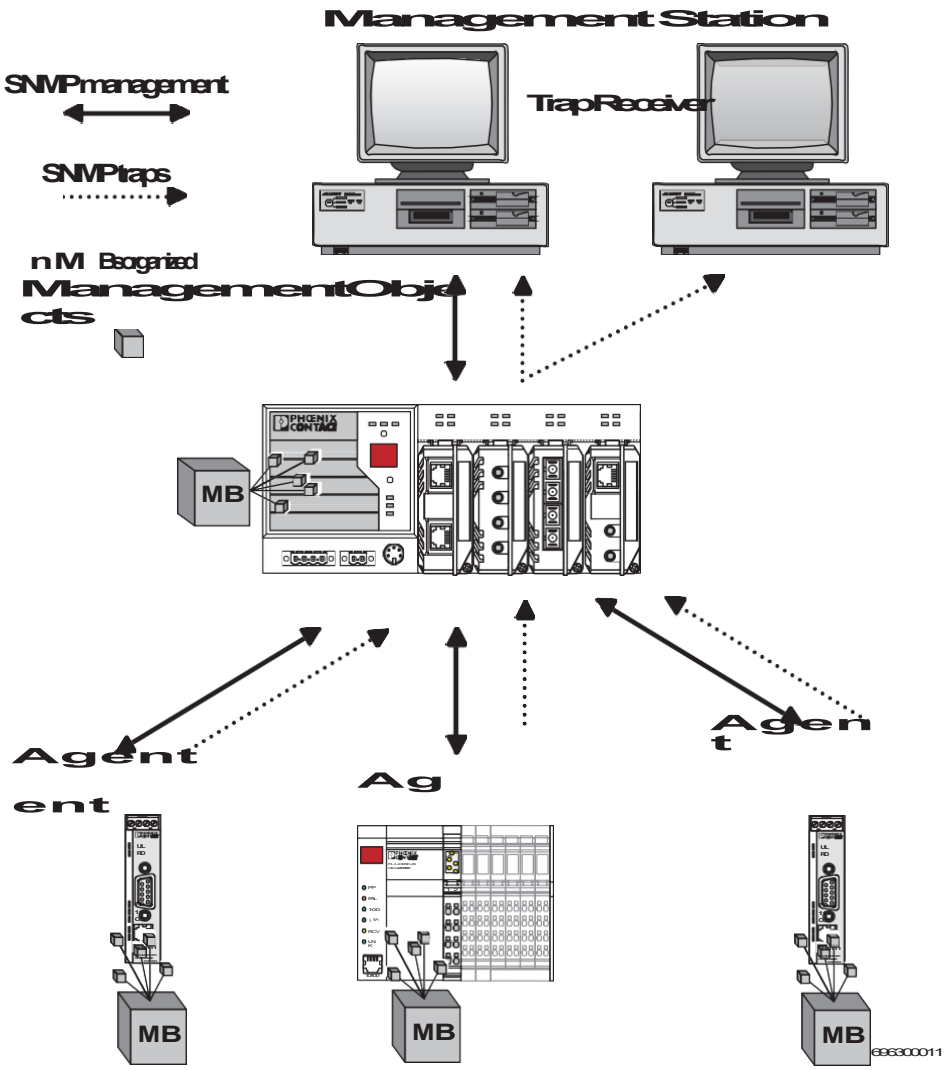


Figure 5-1 Schematic representation of SNMP

6 Service and maintenance

6.1 Emergency configuration

If you have denied yourself the option of configuring WBM devices via the network because, for example, you do not know the static IP address that has been set, you can use the emergency serial access.

To do this, you must have local access to the device and connect a PC with terminal program to the RS-232 interface.

6.1.1 Scope of functions

The following functions are available for emergency configuration:

– Configuration of the IP address / activation of the BootP mechanism
– Deleting all settings (incl. passwords) and resetting to factory settings
– Loading new firmware
– Complete device configuration by loading a file.

6.1.2 Procedure

1. Connect the FL COMSERVER ... 232/422/485 to a serial COM port of a PC (1:1 cable).
2. Open a terminal program, e.g. Hyperterminal in the Windows start menu under "Programs... Accessories... Communication... Hyperterminal".
3. Configure the interface (e.g. COM 1)under "File... Properties" to 9600 bit/s; 8 data bits; No parity; 1 stop bit; No flow control.

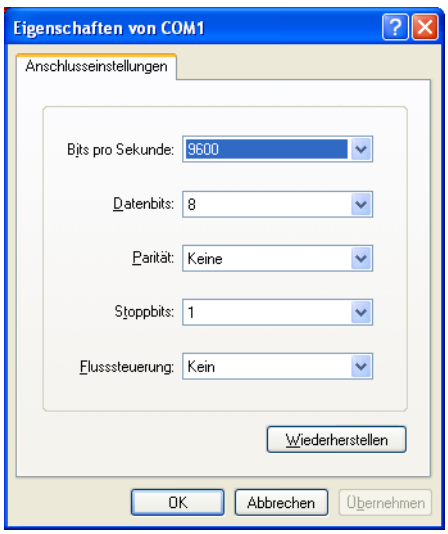


Figure 6-1 Properties" menu in Windows Hyperterminal

4. Confirm the settings with "OK" and close the menu.
5. Check the correct settings in the status bar of Hyperterminal.

Figure 6-2 Status bar in Windows hyperterminal

6. Now perform a voltage reset on the FL COMSERVER ... 232/422/485 and simultaneously hold down the X key on your keyboard.
7. As soon as a response from the FL COMSERVER ... 232/422/485 appears on the screen, press the ENTER key within three seconds.

The following display appears:

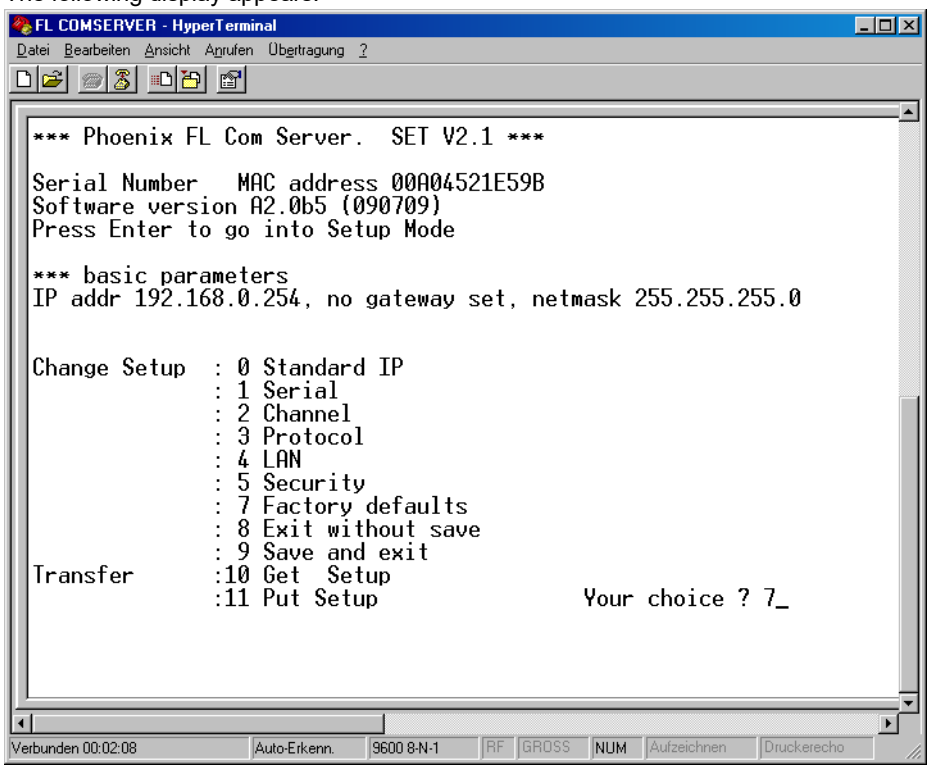


Figure 6-3 Serial setup menu

8. Select the desired option by entering the digit and confirm the selection by pressing the ENTER key.

6.2 Reading out the configuration

For system documentation and easy service and support, the current device configuration can be read from the FL COMSERVER ... 232/422/485 and stored on external data carriers as a text file and printed out.

In addition, in series machine manufacturing, for example, other FL COMSERVER ... 232/422/ 485 can be configured via a TFTP transfer. For this purpose, the reference configuration can be saved in a special format.

6.2.1 Displaying and printing the configuration overview

1. In the WBM, under "General Configuration", select the "Configuration Ma- nagement" menu item.

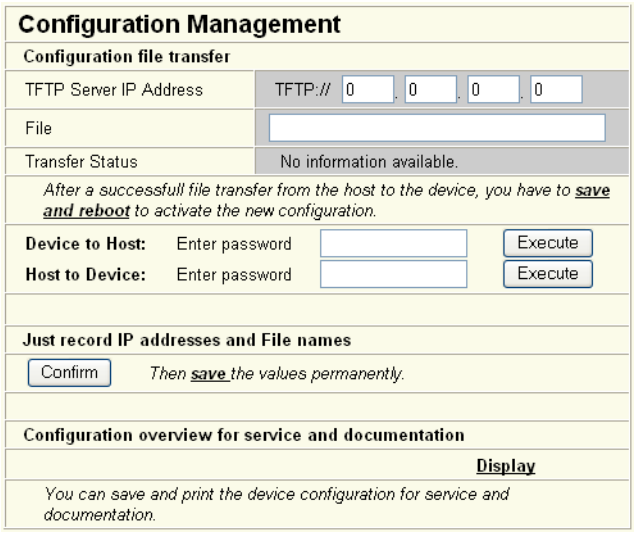
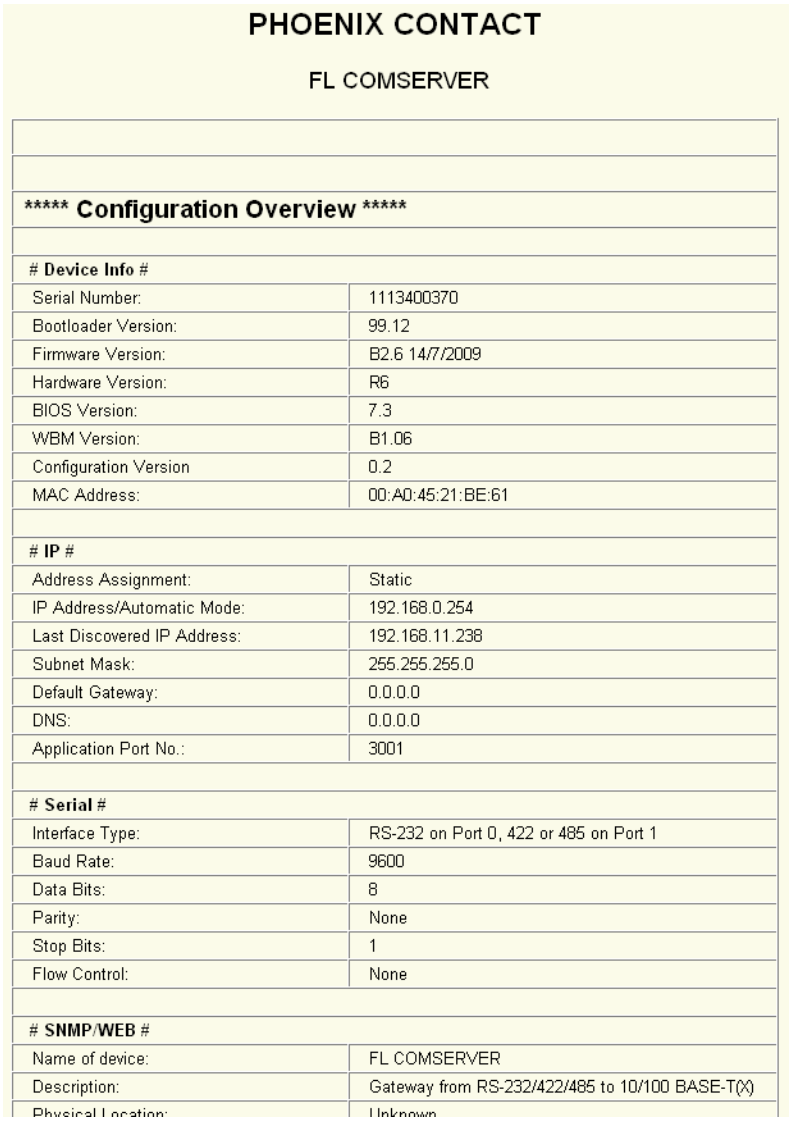


Figure 6-4 Configuration Management" menu

2. Click the "Display" button and open the configuration overview.

3. A new browser window will open.



PHOENIX CONTACT

FL COMSERVER

***** Configuration Overview *****

# Device Info #	
Serial Number:	1113400370
Bootloader Version:	99.12
Firmware Version:	B2.6 14/7/2009
Hardware Version:	R6
BIOS Version:	7.3
WBM Version:	B1.06
Configuration Version	0.2
MAC Address:	00:A0:45:21:BE:61
# IP #	
Address Assignment:	Static
IP Address/Automatic Mode:	192.168.0.254
Last Discovered IP Address:	192.168.11.238
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DNS:	0.0.0.0
Application Port No.:	3001
# Serial #	
Interface Type:	RS-232 on Port 0, 422 or 485 on Port 1
Baud Rate:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None
# SNMP/WEB #	
Name of device:	FL COMSERVER
Description:	Gateway from RS-232/422/485 to 10/100 BASE-T(X)
Physical Location:	Unknown

Figure 6-5Display of the configuration overview

The current values of all variable settings in an HTML file are displayed clearly.

4. For plant documentation, print the overview.
5. Alternatively, you can save this information through the "Save as" menu of the browser either as HTML or TXT file on a data carrier. The configuration can be easily displayed with these file formats using any PC.

This function is only used to display the settings in plain text. Automatic configuration of the device by file download is only possible with the function "Saving the configuration with TFTP" on page 6-5.

6.2.2 Backing up the configuration with TFTP

This function allows you to save the current FL COMSERVER ... 232/422/485 configuration in a backup file (direction: device to host). The configuration cannot be displayed in plain text. The format is used exclusively for automatic configuration of devices by means of a TFTP data transfer.

During a configuration upload from the FL COMSERVER ... 232/422/485 to a PC, the last saved version is transferred. To transfer the current configuration, it is recommended to save it again beforehand ("Save + Reboot" menu).

1. In the WBM, under "General Configuration", select the "Configuration Ma- nagement" menu item.

Before transferring the configuration file with TFTP, make sure that the release is set in the menu "Security - Security Flags" (see chapter 3.4.8).

2. In the "TFTP Server IP Address" field, enter the IP address of the TFTP server to which you want to back up the file.
3. Assign a name for the backup file.
4. Select the direction "device to host".
5. Enter the "Write-Password" (default = private).
6. Click "Execute" and start the data transfer.

6.2.3 Loading the configuration with TFTP

With this function you can load a backup file in the FL COMSERVER ... 232/422/485 (direction: host to device). The function is used for device replacement and for configuration in series production.

Before transferring the configuration file with TFTP, make sure that the release is set in the menu "Security - Security Flags" (see chapter 3.4.8).

1. In the WBM, under "General Configuration", select the "Configuration Ma- nagement" menu item.
2. In the "TFTP Server IP Address" field, enter the IP address of the TFTP server where the backup file is stored.
3. Enter the name of the backup file.
4. Select the direction "host to device".
5. Enter the "Write-Password" (default = private).
6. Click "Execute" and start the data transfer.
7. Perform a reset of the device.

When downloading a configuration from a PC to a FL COMSERVER ... 232/422/ 485, the new configuration is only activated after a reset of the FL COMSERVER ... 232/422/ 485 is activated.

Configuration via a configuration file is used for device replacement. If devices are to be duplicated via configuration file, the following details must be observed:

- Establishing a connection from the FL COMSERVER ... 232/422/485 to an FTP ser- ver or local connection via the RS-232/485 interface of the FL COMSERVER. ... 232/422/485.
- Load the configuration file onto the FL COMSERVER ... 232/422/485.
- Reset the FL COMSERVER ... 232/422/485.
- Adjust IP parameters.
- Save current configuration.

The duplicated FL COMSERVER ... 232/422/485 can now be operated in the network with the adapted IP parameters.

6.3 Configuration up- and download with a terminal program

As an alternative to saving and loading a configuration with TFTP, it is also possible to do this via a terminal program. The connection to the FL COMSERVER ... 232/422/485 is done either via Telnet or RS-232.

6.3.1 Establish connection to FL COM SERVER

The FL COM SERVER... provides two other configuration methods that can be used alternatively to the web-based management.

6.3.1.1 Configuration via Telnet

1. Open under START => Programs => Accessories => Hyperterminal.
2. Set up a Telnet connection to the IP address of the Com Server to the port number 9999.

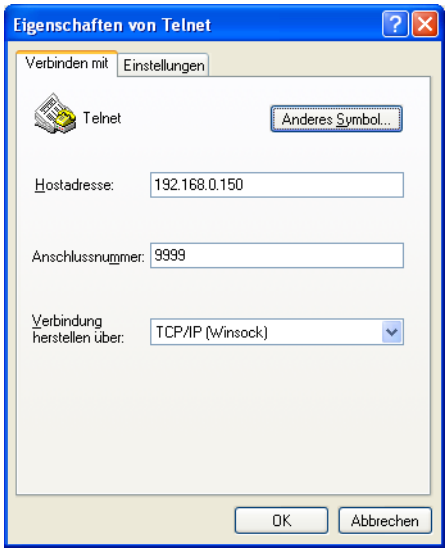


Figure 6-6 Configuration via Telnet

3. After the connection is established, the password is requested (default = private).
4. Confirm the entry with ENTER.

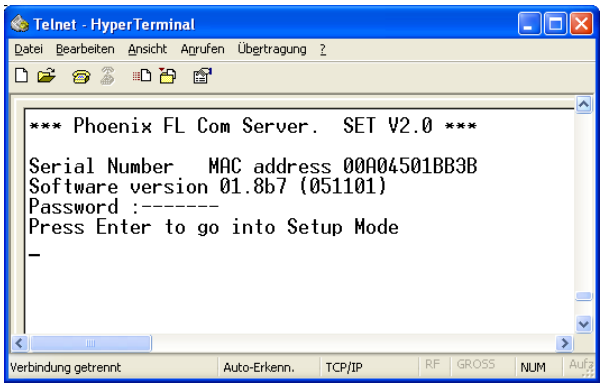


Figure 6-7 Confirm configuration

5. Confirm the entry by pressing ENTER again.

6.3.1.2 Configuration via RS-232

1. Open under START => Programs => Accessories => Hyperterminal.
2. Set up a terminal connection via COM 1 or 2. The serial settings must be set to 9.6 kBit/s, 8 data bits, no parity, 1 stop bit, no handshake.

Figure 6-8 Configuration via RS-232

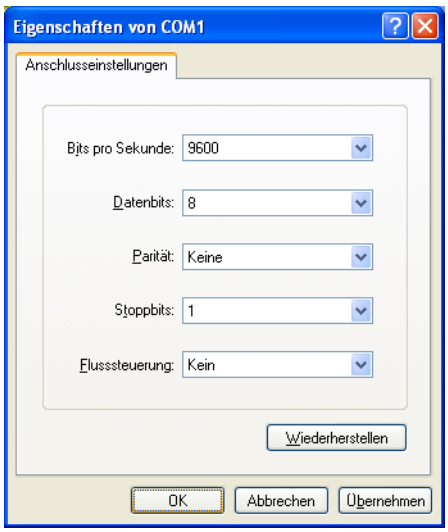


Figure 6-9 Confirm configuration

3. Hold the X key on the keyboard and simultaneously perform a voltage reset on the FL COM SERVER.
4. Confirm the entry with ENTER.

6.3.2 Backup configuration from a comserver to a PC

The following configuration menu is then available.

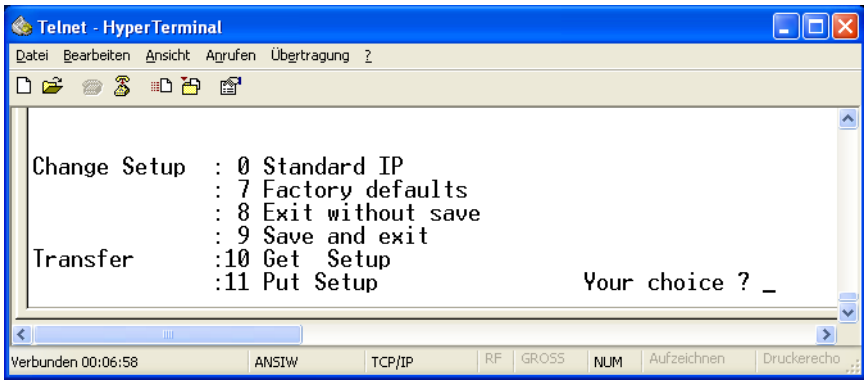


Figure 6-10 Configuration menu

1. Select the item 10 and confirm with ENTER.

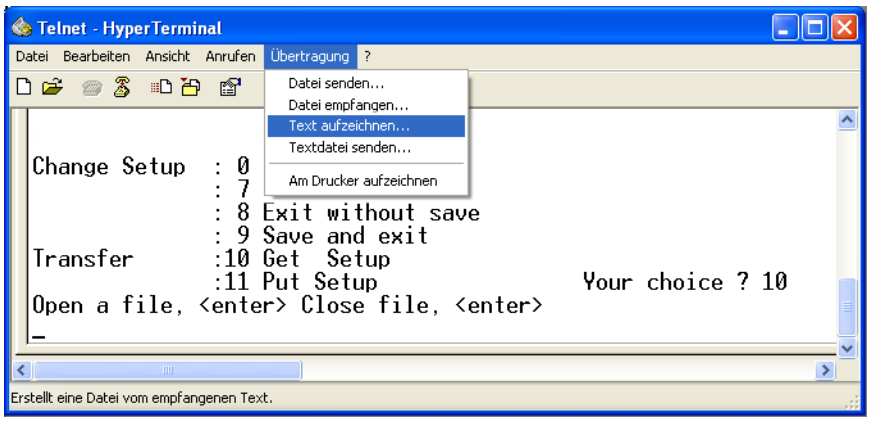


Figure 6-11 Record configuration file

2. Select under TRANSFER => RECORD TEXT.
3. In the following menu, enter a location and file name for the configuration file.

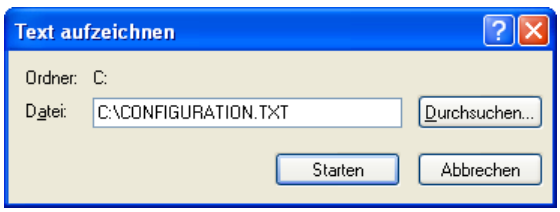


Figure 6-12 Save configuration file

4. After the data transfer close the file under TRANSFER => RECORD TEXT => EXIT.

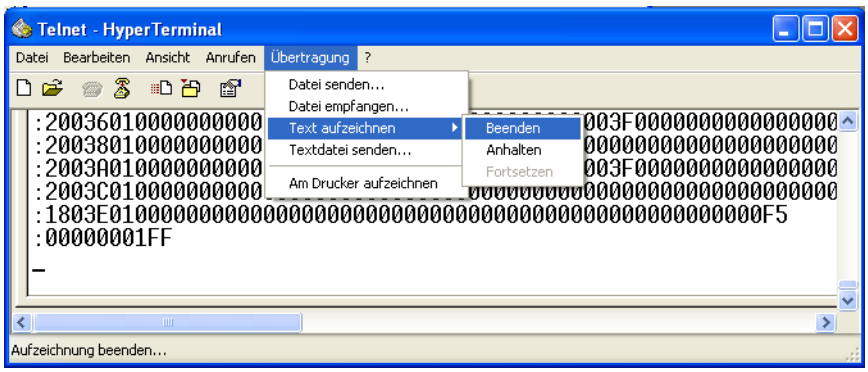


Figure 6-13 Finish recording configuration file

The configuration of the FL COM SERVER is now saved in a file.

6.3.3 Restore configuration from a PC to a comserver

1. After the connection has been successfully established, select item 11 and confirm the entry with ENTER.

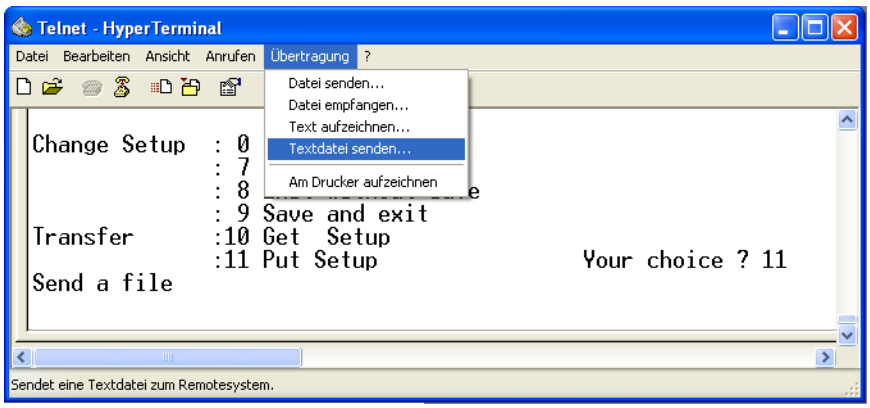


Figure 6-14 Send configuration file

2. Select under TRANSMISSION => SEND TEXT.
3. Select the desired configuration file in the following menu and confirm the entry with ENTER.

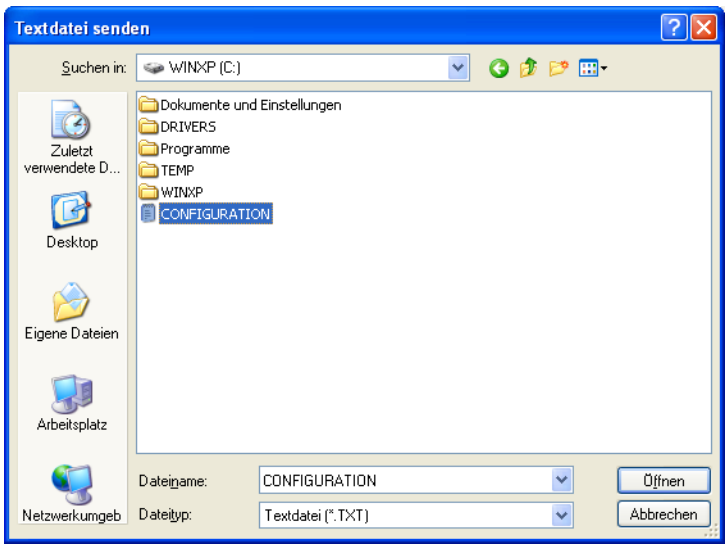


Figure 6-15Open configuration file

The file download starts

automatically.

ATTENTION: Data loss if download is aborted prematurely.

The transmission can take up to one minute. Only very low LED activity can be detected at the interfaces.

4. The successful data transfer is confirmed with the following message.

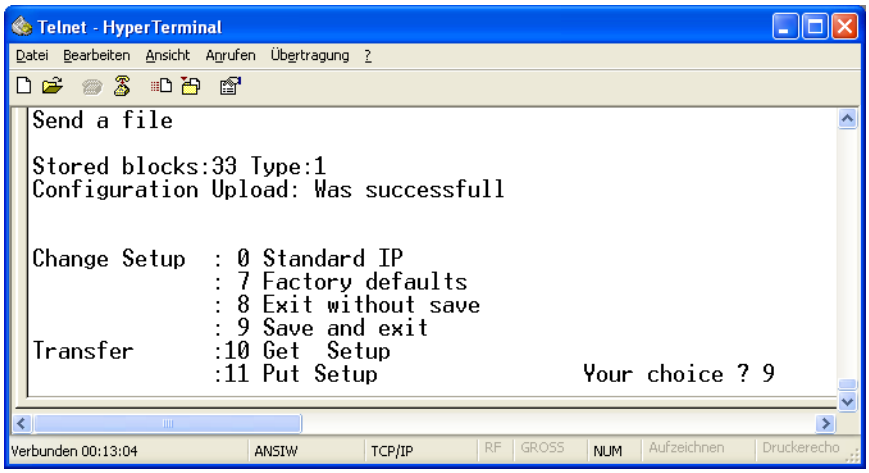


Fig. 6-16 Save new configuration

5. Save the new configuration by entering 9 and confirm the entry with ENTER.
6. The new configuration is saved and is now available.

ATTENTION: For security reasons, the PPP password cannot be saved or restored via a configuration upload/download. This setting can only be made via Web Based Management.

6.4 Update firmware and WBM

By updating the firmware and the web-based management of the FL COMSERVER ... 232/422/485 ensures that the device can always follow the latest technical developments.

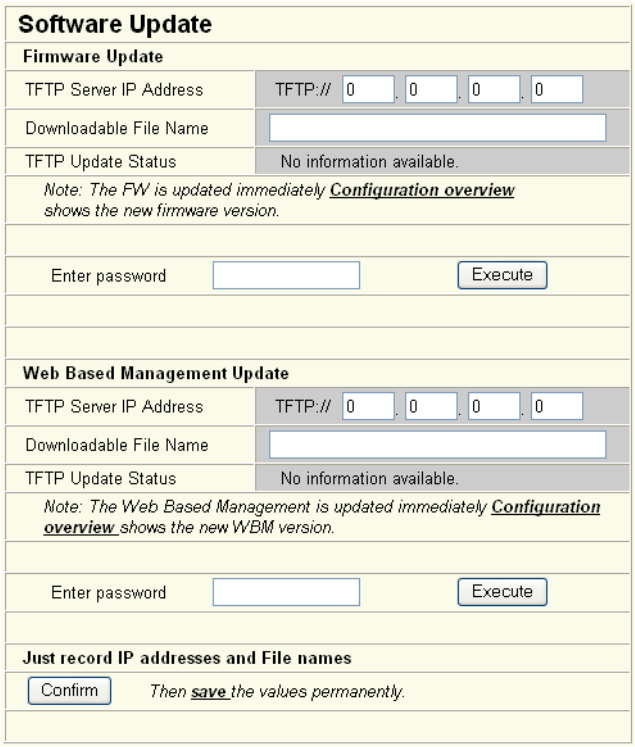


Fig. 6-17 Software update" menu

6.4.1 Performing the software update

The procedure for updating the firmware is identical to that for the WBM.

1. Save the new firmware and WBM files in the root directory of the TFTP server.
2. In the WBM, select the "Software Update" menu item under "General Configuration".
3. In the TFTP Server IP Address field, enter the IP address of the TFTP server where the new software will be deployed.
4. Enter the name of the backup file.
5. Enter the "Write-Password" (default = private).
6. Click "Execute" and start the data transfer.
7. Perform a reset of the device.

When downloading a configuration from a PC to a FL COMSERVER ... 232/422/ 485, the new configuration is only activated after a reset of the FL COMSERVER ... 232/422/ 485 is activated.

8. In the WBM, under "General Configuration", select the "Load Factory Set- tings" menu item.
9. Enter the "Write-Password" (default = private).
10. Click "Execute" and activate the factory settings.
11. The FL COMSERVER ... 232/422/485 can be set again according to the required application.

A Technical appendix

A 1Construction of IP addresses

A 1.1Valid IP parameters

The three elements "IP address", "Subnet mask" and "Default gateway/router" form the IP parameters.

Valid IP addresses are:
000.000.000.001 to 126.255.255.255 and
128,000,000 to 223,255,255,255

Valid subnet masks are:
255,000,000 to 255,255,255,252

Default Gateway/Router:
The IP address of the gateway/router must be in the same subnet as that of the switch.

A 1.2Allocation of IP addresses

The IP address is a 32 bit long address consisting of network part and user part. The network part consists of the network class and the network address.
Five network classes are currently defined, of which classes A, B and C are used for today's applications. Classes D and E are very rarely used. Therefore, it is usually sufficient for a network user to "know" only classes A, B, and C.

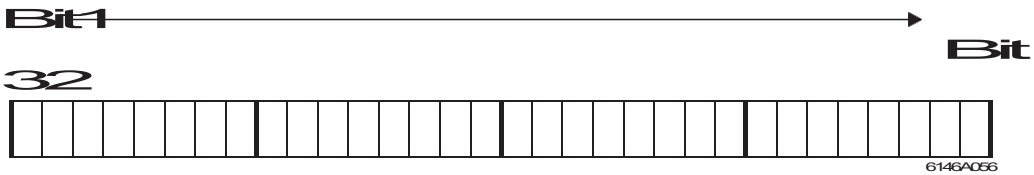


Figure A-1 Position of the bits within the IP address

The network class is represented by the first bits in the binary representation of the IP address. The number of "ones" up to the first "zero" is decisive. The following table shows the assignment of the classes. The free cells of the table are no longer relevant for the network class and already belong to the network address.

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5
Class A	0				
Class B	1	0			
Class C	1	1	0		
Class D	1	1	1	0	
Class E	1	1	1	1	0

The bits of the network class are followed by the bits of the network address and the user address. Depending on the network class, different numbers of bits are available for both the network address (network ID) and the user address (host ID).

	Networ k ID	Host ID
Class A	7 bit	24 bit
Class B	14 bit	16 bit
Class C	21 bit	8 bit
Class D	28 bit multicast identifier	
Class E	27 bit (reserved)	

IP addresses can be represented in decimal or hexadecimal format. In order to represent a logical relationship between the individual octets, the octets are separated by dots in the case of decimal representation (dotted decimal notation).

The dots do not separate the address into network and user address. Only the significance of the first bits (up to the first "zero") provides information about the network class and thus about the number of remaining bits of the address.

Possible address combinations

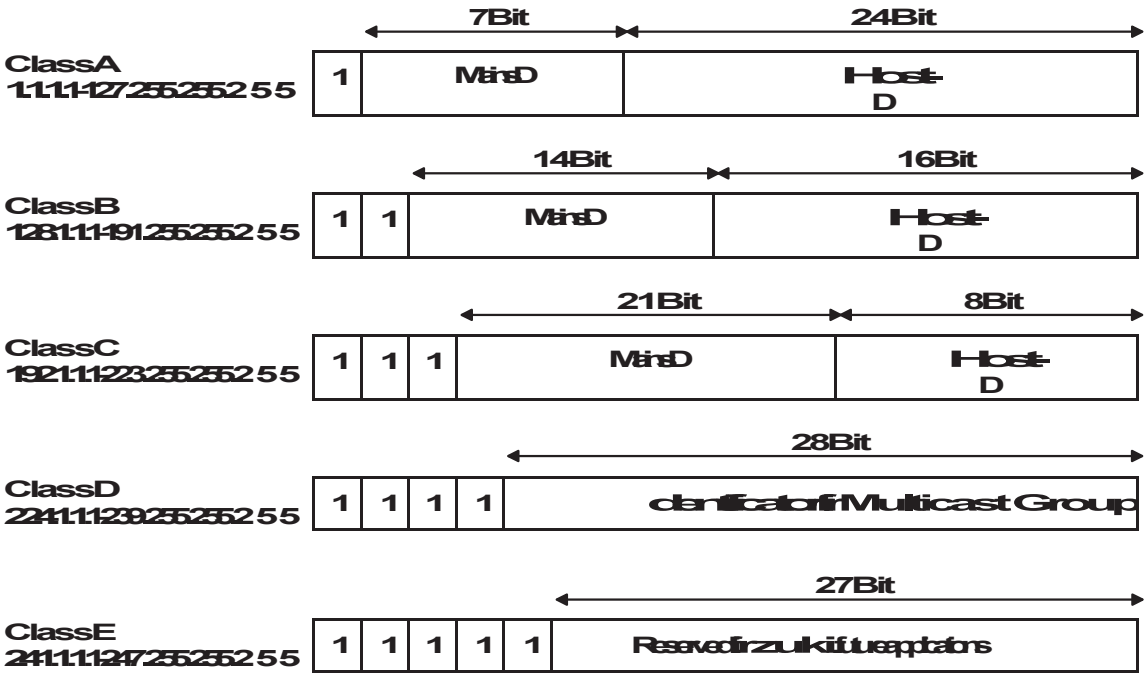


Figure A-2 Structure of the IP addresses

A 1.3IP special addresses for special applications

Some IP addresses are reserved to enable special functions. The addresses listed below should not be assigned as default IP addresses.

127.x.x addresses

The class A network address "127" is reserved for a so-called loopback function on all computers, regardless of the network class. This loopback function may only be used for internal test purposes of the networked computers.

If a telegram with the value 127 in the first octet is addressed to a computer, the receiver immediately sends the telegram back to the sender.

In this way it is possible to check whether, for example, the TCP/IP software is correctly installed and configured.

Since layers 1 and 2 of the ISO/OSI model are not included in the test, the ping function should be used for complete testing.

Value 255 in octet

The value 255 is defined as the broadcast address. The telegram is sent to all computers that are located in the same part of the network. Examples: 004.255.255.255, 198.2.7.255 or 255.255.255.255 (all computers in all networks). If the network is divided into subnets, the subnet masks must be taken into account in the calculation, otherwise not all subscribers will be reached.

0.x.x.x addresses

The value 0 is assigned as the identifier of the own network. If the IP address contains a zero at the beginning, then the recipient is in its own network. Example: 0.2.1.1, this means station 2.1.1 in this network.

According to an older definition, the zero is intended as a broadcast address. If you operate older devices, the use of the IP address 0.x.x.x can lead to unwanted broadcast and thus to a total overload of the network (broadcast storm).

A 1.4 Subnet masks

Routers and gateways divide large networks into several subnets. The subnet mask assigns the IP addresses of the individual devices to specific subnets. The **network part of** an IP address is **not** changed by the subnet mask. An extended IP address is generated from the user address and the subnet mask. Since the masked subnet is only known to the local computers, this extended IP address appears to all other participants as a standard IP address.

Structure of the netmask

The netmask basically contains the same number of bits as an IP address. The same number of bits (at the same position) is set to "one" for the netmask as reflect the network class for the IP address.

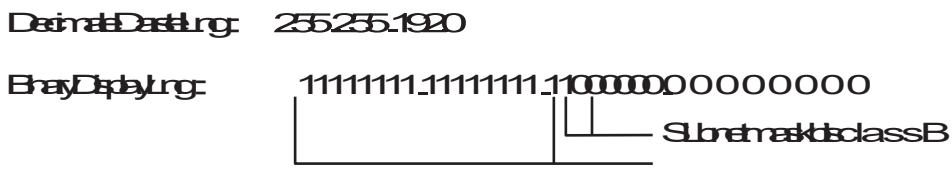
Example: An IP address of class A contains one byte of network address and three bytes of server address. Accordingly, the first byte of the subnet mask may only contain "ones".

The remaining bits (three bytes) then contain the address of the subnet and the computer. An AND operation of the bits of the IP address and the bits of the subnet mask then produces the extended IP address. Since the subnet is only known to the local subscribers, such an IP address appears to all other subscribers as a
"normal" IP address.

Application

If the AND operation of the address bits results in the own local network address and the local subnet address, the station is located in the local network. If the AND operation produces a different result, the data telegram is sent to the subnet router.

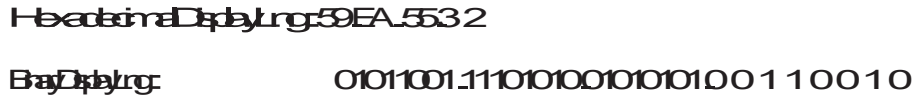
Example of a class B subnet mask:



This subnet mask is used by the TCP/IP protocol software to distinguish between devices connected to the local subnet and devices located in other subnets.

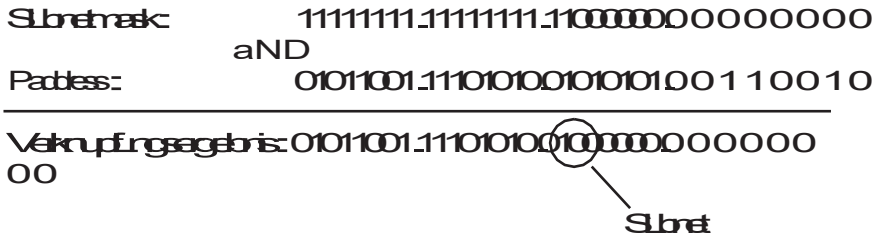
Example: Subscriber 1 with the subnet mask shown above wants to establish a connection with subscriber 2. Subscriber 2 has the IP address 59.EA.55.32.

Representation of the IP address of participant 2:



To determine whether subscriber 2 is on the local subnet, the software now performs a bitwise AND operation on its own subnet mask and the IP address of subscriber 2.

AND operation of subnet mask and IP address of subscriber 2:



After the AND operation, the software determines that the subnet (01) searched for does not correspond to the local subnet (11) and thus forwards the data telegram to a subnet router.

A 1.4.1Examples for subnet masks and number of computer bits

Subnet mask	Computer / Host ID
255.255.255.252	2 bit
255.255.255.248	3 bit
255.255.255.240	4 bit
255.255.255.224	5 bit
255.255.255.192	6 bit
255.255.255.128	7 bit
255.255.2545.0	8 bit
255.255.254.0	9 bit
255.255.252.0	10 bit
255.255.248.0	11 bit
...	
...	
255.128.0.0	23 bit
255.0.0.0	24 bit

A 2Technical data

Supply	
Power supply 1 Frequency	24 V AC/DC ±20% (via plug-in screw terminal COMBICON) 50 ...
Power supply 2 (alternative or redundant)	60 Hz 24 V DC ±5 % (via DIN rail bus connector and system power s u p p l y)
Current	
consumption	
nominal	
operation	< 100 mA (at 24 V)

Serial interfaces	
	According to standard
RS-232	ITU-T V.28, EIA/TIA-232, DIN 66 259-1
RS-422	ITU-T V.11, EIA/TIA-422, DIN 66 348-1
RS-485	EIA/TIA-485, DIN 66 259-4
Connection	
RS-232 RS-422/485	SUB-D 9-pin, male connector via pluggable screw terminal COMBICON
Termination network	390 / 180 / 390 , internally switchable
Device type	DTE (Data Terminal Equipment) / DCE (Data Communication Equipment), adjustable via WBM (Web Based Management)
Data format / coding	Serial asynchronous UART/NRZ, 7/8 data, 1/2 stop, 1 parity, 10/11 bit line length
Data flow control RS-232, RS-422 RS-485	Soft handshake, Xon/Xoff or hardware handshake RTS/CTS self-controlling
Serial transmission rate	300, 600, 1200, 2400, 4800, 7000, 9600, 19200, 38400, 57600, 115200, 187500, 230400Bit/s, adjustable via WBM
Supported protocols	transparent, incl. 3964R protocol

Ethernet interface according to IEEE 802.3	
Connection	RJ45 socket, 8-pin, shielded
Umbrella	DC-coupled on mounting rail
Transmission rate10/100 MBit/s, autonegotation	
Transmission length	100 m (twisted pair shielded)
Supported protocols	TCP/IP, UDP, MODBUS/TCP*, TFTP, HTTP, PPP with CHAP authentication*.
Auxiliary protocols	ARP, DHCP, BOOTP, SNMP, RIP, RARP

* is only supported by FL COMSERVER UNI 232/422/485

Functions	
Configuration and managementwith	standard WEB browser and HTTP protocol with Factory Manager Software FL SWT with SNMP objects locally with terminal program via RS-232 (emergency access) remotely via Ethernet and Telnet (emergency access)

Functions (continued)

LED diagnosis indicators	
Power supply 24 V AC/DC	LED green, UL, static on
Ethernet operating mode	LED green, full duplex operation active, static on
Ethernet transmission speed	LED green, 100 Mbit/s, static on
Ethernet Link	LED green (LNK), with received link signals, statically on
Ethernet data	LED yellow (ACT), data transmission TP port, dynamic
Device error	LED red, error display
RS-232/422/485 Receive data	LED green, RD, Receive
RS-232/422/485 transmit data	LED yellow, TD, Transmit
Switching output	Transistor output on the backplane for connecting accessories, switchable via WBM

General data

CE conformity	EMC Directive 2004/108/EC
Ambient temperature range during operation	-25 °C ... +60 °C
Abbreviation	UL requested
Housing type	ME 22.5 with bus connector and functional earth contact (FE)
Housing material	ABS-V0, green
Weight	150 g
Housing dimensions (H x W x D)	99 mm x 22.5 mm x 114.5 mm
Functional earth	to the EN support rail in the housing
Vibration resistance	5g according to DIN EN 60068-2-6, 1.5 h each in x,y,z direction
Shock test according to IEC 60068-2-27	15g, 11 ms, half-sine shock pulse
Free fall according to IEC 60068-2-32	1 m
Protection class	IP20
Ambient temperature storage	-40 °C ... +70 °C
Separate potential levels	Supply // Ethernet (TP) // RS-232, RS-422, RS-485
Chloroform test	30g, 11 ms, half-sine shock pulse
Test voltage	free from paint wetting impairment substances according to VW AUDI, SEAT central standard P-VW-3.10.757 650
	1.5 kV AC, 50 Hz, 1 min. between all potential levels according to EN 50178 and EN 61131-2

A 2.1 CE conformity

Conformity to EMC Directive 2004/108/EC

Testing of immunity to interference according to EN 61000-6-2a

Static electricity discharge (ESD)	EN 61000-4-2	Criterion Bb	8 kV air discharge 6 kV contact discharge
Electromagnetic RF field	EN 61000-4-3	Criterion [Ac]	
Amplitude modulation Pulse modulation			10 V/m 10 V/m
Fast transients (burst) signal	EN 61000-4-4		
Supply		Criterion Bb[b] Criterion [Ac.]	2 kV/5 kHz 1 kV/5 kHz 2 kV/5 kHz
Surge current load (Surge)	EN 61000-4-5	Criterion Bb[b]	
Signal supply			1 kV 2 kV
Conducted disturbances	EN 61000-4-6	Criterion [Ac.]	10 V

Testing of interference radiation according to EN 61000-6-4

Emitted interference Housing	EN 55022		Boundary curve B

a. EN 61000 corresponds to IEC 61000

b. Criterion B: Temporary impairment of the operating behavior, which the device corrects itself.

c. Criterion A: Normal operating behavior within the specified limits.

A 2.2 Block diagram

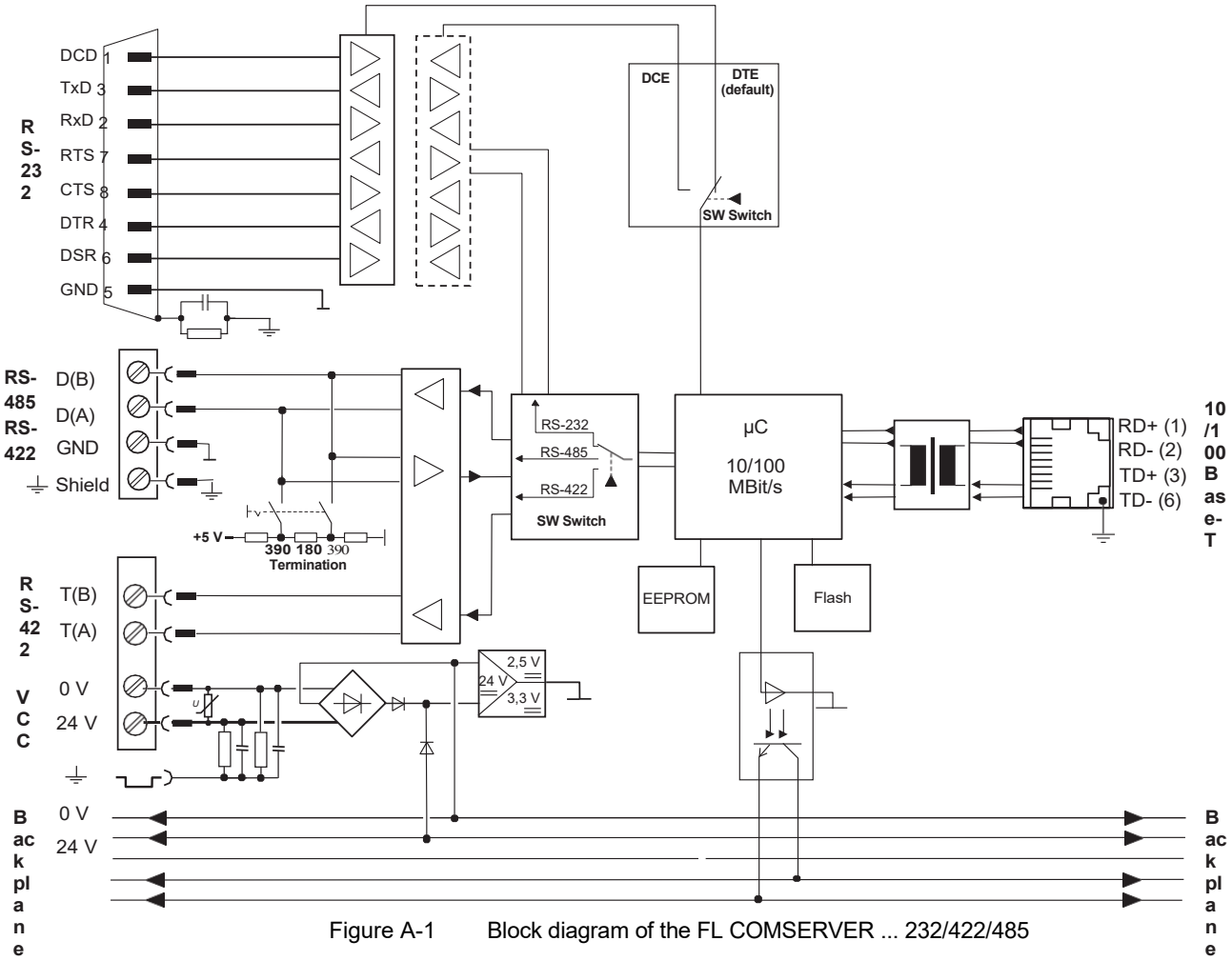


Figure A-1 Block diagram of the FL COMSERVER ... 232/422/485

A 2.3 Dimensions

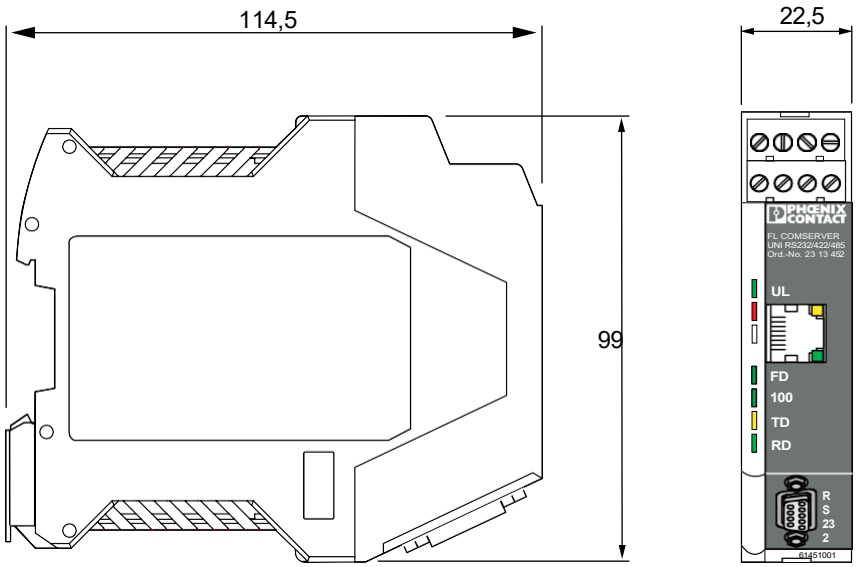


Figure A-2 Dimensions of the FL COMSERVER ... 232/422/485

A 3Explanation of the technical terms

10BASE-FL

Standard describing the transmission of 10 Mbit/s Ethernet connections with fiber optic technology. B-FOC connectors and 850 nm wavelength are prescribed, POF and HCS transmission systems are permitted in accordance with the standard.

10BASE-T

In the definition of the 10BASE-T standard, the physical topology is separated from the logical one. The cabling is implemented in a star configuration with at least two-pair Category 3 cables with 100 Ohm impedance. The transmit and receive data are transmitted separately on one pair of wires each. The connectors used are 8-pin RJ45 types; the maximum segment length is 100 meters. A hub is provided as the central active component, so that line interruptions or short circuits only mean the failure of one subscriber and not that of an entire segment.

100BASE-FX

Standard that describes the transmission of 100 Mbit/s Ethernet connections with fiber optic technology (Fast Ethernet). B-FOC or SC connectors and 1300 nm wavelength are prescribed, POF and HCS transmission systems are permitted in accordance with the standard.

100BASE-TX

Fast Ethernet; 100BASE-T was officially elevated to the IEEE standard as ITU 802.3u. This standard is essentially based on the technologies of 10BASE-T, the Ethernet variant for TP cables. 100BASE-T has several variants, which differ in the physical layer and thus in the transmission media: 100BASE-TX, 100BASE-T2, 100BASE-T4 and 100BASE-FX. All 100BASE-T networks have a star structure and are connected to a central hub. With a transmission rate of 100 Mbit/s, this method retains the MAC layer and thus the classic CSMA/CD access method. As a consequence, only very small distances can be bridged with 100BASE-T and no real-time applications can be carried out. In the case of TP cables (UTP, STP) of category 5, the maximum segment extension is 100 m, and 400 m when using fiber optic cables.

802.xx

Standard in which the Ethernet system is specified by the IEEE.

A

Terminating resistor

A terminator is not required for 10BASE-T/100BASE-TX. For the coaxial network topologies 10BASE5 or 10BASE2, 50 ohm terminators are required.

Administrator

System administrator who is responsible for the assignment of IP parameters and the uniqueness of IP addresses. He has unrestricted access and administration rights for the network in the local network.

Address table

In an address table, the switch automatically stores the MAC address and the port number of connected nodes. This reduces data traffic, since the switch only sends out telegrams on the port that is assigned to the destination address. After the aging time has elapsed, the entry is deleted from the table.

Aging TimeA

learned IP address of a subscriber (source address) is deleted from an address table if no data telegram is received from this source address within the aging time. The device assumes that the device with the source address is no longer in the network.

APIApplication Programming Interface - Software interface that provides functions for software programming. For Ethernet communication under Windows operating systems, the functions are provided by the *WinSock* API.

Application/Applet Applets are small programs that, often embedded in HTML pages, perform narrowly defined tasks, such as making small calculations, recording diagrams or evaluating forms. Applets are usually written in the Java language.

ARPAddress Resolution Protocol - ARP is used to determine the MAC address of a network subscriber that belongs to an IP address. The determined assignments are managed on the respective computer in the ARP table.

ASCII American Standard Code for Information Interchange - Coding for information transmission with a total of 128 characters (= 7 bit ASCII: includes the "simple" alphabet without umlauts and other special characters as well as control codes) or 256 characters (= 8 bit ASCII). E-mails and attachments, for example, consist only of ASCII characters.

Autocrossing A device with autocrossing recognizes independently with which type of device (DTE or DCE) a communication is to be established. This mechanism makes it unnecessary to distinguish between line and crossover connection lines.

Autonegotiation In autonegotiation mode, an Ethernet station automatically adjusts to the data transfer rate (10 Mbps or 100 Mbps) and the transfer mode (half or full duplex) of the device to which it is connected.

Autosensing In autosensing mode, an Ethernet node automatically adjusts to the data transfer rate (10 Mbps or 100 Mbps) of the device to which it is connected.

B

Backplane A system connector integrated in the base that enables fast and error-free assembly of modular stations.

Bandwidth Difference between the lowest and highest frequency possible on a transmission channel. In the field of digital telecommunications, bandwidth is the amount of data that can pass through a transmission channel within a certain period of time. The bandwidth is measured here in bps (bits per second).

Bandwidth length product The bandwidth of an optical fiber is inversely proportional to its length, or the product of bandwidth and length is constant.

Baud Unit of measurement named after the French researcher E. Baudot (1845-1903) for the step rate of a serial signal transmission. One baud corresponds to one change of state per transmission channel and second. "Baud" is often used incorrectly instead of "bps" (bits per second). The two units of measurement are not congruent, since modern data transmission devices can send four or more bits per signal over one channel.

B-FOC connector Fiber optic connector for multi- and singlemode fibers. The attachment is made with a bayonet connection.

BitBinary digit - smallest unit of information in communication technology. A bit can have the value 0 or 1.

BootP
The bootstrap protocol is described in RFC 951 (Request for Comments). The manufacturer-specific additions are explained in RFC 1084. The bootstrap protocol is based directly as an application on the user datagram protocol (UDP). Communication takes place via a single data packet according to the client-server principle. In addition to its own IP address, the client can request the IP address of the next router, the IP address of a specific server or the name of its boot file from the server. In the manufacturer-specific part, specially defined information can also be transmitted.

Bridge
A bridge is a device for connecting two separate networks. The incoming data packets are filtered based on the destination address and forwarded to the second network or discarded.

Broadcast
A broadcast call to all subscribers in the network is called a broadcast. Broadcasts are not forwarded via routers and bridges.

Broadcast address
Telegrams to the broadcast address 255.255.255.255 are sent to all nodes in the network.

Browser (web browser)
(English for "browse"), computer program that makes the pages of the Internet (texts, images) visible on your monitor.

Byte
Data unit with 8 bit content

C

CAT5
EIA/TIA specification for Ethernet cables, connectors and junction boxes. Suitable for 10 and 100 Mbit networks, transmission over 2 wire pairs.

CAT5e
Extended CAT5 specification with more stringent electrical properties. Full duplex operation over 4 wire pairs.

Client
(A hardware or software component that requests services from a server. The client is always the service requester (e.g., a browser that retrieves e-mail via the server).

Collision
A collision occurs when two participants transmit simultaneously on the same medium. A collision is resolved using the CSMA/CD method.

COM redirector
see COM redirector

COM server
Terminal device in TCP/IP networks that provides interfaces for serial devices via the network.

COM interface
Designation of the RS-232 serial interface in a PC.

COM redirection
Software utility to redirect a software with RS-232 communication to a network card, and thus to a TCP/IP communication. The software creates up to 255 virtual COM ports in the operating system.

Crossover cable
Cable configuration that connects two similar devices (DTE/DTE and DCE/DCE). The pin assignment is different at the cable ends to connect the transmitting lines to the receiving lines.

CRCCyclic Redundancy Check - checksum used in data transmission protocols to detect transmission errors in received telegrams.

CHAPChallenge Handshake Authentication Protocol - Authentication mechanism where the password is encrypted with 128-bit and is checked not only at the beginning but also during the connection. An incorrect password during the connection setup or during the ongoing connection leads to an immediate termination of the connection.

CSMA/CDCarrier Sense - Multiple Access with Collision Detection - Method for handling data collisions.

CTS Clear To **Send**, ready to send in hardware handshake, signal of the V.24 interface.

D

Attenuation Measure of the reduction in signal power on a line. Unit "dB" (decibel). The lower the dB value, the better the line

Data packet Related data that is sent bundled over computer networks. Files are not sent as a continuous stream of data (streaming), but are broken down into smaller units (packets) and transmitted individually. Each packet is provided with a header (information on source and destination address, error checking) and formatted into a size suitable for routing. The information in the header means that the individual nodes (routers) at which the packets arrive are not restricted to a particular route. Which way the packets take, the routers decide again and again. The criteria here are: shortest and most favorable or fastest route (depending on the utilization of the transmission lines). Once all data packets have reached their destination, they are reassembled into the original file at the receiving end. The typical protocol for sending data on the Internet is TCP/IP.

dB Abbreviation for "decibel", see dBm

dBm Power normalized to 1 mW for simple addition and subtraction in fiber optic link budgeting, cf. dB.

DCEData Communications Equipment - Infrastructure components in a communication path, e.g. modem, hub, switch. DCE devices can be connected directly, i.e. with 1:1 cables to DTE devices. A direct connection of two DCE devices can only be realized via crossed cables.

Default gateway All telegrams that are not addressed to nodes in the same subnet are forwarded via the default gateway.

Dial-up NetworkingRemote data transmission network. The dial-up network forms the bridge between Internet applications and modem or ISDN card under Microsoft Windows. A connection to the Internet can be established via the dial-up network.

DHCPDynamic Host Configuration Protocol - automatic, dynamic, usually time-limited allocation of IP addresses from a defined address range.

DTEData Terminal Equipment - Terminal equipment that is always installed at the beginning and end of a communication path, e.g. PC, PLC. DTE devices can be connected directly, i.e. with 1:1 cables to DCE devices. A direct connection of two DTE devices can only be realized via crossed cables.

E

Ethernet Standard for networks developed by the companies Intel, DEC and Xerox from 1976 onwards, which is widely used especially in LANs. The Ethernet standard contains regulations on network architecture (bus or star topology), hardware (e.g. cabling with coaxial or twisted pair cables), transmission and access procedures.

Ethernet address see MAC address

F

Fast EthernetFast Ethernet is operated with copper lines of category 5 or with fiber optics, the data transmission rate is 100 MBit/s.

File Transfer Protocol See FTP

Firewall A special computer in a company's computer network that allows employees to access the Internet, but blocks unauthorized access from outside. Firewall programs are also available for private computers.

Firmware Internal software that runs on the respective devices and thus enables the devices to function.

Flash ROM see ROM

Flow control method that regulates the data flow between two devices; it prevents data from being lost when the buffer of one device is full.

FL standard see 10BASE-FL

Flow Control see Flow Control

FO port FO (Fiber Optic) port

F-SMA connector Fiber optic connector for POF and HCS fibers, mounting with union nut, easy connection due to quick-connect technology.

FTP The File Transfer Protocol (FTP) is an Internet protocol for transferring files. To transfer files via FTP, a connection must be established between the client and an FTP server. When logging in to the server, an access ID and a corresponding password must be entered. The default password for read-only access is "pu- blic" and the default password for read/write access is "private".

Full Duplex see full duplex

FX standard see 100BASE-FX

G

Gateway A gateway is a technical device that enables a transition between different networks (e.g. between Ethernet and INTERBUS).

Gateway address see default gateway

H

Half duplex With half duplex, transmission is possible in one or the other direction, but never simultaneously

Half-duplex port A half-duplex port can only receive and transmit data with a time delay, while a full-duplex port can transmit and receive simultaneously.

Hardware handshake Handshake via signal lines. Usually V.24 is signaled either with CTS/RTS or with DTR/DSR.

See CTS, RTS, DTR, DSR

Header The beginning of a data packet is called the header. It contains information about the packet size and the sender and recipient addresses.

HCS Abbreviation for "Hard Cladded Silica", FO mixed fiber, core material glass + cladding material plastic, diameter 200/230 µm, easy assembly with quick-connect plug.

HTML Abbreviation for "Hypertext Markup Language". HTML is not a programming language, but a standardized page description language for WWW pages. HTML documents consist of pure ASCII text so that they can be displayed by all common computers, operating systems and browsers. "Formatting" and "commands" are enclosed in angle brackets so that browsers can distinguish them from the actual content. The HTML standard is approved by the World Wide Web Consortium (W3C) in Geneva.

HTTP Abbreviation of "Hypertext Transfer Protocol". Protocol (transmission standard) that regulates the exchange of data between a WWW server and a WWW client. HTTP is based on TCP/IP.

Hyperlink A hyperlink is a clickable reference in a document to another location in the same or another document.

I

IEEE The Institute of Electrical and Electronic Engineers defines standards. The Ethernet system is described in IEEE 802.xx, where xx is a placeholder for the various sub- standards.

Internet The Internet is the world's largest network interconnection, in which platform-independent services such as e-mail, TFTP, HTTP, etc. can be used by the participants through the use of TCP/IP.

Internet Explorer Internet Explorer is the browser of the Microsoft company.

Intranet A closed network within the boundaries of which Internet-type services can be used by the participants.

IP Internet Protocol - It enables the connection of subscribers positioned in different networks.

IP address An IP address is the unique subscriber address in the Ethernet. It is a numeric code of four numbers between 0 and 255 separated by a dot (Decimal Dot- ted Notation). The IP address is assigned by the network administrator.

J

Jabber Telegrams with invalid CRC and/or a length of more than 1536 bytes.

Java Java was developed by the company Sun Microsystems. This object-oriented, platform-independent programming language was specially adapted to the Internet. Java is integrated into web pages via Java applets (smaller application modules) or JavaBeans (Java program modules). For the execution of Java programs the "Java Virtual Machine" is necessary. In order for your Internet browser to be able to use Java, it must be activated in the browser (usually by default).

Java appletSmall program written in the Java programming language that is loaded from the Internet and interpreted and executed in a Java-enabled browser of the user. Java commands are integrated into HTML pages and converted when the page is loaded. The Java applets run in a so-called "sandbox", the "Java Virtual Machine"(JVM), and thus have no access to local computer resources. Sometimes, however, errors occur in the implementation of the JVM, so that Java applets can still access local files. Therefore, you should only allow Java when accessing what you consider to be trusted sites, such as www.t-online.de.

Java ScriptJavaScript is a script language (not a programming language!) developed by the company Netscape, which is used to make web pages dynamic or interactive. JavaScript is integrated directly into the HTML code and the interpretation is done by the browser. However, there is no "sandbox" here to prevent possible access to files and programs on the computer running JavaScript. The Microsoft-specific variant of JavaScript is called JScript. In order for your Internet browser to use Java, it must be enabled in the browser (usually by default).

Java Virtual Machine Program that interprets and executes the Java byte code in the user's browser.
Java commands are integrated into HTML pages and converted when the page is loaded. The Java programs (Java applets) run in the closed environment of the JVM, which normally has no access to local computer resources. This is why the JVM is also called a "sandbox". Occasionally, however, errors occur in the implementation of the JVM, so that Java applets can still access local files.

K

Collision see Collision

Collision domain A collision domain is bounded by end devices and/or switches, routers. A collision of packets can only occur within these boundaries. The collision domain is often also referred to as a network segment.

L

LAN Local Area Network - Network of computers sharing applications, data, printers and other services. The spatial extent is limited to one building and/or to a group of buildings locally.

Line (1:1) cable Cable configuration that connects two different devices (DTE/DCE).
The pin assignment is identical at both cable ends.

Link StatusBy sending regular link status pulses to the ports of the connected partner devices, the device monitors the valid connection to these partner devices. A valid link is indicated by a green LED.

LWL Abbreviation for optical fiber. **M**

MAC address Worldwide unique identification of network components, consisting of eight bytes and containing a manufacturer ID.

Manchester coding With Manchester coding there is always an edge change in the middle of a bit. This makes the signal DC free. The logical position of the first half of the bit always describes the transmitted information (logical "1" or logical "0").

Master-slave network Association of several communication participants. A master in the system controls all communication in the network. This means that the master is always involved in the communication. A slave-slave communication can only be established using the master as a relay station.
see Multimaster network

MDIMedia Dependant Interface - Ethernet port that can be connected directly to other infrastructure com- ponents without having to use special crossover cables. Such connections are often referred to as "uplink".

MDI-X Media Dependent Interface **Crossover** - Ethernet port to which end devices such as PCs or PLC controllers can be connected directly.

Media converter Converter from wired Ethernet to fiber optic technology.

Signal contact Potential-free switching contact for evaluating device faults.

MIBManagement Information Base - database in which all data (objects and variables) required for network management via SNMP are entered.

Modem An artificial word derived from the term modulator-demodulator. It explains the way a modem works: converting analog signals into digital data and vice versa. With the modem you can connect your computer to the Internet.

Monomode see single mode

Multicast address Telegrams with a multicast address can be received by several nodes that are ready to receive for this address.

Multimaster network Association of several communication participants. All participants can establish, maintain and terminate communication on an equal footing. In principle, any device can communicate directly with any other device.

Multimode Large-core FO that can carry many modes, cf. singlemode

N

Network Spy function that scans specific IP address ranges for active subscribers. You can specify the start and stop IP address of the range to be searched.

Network An association of computers that share files, data, and resources.

Network address See MAC address

Network management Network management is performed by the administrator using software (e.g. Factory Manager from Phoenix Contact). The network can be configured, optimized and monitored. In addition, the cause of malfunctions can be determined.

NICNetwork Interface Card - Adapter card built into a PC that provides the necessary software/hardware for communication over an Ethernet network.

NRZ "Non Return to Zero" - description of data encoding, no edge change when several similar bits are transmitted in sequence.

see Manchester coding

O

OSIOpen System Interconnect **P**

Packet Combination of bits containing data, control information, source and destination address and secured for data transmission.

PAPPassword Authentication Protocol - Authentication mechanism for a PPP connection. The password is transmitted unencrypted, i.e. in plain text, to the communication partner for verification. The password is checked once during the connection setup. A password error during the connection setup leads to an immediate termination of the connection.

Parity Bit in asynchronous data transmission that is used for error detection. Part of the transmission format. Either omitted (No Parity), constant one (Mark) or zero (Space). With even parity the bit is set if the number of bits in the data is even. Analogous for odd parity with odd number.

Peer-to-peer connection "Peer" means equal in English. Communication in which both sides are equally responsible for initiating, maintaining and terminating the ses- sion. P2P (peer-to-peer) networks are a way to implement a serial cable replacement over the network.

PingPacket Internet Groper - A ping is used to measure the reliability of a network connection and the response time of a server. A client contacts a server on its ping port. As soon as the server answers, the client calculates the elapsed time in milliseconds. It also determines whether pings (small data packets) have been lost. To get realistic results, it is possible to send pings with different byte sizes (Factory Manager: 1 byte to 32 bytes).

POF Polymer Optical Fiber, see polymer fiber.

Polymer fiber FO made of 100 % plastic, easy assembly with F-SMA quick-connect plugs, diameter 980/1000 µm

Port (I) Interface for data transfer to a PC. An Internet service can only be reached with the Internet address and the corresponding port. There are fixed port numbers for defined services, e.g. port 80 for web servers or port 21 for FTP servers.

Port (II) Ethernet interface (in fiber optics or copper) of the Factory Line devices.

PPPPoint-to-Point protocol - Successor to the SLIP protocol. Enables data transmission via leased lines and dial-up connections in analog and digital fixed and mobile networks. Required when the PC is connected to the Internet via telephone lines.

PPPoE Abbreviation for "Point to Point Protocol over Ethernet".

Protocol Convention for exchanging data between computers on a network. Protocols specify the following: Structure, composition and coding of data packets.

Point to point connection Communication between exactly two participants on one line, cf. master-slave and multimaster networks

PROMProgrammable ROM - Read Only Memory where the memory contents can be changed.

Q

R

RARPReverse Address Resolution Protocol. Displays the IP address assigned to a specific MAC address.

Redundancy manager A FL SWITCH ... operating as a redundancy manager monitors the backbone network segments connected to it. monitors the network segments connected to it (backbone) and switches to the redundant connection in the event of a failure.

RFCRequest For Comment - Standardization document of the Internet Research and Development Group, e.g. for defining protocols or services.

RIPRouting Information Protocol - Protocol for exchanging routing information between routers.

RJ45 Most common connector for Ethernet and ISDN connections. Often also referred to as Western connector.

ROM Read Only Memory - memory that permanently stores data (even in the event of a power failure). An extension is the Flash ROM, which can be rewritten by the user. This makes a firmware update possible.

Router Routers connect different networks with each other. The IP address is used to decide which IP packet is to be routed to which network.

RS-232 interface The RS-232 interface is defined in the American EIA-232 standard and in the international CCITT V.24 standard. This serial interface realizes the data exchange between two devices in full duplex operation (point-to-point connection). The maximum transmission rate is 115.2 kBit/s, the maximum transmission length is 15 m.

see DCE, DTE

RTSRequest To Send - send request in hardware handshake, signal of V.24 interface.

RTS/CTS control see hardware handshake

S

SC duplex connector Plastic fiber optic connector (usually separable) for multimode and singlemode fibers. The connector is locked onto the transceiver components by a push-pull mechanism.

Interface Defined boundary between two hardware components, two software components or between hardware and software components, which delimits technical functions and/or administrative responsibilities of technical devices from one another. Examples of interfaces are the transitions from computers to data transmission devices or from communication devices to each other.

Session A connection to a network service is called a session.

Serial transmissionMethod of data transmission in which the bits of a data character are transmitted sequentially over a single data channel.

Server (In the hardware sector, this refers to a computer in a network that provides services to other participants. In the software sector, it refers to a program on a server computer that provides certain services.

see client-server principle

Singlemode FO in which only a single mode can be propagated at the operating wavelength of the FO cable. Core diameter about 9 µm at 1300 nm wavelength

SLIP Serial Line Internet Protocol - obsolete protocol for establishing a TCP/IP connection over serial connections. Has been replaced by the PPP.

SNMPSimple Network Management Protocol - vendor-neutral standard for Ethernet management.

Software handshake Handshake by specified characters. Not suitable for binary transfers without a transfer protocol, since the data may also contain the reserved handshake characters. The most common characters are XON/XOFF.

see XON, XOFF

Source code Program code that is neither compiled nor assembled.

Socket Describes the combination of the IP address and the communication port, where the unique connection assignment is ensured.

Spanning tree The spanning tree algorithm is a method for loop suppression (loops) in (redundantly) coupled networks. The physical redundant network structures are determined and converted into a loop-free structure by means of targeted port shutdowns. This measure reduces the active connection paths of an arbitrarily meshed structure. The resulting tree structure has two significant properties:

– All networked points (ports) are connected by only one path.
– All networked points are accessible from all networked points.

The algorithm is implemented in the corresponding nodes, with each switch calculating the path to the root switch based on defined quality criteria. Distances, capacities, costs, utilization, etc. can be used as quality criteria.

Leased line Special telephone or other telecommunications line where the connection is constantly active. This means that a connection does not first have to be established for data exchange. Such lines are used, for example, by companies between their branches or as a connection to an Internet service provider.

Start bit Bit in asynchronous transmission that indicates the start of a data word. Always logical "0".

Stop bit One or two bits in asynchronous transmission that indicate the end of a data word. Always logical "1".

STPShielded Twisted Pair - Shielded data cable in which the associated data wires are twisted together.

ST connector see B-FOC connector, AT&T trademark

Subnet mask The subnet mask determines which part of the IP address is used as the subnet address. Example: In a Class A network (subnet mask 255.0.0.0), the first field of the IP address represents the subnet. The IP address is 207.142.2.1, so the subnet address is 207.0.0.0 and the subscriber address 142.2.1.

Switch So-called "LAN switches" are used in local networks. These connect areas of the network that operate at different speeds (10 or 100 Mbit/s), for example, or keep areas with very large traffic (data volume per time) separate from other areas of the network. The switch recognizes which area of the network data packets are destined for and forwards them to the other segment only if necessary. This increases the usable total bandwidth of the network.

Synchronous connectionConnection in which a clock signal is transmitted in addition to the user data so that start and stop bits, as in an asynchronous connection, can be dispensed with. Faster due to this.

System reserve Optical safety reserve. In order to compensate for the technically induced aging of the transmitting diodes in the long term, it must be taken into account when planning fiber optic links (typically 3 dB).

T

TCP/IP Transmission Control Protocol - TCP is based on IP and ensures the correctness of data and the correct sequence of data packets during transmission.

TCP/IP stackPart of the operating system or a driver that provides all the drivers and functions needed to support the IP protocol.

Telegram length Length of the entire telegram from the destination address to the CRC field. The maximum length is 1536 bytes.

Telnet **Terminal** over Network - standard protocol used to establish an interactive connection to other devices via Ethernet. Telnet is based on TCP/IP as a transmission and backup protocol.

Terminal program Simple communication program for transferring ASCII and binary data. Implemented by default in PC operating systems, e.g. Windows Hyperterminal.

Terminator A terminator is not required for 10BASE-T / 100BASE-TX. For the coaxial network topologies 10BASE5 or 10BASE2, 50 Ohm terminators are required.

TFTPTrivial File Transfer Protocol - The protocol is suitable for transferring entire files, using a minimum of commands and UDP as the transfer protocol.

TFTP server Server from which the factory line components can load new firmware/configurations via TFTP.

Topology The spatial arrangement and connection of the network nodes is referred to as topology. A distinction is made between ring, bus, star or tree topology.

TP see Twisted Pair

Trap Traps are SNMP alarm or event messages that are transmitted with the highest priority to different addresses and then displayed in plain text by the management station.

Trap Targets Trap targets are the targets that evaluate traps (alarm or event messages).

Twisted pair data cable in which two data wires are twisted together. The twisting of the "outward and return line" results in significantly reduced crosstalk behavior. A distinction is made between STP (Shielded Twisted Pair) and UTP (Unshielded Twisted Pair).

U

UARTUniversal Asynchronous Receiver and Transmitter - Integrated circuit that converts between serial and parallel signals. It provides transmission clocking and stores data in a buffer that is sent to or from a computer.

UDPUser Datagram Protocol - UDP is a connectionless protocol that is based on IP but has no security measures. UDP enables higher speeds for data transmission.

UTP Unshielded Twisted Pair - unshielded data cable with two twisted wires each.

V

Full duplex Simultaneous, independent two-way transmission in both directions.

W

WANWide Area Network - A network that uses common transmission mechanisms. The network extent covers a large geographic area such as countries or continents.

WBM Web Based Management - With WBM, HTML pages are loaded from the devices into the web browser for diagnostic and configuration purposes.

WINSOCK Standard API of the Windows operating system, which contains all functions for network communication.

X

XON/XOFF Designation for start and stop bit in software handshake mode of an RS-232 connection.

Y

Z

B Directory Annex

B 1 List of figures

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

B 2 List of tables

Chapter 1

Chapter 2

Chapter 4

C Appendix help

C 1 Hotline

In case of problems that cannot be solved with the help of this documentation, please contact our hotline:


+ 49 - (0) 52 81 - 946 28 88


factoryline-service@phoenixcontact.com