INTERFACE

User Manual

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

Order No.: —

Installing and starting up the
FL COMSERVER BASIC 232/422/485 and
FL COMSERVER UNI 232/422/485 hardware and software

PHOENIX CONTACT
INSPIRING INNOVATIONS

DOWNLOADED FROM WWW.SCATTS.CO.UK

INTERFACE

User Manual

Installing and starting up the FL COMSERVER BASIC 232/422/485 and FL COMSERVER UNI 232/422/485 hardware and software

11/2009

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

Revision: 01

Order No.: —

This user manual is valid for:

Designation	Order No.
FL COMSERVER BASIC 232/422/485	2313478
FL COMSERVER UNI 232/422/485	2313452

Please observe the following notes

In order to ensure the safe use of the product described, you have to read and understand this manual. The following notes provide information on how to use this manual.

User group of this manual

The use of products described in this manual is oriented exclusively to qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.

Phoenix Contact accepts no liability for erroneous handling or damage to products from Phoenix Contact or third-party products resulting from disregard of information contained in this manual.

Explanation of symbols used and signal words

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

DANGER
This indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING
This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION
This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

The following types of messages provide information about possible property damage and general information concerning proper operation and ease-of-use.

NOTE
This symbol and the accompanying text alerts the reader to a situation which may cause damage or malfunction to the device, either hardware or software, or surrounding property.

This symbol and the accompanying text provides additional information to the reader. It is also used as a reference to other sources of information (manuals, data sheets, literature) on the subject matter, product, etc.

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular data sheets, installation instructions, manuals, etc.) does not constitute any further duty on the part of Phoenix Contact to furnish information on alterations to products and/or technical documentation. Any other agreement shall only apply if expressly confirmed in writing by Phoenix Contact. Please note that the supplied documentation is product-specific documentation only and that you are responsible for checking the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. Although Phoenix Contact makes every effort to ensure that the information content is accurate, up-to-date, and state-of-the-art, technical inaccuracies and/or printing errors in the information cannot be ruled out. Phoenix Contact does not offer any guarantees as to the reliability, accuracy or completeness of the information. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed. This information does not include any guarantees regarding quality, does not describe any fair marketable quality, and does not make any claims as to quality guarantees or guarantees regarding the suitability for a special purpose.

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

The aforementioned limitations of liability and exemptions from liability do not apply, in so far as liability must be assumed, e.g., according to product liability law, in cases of premeditation, gross negligence, on account of loss of life, physical injury or damage to health or on account of the violation of important contractual obligations. Claims for damages for the violation of important contractual obligations are, however, limited to contract-typical, predictable damages, provided there is no premeditation or gross negligence, or that liability is assumed on account of loss of life, physical injury or damage to health. This ruling does not imply a change in the burden of proof to the detriment of the user.

Statement of legal authority

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
www.phoenixcontact.com.

Make sure you always use the latest documentation.
It can be downloaded at:
www.phoenixcontact.net/download.

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at www.phoenixcontact.com.

Published by

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

PHOENIX CONTACT
P.O. Box 4100
Harrisburg, PA 17111-0100
USA
Phone +1-717-944-1300

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to
tecdoc@phoenixcontact.com.

Table of Contents

1 Preface

1.1 Description

Ethernet now has a high level of acceptance in industrial applications. However, automation equipment is not always network capable. A solution is available in the form of the new FL COMSERVER ... 232/422/485 serial device server. It enables serial V.24 (RS-232), RS-422, and RS-485 interfaces to be easily integrated into industrial 10/100 Base-T(X) networks.

This means that in theory Ethernet networks can be used to perform the following tasks from anywhere in the world:

– Request the system state
– Transmit visualization data
– Initiate a program or firmware download
– Carry out remote maintenance for servicing

Network integration eliminates the need for costly cable installations. Serial connections are converted to Ethernet and tunneled through the network using either the TCP or UDP protocol. In addition, Modbus gateways and PPP connections can be implemented.

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

Table 1 Supported data protocols

	Data protocols			
FL COMSERVER ...	**TCP/IP**	**UDP**	**Modbus/ TCP**	**PPP with CHAP**
... UNI 232/422/485 Order No. 2313452	x	x	x	x
... BASIC 232/422/485 Order No. 2313478	x	x	–	–

With the aid of virtual COM ports, existing application software that only supports serial communication can be redirected to the network card of a Windows PC using the COM port redirector software, which is available free of charge.

Easy configuration and diagnostics

Configuration and diagnostics can be carried out without the need for additional software via standard web browsers using web-based management. The menu structures are organized clearly according to topics to allow intuitive configuration, and the web pages adapt dynamically to the desired application. If, however, configuration and diagnostics are to be implemented directly using a process visualization, the relevant SNMP objects are available for integration in OPC databases.

Performance for industrial requirements

To ensure safe and permanent operation under harsh industrial conditions, the **FL COMSERVER ... 232/422/485** offers high-quality 3-way electrical isolation (VCC // V.24 (RS-232), RS-422, RS-485 // Ethernet) as well as a redundant supply option for the 24 V power supply. A high level of availability is also ensured by the high

electromagnetic compatibility of the devices. Both hardware and software are designed to meet specific industrial requirements. The 3964R protocol, for example, is supported, as are the various Modbus protocols or status messages via SNMP objects.

The **FL COMSERVER ... 232/422/485** has been specifically developed for industrial applications in the control cabinet. It offers the following features:

- Mounting on EN DIN rails
- Extended temperature range
- 22.5 mm slim design width
- 10/100Base-T(X), auto negotiation
- 24 V AC/DC ±20% power supply
- Redundant power supply and modular station structure with T-BUS connectors supported
- High-quality 3-way isolation (VCC // V.24 (RS-232), RS-422, RS-485 // Ethernet)
- Comprehensive diagnostic indicators
- Integration in network management tools and visualization systems with the support of SNMP services
- Configuration using web-based management, including password protection
- Support of all popular network protocols
- PPP protocol with CHAP (128-bit password encryption)
- Modbus TCP support
- COM redirector software supplied as standard

1.2 Contents

This user manual describes the easy startup of an **FL COMSERVER ... 232/422/485** as follows:

1. Mounting the **FL COMSERVER ... 232/422/485**
2. Selecting and configuring the application options
3. Checking the settings
4. Startup

1.3 Hardware and software requirements

For configuration and startup, a PC with the following configuration is necessary:

- Ethernet network connection
- HTML browser, e.g., Internet Explorer 5.0 or later, or Netscape Navigator 4.6 or later

1.4 Trademarks

Windows® is a registered trademark of the Microsoft Corporation.

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 slip, which contains installation instructions. Please read the complete package slip carefully before unpacking the FL COMSERVER ... 232/422/485.

2.1.1 Scope of supply

The package contains the following items:

– FL COMSERVER BASIC 232/422/485 Order No. 2313478 or
  FL COMSERVER UNI 232/422/485 Order No. 2313452
– Multi-lingual package slip
– CD with user manual in PDF format, COM redirector software, and MIB files

2.2 Connection and operating elements

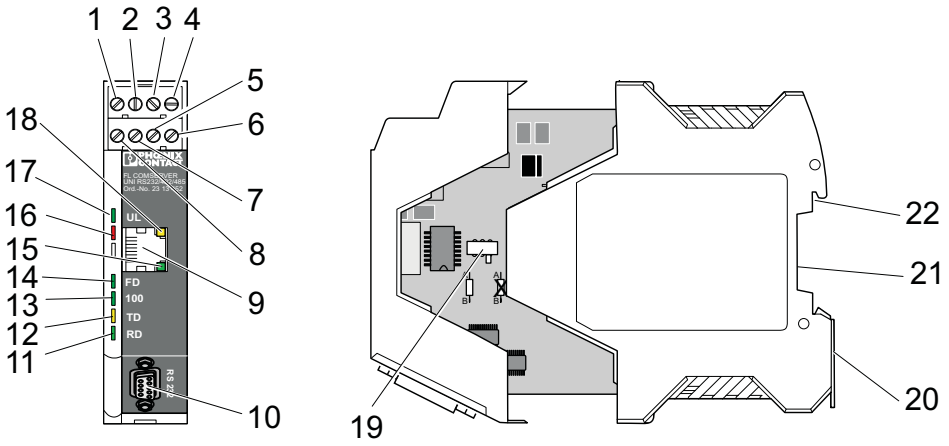


Figure 2-1 Structure of the FL COMSERVER ... 232/422/485

1. 24 V AC/DC ±20% power supply connection
2. 0 V power supply connection
3. T(A), RS-422 connection
4. T(B), RS-422 connection
5. D(A), RS-422/RS-485 connection
6. D(B), RS-422/RS-485 connection
7. GND
8. ⏚ Shield, same potential as FE
9. Ethernet connection, RJ45
10. V.24 (RS-232) connection, 9-pos. D-SUB pin strip
11. Green LED, RD, receive data
12. Yellow LED, TD, transmit data
13. Green LED, 100, 100 Mbps transmission speed
14. Green LED, FD, full duplex mode active
15. Green LED, LINK status of TP port
16. Red LED, error display
17. Green LED, UL, power supply
18. Yellow LED, ACT data transmission via TP port, dynamic
19. Slide switch for RS-422/RS-485 termination network (390 Ω/180 Ω/390 Ω)
20. Snap-on foot for DIN rail mounting
21. Bus connector for redundant power supply (covered)
22. FE, functional earth ground contact (covered)

2.3 Configuration

2.3.1 Activating/deactivating the termination network

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

The FL COMSERVER ... 232/422/485 is equipped with a switchable termination network upon delivery. Depending on the location on the RS-485 bus cable, the termination network must be activated or deactivated.

2.3.2 Opening/closing the housing

To set the required operating mode via the termination network, the housing of the FL COMSERVER ... 232/422/485 must be opened.

To do this, proceed as follows:

1. Open the housing cover using a suitable screwdriver (see Figure 2-2, ①)
2. Pull the PCB out of the housing as far as possible (see Figure 2-2, ②)
3. Depending on the location on the bus system, activate/deactivate the termination network (see Section 2.3)
4. Carefully reinsert the PCB as far as it will go
5. Snap the housing cover into place

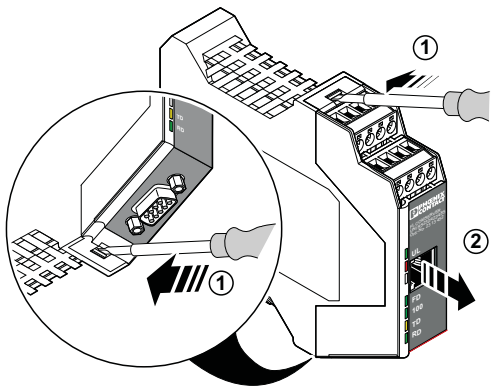


Figure 2-2 Opening/closing the housing

2.3.3 Setting the operating mode

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

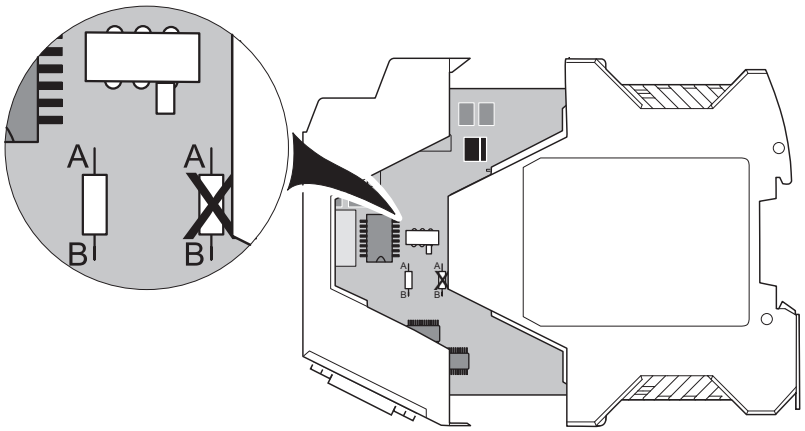


Figure 2-3 Position of the slide switch

Operating mode/device	Switch position	Resistor network
RS-422	Left	Activated
RS-485 termination device	Left	Activated
RS-485 device*	Right	Deactivated

* Default setting

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

NOTE:
Only mount the FL COMSERVER ... 232/422/485 when the power supply is disconnected.

2.4.1 DIN rail (single device)

To mount on the DIN rail, proceed as follows:

1. Place the device onto the DIN rail from above, so that the upper housing keyway hooks onto the top edge of the DIN rail (see Figure 2-4 A).
2. Holding the device by the housing cover, carefully push the device towards the mounting surface.
3. Once the snap-on foot has been snapped onto the DIN rail, check that it is fixed securely.

To remove, proceed as follows:

1. Use a suitable screwdriver to release the locking mechanism on the snap-on foot of the device (see Figure 2-4 B).
2. Hold onto the device by the housing cover and carefully tilt it upwards.
3. Carefully detach the device from the DIN rail bus connector and the DIN rail.

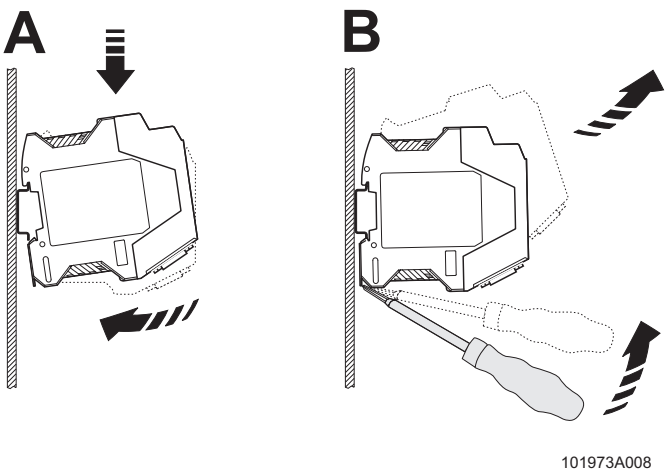


Figure 2-4 Mounting and removal (single device)

2.4.2 DIN rail bus connector (connection station)

For modular electronic housing in the ME.../TBUS series, DIN rail bus connectors of various widths are required in a connection station.

By connecting together the DIN rail connectors (see Figure 2-5 A) and inserting them in the 35 mm wide DIN rail (see Figure 2-5 B/C), the power supply is routed to the backplane (see Figure 2-5).

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

NOTE: Damage to equipment in the event of excess current load.

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

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

When using the FL COMSERVER ... 232/422/485 in a connection station, use a 22.5 mm wide DIN rail bus connector (Order No. 2707437).

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

To mount on the DIN rail bus connector, proceed as follows:

Make sure that the DIN rail bus connector and device are aligned correctly.

- DIN rail bus connector (connector part) on the left
- Device (snap-on foot) below

1. Place the device onto the DIN rail from above, so that the upper housing keyway hooks onto the top edge of the DIN rail (see Figure 2-5, detail D).
2. Holding the device by the housing cover, carefully push the device towards the mounting surface so that the device bus connector is securely fixed onto the DIN rail bus connector.
3. Once the snap-on foot has been snapped onto the DIN rail, check that it is fixed securely.

The device is only secured mechanically via the DIN rail.

To remove, proceed as follows:

1. Use a suitable screwdriver to release the locking mechanism on the snap-on foot of the device (see Figure 2-5 E).
2. Hold onto the device by the housing cover and carefully tilt it upwards.
3. Carefully detach the device from the DIN rail bus connector and the DIN rail (see Figure 2-5 E).

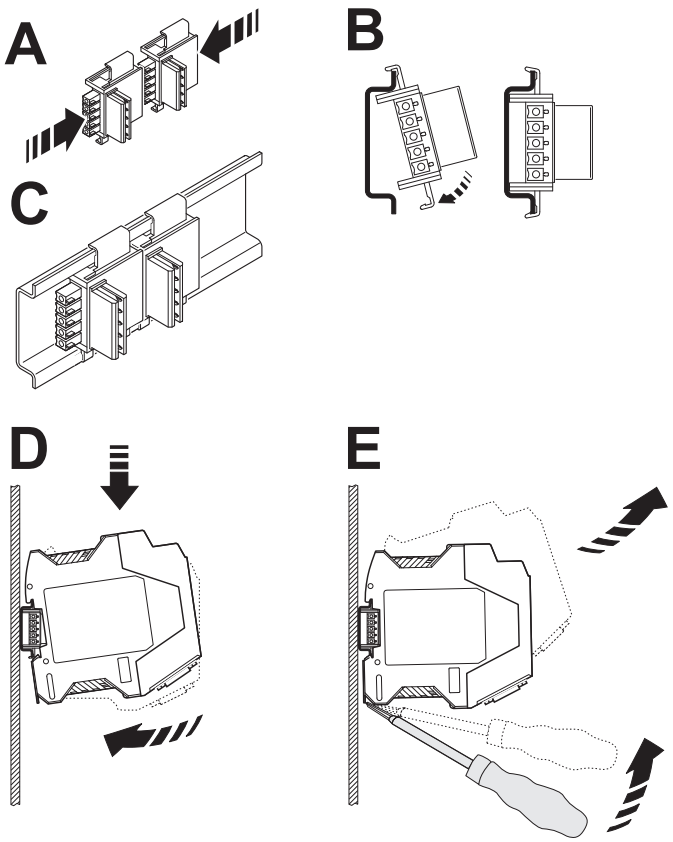


Figure 2-5 Mounting and removal (connection station)

2.5 Connecting the V.24 (RS-232) connecting cable

Connect the FL COMSERVER ... 232/422/485 to the V.24 (RS-232) device to be connected, e.g., a PC, via the PSM-KA-9SUB 9/BB/2 METER V.24 (RS-232) cable (Order No. 2799474). The cable is an interface cable with 1:1 connected contacts.

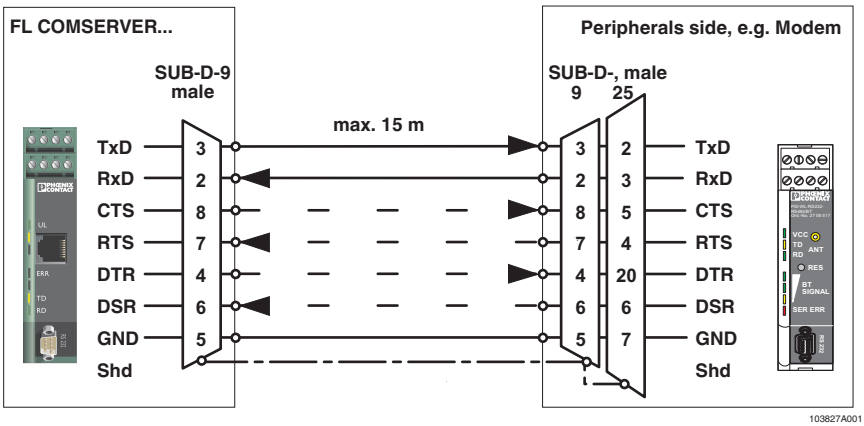


Figure 2-6 Pin assignment of the V.24 (RS-232) interface

The V.24 (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.

By default upon delivery (DTE), the interface acts like a PC.

Please note the different interface configuration when switching from an FL COM SERVER... (previous version) to the FL COMSERVER ... 232/422/485 and reusing the existing V.24 (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 (default upon delivery)
INTERBUS controller (DCE)	DTE (default upon delivery)
Siemens S7 with MPI adapter (DTE)	DCE

NOTE:

The FL COM SERVER RS... must only be connected to devices, which meet the requirements of EN 60950 ("Safety of Information Technology Devices").

2.6 Connecting the RS-422 connecting cable

RS-422 pin assignment

In RS-422 mode, a point-to-point connection can be established.

Use a twisted pair, common shielded bus cable to connect the I/O device.

Connect the individual conductors of the data cable to the COMBICON plug-in screw terminal block.

Make sure the signal assignment is correct.

This operating mode supports full duplex transmission mode.

FL COMSERVER ... RS232/422/485

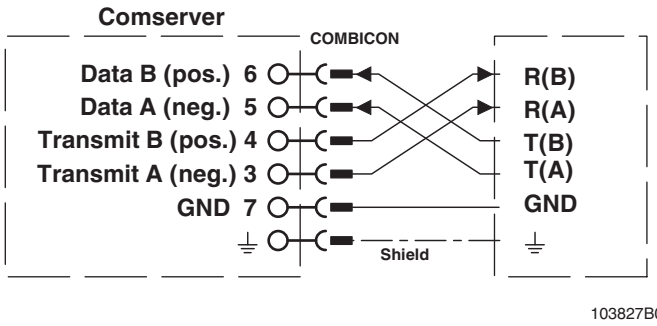


Figure 2-7 RS-485 pin assignment

Fit this bus cable with a termination network at each I/O device.

Activate the termination network integrated in the FL COMSERVER ... 232/422/485 (see Section 2.3).

NOTE:

The FL COM SERVER RS... must only be connected to devices, which meet the requirements of EN 60950 ("Safety of Information Technology Devices").

The shield connection of the RS-422 bus cable must only be connected to the FL COMSERVER ... 232/422/485 on one side.

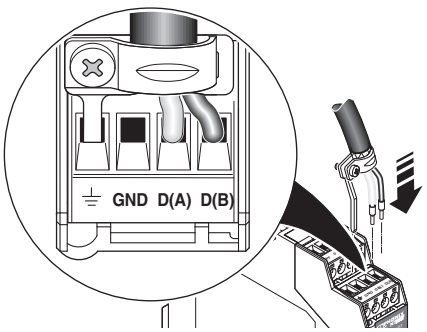


Figure 2-8 Shield connection

2.7 Connecting the RS-485 connecting cable

In RS-485 mode, an RS-485 network with several I/O devices can be created. Use a twisted pair, common shielded bus cable to connect the I/O devices.

Connect the individual conductors of the data cable to the COMBICON plug-in screw terminal block..

NOTE: Observe the polarity of the RS-485 cable.

Fit this bus cable with a termination network at the two furthest points of the RS-485 network.

Activate the termination network integrated in the FL COMSERVER ... 232/422/485 (see Section 2.3).

FL COMSERVER ... 232/422/485

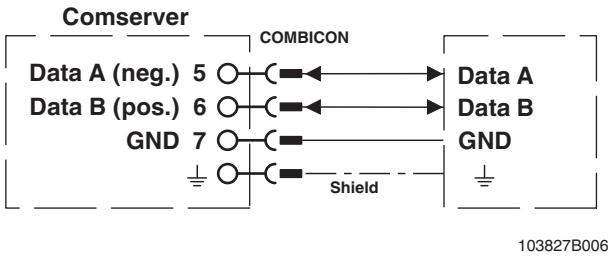


Figure 2-9 RS-485 pin assignment

Fit this bus cable with a termination network at each I/O device.

Activate the termination network integrated in the FL COMSERVER ... 232/422/485 (see Section 2.3).

NOTE:

The FL COM SERVER RS... must only be connected to devices, which meet the requirements of EN 60950 ("Safety of Information Technology Devices").

The shield connection of the RS-422 bus cable must only be connected to the FL COMSERVER ... 232/422/485 on one side.

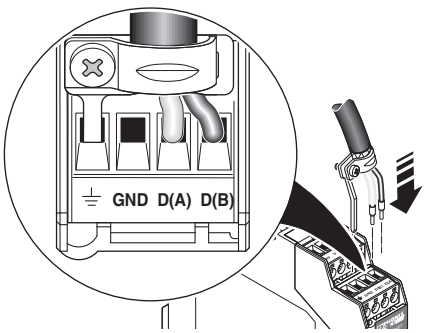


Figure 2-10 Shield connection

2.8 Connecting the Ethernet network

2.8.1 Twisted pair interface (TP)

The FL COMSERVER ... 232/422/485 has an Ethernet interface on the front in RJ45 format, to which only twisted pair cables with an impedance of 100 Ω can be connected. The data transmission rate is either 10 or 100 Mbps. The FL COMSERVER ... 232/422/485 supports the auto negotiation function for automatic selection of the transmission speed.

2.8.2 Connection

Push the Ethernet cable with the crimped RJ45 connector into the TP interface until it engages with a click.

NOTE: Possible malfunction of the device, device environment, hardware or software.

Only use shielded twisted pair cables and corresponding shielded RJ45 connectors.

Make sure the signal assignment of the connector is correct.

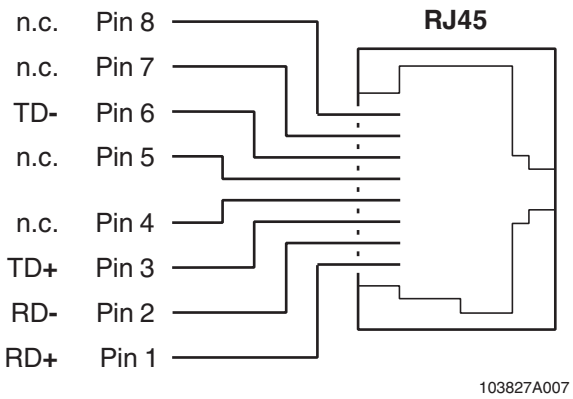


Figure 2-11 RJ45 pin assignment

2.8.3 Selecting the correct connecting cables

To connect Ethernet components, use either crossed cable pairs (**C**ROSS**O**VER) or linear connected cable pairs (**LI**NE, 1:1). In general, linear wired cables are required between structure components and termination devices, whereas crossover cables are used for connections between two structure components and for connections between two termination devices. The correct cable can be selected using the following table. To distinguish between the two cable types, green bend protection sleeves (protective caps) should be used for crossover cables, and gray bend protection sleeves (protective caps) should be used for linear wired cables (LINE, 1:1).

Table 2-1 Connection methods of various Ethernet components

• LINE 1:1 = Gray protective caps • CROSSOVER = Green protective caps	PC/RFC	INTERBUS gateway	I/O bus terminal	COM server	Switch	Hub	Media converter
PC/RFC	Cross	Cross	Cross	Cross	Line	Line	Line
INTERBUS gateway	Cross	Cross	Cross	Cross	Line	Line	Line
I/O bus terminal module	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

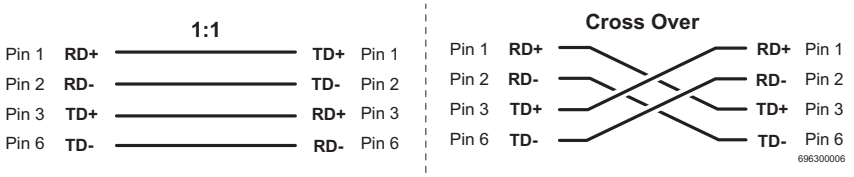


Figure 2-12 Pin assignment of Ethernet connecting cables

2.8.4 Ethernet operating indicators

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

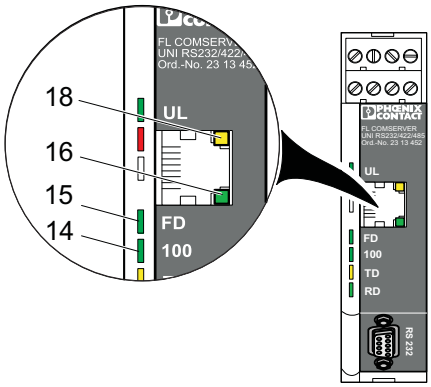


Figure 2-13 Diagnostic indicators for the TP port

No.	Des.	Function
14	100	The green 100 LED lights up when data is being transmitted at 100 Mbps.
15	FD	The green FD LED lights up when data is being transmitted in full duplex mode.
16	LINK	The line monitoring function checks the cable segment for an interrupt. The partner must transmit link or data signals. The green LINK LED lights up if no error has occurred. An interface that is not being used or a termination device that is switched off is indicated as an error and the LED goes out.
18	Activity	The yellow Activity LED flashes according to the amount of data that is currently being transmitted or received at the TP port.

2.9 Connecting the power supply

CAUTION: Incorrect connection may result in damage to equipment and/or serious personal injury.

Only qualified personnel may connect the power, start up, and operate this device. According to the safety instructions in this text, qualified personnel are persons who are authorized to start up, to ground, and to mark devices, systems, and equipment according to the standards of safety technology. In addition, these persons must be familiar with all warning instructions and maintenance measures in this text.

Disregarding this warning may result in damage to equipment and/or serious personal injury.

The FL COMSERVER ... 232/422/485 is operated using a +24 V DC SELV.

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

Alternatively, the devices in a connection station are supplied from a redundant power supply via the DIN rail bus connector (see Section 2.4.2).

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

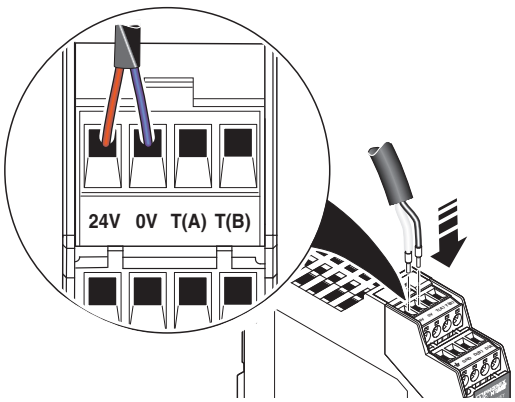


Figure 2-14 Connecting the supply voltage without a T-BUS connector

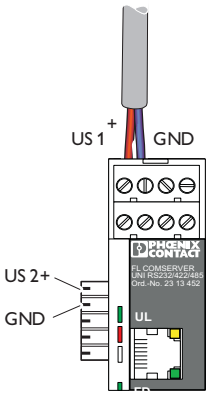


Figure 2-15 Connecting the supply voltage, module snapped onto a T-BUS connector

3 Configuration and startup

3.1 Default upon delivery/default settings

By default upon delivery or after the system is reset to the default settings (with the exception of the IP parameters), the following functions and features are available:

– 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 remain the same when the device is reset to its default settings. This means that web-based management can be accessed immediately.

– BootP and DHCP are activated as the addressing mechanism.
– No password is set for read access.
– The password for write access is "**private**".
– WBM (web-based management) can be addressed by any IP address.
– The serial interface is configured as follows:
  Interface type: Port 0 V.24 (RS-232)
  Transmission speed: 9600 bps
  Data bits: 8
  Parity: None
  Stop bits: 1
  Flow control: None
  V.24 (RS-232) interface type: DTE

By default upon delivery (DTE), the interface acts like a PC.

The V.24 (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.

Please note the different interface configuration when switching from an FL COM SERVER... (previous version) to the FL COMSERVER ... 232/422/485 and reusing the existing V.24 (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 information collected by the SNMP agent is deleted.
– No trap receiver is specified.

3.2 Configuring the IP address

Each device in an Ethernet network must have a unique address, which is used to control communication and data exchange, see phone numbers with international and local dialing codes. This Internet protocol address (IP address) is a numerical code made up of four digits between 0 and 255, which are separated by a dot (dotted decimal notation). The IP address is assigned by the network administrator.

By default upon delivery, a private IP address (IP = 192.168.0.254, subnetwork = 255.255.255.0) is set for the FL COMSERVER ... 232/422/485. BootP and DHCP modes are also activated.

Valid IP parameters must be assigned for the management function and further configuration.

Additional information and details about the assignment of IP addresses can be found in "Assigning IP addresses" on page A-1.

3.2.1 Configuration via WBM

1. Set the IP address of your PC to the subnetwork of the COM server (e.g., IP = 192.168.0.10, subnetwork = 255.255.255.0).
2. Switch to your web browser and enter the IP address of the COM server in the address line (default = **192.168.0.254**).
3. WBM responds immediately.

If the WBM of the FL COMSERVER ... 232/422/485 does not send confirmation, first check the IP parameters of your PC.
If everything is set correctly, check whether there are any proxy settings loaded in the web browser. The settings must be set to "Load automatically" or "Deactivated" in order to function correctly.

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

Figure 3-1 Password request

6. The "IP Configuration" menu opens:

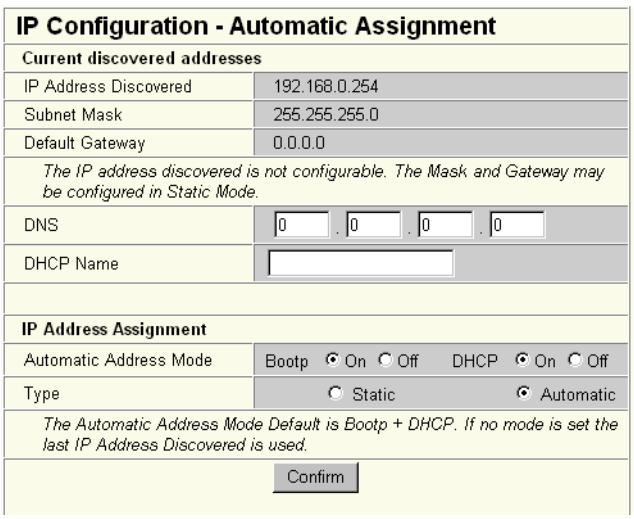


Figure 3-2 "IP Configuration" menu

7. To make changes to the IP address or subnet mask, select "Type" → "Static" 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 store and activate the new configuration, switch to the "Save and Reboot" menu.

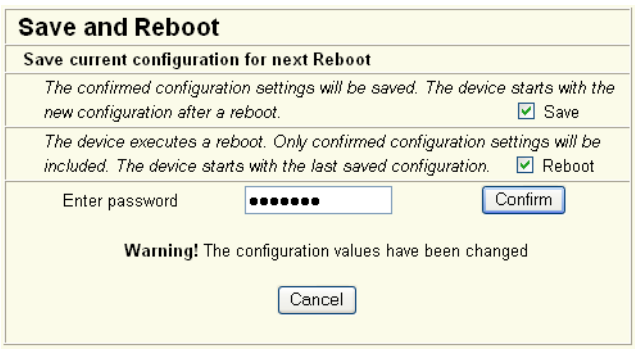


Figure 3-3 "IP Configuration" menu

10. Enter "**private**" as the password and apply/activate the new configuration.

3.2.2 Configuration via the V.24 (RS-232) interface

1. Connect the FL COMSERVER ... 232/422/485 to a serial COM interface on a PC (1:1 cable).
2. Open a terminal program, e.g., HyperTerminal, in the Windows Start menu via "Programs... Accessories... Communications... HyperTerminal".
3. Configure the interface (e.g., COM 1) via "File... Properties" to 9600 bps; 8 data bits; no parity; 1 stop bit; no flow control.

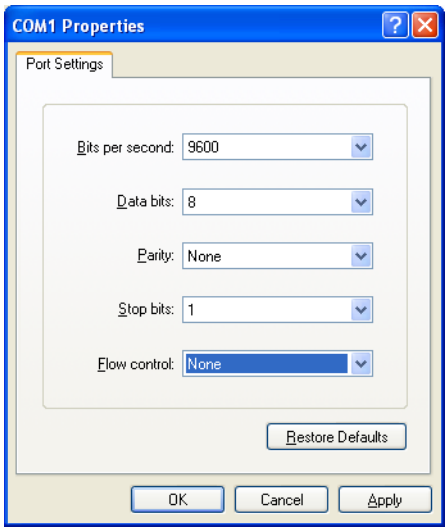


Figure 3-4 "Properties" menu in Windows HyperTerminal

4. Confirm the settings with "OK" and close the menu.
5. Check that the settings are correct in the status bar in HyperTerminal.

Figure 3-5 Status bar in Windows HyperTerminal

6. Reset the voltage at the FL COMSERVER ... 232/422/485 and simultaneously hold down the "X" key on your keyboard.
7. As soon as confirmation from the FL COMSERVER ... 232/422/485 is displayed, press ENTER within three seconds.

The following is displayed:

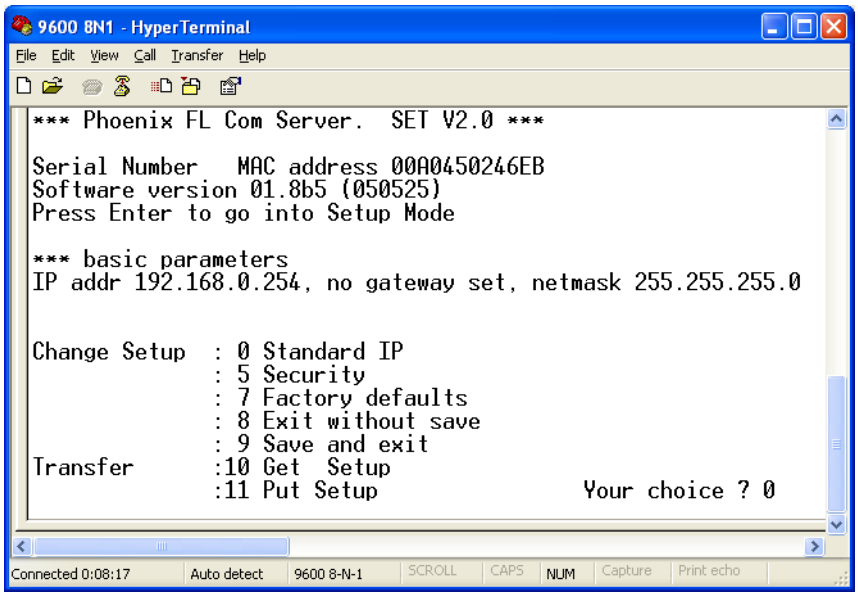


Figure 3-6 Serial setup menu

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

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

	Network bits	Computer 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 additional examples, please refer to "Subnet masks" on page A-4.

11. Press "9" to save and exit the entry.

The other device settings can now be entered using a browser via web-based management. To do this, enter the IP address that was specified above 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, which is printed on the FL COMSERVER ... 232/422/485. On Phoenix Contact Factory Line products this always starts with 00.A0.45.xx.xx.xx.
2. Enter the MAC address and the desired IP address, subnet mask, and gateway address for the BootP server.
3. On the next BootP request from the FL COMSERVER ... 232/422/485, the BootP server responds to the request with the desired IP address.
4. The FL COMSERVER ... 232/422/485 can be accessed immediately via the assigned IP address.

3.2.4 Configuration via ARP command and Telnet

3.2.4.1 Assigning a temporary IP address

1. Switch to the DOS command prompt window. It can be found in the Windows Start menu via "Start... Programs... Accessories... Command Prompt".

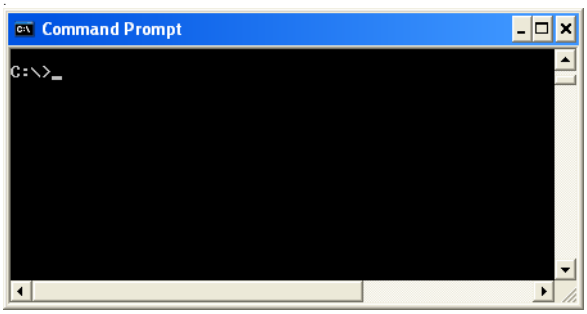


Figure 3-7 DOS command prompt window

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

E.g., arp -s 192.168.0.17 00-A0-45-21-BE-61

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

Please note that dashes are used when entering the MAC address in the ARP command.

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

E.g., telnet 192.168.0.17 1

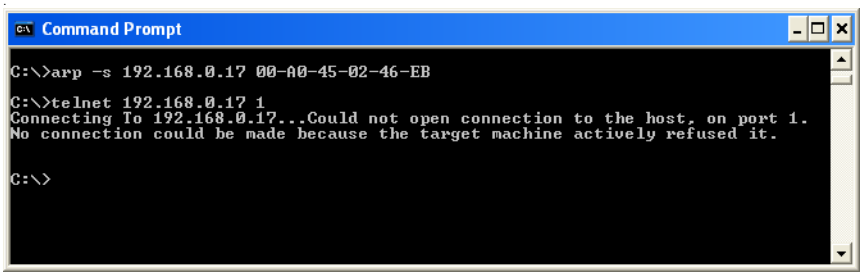


Figure 3-8 DOS command prompt window

A message indicates that the connection cannot be established.

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

3.2.4.2 Calling the 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.

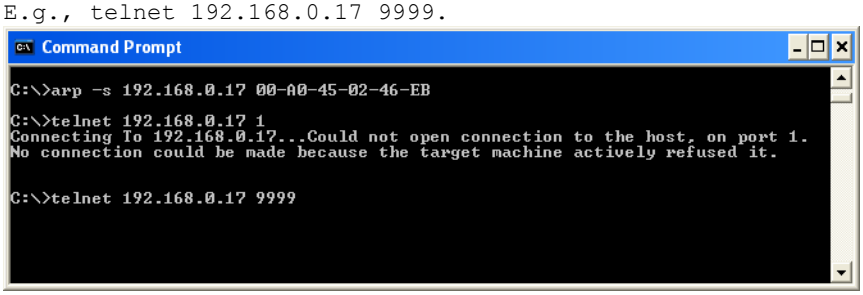


Figure 3-9 ARP command and Telnet configuration

2. Enter the system password in the following password request (default = private).

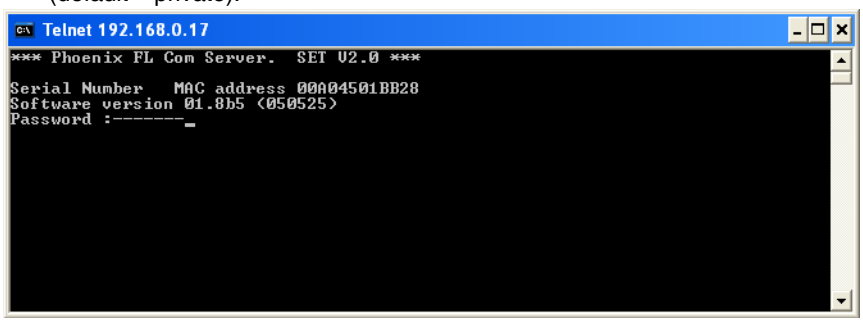


Figure 3-10 Password entry

3. Press ENTER twice to confirm the entry.

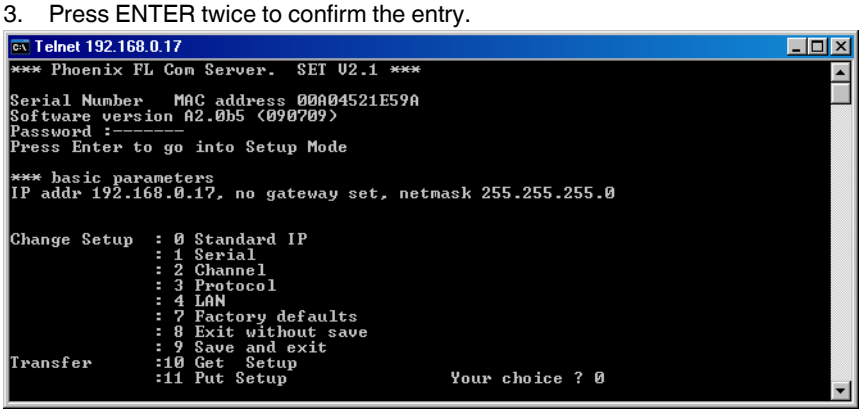


Figure 3-11 Telnet configuration menu

A new IP address can now be configured or the device can be reset to the default settings (all passwords and application settings are reset) using "Change Setup". Please also refer to "Default upon delivery/default 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
```

Figure 3-12 Default upon delivery/default settings

1. Change the IP address
2. Select the gateway settings
3. Set the subnet mask

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

	Network bits	Computer 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 additional examples, please refer to "Subnet masks" on page A-4.

Setup 1 – Serial settings

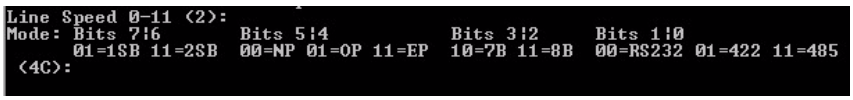


Figure 3-13 Serial settings

1. Select your serial transmission speed

Serial speed (bps)	Setup No.	
300	7	
600	6	
1200	5	
2400	4	
4800	3	
7000	11	
9600	**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
V.24 (RS-232)							0	0
RS-422							0	1
RS-485, 2-wire							1	1
7 bits					1	0		
8 bits					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 interface mode settings

Interface	Bits	Parity	Stop bits	Binary	Hex	
V.24 (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. Set the actual port used by the application for communication
2. Set the IP address of the partner
3. Set the port number of the partner

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 3-15 Mode settings

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

Setup 7 – Factory defaults

This option can be used to reset the device configuration (all passwords and application settings) to the default settings.

The IP address cannot be reset here.

Setup 8 – Exit without save

This option can be used to exit the Telnet session without saving the modified parameters.

Setup 9 – Save and exit

This option can be used to save all modified parameters and exit the Telnet menu.

Setup 10 and 11 – Get/Put Setup

These options can be used to upload and download external device configurations.

Specific instructions for these options are available on request.

3.3 Sending a ping

The PING command can be used to check whether it is possible to connect to the desired device.

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

   ```
   PING 192.168.0.162
   ```
3. The device responds with three standard confirmations:

   ```
   Reply from 192.168.0.162: bytes=32 time=10ms TTL=32
   ```
4. If there is no confirmation, the system indicates a timeout:

   ```
   Request timed out
   ```

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

-t	Repeats the ping command until the user aborts via <CTRL> C.
-n "count"	Repeats the ping command as many times as is specified in "count".
-l "size"	The packet is filled with the number of bytes specified in "size".
-w "timeout"	The "timeout" time (in milliseconds) to wait for a confirmation.

3.4 Web-based management (WBM)

3.4.1 General function

Online diagnostics

The user-friendly web-based management interface can be used to manage the FL COMSERVER ... 232/422/485 from anywhere in the network using a standard browser. Comprehensive configuration and diagnostic functions are clearly displayed on a graphic user interface. Every user with a unique password for a network connection to the device has read access to that device via a browser. Depending on 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 state can be viewed.

Access can only be obtained by entering the valid password. By default upon delivery, the password for write access is "**private**".

For security reasons, we recommend you enter a new, unique password.

3.4.2 Requirements for the use of WBM

As the web server operates using the Hyper Text Transfer Protocol (HTTP), a standard browser can be used. Access is via the URL "http://<IP address of the device>". Example: "http://192.168.0.112".
For full operation of the web pages, the browser must support Cascading Style Sheets Level 1. We recommend the use of Microsoft Internet Explorer 5.5 or later.

WBM can only be called using a valid IP address. By default upon delivery, the IP address of the FL COMSERVER ... 232/422/485 is 192.168.0.254.
Please also refer to "Configuring the IP address" on page 3-2.

3.4.2.1 Structure of the web pages

The web pages are divided into four areas:

– Device type and device logo
– Device name (specified by the user) and loading time, to prevent mix-ups
– Site map on the left-hand side
– Information tables, which contain current device information during runtime

3.4.2.2 Procedure for making changes to the configuration

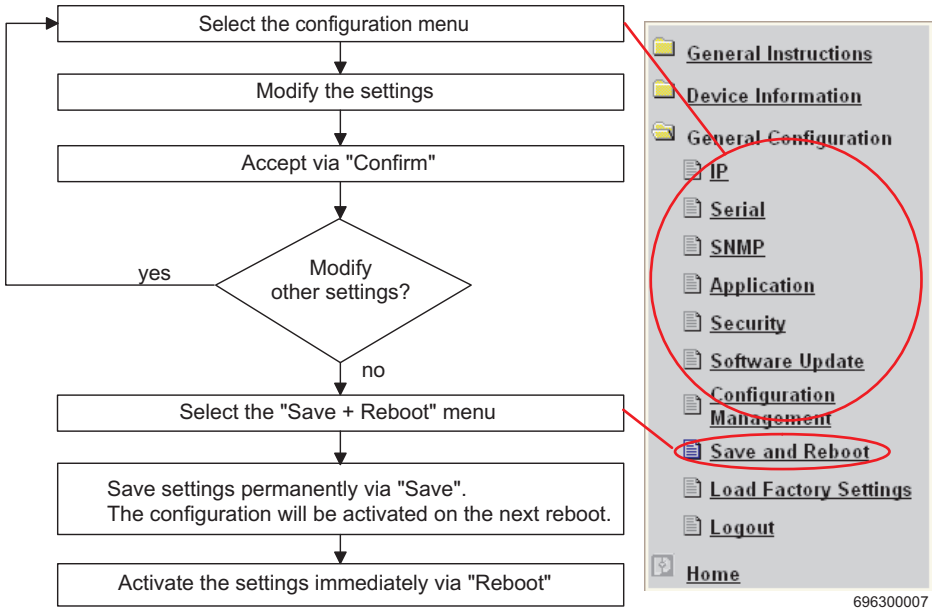


Figure 3-16 Procedure for making changes to the configuration using WBM

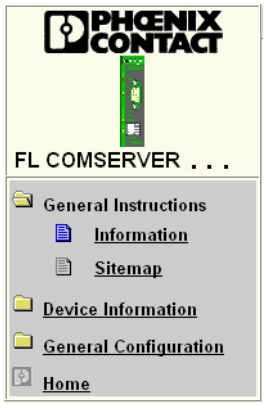
The modified settings must first be confirmed via "Confirm" and then permanently saved via "Save current configuration for next reboot" on the "Save and Reboot" web page.

3.4.3 Functions and information in WBM

The site map provides direct access to the following three areas:

– **General Instructions**
  Basic information about 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
Contains a brief description of WBM.

"Sitemap" menu
Contains a complete site map, which is linked to every page of WBM.

3.4.3.2 Device Information

"General" menu
Contains information about the device and the manufacturer (e.g., address, designation, serial number and version number, etc.).

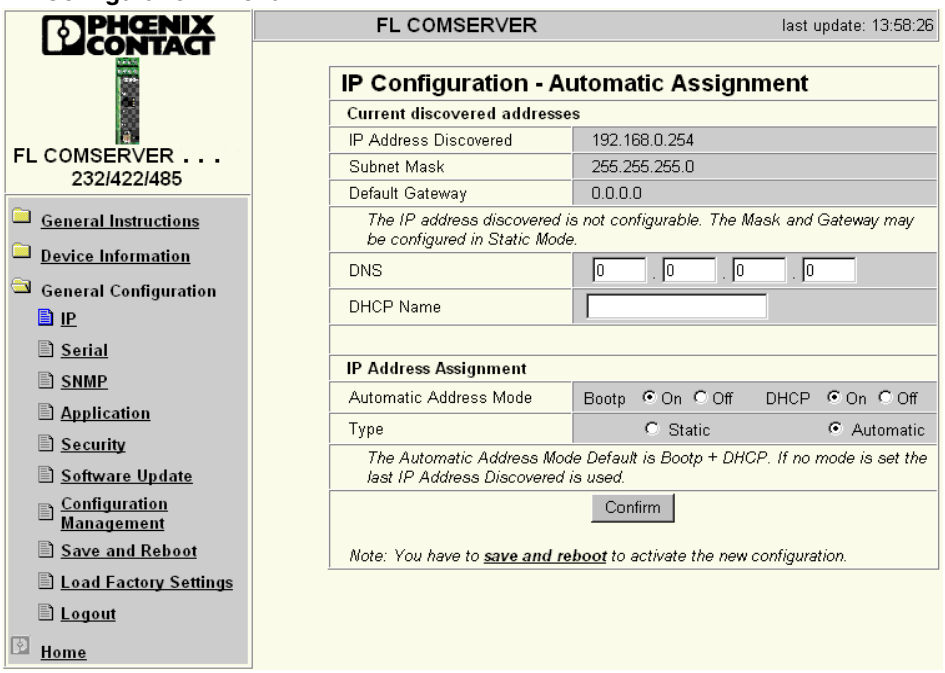
"Technical Data" menu
This page lists the main technical data.

"Hardware Installation" menu
This page contains a diagram for connecting the redundant power supply and a connection scheme for the V.24 (RS-232)/RS-485 interface.

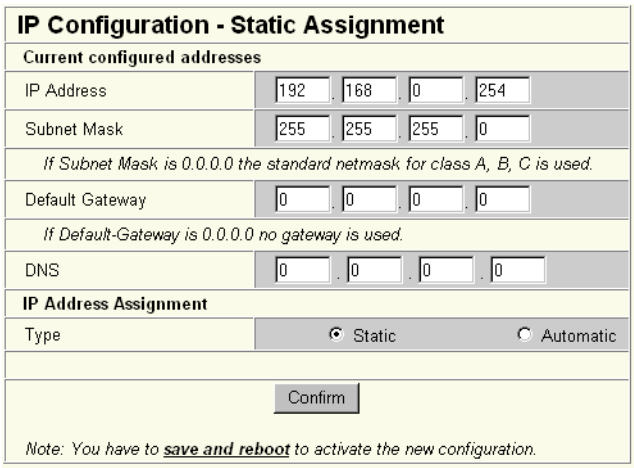
"Local Diagnostics" menu
This page describes the integrated diagnostic LEDs and the current status of the indicators.

3.4.4 Modifying the IP settings

"IP Configuration" menu

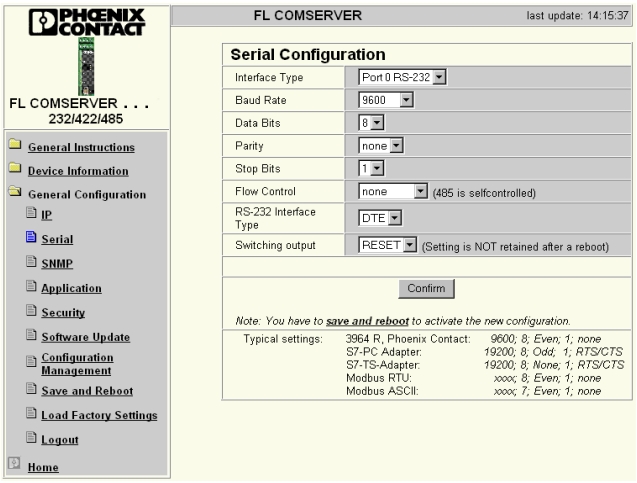


The current IP parameters and the addressing mechanism are displayed in this menu. To change the IP parameters via WBM, "Static" assignment must be selected.



3.4.5 Configuring the serial interface

3.4.5.1 V.24 (RS-232) device



In this menu, specify the settings for the serial interface of the FL COMSERVER ... 232/422/485 according to the application requirements.

Interface Type	Select the serial interface that is to be used for communication. The following settings are possible: - RS-232 - RS-422 - RS-485
RS-232 Interface Type	Switch between DTE and DCE. By default upon delivery, the FL COMSERVER ... 232/422/485 is set to DTE.

3.4.5.2 Switching output

The FL COMSERVER ... 232/422/485 has a transistor switching output for connecting accessories, e.g., the PSI-MODEM-SPLITTER (Order No. 2708766), (see "Point-to-point/ PSI-MODEM-SPLITTER" on page 4-1).

The transistor switching output is on the backplane and should be used in a connection station with T-BUS connectors (see Section 2.4.2).

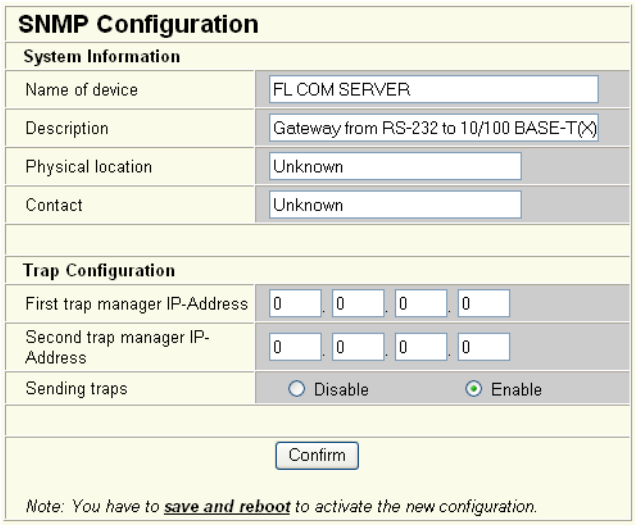
To switch the output, set the "Switching output" setting to SET.
To reset the output, select the "Reset" setting.
The output is also reset after a voltage failure or a device reboot.

3.4.6 Configuring SNMP traps

"SNMP Configuration" menu

System Information This part of the table is used to display or modify user-specific device data, e.g., location, device name or function.

Trap Configuration This part of the table is used to view or modify the IP addresses of the two trap receivers. It is also used to activate or deactivate the "send traps" function.



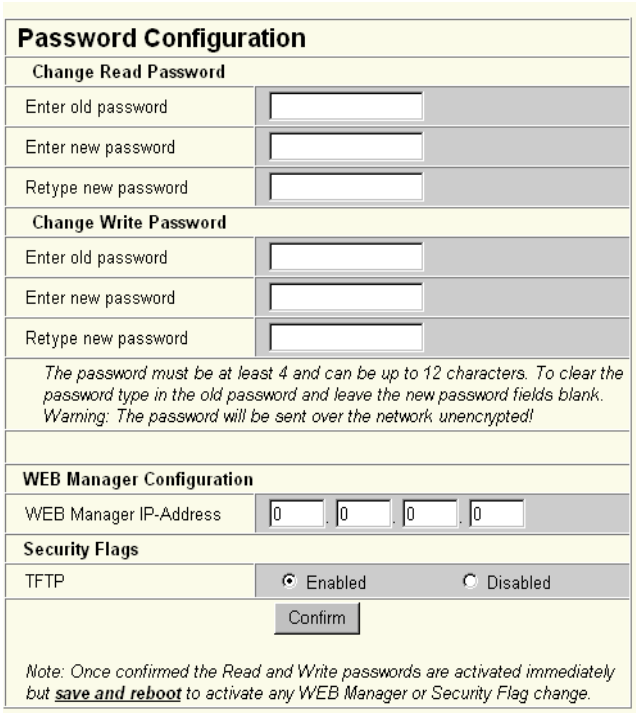
3.4.7 Application Settings

"Application Settings" menu

In this menu, the settings for the desired application can be specified. These include, for example, the protocol used, port number, destination IP, etc. This menu is described separately in "Applications" on page 4-1.

3.4.8 Changing the password

"Password Configuration" menu



Enter the current password and then specify a new, unique password. By default upon delivery, the password is "private" for write access (please note that it is case-sensitive). By default upon delivery, no password is set for read access.

The password must be between four and twelve characters long. Please note that the password is always transmitted via the network in unencrypted format.

Forgotten your password?
Emergency access is available via the serial interface. In this way, you can reset the device to its default settings using HyperTerminal, for example (see Section 3.2.4.2).

WEB Manager IP-Address

The IP address of a PC in the network can be entered here.
Only this PC (IP address) can then be used to access the FL COMSERVER ... 232/422/485.

Security Flags – TFTP

The transfer of configuration files via a TFTP server can be enabled or disabled here (see Section 6.2.2 and Section 6.2.3).

3.4.9 Updating the software and firmware

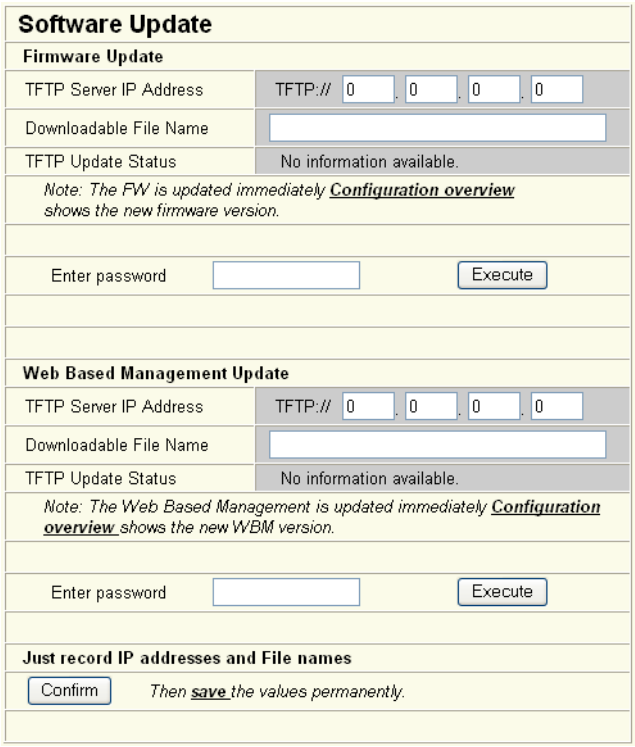
"Software Update" menu

Firmware Update

This option can be used to view or modify the parameters for a firmware update and initiate the update.

Web Based Management Update

This option can be used to view or modify the parameters for a WBM update and initiate the update.



Following a firmware or WBM update, a reset is required to activate the new version.

Just record IP addresses and file names

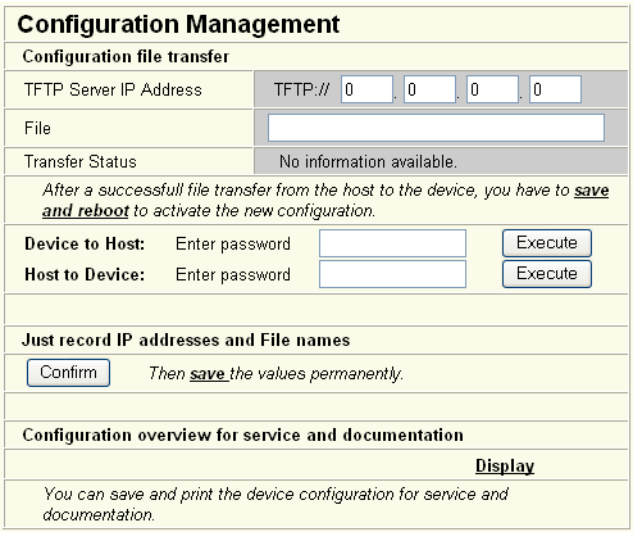
This item can be used to permanently enter the IP address of the TFTP server and the stored file name of the firmware file.

3.4.10 Saving and loading the device configuration

"Configuration Management" menu

Configuration file transfer

This option can be used to save the active configuration of the FL COMSERVER ... 232/422/485 in a back-up file (direction: device to host). Conversely, a back-up file can be restored in the FL COMSERVER ... 232/422/485 (direction: host to device). This function can be used in particular for series production.



When a configuration is uploaded from the FL COMSERVER ... 232/422/485 to a PC, the last saved version is transmitted. If you want to transmit the active configuration, first save it again ("Save and Reboot" menu).

When a configuration is downloaded from the PC to an FL COMSERVER ... 232/422/485, the new configuration is only activated once the FL COMSERVER ... 232/422/485 has been reset.

Configuration using a configuration file is used when replacing devices. To duplicate devices using a configuration file, observe the following:

– Establish a connection from the FL COMSERVER ... 232/422/485 to an FTP server or local connection via the V.24 (RS-232) interface of the FL COMSERVER ... 232/422/485.
– Load the configuration file on the FL COMSERVER ... 232/422/485.
– Reset the FL COMSERVER ... 232/422/485.
– Adjust the IP parameters.
– Save the configuration ("Save current configuration" function).

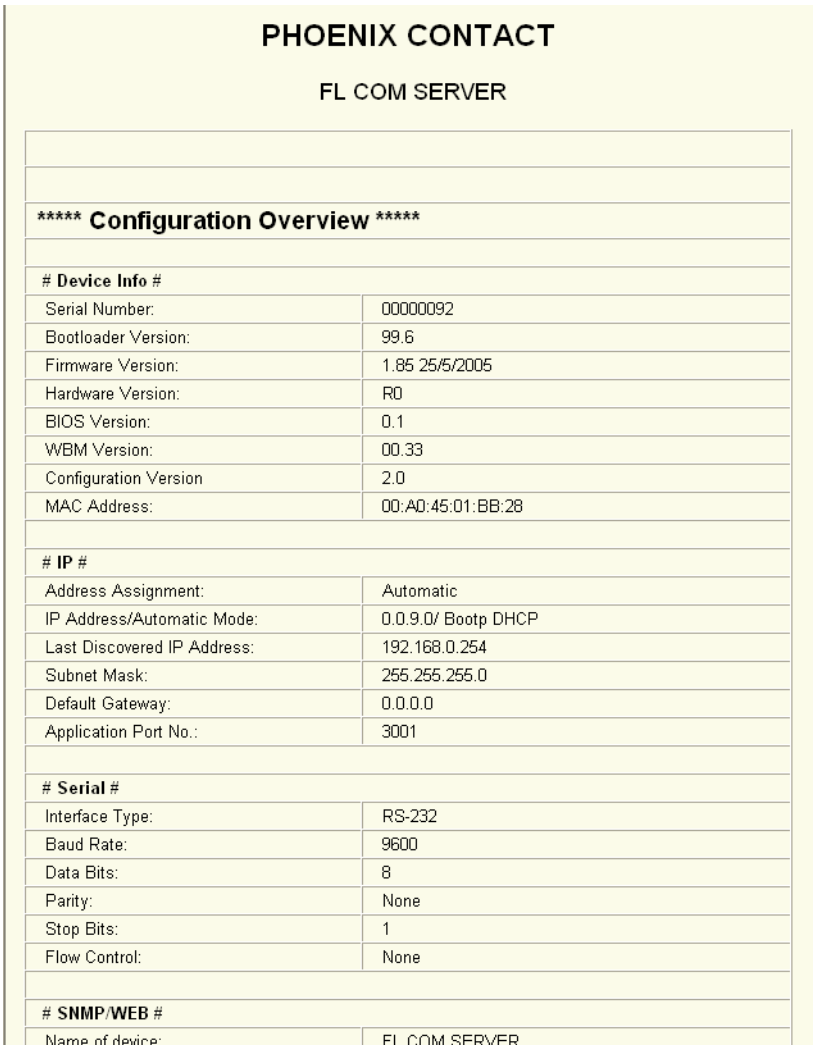
The duplicated FL COMSERVER ... 232/422/485 can now be operated in the network using the adjusted IP parameters.

Just record IP addresses and file names

This item can be used to permanently enter the IP address of the TFTP server and the file name of the stored configuration file.

Configuration overview...

A new window opens in the browser for this item. Here, the current values of all variable settings are displayed clearly in an HTML file. This configuration overview can be easily printed for the system documentation. Alternatively, you can save this information as an HTML or TXT file onto a data carrier via the "Save As" menu in the browser.



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 used exclusively to display the settings in plain text. Automatic configuration of the device via file download is only possible using "Configuration file transfer" on page 3-23.

For additional information about the "Configuration Management" menu, please refer to Section 6.2.

3.4.11 Applying the changes to the configuration and restarting the device

"Save and Reboot" menu

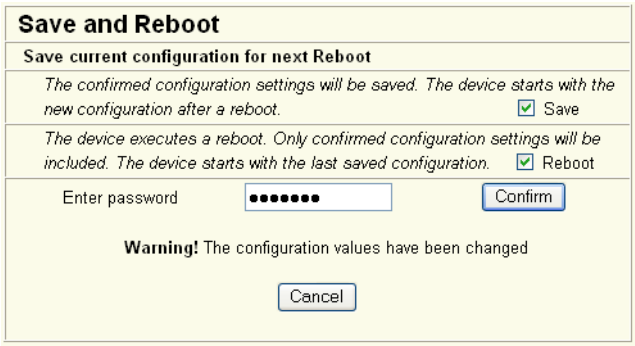


Figure 3-17 "Save and Reboot" menu with present changes

Save current configuration for next reboot

This option enables you to permanently save the active configuration and/or restart the device once the valid password has been entered.

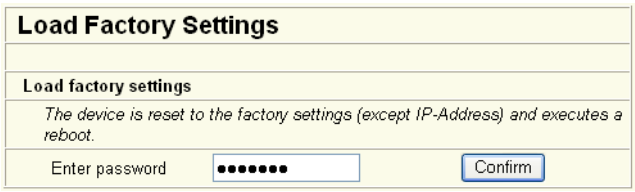
As soon as the changes to the configuration have been confirmed, the "Save" checkbox is activated and a warning is displayed (see Figure 3-17).

The new configuration is not activated until the device is next rebooted. Activate the "Reboot" checkbox.

Changes to the configuration, which have only been confirmed and which have not yet been permanently saved, can be rejected by deactivating the "Save" checkbox and activating the "Reboot" checkbox.

3.4.12 Resetting to the default settings

"Load Factory Settings" menu



Load factory settings

This option can be used to reset the configuration of the FL COMSERVER ... 232/422/485 to the default settings by entering a valid password.

This excludes the IP settings, which means that the FL COMSERVER ... 232/422/485 can still be configured via WBM.

3.4.13 Exiting the configuration session

"Logging out" menu

Logging out

This option can be used to exit the configuration session completely and immediately. If you wish to continue with the configuration, you will be prompted to enter the password again. It is not possible to go back via the browser "Back" button.

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

4 Applications

4.1 Overview and selection

Thanks to a wide range of integrated functions, the device can be used in various ways for different applications. Web-based management provides user-friendly support during configuration. The following applications are supported by the FL COMSERVER ... 232/422/485.

Point-to-point/tunnel
(see "Cable replacement with peer-to-peer connection" on page 4-9)

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 using two FL COMSERVER ... 232/422/485 devices, which removes any range restrictions, such as a maximum of 15 m for V.24 (RS-232).

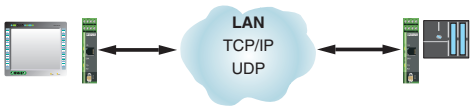


Figure 4-1 Point-to-point connection/tunnel

Point-to-point/PSI-MODEM-SPLITTER

In another application, the PSI-MODEM-SPLITTER add-on device (Order No. 2708766) enables interface conversion between two V.24 (RS-232) channels or ports.

The point-to-point connection is switched via either the WBM of the FL COMSERVER ... 232/422/485 or the switch on the front of the splitter (see Section 3.4.5.2).

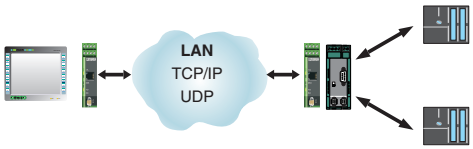


Figure 4-2 Point-to-point connection (two control systems)

Client/server mode
(see ""Application Settings" menu" on page 4-5)

If, however, the serial data of an application software program is to be available in the network, only one FL COMSERVER ... 232/422/485 is installed at the serial device. In its function as a client or server, the FL COMSERVER ... 232/422/485 can then make the data available and transmit it in TCP/IP or UDP. The sockets of the application software can thus directly access the serial data in the field.

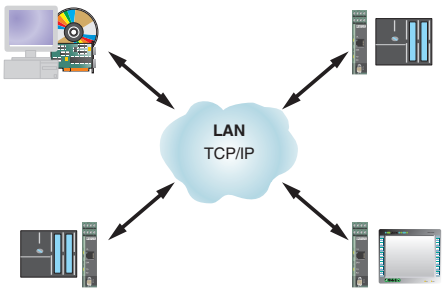


Figure 4-3 Client/server mode

Redirector/virtual COM ports
(see "COM port redirector" on page 4-11)

In many cases, the existing application software does not support Ethernet communication. However, in the face of increasing networking, local connections, e.g., to programming interfaces, often have to be established via the existing network card of the PC and the connected network. Help comes in the form of the COM port redirector software, which is supplied as standard. It creates virtual COM ports on the PC that can be used by the existing application software. No changes have to be made to the application software so it is easy to establish a connection to the programming interfaces with all the advantages of networking.

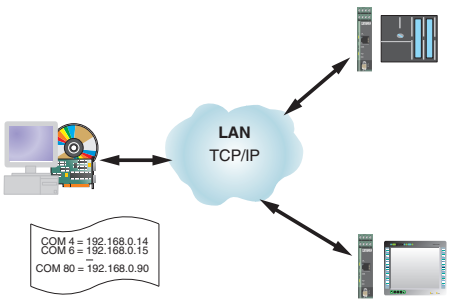


Figure 4-4 Redirector/virtual COM ports

Modbus gateway/multi-drop networks
(see "Modbus gateway" on page 4-26)

Even conventional RS-485 multi-drop networks can be extended or replaced by modern network technology with the FL COMSERVER UNI 232/422/485. Modbus is the most well-known version 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 complete gateway function enables use with Modbus masters and slaves, and therefore the integration of any number of serial Modbus devices into Modbus TCP networks.

Other multi-drop networks can be addressed directly using simple broadcast addressing sent out to all network devices or using intelligent mechanisms. The required destination address is read directly from the serial data stream and used for addressing.

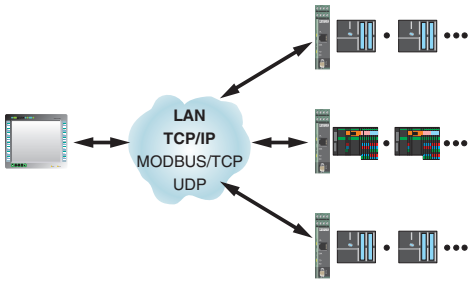


Figure 4-5 Modbus gateway and other multi-drop networks

Remote access in remote networks
(see "PPP applications" on page 4-30)

Dialing into remote networks that are otherwise difficult to access (e.g., wind parks) can now be easily ensured 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 Handshake Authentication Protocol). Unauthorized access to the network is prevented by 128-bit password encryption. This means that remote maintenance and diagnostics for remote network devices is as simple as dialing into the Internet at home.

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

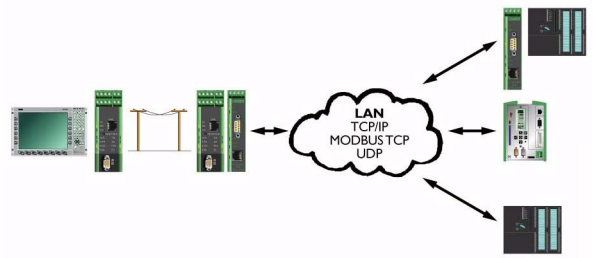


Figure 4-6 Dialing into remote networks using a RAS server

4.2 General method of operation

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

Table 4-1 Differences between Ethernet protocols

Feature	UDP	TCP
Unique connection	No	Yes
Connection controlled by specifically opening and closing the connection	No	Yes
Correct packet order ensured	No	Yes
Timeout possible	No	Yes
Acknowledgment of data transmission	No	Yes
Data transmission ensured by checksum	Yes	Yes

In UDP mode, pending data is transmitted immediately. However, the communication partner does not send a confirmation to indicate that it was transmitted correctly. Damaged or lost packets must either be requested again by the connected application software or the application must permit such transmission errors, e.g., for temperature values.

In TCP/IP and Modbus TCP mode, there is a permanent connection between two devices. The communication partner confirms whether data is being transmitted correctly. The device that initiates the connection is referred to as the client. The device that accepts the connection is referred to as the server.

UDP: For constantly changing communication partners or when data integrity is ensured by the connected application software.
TCP: For large amounts of data, continuous data traffic, and a high level of data integrity.

Data is transmitted in several individual steps:

– The FL COMSERVER ... 232/422/485 unpacks the serial data from the serial packet and repacks it in a TCP/IP packet.
– The FL COMSERVER ... 232/422/485 sends the data via the LAN.
– The data is transmitted by 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 repacks it in serial data packets.
– The FL COMSERVER ... 232/422/485 transmits the data to the serial device.

This method of operation results in delays, which can also considerably reduce the available network capacity.

4.3 "Application Settings" menu

The structure of the "Application Settings" menu changes dynamically according to the settings made. The menu items that are relevant for the application are displayed.

The "Operation Mode" and "Multi device setting" menu items are dynamically adapted following confirmation via "Confirm". There are three possible menu structures.

Following the selection of "Operation Mode" and "Multi device setting", confirm the settings via "Confirm" to update the menu structure.

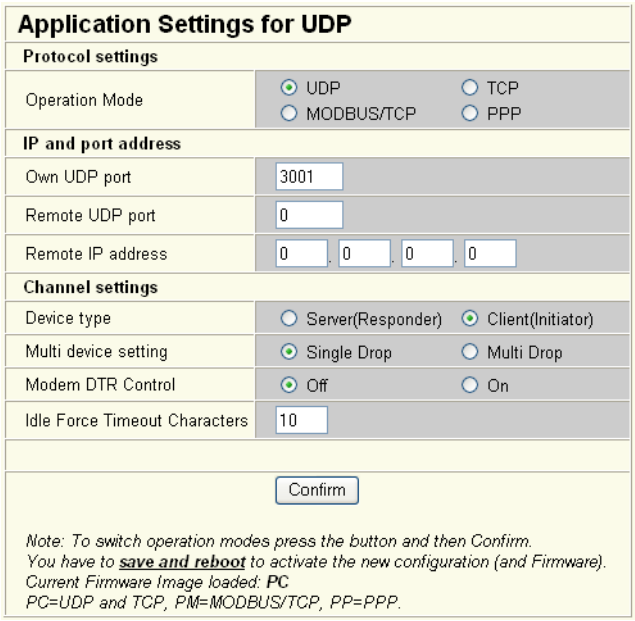


Figure 4-7 "Application Settings" menu for UDP, single drop mode

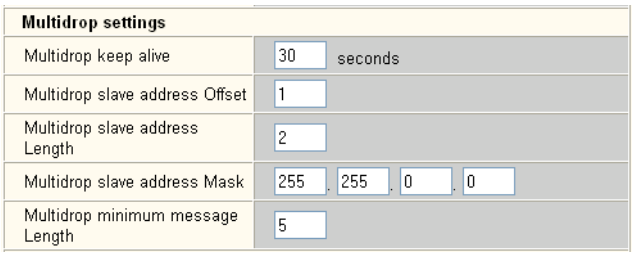


Figure 4-8 Menu extensions for multi-drop mode

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 communication
Multi device setting	Single Drop	Point-to-point connection
	Multi Drop	Multi-point connection
Modem DTR Control	Off	The DTR control signal is ignored
	On	The DTR control signal is taken into consideration/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 because a data packet is transmitted for a low number of characters.

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

Menu heading	Menu selection	Explanation
Options for multi-drop mode		
Multidrop settings		
Multidrop keep alive	30 seconds	Time interval in seconds, in which the FL COMSERVER ... 232/422/485 responds with a sign of life at the bus slaves 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 (4 bytes, maximum)
Multidrop slave address Mask	255.255.0.0	Mask which can be used to mask out individual bits 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. Short telegrams (e.g., acknowledge) are treated specially and forwarded directly to the last sender address.
Options for TCP mode		
Remote Domain name		Instead of the static IP address, the name of a network device can be entered here.
Modem Mode	Off	Modem mode is deactivated
	On without echo	TCP connection establishment is controlled by AT commands.
	On with echo	TCP connection establishment is controlled by AT commands. The sent AT commands are sent back to the sender as an echo to be evaluated.
Disconnect with inactivity timeout	0 minutes 0 seconds	The TCP connection is closed if no data is transmitted in the set time (IDLE). 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.

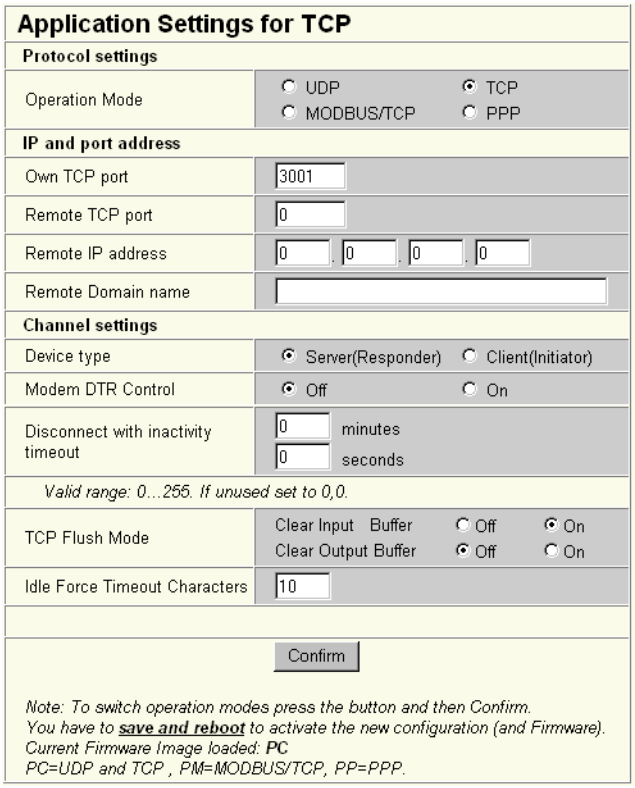


Figure 4-9 "Application Settings" menu for TCP mode

4.4 Cable replacement with peer-to-peer connection

A peer-to-peer connection (tunneling) is an easy way to connect two V.24 (RS-232)-based termination devices in a point-to-point connection via an existing network. This connection also operates across subnetworks and gateways. Both FL COMSERVER ... 232/422/485 devices are logically linked with one another via the destination and source IP.

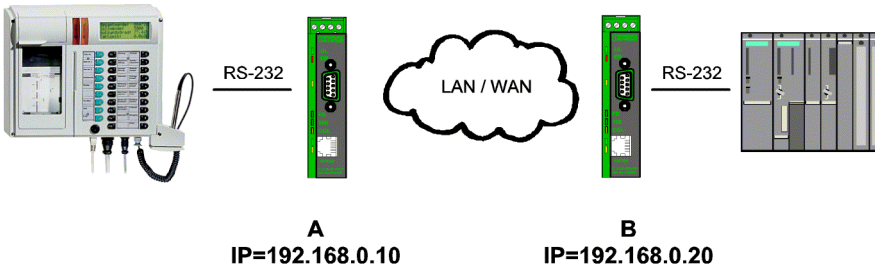


Figure 4-10 Application example for a peer-to-peer connection

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

The UDP protocol is connectionless. Data is transmitted as soon as it appears at the V.24 (RS-232) interface.

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

Connection establishment:

– Permanent network connection after power up
– If DTR is active
– If a character is received at the serial port

Connection release:

– If serial connection was "idle" (can be set from 0 to 255 minutes: 255 seconds)
– If the DTR signal is inactive

4.4.1 Settings in UDP 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 initiated equally from both sides as soon as a character 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 Characters	10	10	

4.4.2 Settings in TCP/IP and Modbus mode

Table 4-4 Application settings in TCP/IP 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 active communication
Modem DTR Control	Off	Off	Off = DTR signal is ignored On = DTR signal is evaluated. The client establishes or aborts the TCP connection.
Modem Mode	Off	Off	Deactivated, as it is a point-to-point connection
Disconnect with inactivity timeout	0:0	0:0	TCP connection is aborted after xx minutes and zz seconds with no data transmission. 0:0 if the TCP connection is never to be closed.
TCP Responder Flush Mode	Clear Input Buffer	Clear Input Buffer	V.24 (RS-232)/RS-485 data, which was written to the FL COMSERVER ... 232/422/485 before the TCP/IP connection was established, is deleted.
Idle Force Timeout Characters	10	10	

Exit the configuration settings each time with "Confirm".

The new configuration is not activated until the device is next rebooted. Activate and start the reboot process by entering the valid password in the "Save and Reboot" menu.

4.5 COM port redirector

4.5.1 Application

The redirector application is a special peer-to-peer connection.

Existing application software, which only communicates via serial COM interfaces, can be redirected to remote COM ports.

To do this, the COM port redirector creates virtual COM ports on the PC, which the software can use for communication. The virtual COM ports are physically redirected to the network card and a destination IP in the network. **One** FL COMSERVER ... 232/422/485 with a corresponding IP address is configured as the receiver in the network for each COM port.

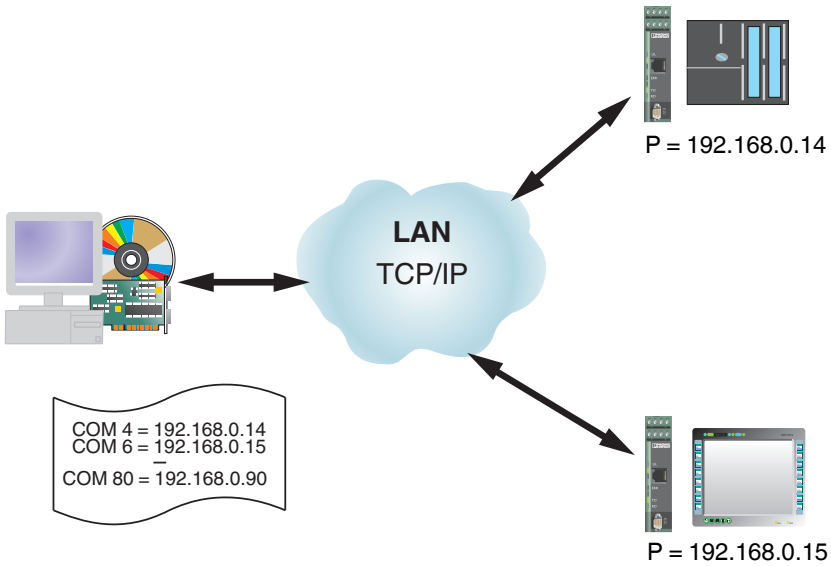


Figure 4-11 Application example for the COM port redirector

Communication only takes place with the TCP/IP protocol.

4.5.1.1 Marginal conditions

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

- The COM port redirector unpacks the serial data from the serial packet and repacks it in a TCP/IP packet.
- The COM port redirector then sends the data via the network card in the LAN.
- The data is transmitted by 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 repacks it in serial data packets.
- The FL COMSERVER ... 232/422/485 transmits the data to the serial device.

This method results in delays in communication, which can also considerably reduce the available Ethernet network capacity.

Some software applications respond to these system-dependent transmission delays with a timeout, as the software assumes that the opposite device is not responding.

Communication via the COM port redirector results in delays, which some software applications acknowledge with a timeout.

Activate the "No Net Close" option if timeout problems occur. This option maintains the TCP/IP connection if the COM port is closed by the software application. This means that a new TCP/IP connection does not have to be established, which would result in additional delays.

Other marginal conditions

– The COM port redirector is always the client and establishes the connection
– Communication only takes place via the TCP/IP protocol
– Up to 80 virtual COM ports can be set up

4.5.2 Configuring the FL COMSERVER ... 232/422/485

1. Assign an IP address to the FL COMSERVER ... 232/422/485.
2. In web-based management, specify the serial interface settings according to the requirements of the connected device under "General Configuration... Serial".

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

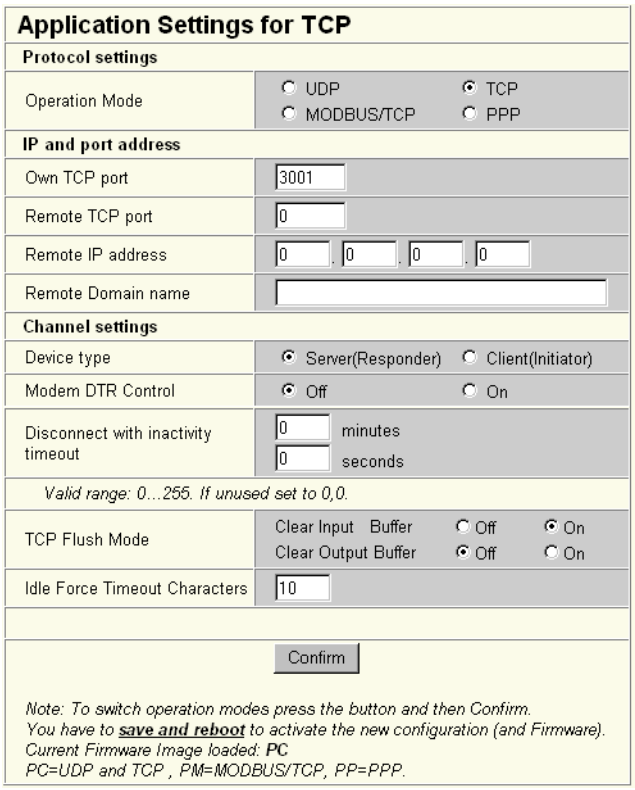


Figure 4-12 Application settings for redirector connection

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	Deactivated, as it is a point-to-point connection
Disconnect with inactivity timeout	0:0	TCP connection is aborted after xx minutes and zz seconds with no data transmission. 0:0 if the TCP connection is never to be closed.
TCP Responder Flush Mode	Clear Input Buffer	V.24 (RS-232)/RS-485 data, which was written to the FL COMSERVER ... 232/ 422/485 before the TCP/IP connection was established, is deleted.
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 because a data packet is transmitted for a low number of characters.

Exit the configuration settings each time with "Confirm".

The new configuration is not activated until the device is next rebooted. Activate and start the reboot process by entering the valid password in the "Save and Reboot" menu.

4.5.3 Installing the redirector software

The COM port redirector software is provided on the CD supplied with this manual.

1. Insert the CD in the CD-ROM drive. The CD starts automatically.
2. If the auto start mechanism is deactivated, switch to the CD-ROM drive in Explorer and double-click on the "start.html" file to start the CD.
3. Select the desired language.
4. Start the software installation by double-clicking on the "red32bit.exe" file.

An automatic installation routine will appear.

Figure 4-13 Welcome screen

5. Click "Next".

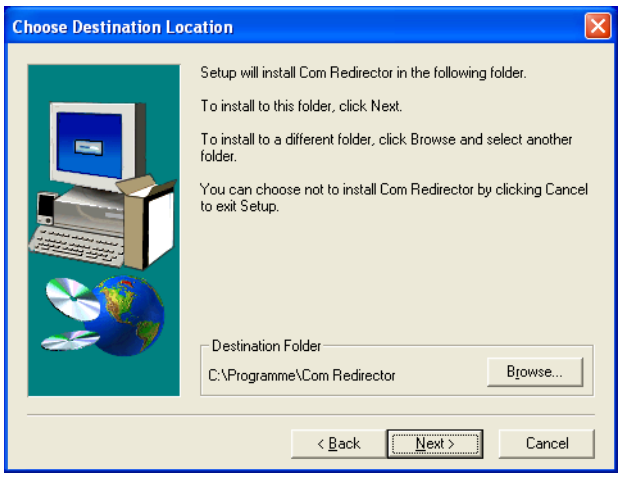


Figure 4-14 Selecting the installation path

6. If necessary, select a different installation path. Click "Next" to confirm the selection.

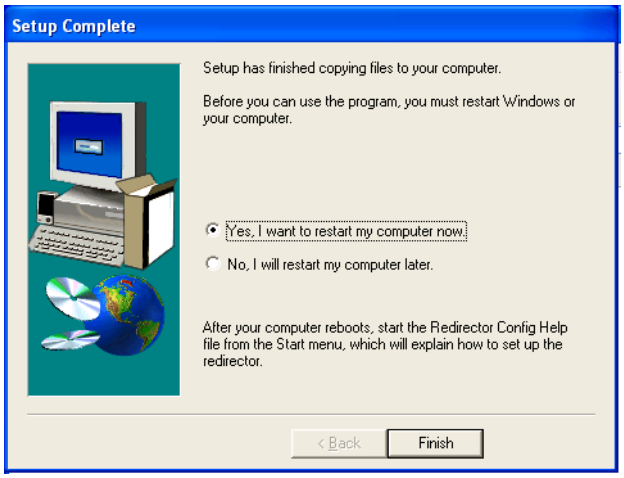


Figure 4-15 Completing the installation

7. Restart the computer.

The software has been installed successfully.

4.5.4 Selecting and configuring the virtual COM port

Once installed, the program can be started via "Start... Programs... Redirector... Configuration". The main menu window is opened.

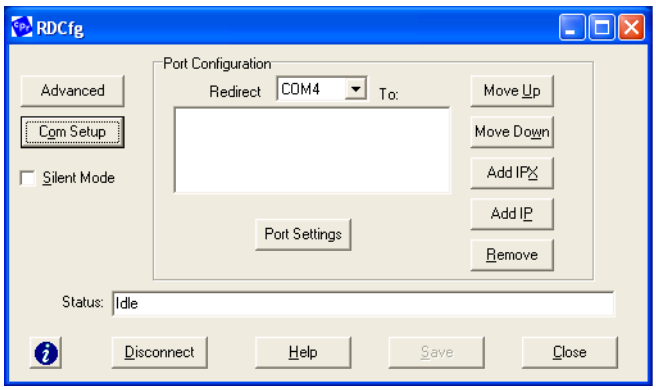


Figure 4-16 Redirector main menu

1. Activate the port numbers that are to be supported in the "Port Setup" menu.

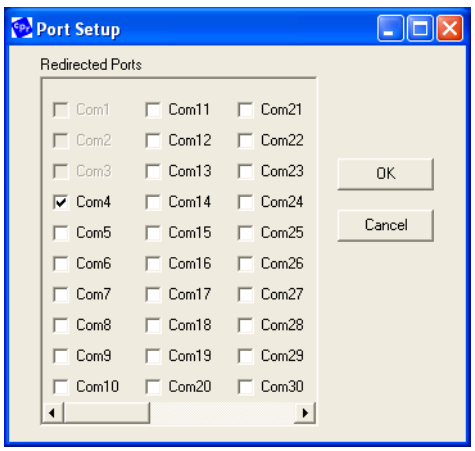


Figure 4-17 "Port Setup" menu

2. Confirm the selection with "OK" and return to the main menu.
3. Select a COM port that was previously activated in the drop-down menu.
4. Then click on "Add IP".

The "IP Service Setup" window is opened.

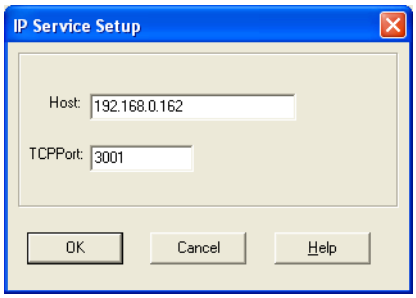


Figure 4-18 "IP Service Setup" menu

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

The "Port Settings" window is opened.

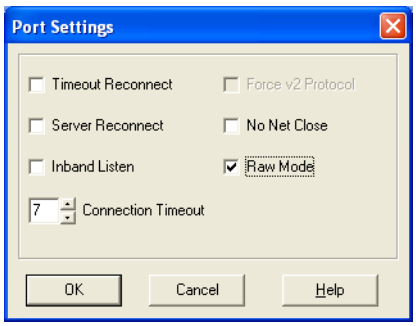


Figure 4-19 "Port Settings" menu

9. Activate the "Raw Mode" option.

Raw mode must **always** be activated for redirector applications.

10. Select other options for establishing and aborting a connection according to the application.

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 yet been established, the connection was interrupted by a timeout (TCP keep alive) or "Cancel" was pressed. The mechanism is terminated if the software application closes the COM port or if "Disconnect" is pressed.
Server Reconnect	With this option the COM port redirector re-establishes the TCP connection if the FL COMSERVER ... 232/422/485 interrupted the connection, the connection has not yet been established or "Cancel" was pressed. The mechanism is terminated if the software application closes the COM port or if "Disconnect" is pressed.
Inband Listen	Not used. The FL COMSERVER ... 232/422/485 does not support "Inband Listen" mode.
Connection Timeout	Specifies the maximum time in seconds until the COM port redirector aborts connection establishment. If "Timeout Reconnect" is also activated, each connection establishment lasts the set time. Without the "Timeout Reconnect" option, connection establishment is aborted after the set time has elapsed.
Force v2 Protocol	Not used. The FL COMSERVER ... 232/422/485 does not support V2 protocols.
No Net Close	With this option, the TCP/IP connection is not disconnected if the COM port is closed by the software application. This enables faster communication, as there is no time delay to establish an Ethernet connection.
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) by default. This parameter is not usually changed.

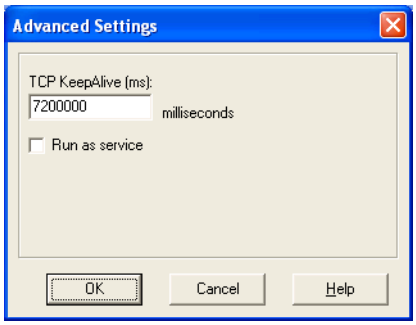


Figure 4-20 "Advanced Settings" menu

All the parameters for the selected COM port are set.

If necessary, repeat the settings for other COM ports.

NOTE: Possible malfunction of the device, device environment, hardware or software.

Restart the PC to ensure that the virtual COM ports are available in the operating system.

4.5.5 Checking the connection

Once all settings have been made, you can check the connection. The easiest way to do this is with Windows HyperTerminal.

1. Open the program in the Windows Start menu via "Programs... Accessories... Communications... HyperTerminal".
2. Configure a connection using the new virtual COM port.
3. Confirm with "OK".
4. HyperTerminal opens the COM port and a pop-up window is displayed.

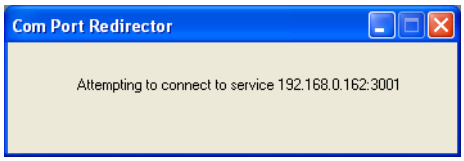


Figure 4-21 COM port redirector connection establishment

5. The successfully established or failed connection is displayed in the pop-up window.

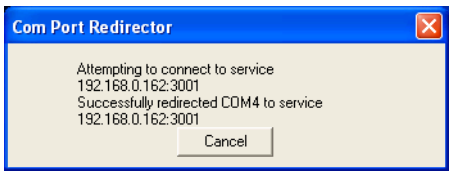


Figure 4-22 Successfully established connection

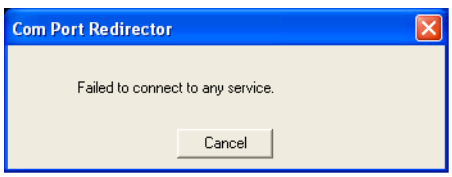


Figure 4-23 Failed connection

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

4.6 Modem mode

In modem mode, the FL COMSERVER ... 232/422/485 behaves like a dial-up modem. This means connection establishment and release is controlled via AT commands. Costly modem connections can thus be easily replaced by a cost-effective network connection.

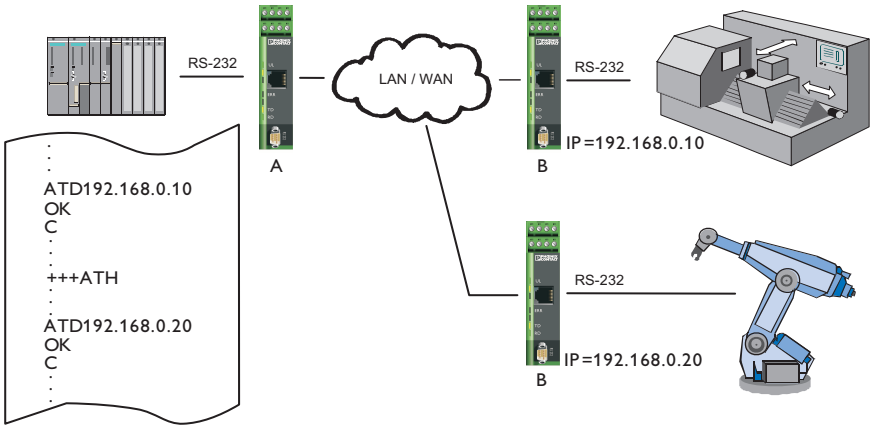


Figure 4-24 Modem mode

Communication can only take place with the TCP/IP protocol.

Connection establishment:

– Dial up with an AT command, followed by the IP address and port number.

Connection release:

– AT command +++ATH
– DTR control signal
– Close the TCP connection using the communication partner

4.6.1 Settings in modem mode

Table 4-7 Application settings in modem 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 active communication
Modem DTR Control	On	Off	Off = DTR signal is ignored On = DTR signal is evaluated. The client establishes or aborts the TCP connection.
Modem Mode	On	Off	In "On with echo" mode, the FL COMSERVER ... 232/422/485 sends the AT commands back to the sender.
Disconnect with inactivity timeout	0:0	0:0	TCP connection is aborted after xx minutes and zz seconds with no data transmission. 0:0 if the TCP connection is never to be closed.
TCP Responder Flush Mode	Clear Input Buffer	Clear Input Buffer	V.24 (RS-232)/RS-485 data, which was written to the FL COMSERVER ... 232/422/485 before the TCP/IP connection was established, is 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 because a data packet is transmitted for a low number of characters.

Exit the configuration settings each time with "Confirm".

The new configuration is not activated until the device is next rebooted. Activate and start the reboot process by entering the valid password in the "Save and Reboot" menu.

The FL COMSERVER ... 232/422/485 only accepts upper case letters when entering the AT command.

Table 4-8 AT command set

AT command	Function
AT	Attention string, which starts every modem command
ATS?	The set values of the remote IP and remote port number from the FL COMSERVER ... 232/422/485 are displayed
Either: 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 establishment to <IP address> and <Port number>
Either: ATD<IP address> ATDT<IP address>	Connection establishment to <IP address>. The remote port number set in the FL COMSERVER ... 232/422/485 is used as the communication port.
Either: ATD ATDT	Connection establishment to the communication partner, which is permanently set as the remote IP and remote port number in the FL COMSERVER ... 232/422/485.
C	Connected. The TCP connection to the communication partner has been established. The FL COMSERVER ... 232/422/485 has switched from "Command mode" status to "Data mode" status.
D	Disconnect. The TCP connection was interrupted or could not be established. The FL COMSERVER ... 232/422/485 has switched from "Data mode" status to "Command mode" status.
E	Error. An error has occurred.
OK	The FL COMSERVER ... 232/422/485 executed a modem command.
+++	Abort sequence for switching from data mode to command mode
ATH	Terminates the connection and switches back to command mode

All other AT commands do not have a function and are acknowledged in command mode by the FL COMSERVER ... 232/422/485 with **Not Accepted**, followed by details of possible AT commands.

4.6.2 Switching from data mode to command mode

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

– Data traffic must be idle for at least 1 second before the **+++** abort sequence can be sent.
– The period of time between the input of the individual plus characters must not be greater than 1 second.
– Another 1-second pause must follow the **+++** abort sequence.
– When the FL COMSERVER ... 232/422/485 has switched to command mode, it responds with **OK**.
– Enter **ATH** and press **ENTER**. When "On with echo" modem mode is activated, another **OK** signal is received.

4.7 Modbus gateway

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

Master/slave mode is based on RS-485 networking. This means that a bus master sends an addressed call and receives the response from the addressed slave. The RS-485 network can be easily replaced by an existing Ethernet network using the FL COMSERVER UNI 232/422/485.

This operating mode enables serial Modbus devices to be easily integrated into a Modbus TCP network. This means that even entire bus systems can be operated at the FL COMSERVER UNI 232/422/485. The FL COMSERVER UNI 232/422/485 supports both Modbus RTU and Modbus ASCII. However, the entire system can only ever be operated in one operating mode (RTU or ASCII). Of course, the Modbus TCP master can also control the network directly, i.e., without the FL COMSERVER UNI 232/422/485.

The configuration differs depending on whether the FL COMSERVER UNI 232/422/485 is connected to the bus master or one of the bus slaves. Two mechanisms are available for configuring the bus master:

– The FL COMSERVER UNI 232/422/485 at the Modbus master receives a list indicating which slave addresses can be addressed by the IP addresses. This means that an entire bus system can be connected to the FL COMSERVER UNI 232/422/485.
– The FL COMSERVER UNI 232/422/485 at the Modbus master extracts the called slave address from the serial data stream and thus completes the last byte of the destination IP address. Only individual Modbus devices can be connected to an FL COMSERVER UNI 232/422/485 in this operating mode.

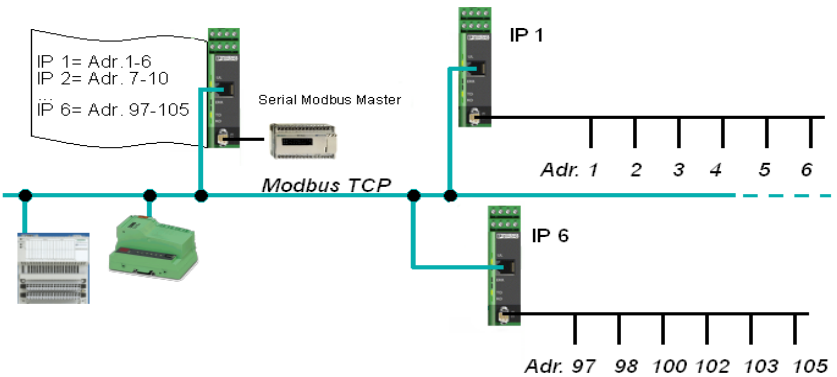


Figure 4-25 Modbus application

4.7.1 Master configuration

A PC with a network card and soft PLC can be used as a Modbus TCP master or a serial master can be converted into a Modbus TCP master using an FL COMSERVER UNI 232/422/485 (see Figure 4-26).

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

1. First switch to the "General Configuration... Application" menu in WBM.
2. Activate "MODBUS/TCP" mode.
3. Confirm the selection via "Confirm" at the bottom of the menu. The menu is adapted dynamically.
4. Activate "Channel settings... Device type... Master".
5. Enter the IP addresses of the FL COMSERVER UNI 232/422/485 to which the bus slaves are connected under "Master Address Lookup Table".
6. After the colon, enter the address area of the Modbus slaves, which can be accessed via this IP address.

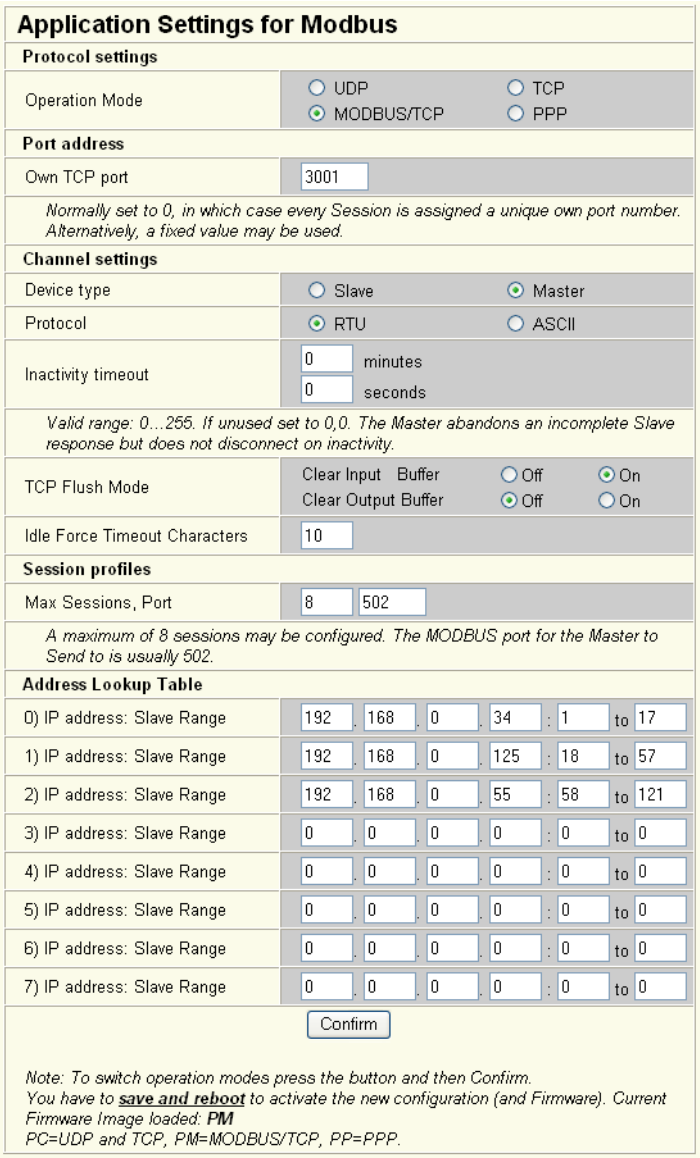


Figure 4-26 Settings at the Modbus master with a slave list

4.7.2 Slave configuration

The settings for the FL COMSERVER UNI 232/422/485 at the bus slaves is identical for both versions and must be made as follows (see Figure 4-27):

1. First switch to the "General Configuration... Application" menu in WBM.
2. Activate "MODBUS/TCP" mode.
3. Confirm the selection via "Confirm" at the bottom of the menu. The menu is adapted dynamically.
4. Activate "Channel settings... Device type... Slave".
5. Enter port "502" under "Slave Remote TCP port".
6. Enter the IP address, which can be used to access the Modbus master, under "Slave Remote IP address".

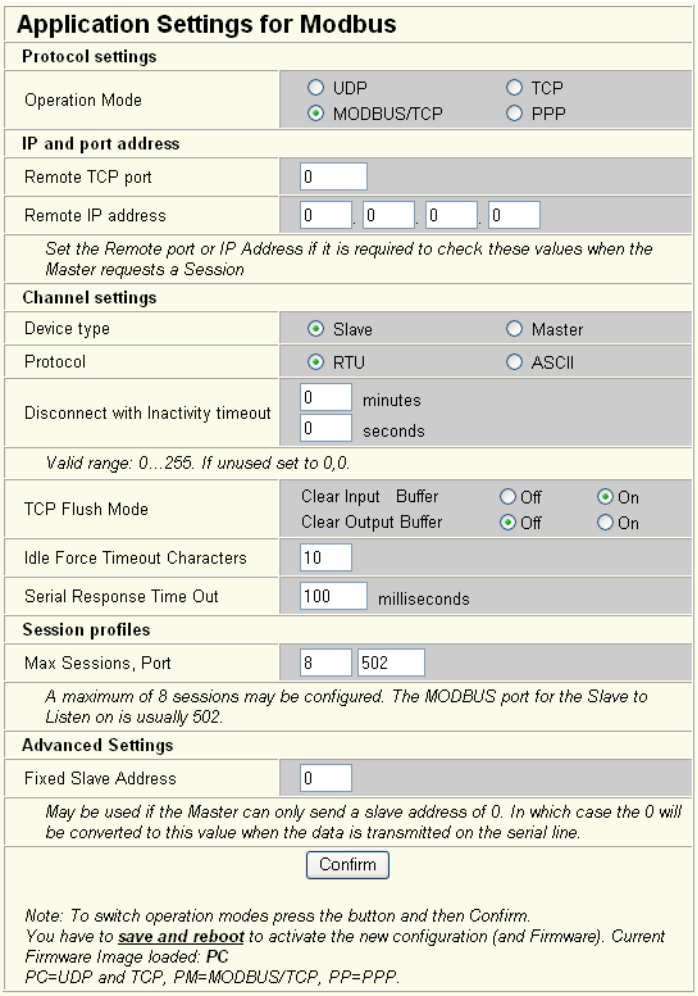


Figure 4-27 Settings at the slaves

4.8 PPP applications

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

4.8.1 Possible applications

The firmware and therefore the scope of functions of the new FL COMSERVER UNI 232/422/485 has been extended so that numerous new PPP applications are supported.

4.8.1.1 Permanent line connection between two Ethernet networks

This application can be implemented via various physical transmission paths:

– Direct connection between two COM servers over up to 1000 m using the integrated RS-422 interface (see Figure 4-28)
– A distance of up to 20 km can be covered using simple two-wire cables with an additional permanent line modem, e.g., PSI-DATA/FAX-MODEM/RS232, Order No. 2708203 (see Figure 4-29)
– Wireless connection over up to 2000 m using wireless modems, e.g., RAD-ISM-2400-DATA-BD-BUS, Order No. 2867872 (see Figure 4-30)

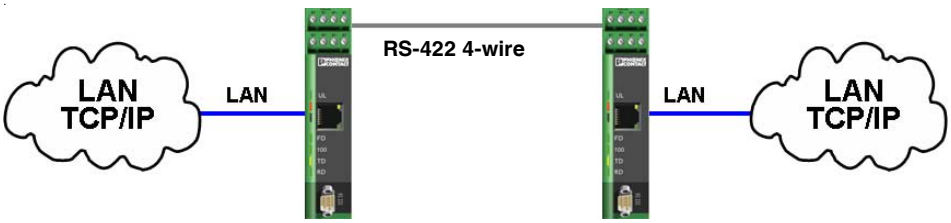


Figure 4-28 Direct RS-422 connection

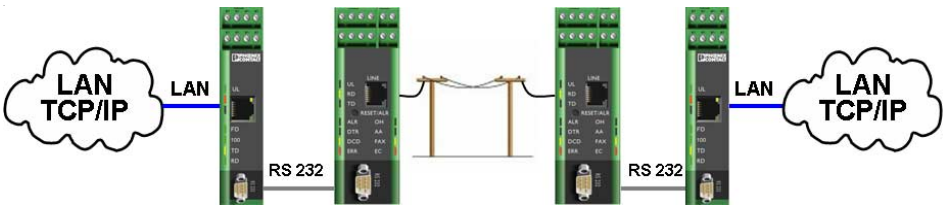


Figure 4-29 Two-wire permanent line connection

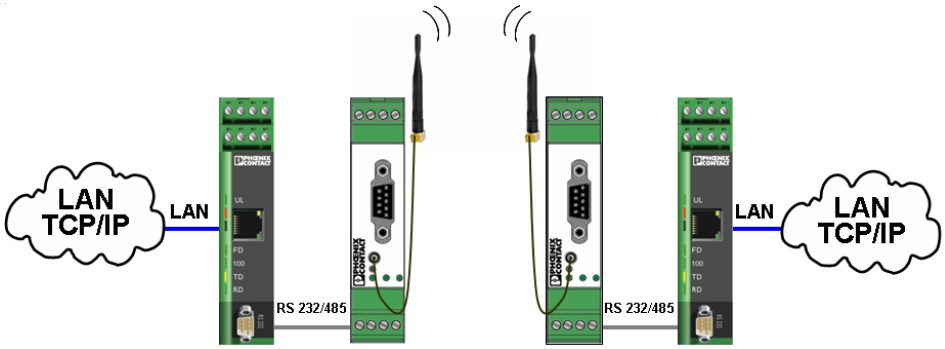


Figure 4-30 Wireless connection

For configuration, please refer to Section 4.8.2 "Configuration of a permanent line connection".

4.8.1.2 Dial-up connection between two Ethernet networks

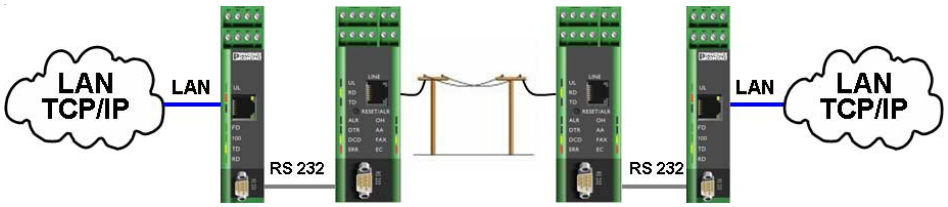


Figure 4-31 Dial-up connection

Alternatively, this application can be implemented using the integrated version PSI-MODEM/ETH, Order No. 2313300.

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

4.8.1.3 Remote maintenance of a remote network via a modem connection

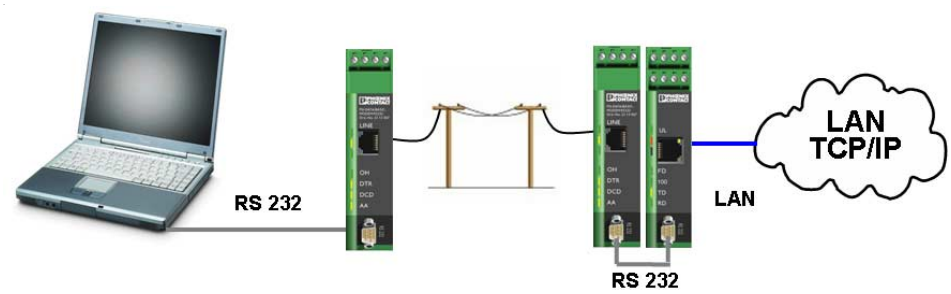


Figure 4-32 Modem connection

Phoenix Contact offers an integrated preconfigured solution for this application, which reduces installation time considerably. This product can be ordered under the designation PSI-MODEM/ETH, Order No. 2313300.

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

4.8.1.4 Combined operation of a dial-up connection and remote maintenance

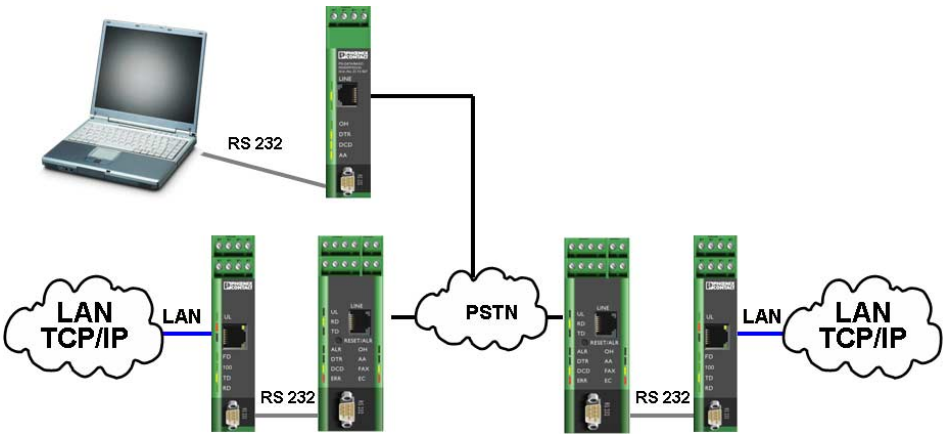


Figure 4-33 Dial-up connection and remote maintenance

This configuration supports both connection establishment from a remote network to a higher-level network (e.g., in the event of an error in a system that otherwise operates autonomously) and dialing 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 permanent line connection

The configuration is described using the example of a direct RS-422 connection. If the alternative option of additional modems is used, configure the serial interface to V.24 (RS-232) mode.

4.8.2.1 Setting up the FL COMSERVER UNI 232/422/485

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

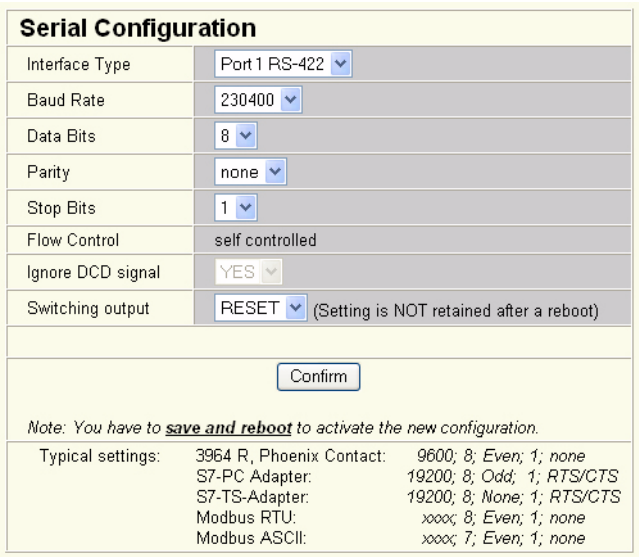


Figure 4-34 Configuring the serial interface

2. Configure the application to PPP mode under "General Configuration... Application Settings".
3. Confirm the entry with "Confirm". Web-based management now indicates 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 then entering the system password (default: private).
5. Repeat steps 1 - 4 for the second FL COMSERVER UNI 232/422/485.

Configuring COM server 1 (server) in the main network

The FL COMSERVER UNI 232/422/485 integrates remote subnetworks in a main network. In the example, the subnetwork with subnet mask 255.255.255.192 (COM server 2) is connected to the main network with subnet mask 255.255.255.0 (COM server 1).

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

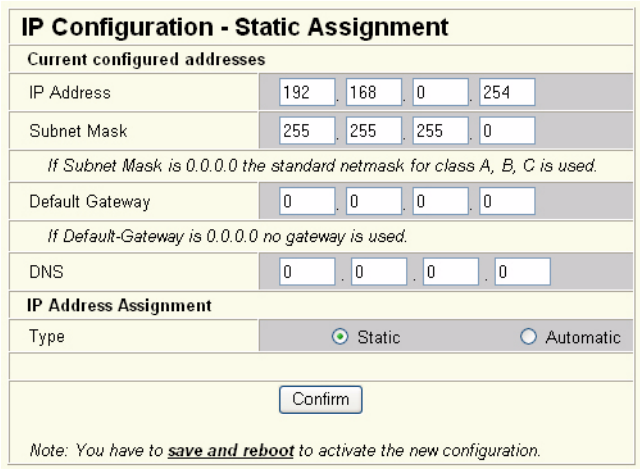


Figure 4-35 Setting the IP address (server)

7. Confirm the setting with "Confirm".
8. Switch to the "General Configuration… Application" menu.
   Enter the configuration as follows:

PPP Link type =	Dedicated
Device type =	Server (Router)
Assign Client IP address =	Set the IP address of the second COM server here
Assign Client Subnetmask =	Set the subnet mask of the remote subnetwork here
User name =	This entry is optional
Password =	Enter a password of at least four characters here

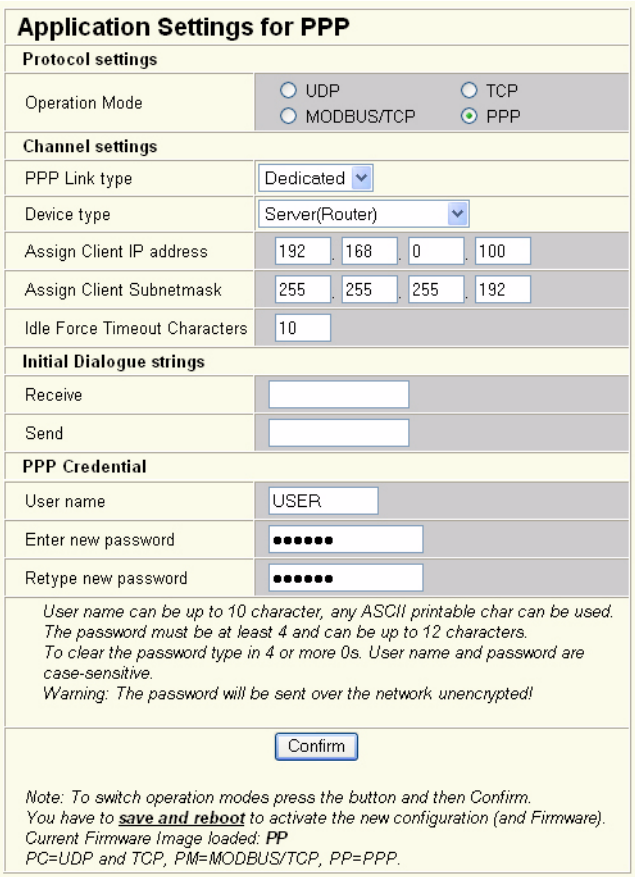


Figure 4-36 Application settings for permanent line connection (server)

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 then entering the system password (default: private).

This completes the configuration of the first device (server).

Configuring COM server 2 (client) in the subnetwork

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

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

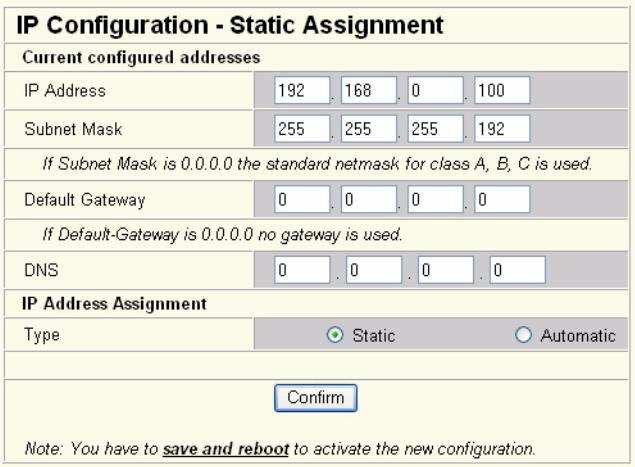


Figure 4-37 Setting the IP address (client)

12. Confirm the setting with "Confirm".
13. Switch to the "General Configuration… Application" menu.
    Enter the configuration as follows:

PPP Link type =	Dedicated
Device type =	Client (Gateway)
Filter IP address =	Optional entry to limit data traffic via the slower serial modem connection. Permitted IP address (area) that can communicate via the modem path. Data packets from other IP addresses are rejected. The address area is defined together with the filter subnet mask. An entry of 0.0.0.0 deactivates the filter and permits all devices to communicate.
Filter Subnetmask =	Subnet mask that together with the filter IP address defines an address area that can communicate via the modem path. Special case: Subnet mask = 0.0.0.0, only the specified IP address is valid.
User name =	This entry is optional
Password =	Enter a password of at least four characters here

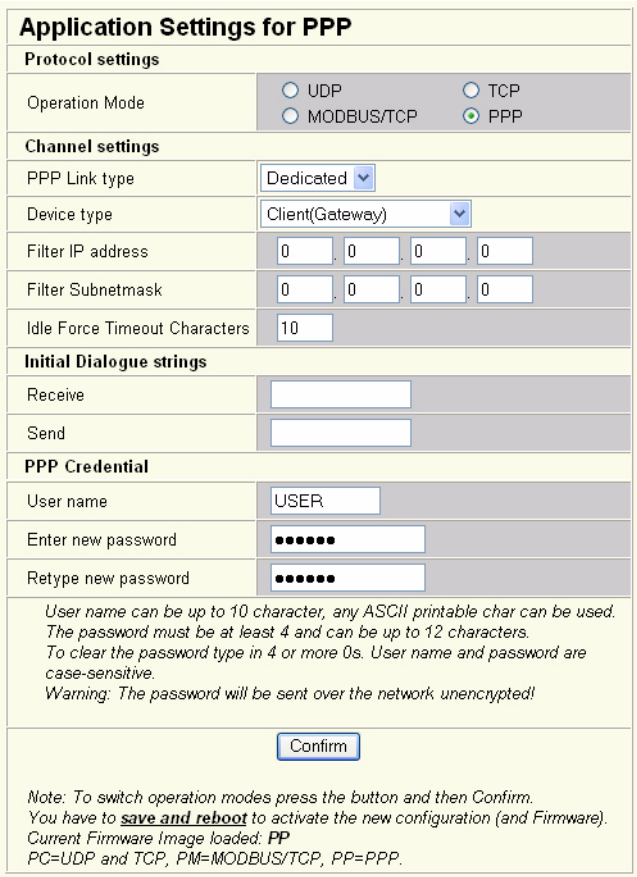


Figure 4-38 Application settings for permanent line connection (client)

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

This 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 devices of the subnetwork.

4.8.3 Configuration of a dial-up connection

4.8.3.1 Function description

The connection of remote subnetworks to higher-level networks via dial-up modems is particularly useful if the remote system operates autonomously and only has to connect to higher-level devices in the event of an error. In this case, a telegram to the configured gateway address (COM server) starts connection establishment. The FL COMSERVER UNI 232/422/485 controls the connected modem using AT commands. During connection establishment, received packets are rejected by the FL COMSERVER UNI 232/422/485. As soon as the connection has been established successfully, bidirectional data exchange begins.

In the event that a connection cannot be established, a second number can be configured as an alternative that is used after a configurable timeout time.

4.8.3.2 Setting up the COM server

The configuration only differs from the permanent line connection in the "Application" menu.

Please refer to steps 1 - 6 and 10 - 11 in Section 4.8.2 "Configuration of a permanent line connection".

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

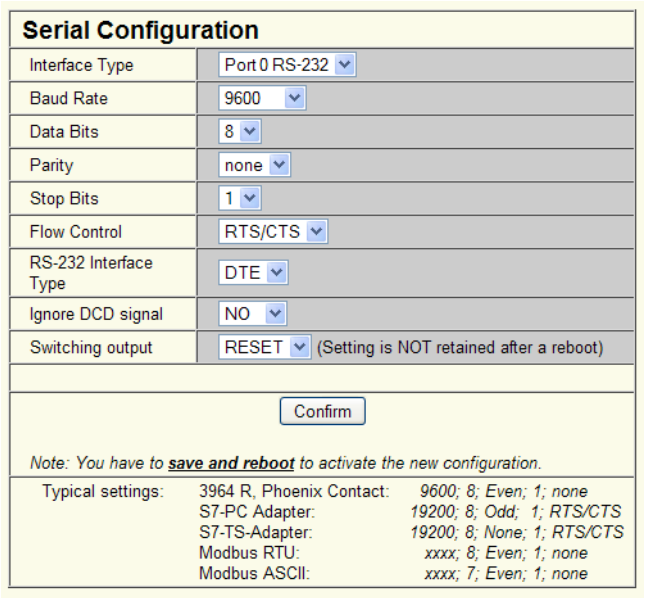


Figure 4-39 Configuring the serial interface

Configuring COM server 1 (server) in the main network

2. Switch to the "General Configuration… Application" menu.
   Enter the configuration as follows:

PPP Link type =	Dial-up
Device type =	Server (Router)
Assign Client IP address =	Set the IP address of the second COM server here
Assign Client Subnetmask =	Set the subnet mask of the remote subnetwork here
User name =	This entry is optional
Password =	Enter a password of at least four characters here

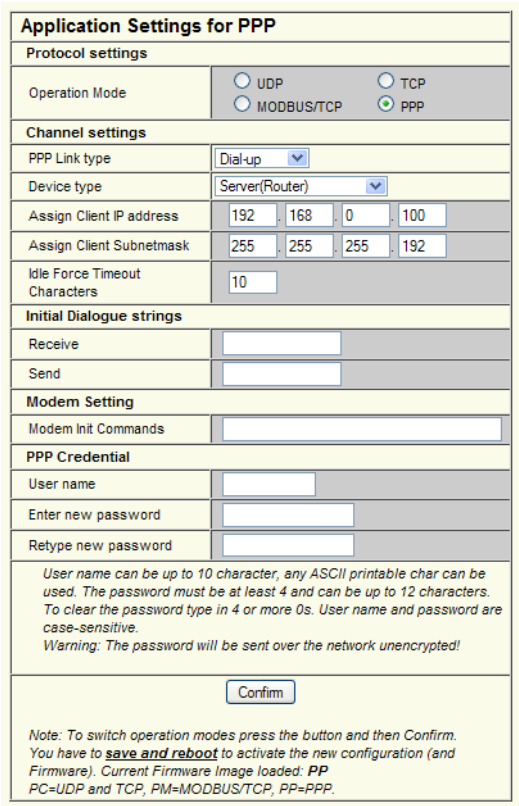


Figure 4-40 Application settings for dial-up connection (server)

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

This completes the configuration of the first device (server).

Configuring COM server 2 (client) in the subnetwork

5. Switch to the "General Configuration… Application" menu.
   Enter the configuration as follows:

PPP Link type =	Dial-up
Device type =	Client (Gateway)
Filter IP address =	Optional entry to limit data traffic via the slower serial modem connection. Permitted IP address (area) that can communicate via the modem path. Data packets from other IP addresses are rejected. The address area is defined together with the filter subnet mask. An entry of 0.0.0.0 deactivates the filter and permits all devices to communicate.
Filter Subnetmask =	Subnet mask that together with the filter IP address defines an address area that can communicate via the modem path. Special case: Subnet mask = 0.0.0.0, only the specified IP address is valid.
Dialup Timeout =	Waiting time in which the connection must be established successfully. Once this time has elapsed, connection establishment is attempted using the back-up number. If no back-up number is configured, connection establishment is aborted after the waiting time has elapsed.
Link idle Timeout =	If data is no longer being transmitted, the connection is released after the set waiting time has elapsed.
Dialup Phone number =	Phone number of the higher-level network
Dialup Phone number (fallback) =	Alternative (back-up) phone number that is used if connection establishment fails
User name =	This entry is optional
Password =	Enter a password of at least four characters here

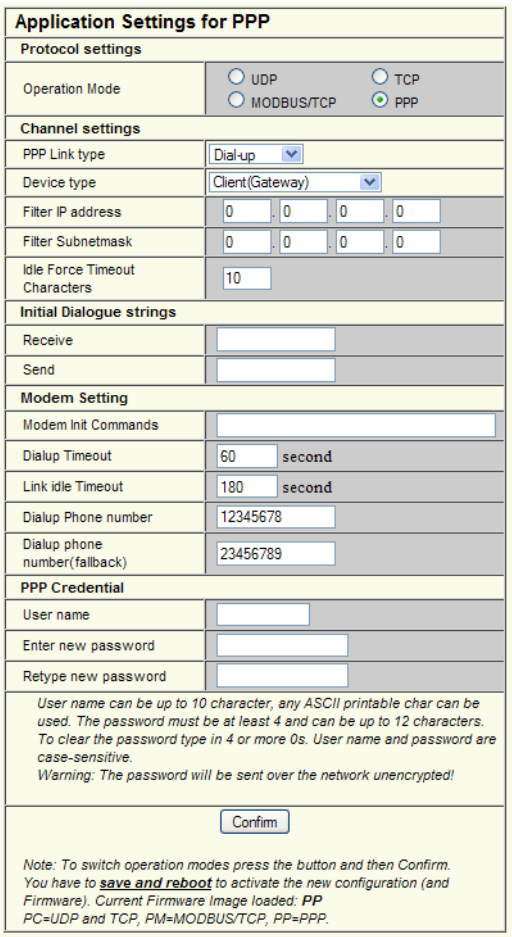


Figure 4-41 Application settings for dial-up connection (client)

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 then entering the system password (default: private).

This 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 devices of the subnetwork.

Now configure the connected modems as required.

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

If the remote network is to be connected both via a dial-up connection to a higher-level network and to be available for configuration purposes via a dial-up connection, the FL COMSERVER UNI 232/422/485 can be configured accordingly.

Additional settings at COM server 2 (client)

Device type =	Client/Server (Gateway)
Initial Dialogue strings (Receive) =	CLIENT
Initial Dialogue strings (Send) =	CLIENTSERVER

Initial dialog strings must always be entered in UPPER CASE.

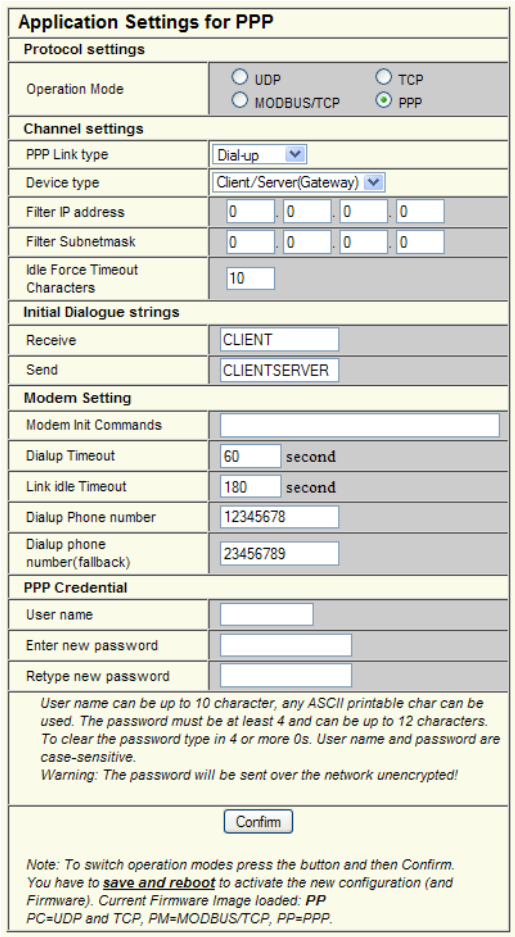


Figure 4-42 Application settings for combined dial-up connection and remote access (client)

4.8.4 Configuration of a remote maintenance connection

4.8.4.1 Setting up the COM server

1. Configure the serial V.24 (RS-232) interface of the FL COMSERVER UNI 232/422/485 under "General Configuration... Serial" to 8 data bits, no parity, one stop bit, and hardware handshake (RTS/CTS).
2. Configure the application to PPP mode 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 selecting the "Save" and "Reboot" items and then entering the system password (default: private).
5. Switch to the "General Configuration … Application" menu.
   Enter the configuration as follows:

PPP Link type =	Dial-up
Device type =	Server (Router)
Assign Client IP address =	Set a free IP address from the remote subnetwork here
Assign Client Subnetmask =	Set the subnet mask of the remote subnetwork here
User name =	This entry is optional
Password =	Enter a password of at least four characters here

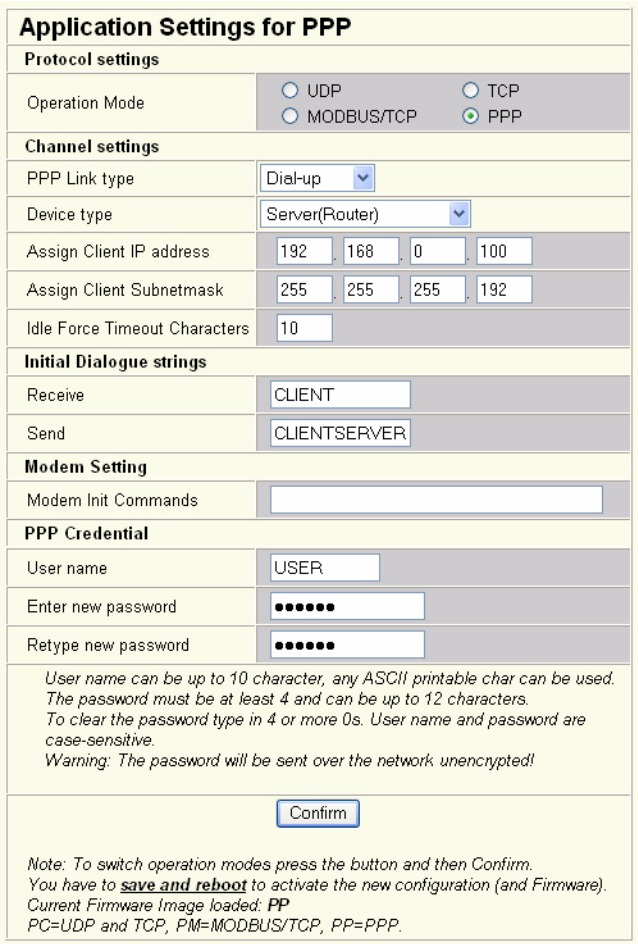


Figure 4-43 Application settings for remote maintenance connection

6. Confirm the entries with "Confirm".
7. Then save and activate the new settings under "General Configuration... Save and Reboot" by selecting the "Save" and "Reboot" items and then entering the system password (default: private).
8. Also, configure the serial interface of the modem to
   8 data bits, 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 of the FL COMSERVER UNI 232/422/485 and modem.

4.8.5 Setting up a dial-up connection under Windows XP

1. Install a new network connection via "Start... Settings... Network Connections... New Connection".

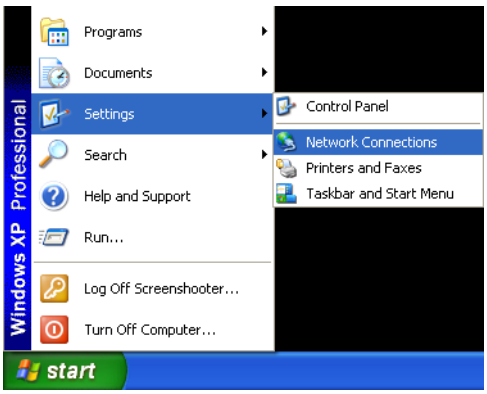


Figure 4-44 Network connections

2. A wizard displays a welcome message.

Figure 4-45 New Connection Wizard

3. Select "Connect to the network at my workplace".

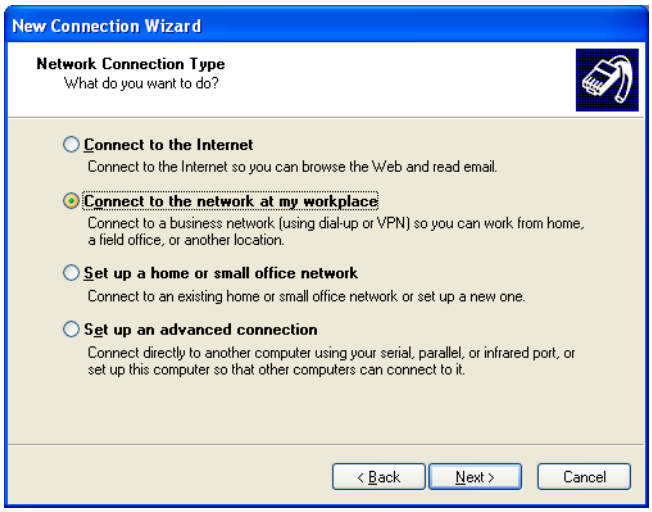


Figure 4-46 Network connections

4. Select "Dial-up connection".

Figure 4-47 Dial-up connection

5. Enter a connection name.

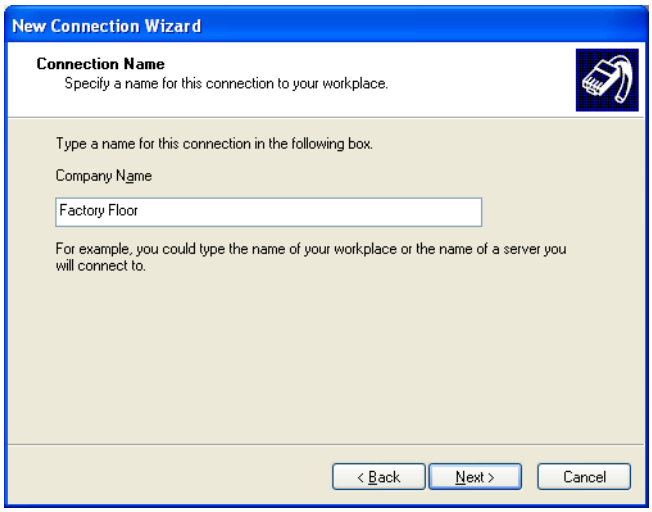


Figure 4-48 Connection name

6. Enter the phone number.

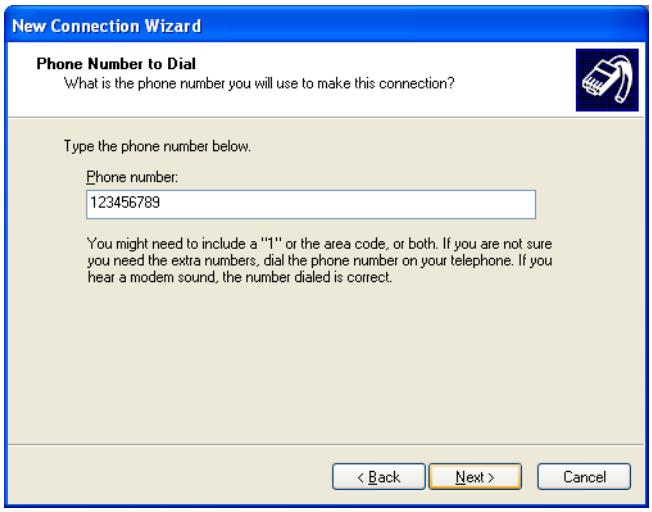


Figure 4-49 Phone number

7. Specify whether the connection should be available only in your user profile or to all users of the computer.

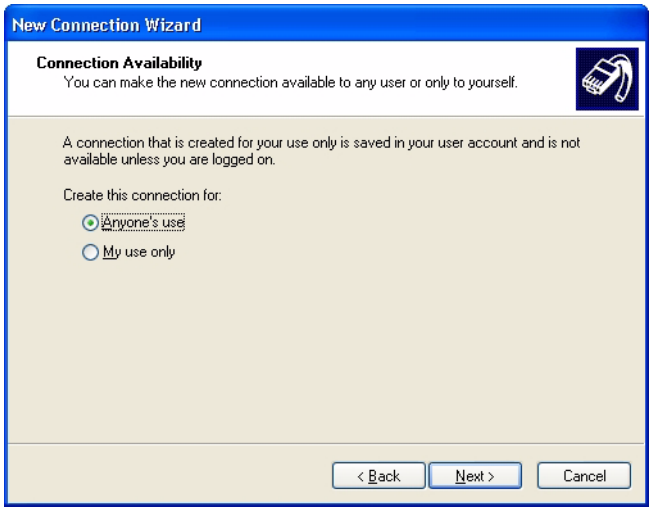


Figure 4-50 Availability of the connection

8. A shortcut on your desktop makes it easier to start subsequent connection establishment.

Figure 4-51 Exiting the wizard

9. Double-click to start dial-up connection establishment.
10. The "Connect to <Connection name>" window is displayed. Select "Properties".

11. A window with five tabs appears under "Properties".

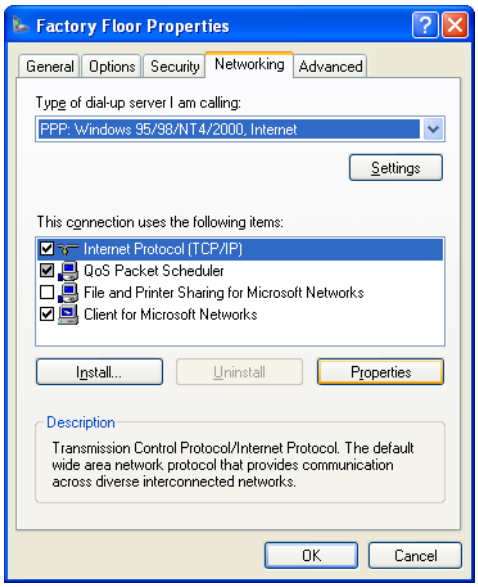


Figure 4-52 Overview of connection properties

12. Select "Networking... Settings" and deactivate software compression.

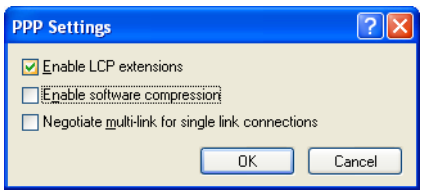


Figure 4-53 PPP settings

13. Select "Networking... Properties" and then "Advanced".

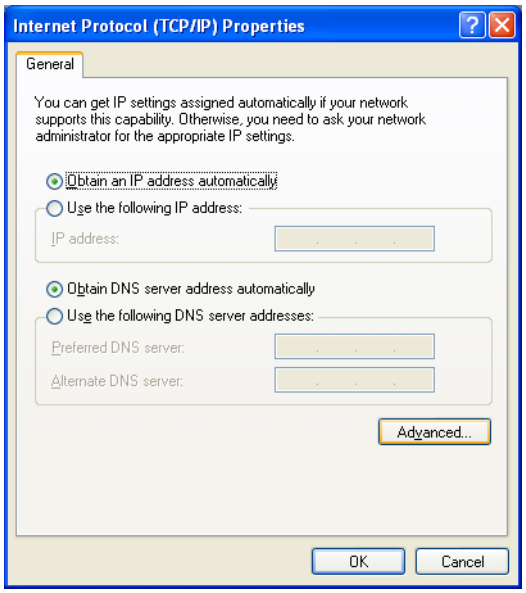


Figure 4-54 IP configuration properties

14. Deactivate IP header compression

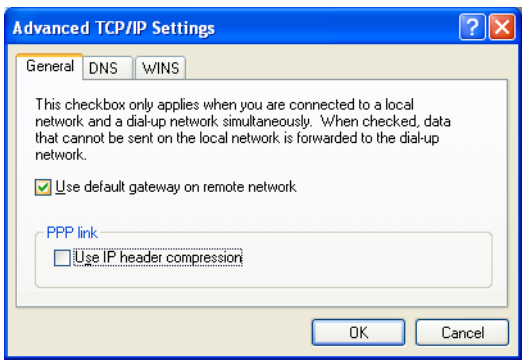


Figure 4-55 Advanced IP configuration

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

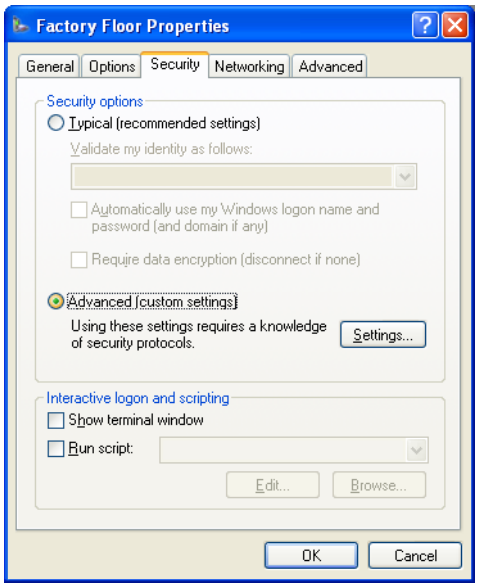


Figure 4-56 User-defined security settings

16. Deactivate all "unsecure" protocols and then activate the "Challenge Handshake Authentication Protocol (CHAP)".

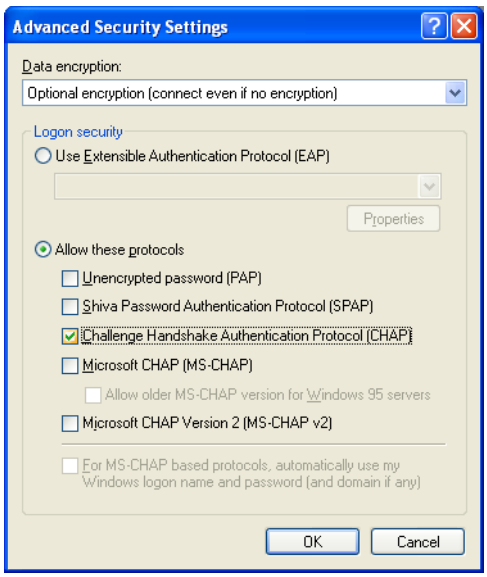


Figure 4-57 Activating the CHAP protocol

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

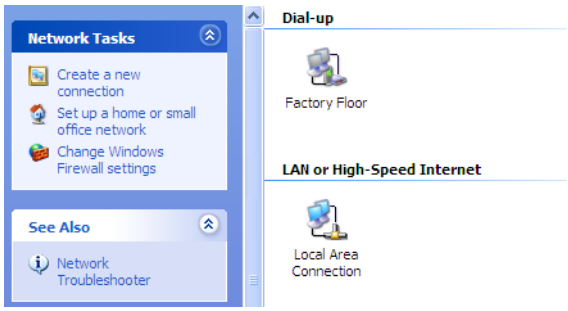


Figure 4-58 Network connections

18. Check the entered password and the specified phone number before clicking "Dial" to start connection establishment.

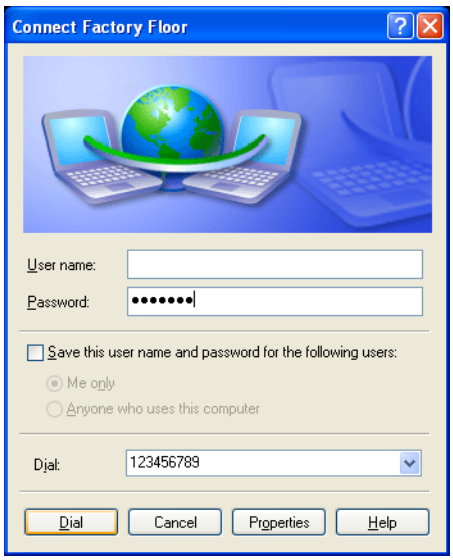


Figure 4-59 Connection establishment

19. As soon as the modem connection has been established successfully, the computer is registered in the network and the password is checked. Once this process has been completed successfully, the window is minimized to an icon in the status bar.

Figure 4-60 Network registration

5 SNMP management

5.1 General function

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) is a manufacturer-independent standard for Ethernet management and defines commands for reading and writing error and status message information and formats. SNMP is also a structured model, which comprises agents and their relevant MIB (Management Information Base) and a manager. The manager is a software tool, which is executed on a network management station. The agents are located inside 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 regularly requests and displays this information. The devices can be configured by writing data from the manager to the MIB. In the event of an emergency, the agents can also send messages (traps) directly to the manager.

SNMP interface

All managed Factory Line components have an SNMP agent. This agent controls the Management Information Base II (MIB 2) according to RFC 1213, RMON MIB, Bridge MIB, If MIB, Etherlike MIB, and private SNMP objects from Phoenix Contact.

Network management stations, such as a PC with Factory Manager, can read and modify configuration and diagnostic data from network devices via the Simple Network Management Protocol (SNMP). In addition, any SNMP tools or network management tools can be used to access Factory Line products via SNMP. The MIBs supported by the relevant device must be made available to the SNMP management tools.

On the one hand, these are globally valid MIBs, which are specified and described in RFCs (Request for Comments). This includes, for example, MIB2 according to RFC 1213, which is supported by all SNMP-compatible network devices. On the other hand, manufacturers can specify their own private SNMP objects, which are then assigned to a private manufacturer area in the large SNMP object tree. Manufacturers are then responsible for their own private (enterprise) areas, i.e., they must ensure that only one object is assigned to an object ID (object name and parameters) and can be published. If an object is no longer needed, it can be labeled as "expired", but it cannot be reused with other parameters under any circumstances.

Phoenix Contact provides notification of ASN1 SNMP objects by publishing their descriptions on the Internet.

Reading SNMP objects is not password-protected. However, a password is required for read access in SNMP, but this is set to "public", which is usual for network devices, and cannot be modified. By default upon delivery, the password for write access is "private" and can be changed by the user.

SNMP, the web interface, and the serial terminal all use the same password, which can be changed by the user.

Another benefit for the user is the option of sending traps using the Simple Network Management Protocol.

Management Information Base

Database which contains all the data (objects and variables) required for network management.

Agent

An agent is a software tool, which collects data from the network device on which it is installed, and transmits this data on request. Agents reside in all managed network components and transmit the values of specific settings and parameters to the management station. On a request from a manager or on a specific event, the agent transmits the collected information to the management station.

Traps

Traps are spontaneous SNMP alarm or information messages, which are sent by an SNMP-compatible device when specific events occur. Traps are transmitted with maximum priority to various addresses (if required) and can then be displayed by the management station in plain text. The IP addresses that are to receive these traps (trap targets/receivers) must be set by the user on the relevant device.

5.2 Supported MIBs

The FL COMSERVER ... 232/422/485 supports MIB2 according to RFC 1213 and the private FL COM SERVER.mib. The MIB files can be found on the CD provided with this user manual and on the Internet under www.factoryline.de.

5.2.1 Diagram of SNMP management

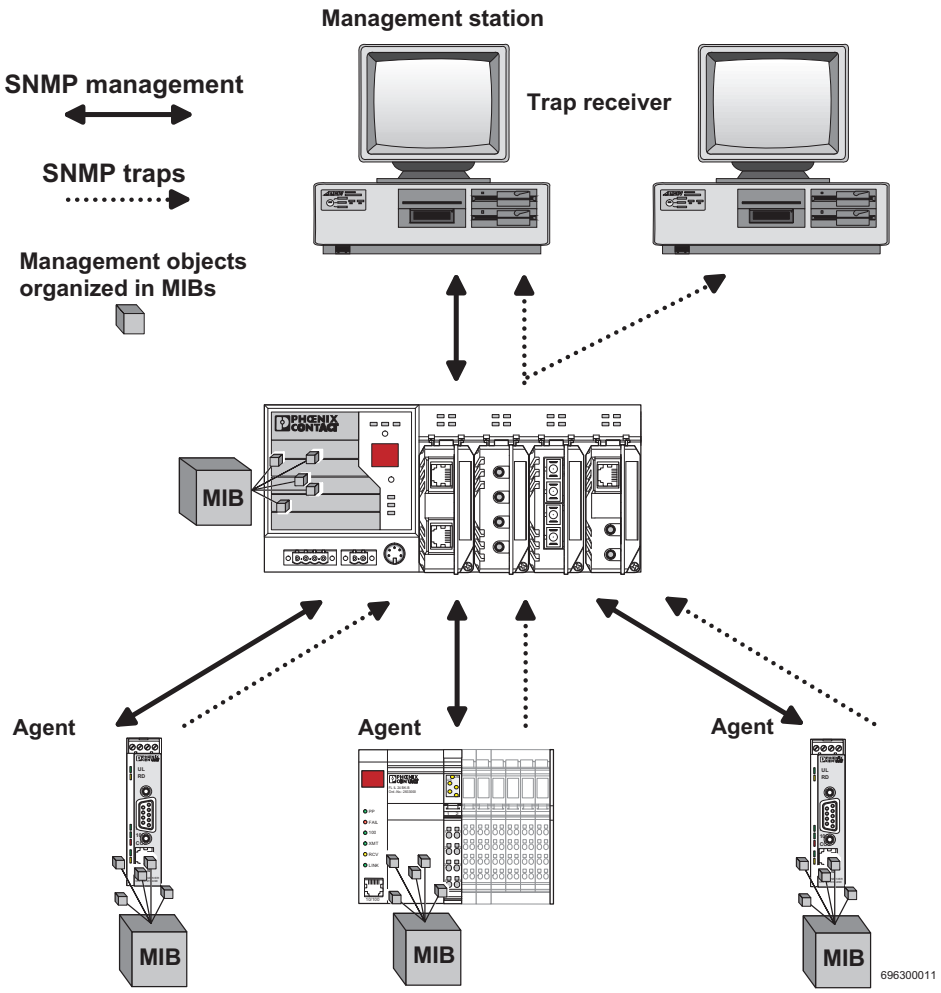


Figure 5-1 Diagram of SNMP

6 Service and maintenance

6.1 Emergency configuration

If you are unable to carry out WBM device configuration via a network, e.g., because the set static IP address is unknown, serial emergency access can be used.

Local access to the device is required and a PC with a terminal program must be connected to the V.24 (RS-232) interface.

6.1.1 Scope of functions

The following functions are available for emergency configuration:

– Configuring the IP address/activating the BootP mechanism
– Deleting all settings (including passwords) and resetting to the default 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 interface on a PC (1:1 cable).
2. Open a terminal program, e.g., HyperTerminal, in the Windows Start menu via "Programs... Accessories... Communications... HyperTerminal".
3. Configure the interface (e.g., COM 1) via "File... Properties" to 9600 bps; 8 data bits; no parity; 1 stop bit; no flow control.

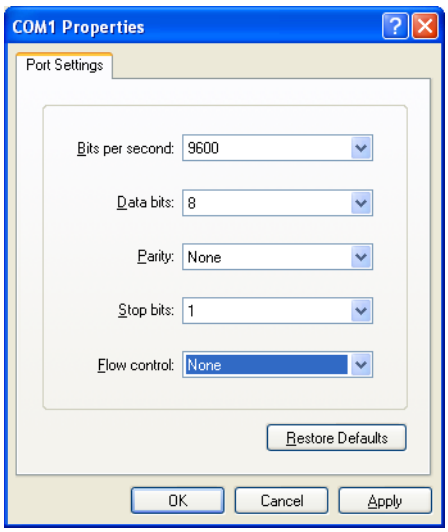


Figure 6-1 "Properties" menu in Windows HyperTerminal

4. Confirm the settings with "OK" and close the menu.
5. Check that the settings are correct in the status bar in HyperTerminal.

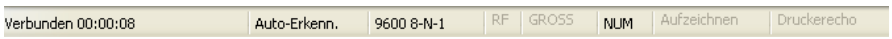


Figure 6-2 Status bar in Windows HyperTerminal

6. Reset the voltage at the FL COMSERVER ... 232/422/485 and simultaneously hold down the "X" key on your keyboard.
7. As soon as confirmation from the FL COMSERVER ... 232/422/485 is displayed, press ENTER within three seconds.

The following is displayed:

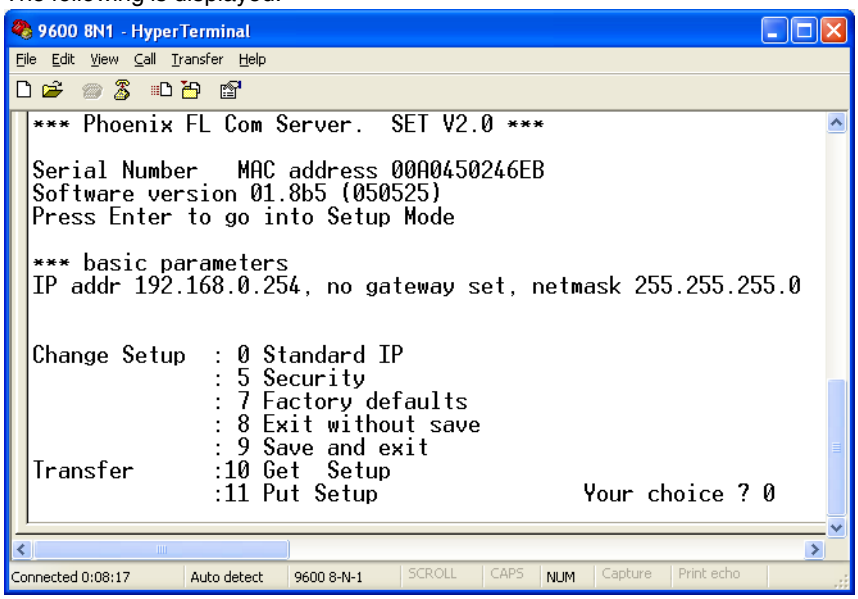


Figure 6-3 Serial setup menu

8. Select the desired option by entering the relevant number and press ENTER to confirm your selection.

6.2 Reading the configuration

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

In addition, other FL COMSERVER ... 232/422/485 devices can be configured via a TFTP transfer, e.g., in standard machine production. The reference configuration can be saved in a special format.

6.2.1 Displaying and printing the configuration overview

1. In WBM, select the "Configuration Management" menu item under "General Configuration".

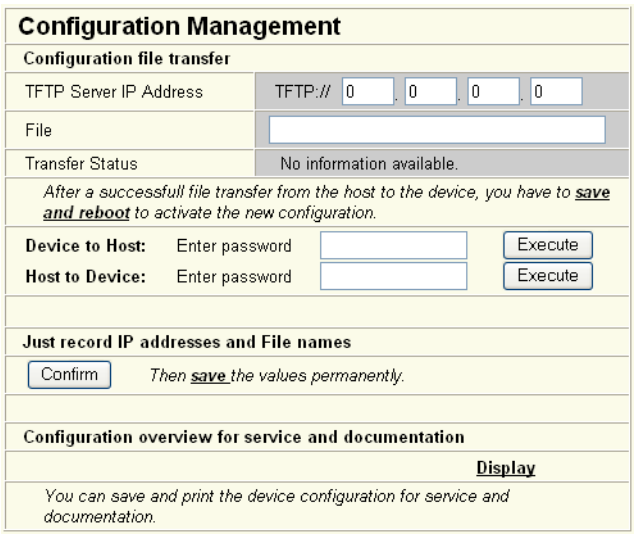
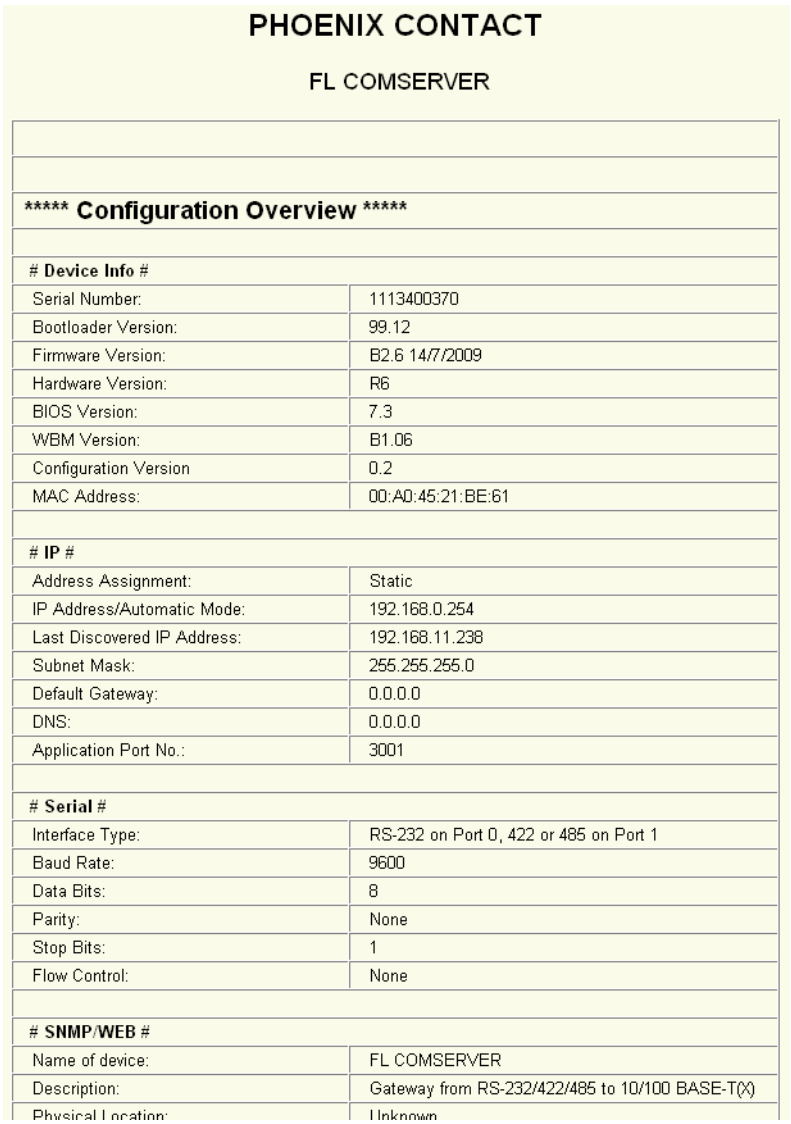


Figure 6-4 "Configuration Management" menu

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

3. A new browser window is opened.



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 6-5 Configuration overview

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

4. Print the overview for the system documentation.
5. Alternatively, you can save this information as an HTML or TXT file onto a data carrier via the "Save As" menu in the browser. The configuration can be easily displayed in these file formats on any PC.

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

6.2.2 Saving the configuration using TFTP

This function can be used to save the active FL COMSERVER ... 232/422/485 configuration in a back-up file (direction: device to host). The configuration cannot be displayed in plain text. The format is used exclusively for the automatic configuration of devices using TFTP data transfer.

When a configuration is uploaded from the FL COMSERVER ... 232/422/485 to a PC, the last saved version is transmitted. If you want to transmit the active configuration, first save it again ("Save and Reboot" menu).

Before transferring the configuration file via TFTP, make sure that TFTP is enabled in the "Security – Security Flags" menu (see Section 3.4.8).

1. In WBM, select the "Configuration Management" menu item under "General Configuration".
2. In the "TFTP Server IP Address" field, enter the IP address of the TFTP server where you wish to save the file.
3. Enter a name for the back-up file.
4. Select the "device to host" direction.
5. Enter the "write password" (default = private).
6. Click "Execute" and start the data transfer.

6.2.3 Loading the configuration using TFTP

This function can be used to load a back-up 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 via TFTP, make sure that TFTP is enabled in the "Security – Security Flags" menu (see Section 3.4.8).

1. In WBM, select the "Configuration Management" menu item under "General Configuration".
2. In the "TFTP Server IP Address" field, enter the IP address of the TFTP server where the back-up file is saved.
3. Enter the name of the back-up file.
4. Select the "host to device" direction.
5. Enter the "write password" (default = private).
6. Click "Execute" and start the data transfer.
7. Reset the device.

When a configuration is downloaded from the PC to an FL COMSERVER ... 232/422/485, the new configuration is only activated once the FL COMSERVER ... 232/422/485 has been reset.

Configuration using a configuration file is used when replacing devices. To duplicate devices using a configuration file, observe the following:

– Establish a connection from the FL COMSERVER ... 232/422/485 to an FTP server or local connection via the V.24 (RS-232)/RS-485 interface of the FL COMSERVER ... 232/422/485.
– Load the configuration file on the FL COMSERVER ... 232/422/485.
– Reset the FL COMSERVER ... 232/422/485.
– Adjust the IP parameters.
– Save the configuration ("Save current configuration" function).

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

6.3 Configuration upload and download using a terminal program

As an alternative to saving and loading a configuration using TFTP, it is possible to use a terminal program instead. The connection to the FL COMSERVER ... 232/422/485 is established either via Telnet or V.24 (RS-232).

6.3.1 Establishing a connection to the FL COM SERVER

In addition to web-based management, the FL COM SERVER... offers two alternative configuration options.

6.3.1.1 Configuration via Telnet

1. Open the dialog box via START => Programs => Accessories => HyperTerminal.
2. Set up a Telnet connection to the IP address of the COM server with port number 9999.

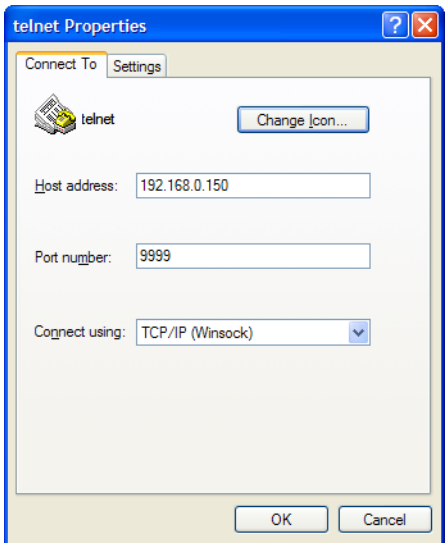


Figure 6-6 Configuration via Telnet

3. Following connection establishment, the password is requested (default = private).
4. Confirm the entry by pressing ENTER.

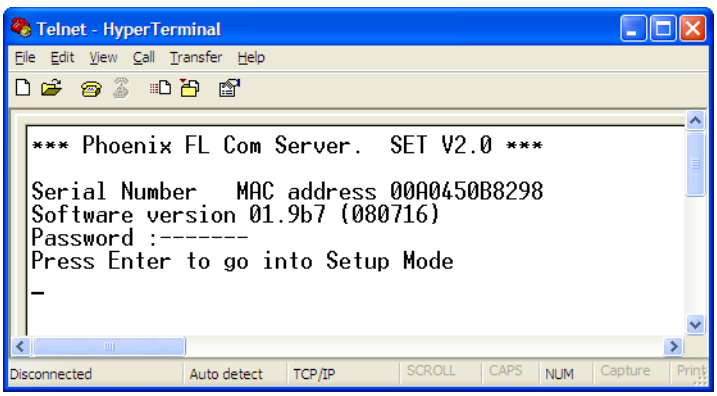


Figure 6-7 Confirming the configuration

5. Confirm the entry by pressing ENTER again.

6.3.1.2 Configuration via V.24 (RS-232)

1. Open the dialog box via START => Programs => Accessories => HyperTerminal.
2. Set up a terminal connection via COM 1 or 2. The serial settings should be 9.6 kbps, 8 data bits, no parity, 1 stop bit, and no handshake.

Figure 6-8 Configuration via V.24 (RS-232)

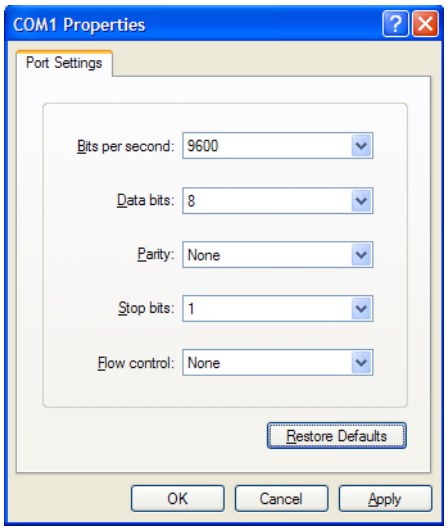


Figure 6-9 Confirming the configuration

3. Hold down the "X" key on your keyboard and simultaneously reset the voltage on the FL COM SERVER.
4. Confirm the entry by pressing ENTER.

6.3.2 Saving a COM server configuration on a PC

The following configuration menu is then displayed.

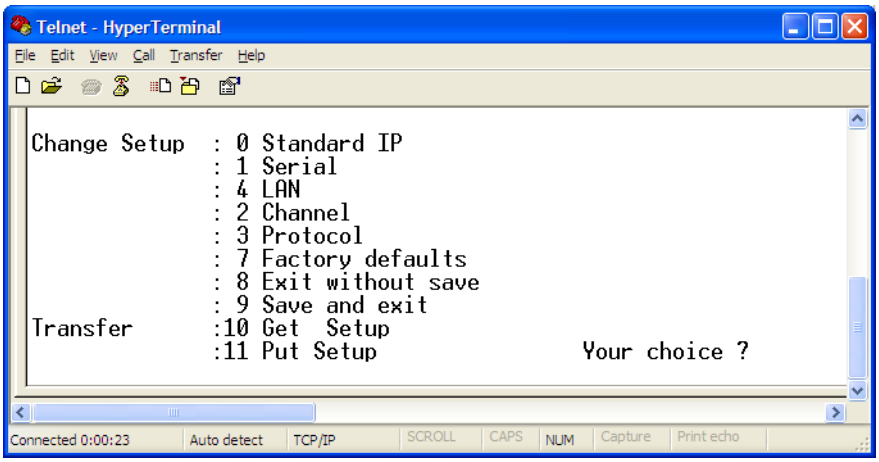


Figure 6-10 Configuration menu

1. Select item 10 and confirm with by pressing ENTER.

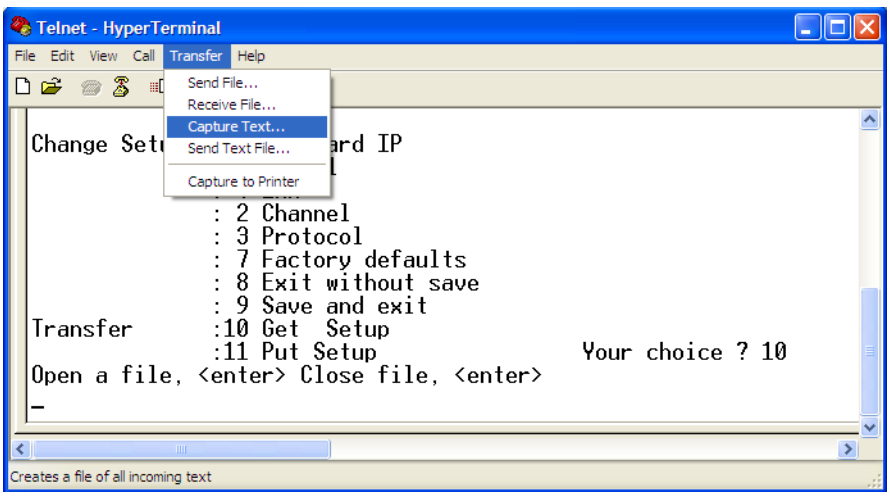


Figure 6-11 Capturing the configuration file

2. Select "Transfer" => "Capture Text...".
3. In the menu that opens, enter a storage location and a file name for the configuration file.

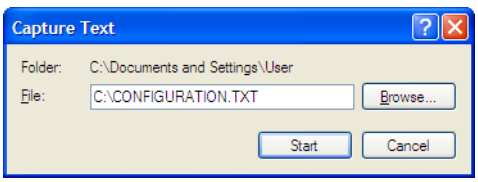


Figure 6-12 Saving the configuration file

4. After data transfer, close the file under "Transfer" => "Capture Text..." => "Stop".

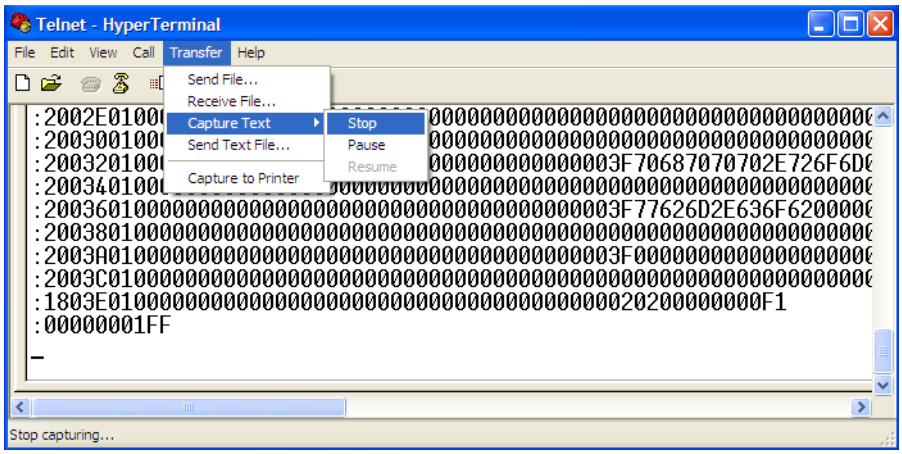


Figure 6-13 Stopping configuration file capture

The FL COM SERVER configuration is now saved to a file.

6.3.3 Downloading a COM server configuration from a PC

1. Following successful connection establishment, select item 11 and confirm the entry by pressing ENTER.

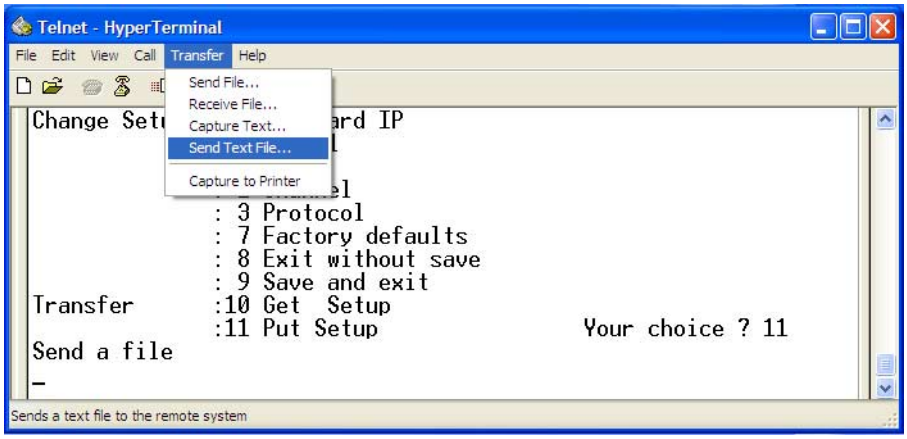


Figure 6-14 Sending the configuration file

2. Select "Transfer" => "Send Text File...".
3. In the menu that opens, select the desired configuration file and confirm the entry by pressing ENTER.

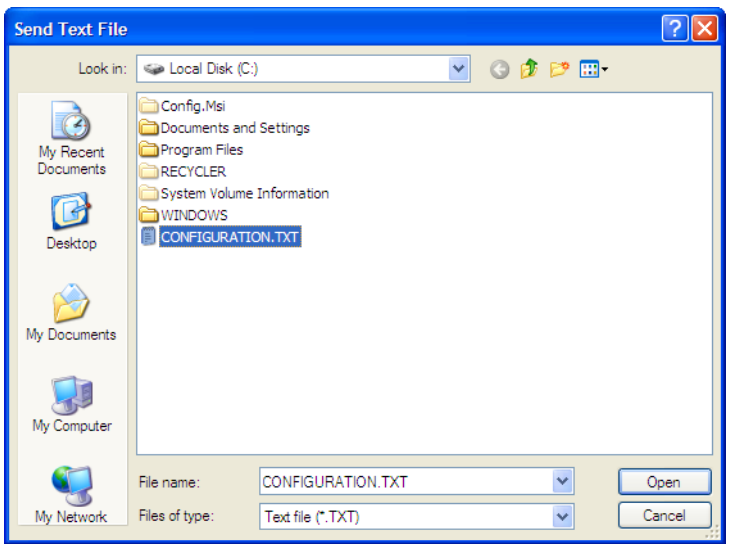


Figure 6-15 Opening the configuration file

File download starts automatically.

NOTE: Aborting the download prematurely may result in data loss.

Transmission can take up to one minute. Only very slight LED activity can be detected at the interfaces during this time.

4. Successful data transfer is confirmed with the following message.

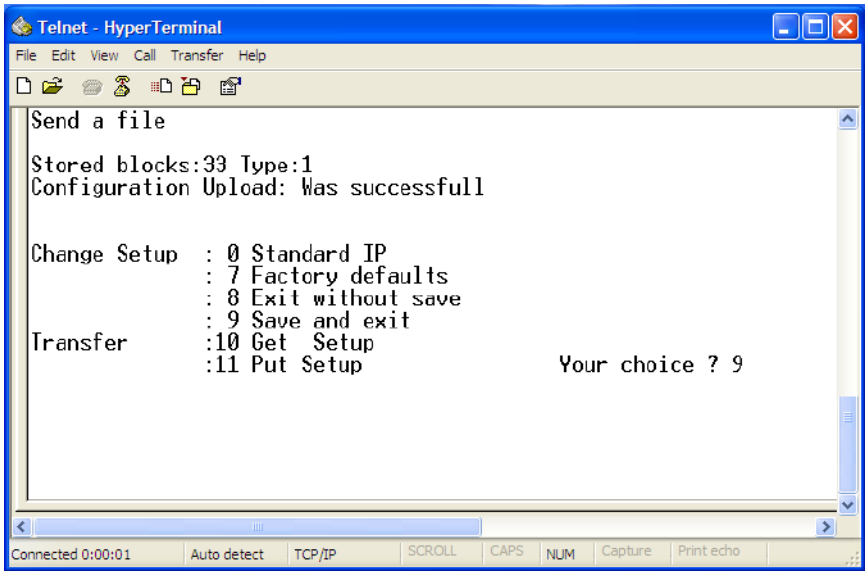


Figure 6-16 Saving the new configuration

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

NOTE: For security reasons, the PPP password cannot be transferred via a configuration upload/download. This setting can only be made via web-based management.

6.4 Updating the firmware and WBM

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

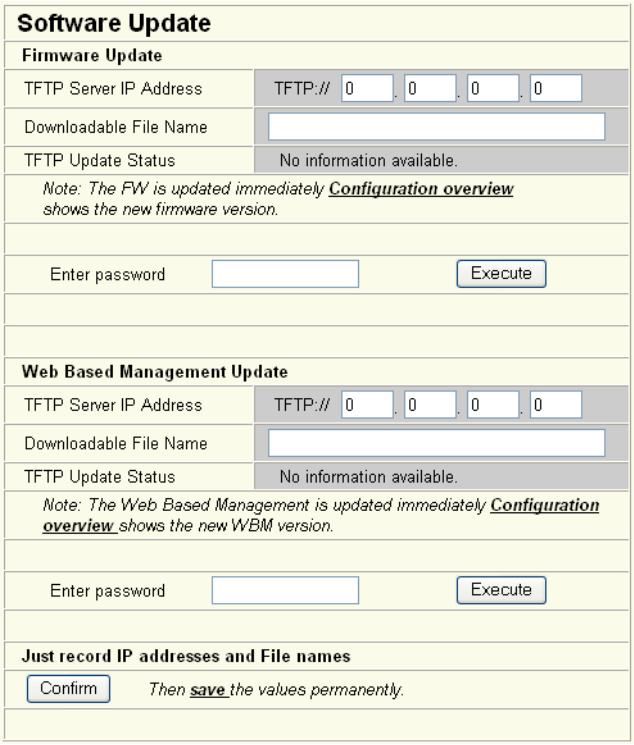


Figure 6-17 "Software Update" menu

6.4.1 Updating the software

The update procedure is identical for both the firmware and WBM.

1. Save the new firmware and WBM files in the root directory of the TFTP server.
2. In 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 is located.
4. Enter the name of the back-up file.
5. Enter the "write password" (default = private).
6. Click "Execute" and start the data transfer.
7. Reset the device.

When a configuration is downloaded from the PC to an FL COMSERVER ... 232/422/485, the new configuration is only activated once the FL COMSERVER ... 232/422/485 has been reset.

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

A Technical appendix

A 1 Structure of IP addresses

A 1.1 Valid IP parameters

IP parameters comprise the following three elements: "IP address", "subnet mask", and "default gateway/router".

Valid IP addresses are:
000.000.000.001 to 126.255.255.255
128.000.000.000 to 223.255.255.255

Valid subnet masks are:
255.000.000.000 to 255.255.255.252

Default gateway/router:
The IP address of the gateway/router must be in the same subnetwork as the address of the switch.

A 1.2 Assigning IP addresses

The IP address is a 32-bit address, which consists of a network part and a user part. The network part consists of the network class and the network address.
There are currently five defined network classes; Classes A, B, and C are used in modern applications, while Classes D and E are hardly ever used. It is therefore usually sufficient if a network device only "recognizes" Classes A, B, and C.

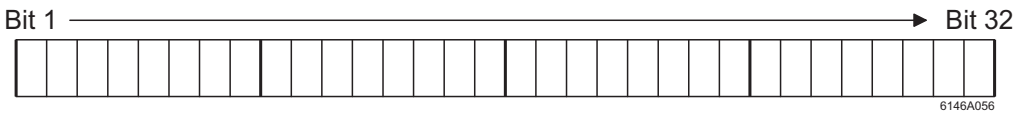


Figure A-1 Position of bits within the IP address

With binary representation of the IP address the network class is represented by the first bits. The key factor is the number of "ones" before the first "zero". The assignment of classes is shown in the following table. The empty cells in the table are not relevant to the network class and are already used for 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 for the network class are followed by those for the network address and the user address. Depending on the network class, a different number of bits are available, both for the network address (network ID) and the user address (host ID).

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

IP addresses can be represented in decimal or hexadecimal form. In decimal notation, bytes are separated by dots (dotted decimal notation) to show the logical grouping of the individual bytes.

The decimal points do not divide the address into a network and user address. Only the value of the first bits (before the first "zero") specifies the network class and thus the number of remaining bits in the address.

Possible address combinations

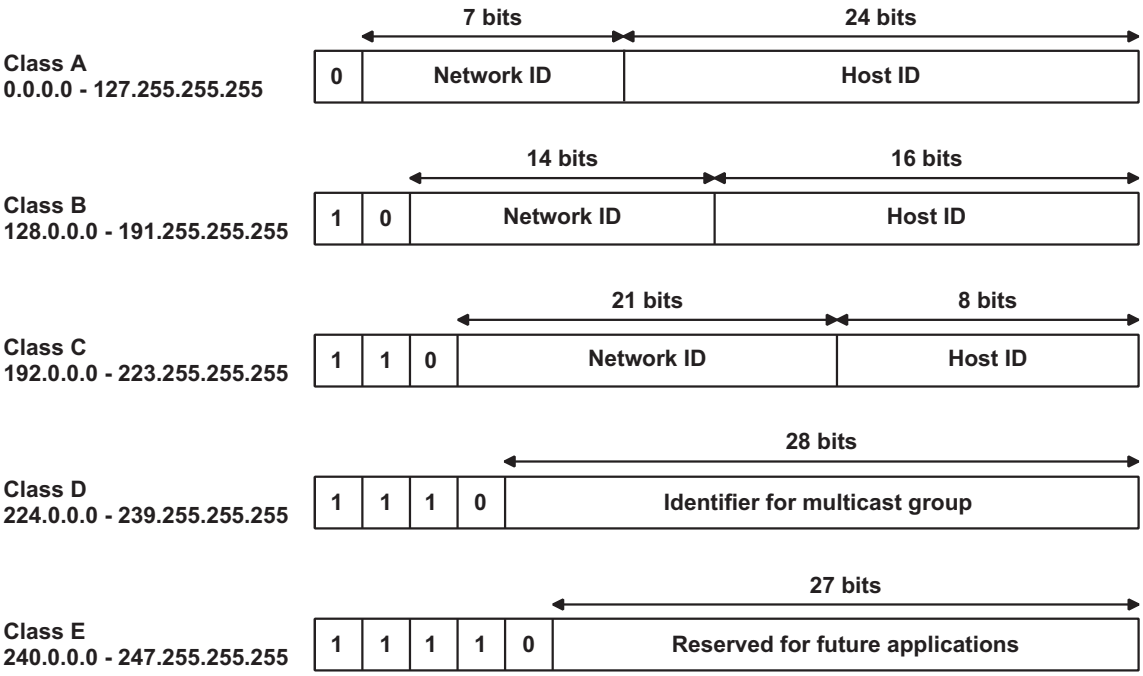


Figure A-2 Structure of IP addresses

A 1.3 Special IP addresses for special applications

Certain IP addresses are reserved for special functions. The following addresses should not be used as standard IP addresses.

127.x.x.x addresses

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

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

Correct installation and configuration of the TCP/IP software, for example, can be checked in this way.

As Layers 1 and 2 of the ISO/OSI reference model are not included in the test they should be tested separately using the ping function.

Value 255 in the byte

Value 255 is defined as a broadcast address. The telegram is sent to all the computers that are in the same part of the network. Examples: 004.255.255.255, 198.2.7.255 or 255.255.255.255 (all the computers in all the networks). If the network is divided into subnetworks, the subnet masks must be observed during calculation, otherwise some devices may be omitted.

0.x.x.x addresses

Value 0 is the ID of the specific network. If the IP address starts with a zero, the receiver is in the same network. Example: 0.2.1.1 refers to device 2.1.1 in this network.

The zero previously signified the broadcast address. If older devices are used, unauthorized broadcast and complete overload of the entire network (broadcast storm) may occur when using IP address 0.x.x.x.

A 1.4 Subnet masks

Routers and gateways divide large networks into several subnetworks. The IP addresses for individual devices are assigned to specific subnetworks by the subnet mask. The **network part** of an IP address is **not** modified by the subnet mask. An extended IP address is generated from the user address and subnet mask. Because the masked subnetwork is only recognized by the local computers, this extended IP address appears as a standard IP address to all the other devices.

Structure of the subnet mask

The subnet mask always contains the same number of bits as an IP address. The subnet mask has the same number of bits (in the same position) set to "one", which is reflected in the IP address for the network class.

Example: An IP address from Class A contains a 1-byte network address and a 3-byte computer address. Therefore, the first byte of the subnet mask may only contain "ones".

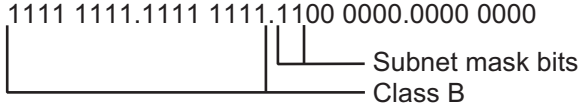
The remaining bits (three bytes) then contain the address of the subnetwork and the computer. The extended IP address is created when the bits of the IP address and the bits of the subnet mask are ANDed. Because the subnetwork is only recognized by local devices, the corresponding IP address appears as a "normal" IP address to all the other devices.

Application

If the ANDing of the address bits gives the local network address and the local subnetwork address, the device is located in the local network. If the ANDing gives a different result, the data telegram is sent to the subnetwork router.

Example for a Class B subnet mask:

Decimal notation:	255.255.192.0
Binary notation:	1111 1111.1111 1111.1100 0000.0000 0000



Using this subnet mask, the TCP/IP protocol software differentiates between the devices that are connected to the local subnetwork and the devices that are located in other subnetworks.

Example: Device 1 wants to establish a connection with device 2 using the above subnet mask. Device 2 has IP address 59.EA.55.32.

IP address representation for device 2:

Hexadecimal notation:	59.EA.55.32
Binary notation:	0101 1001.1110 1010.0101 0101.0011 0010

The individual subnet mask and the IP address for device 2 are then ANDed bit-by-bit by the software to determine whether device 2 is located in the local subnetwork.

ANDing the subnet mask and IP address for device 2:

Subnet mask:		1111 1111.1111 1111.1100 0000.0000 0000
	AND	
IP address:		0101 1001.1110 1010.0101 0101.0011 0010
Result after ANDing:		0101 1001.1110 1010.0100 0000.0000 0000

Subnetwork

After ANDing, the software determines that the relevant subnetwork (01) does not correspond to the local subnetwork (11) and the data telegram is forwarded to a subnetwork router.

A 1.4.1 Examples for subnet masks and number of computer bits

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

A 2 Technical data

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

Serial interfaces	
	According to standard:
V.24 (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	
V.24 (RS-232) RS-422/RS-485	9-pos. D-SUB pin strip Via COMBICON plug-in screw terminal block
Termination network	390 Ω/180 Ω/390 Ω, can be connected internally
Device type	DTE (data terminal equipment)/DCE (data communication equipment), can be set via WBM (web-based management)
Data format/encoding	Serial asynchronous UART/NRZ, 7/8 data, 1/2 stop, 1 parity, 10/11-bit character length
Data flow control	
V.24 (RS-232), RS-422 RS-485	Software handshake, Xon/Xoff or hardware handshake RTS/CTS Automatic control
Serial transmission speed	300, 600, 1200, 2400, 4800, 7000, 9600, 19200, 38400, 57600, 115200, 187500, 230400 bps, can be set via WBM
Supported protocols	Transparent, including 3964R protocol

Ethernet interface according to IEEE 802.3	
Connection	RJ45 female connector, 8-pos., shielded
Shield	DC coupled to DIN rail
Transmission speed	10/100 Mbps, auto negotiation
Transmission length	100 m (twisted pair, shielded)
Supported protocols	TCP/IP, UDP, Modbus/TCP*, TFTP, HTTP, PPP with CHAP authentication*
Secondary protocols	ARP, DHCP, BOOTP, SNMP, RIP, RARP

* Only supported by the FL COMSERVER UNI 232/422/485

Functions	
Configuration and management	Using standard web browser and HTTP protocol
	Using FL SWT Factory Manager software
	Using SNMP objects
	Locally using terminal program via V.24 (RS-232), (emergency access)
	Remotely using Ethernet and Telnet (emergency access)

Functions (continued)	
LED diagnostic indicators	
24 V AC/DC power supply	Green LED, UL, static ON
Ethernet mode	Green LED, full duplex mode active, static ON
Ethernet transmission speed	Green LED, 100 Mbps, static ON
Ethernet link	Green LED (LNK), when link signals are being received, static ON
Ethernet data	Yellow LED (ACT), data transmission via TP port, dynamic
Device error	Red LED, error indicator
V.24 (RS-232)/RS-422/RS-485 receive data	Green LED, RD, receive
V.24 (RS-232)/RS-422/RS-485 transmit data	Yellow LED, TD, transmit
Switching output	Transistor output on the backplane to connect accessories, can be switched via WBM

General data	
CE conformance	EMC directive 2004/108/EC
Approval	UL applied for
Ambient operating temperature range	-25°C ... +60°C
Housing type	ME 22,5 with bus connector and functional earth ground contact (FE)
Housing material	ABS-V0, green
Housing dimensions (H x W x D)	99 mm x 22.5 mm x 114.5 mm
Weight	150 g
Functional earth ground	To EN DIN rail in the housing
Vibration resistance	5g according to DIN EN 60068-2-6, 1.5 h each in x, y, and z direction
Shock test according to IEC 60068-2-27	
Operation Storage	15g, 11 ms, half-sine shock pulse 30g, 11 ms, half-sine shock pulse
Free fall according to IEC 60068-2-32	1 m
Degree of protection	IP20
Separate ground levels	Supply // Ethernet (TP) // V.24 (RS-232), RS-422, RS-485
Test voltage	1.5 kV AC, 50 Hz, 1 min. between all ground levels according to EN 50178 and EN 61131-2
Chloroform test	Free from substances that would hinder coating with paint or varnish according to central standard P-VW-3.10.757 650 of VW, Audi, and Seat

A 2.1 CE conformance

Conformance with EMC Directive 2004/108/EC			
Noise immunity test according to EN 61000-6-2[a]			
Electrostatic discharge (ESD)	EN 61000-4-2	Criterion B[b]	8 kV air discharge 6 kV contact discharge
Electromagnetic HF field	EN 61000-4-3	Criterion A[c]	
Amplitude modulation			10 V/m
Pulse modulation			10 V/m
Fast transients (burst)	EN 61000-4-4		
Signal		Criterion B[b.] Criterion A[c.]	2 kV/5 kHz 1 kV/5 kHz
Supply			2 kV/5 kHz
Surge current load (surge)	EN 61000-4-5	Criterion B[b.]	
Signal			1 kV
Supply			2 kV
Conducted interference	EN 61000-4-6	Criterion A[c.]	10 V
Noise emission test according to EN 61000-6-4			
Noise emission of housing	EN 55022		Limiting curve B

a. EN 61000 corresponds to IEC 61000

b. Criterion B: Temporary adverse effects on the operating behavior, which the device corrects automatically.

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

A 2.2 Block diagram

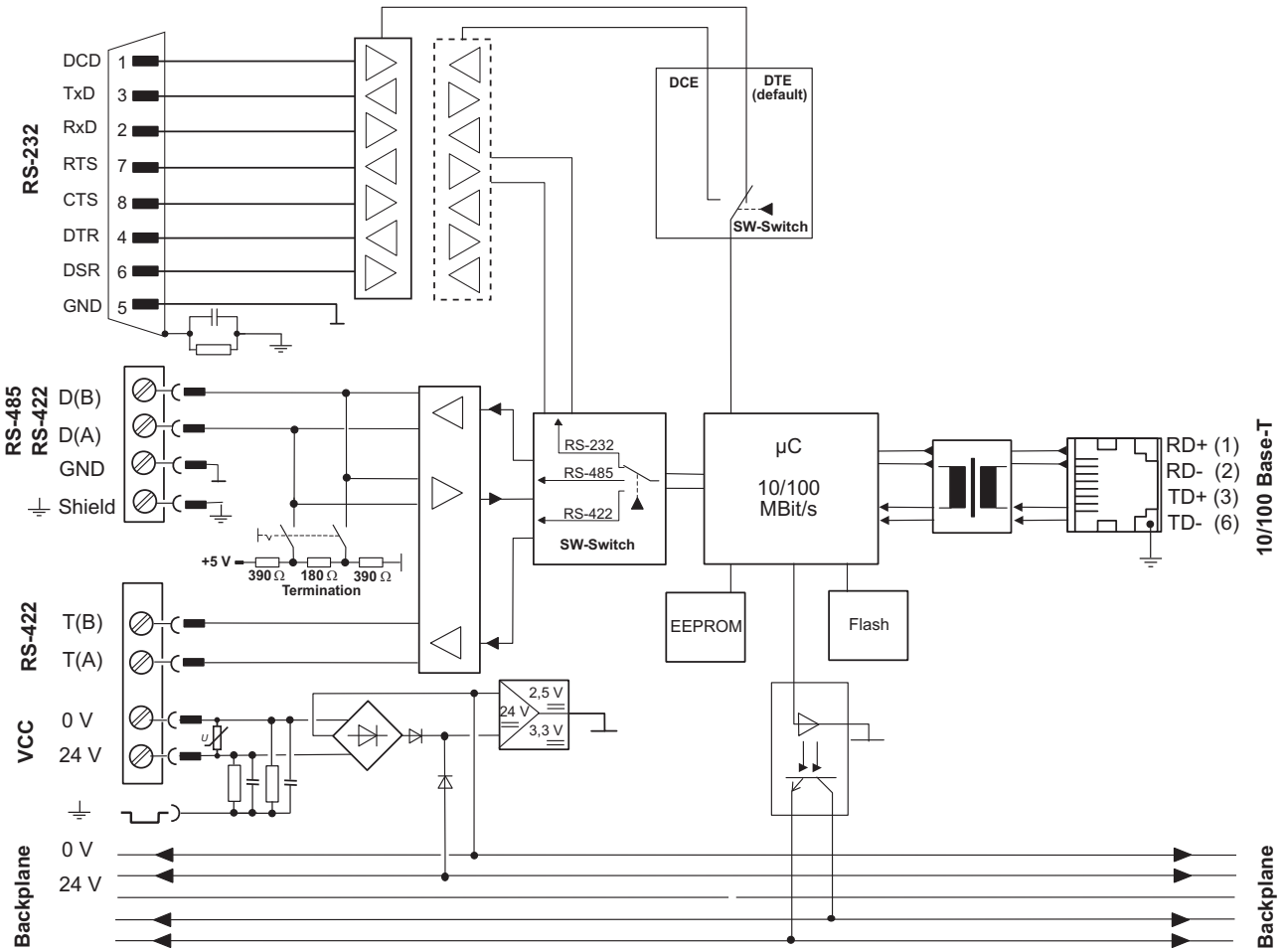


Figure A-1 Block diagram for the FL COMSERVER ... 232/422/485

A 2.3 Dimensions

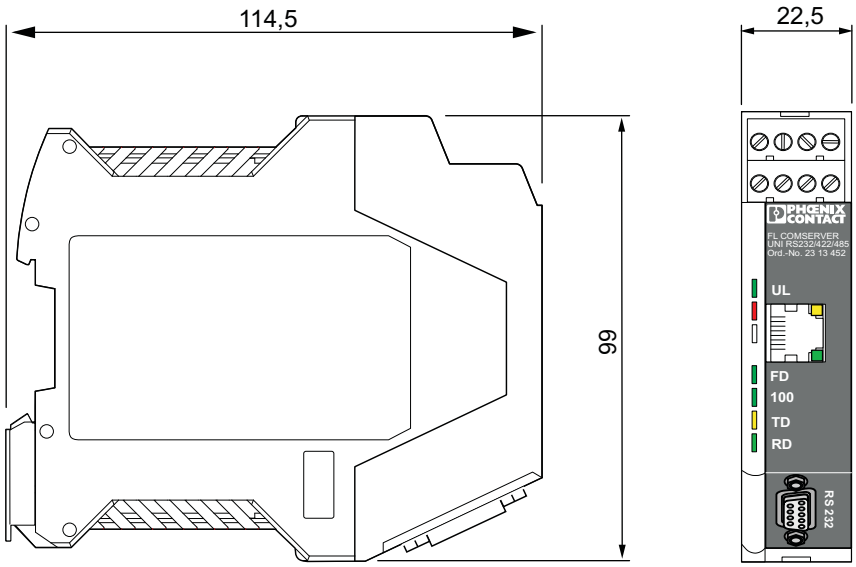


Figure A-2 Dimensions of the FL COMSERVER ... 232/422/485

A 3 Explanation of terms

10Base-FL

Standard which describes the transmission of 10 Mbps Ethernet connections with fiber optic technology. B-FOC connectors and 850 nm wavelengths are required, POF and HCS transmission systems are permitted according to the standard.

10Base-T

In the definition of the 10Base-T standard, the physical topology is separated from the logical topology. The cabling is implemented with at least Category 3 twisted pair cables with an impedance of 100 Ohm in star formation. The transmit and receive data is transmitted separately in one wire pair each. 8-pos. RJ45 connectors are used; the maximum segment expansion is 100 m. A hub is used as the central active component so that cable interrupts or short circuits can only result in the failure of one device and not the entire segment.

100Base-FX

Standard which describes the transmission of 100 Mbps Ethernet connections with fiber optic technology (Fast Ethernet). B-FOC or SC connectors and 1300 nm wavelengths are required, POF and HCS transmission systems are permitted according to the standard.

100Base-TX

Fast Ethernet – 100Base-T has been officially elevated to an IEEE standard as ITU 802.3u. This standard is generally based on technologies for 10Base-T, the Ethernet version for twisted pair cables. There are several recognized versions of 100Base-T, which differ with regard to the Physical Layer and therefore the transmission media: 100Base-TX, 100Base-T2, 100Base-T4, and 100Base-FX. All 100Base-T networks are designed with a star formation and are connected to a central hub. With this method, the MAC level and therefore the conventional CSMA/CD access method are retained at a transmission speed of 100 Mbps. As a result, only very short distances can be covered with 100Base-T and realtime applications cannot be implemented. In the case of Category 5 twisted pair cables (UTP, STP), the maximum segment expansion is 100 m; when using fiber optics it is 400 m.

802.xx

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

A

Address table

The switch automatically stores the MAC address and port number of connected devices in an address table. Data traffic is reduced as the switch only sends telegrams to the port that is assigned to the destination address. After the aging time has elapsed, the entry is deleted from the table.

Administrator

System manager who is responsible for assigning IP parameters and unique IP addresses. In the local network, he/she has unlimited access and management rights for the network.

Aging time

A learnt IP address of a device (source address) is deleted from an address table if no data telegrams are 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.

Alarm contact

Floating switch contact for evaluating device faults.

API

Application **P**rogramming **I**nterface – 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 are often embedded in HTML pages and perform very limited tasks, e.g., execute simple calculations, plot diagrams or evaluate forms. Applets are usually written in Java.

ARP

Address **R**esolution **P**rotocol – ARP is used to determine the MAC address of a network device that belongs to an IP address. The determined assignments are managed on the relevant computer in the ARP table.

ASCII

American **S**tandard **C**ode for **I**nformation **I**nterchange – Encoding for information transmission with a total of 128 characters (= 7-bit ASCII: includes the "basic" alphabet without umlauts and other special characters and control codes) or 256 characters (= 8-bit ASCII). E-mails and attachments, for example, are made up only of ASCII characters.

Attenuation

Measurement of the reduction in signal output on a cable. The unit of attenuation is "dB" (decibel). The lower the dB value, the better the cable.

Auto crossing

A device with auto crossing (DTE or DCE) automatically detects which type of device should be used to establish communication. With this mechanism there is no need to distinguish between line and crossover connecting cables.

Auto negotiation

In auto negotiation mode, an Ethernet device automatically sets itself to the data transmission rate (10 Mbps or 100 Mbps) and the transmission mode (half or full duplex) of the device it is connected to.

Auto sensing

In auto sensing mode, an Ethernet device automatically sets itself to the data transmission rate (10 Mbps or 100 Mbps) of the device it is connected to.

B

Backplane

A system connector that is integrated in the foot. It enables modular stations to be created quickly and easily.

Bandwidth

Difference between the lowest and the highest frequency that is possible on a transmission channel. In digital telecommunications, bandwidth refers to the volume of data that can be transmitted via a transmission channel in a specific period of time. Here, the bandwidth is measured in bps (bits per second).

Bandwidth length product

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

Baud

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

B-FOC connector

Fiber optic connector for multi-mode and single mode fibers. The connector is secured with bayonet locking.

Bit

Binary digi**t** – Smallest information unit in communication technology. A bit can have the value 0 or 1.

BootP

The Bootstrap Protocol is described in RFC 951 (Request for Comments). Manufacturer-specific extensions are detailed in RFC 1084. The Bootstrap Protocol is directly based on the User Datagram Protocol (UDP) in terms of its application. Communication takes place via a single data packet according to the client/server principle. In addition to the server IP

	address, the client can also request the IP address of the next router, the IP address of a specific server or the name of the server's boot file. In the manufacturer-specific part, specially defined information can also be transmitted.
Bridge	A bridge is a device used to connect two separate networks. The incoming data packets are filtered using the destination address and are forwarded to the second network or rejected.
Broadcast	A broadcast is sent to all the devices in the network. Broadcasts are not forwarded via routers and bridges.
Broadcast address	Telegrams to broadcast address 255.255.255.255 are sent to all the devices in the network.
Browser (web browser)	Computer program used to view Internet pages (text, images) on your monitor.
Byte	Data unit that contains 8 bits.
C	
CAT5	EIA/TIA specification for Ethernet cables, connectors, and outlet boxes. Suitable for 10 and 100 Mbps networks, transmission via 2 wire pairs.
CAT5e	Extended CAT5 specification with greater electrical properties. Full duplex mode via 4 wire pairs.
CHAP	**C**hallenge **H**andshake **A**uthentication **P**rotocol – Authentication mechanism where the password is encrypted with 128 bits and is checked both at the start and during connection. In the event of an invalid password when establishing a connection or while the connection is active, the connection is aborted immediately.
Client	A hardware or software component that accepts services from a server. The client is always the service requester (e.g., a browser that calls e-mails via the server).
Collision	A collision occurs when two devices simultaneously attempt to send data on the same medium. A collision is resolved according to the CSMA/CD method.
Collision domain	A collision domain is limited by termination devices and/or switches, and routers. A packet collision can only occur within these limits. The collision domain is often also called the network segment.
COM interface	Name of the serial V.24 (RS-232) interface in a PC.
COM redirector	Software utility used to redirect a software program with V.24 (RS-232) communication to a network card and therefore to TCP/IP communication. The software creates up to 255 virtual COM ports in the operating system.
COM server	Termination device in TCP/IP networks, which provides interfaces for serial devices via the network.
CRC	**C**yclic **R**edundancy **C**heck – Checksum used in data transmission protocols to detect transmission errors in received telegrams.

Crossover cable Cable configuration that connects two devices of the same type (DTE/DTE and DCE/DCE). The connector pin assignment is different at the cable ends so that transmit cables can be connected to receive cables.

CSMA/CD **C**arrier **S**ense - **M**ultiple **A**ccess with **C**ollision **D**etection – Method for dealing with data collisions.

CTS **C**lear **T**o **S**end in the hardware handshake, signal of the V.24 (RS-232) interface.

D

Data packet Associated data that is sent via computer networks bundled together. The files are not sent as a continuous data flow (streaming), but are divided into small units (packets) and transmitted individually. Each packet has a header (information about the source and destination address, error check) and is formatted in a size suitable for forwarding (routing). The information in the header does not determine a specific path for the individual servers (routers) in which the packets appear. The path the packets take is always decided individually by the routers. This decision is based on the following criteria: the shortest and most efficient or quickest path (depending on the load of the transmission cables). Once all the data packets arrive at the destination, they are put back together again at the receiver to form the original file. The protocol typically used to send data on the Internet is TCP/IP.

dB Abbreviation for "**d**eci**b**el", see dBm.

dBm Power value standardized to 1 mW for easy addition and subtraction when budgeting a fiber optic path; see dB.

DCE **D**ata **C**ommunications **E**quipment – 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. Direct connection of two DCE devices can only be implemented using crossed cables.

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

DHCP **D**ynamic **H**ost **C**onfiguration **P**rotocol – Automatic, dynamic, and usually temporary assignment of IP addresses from a defined address area.

Dial-up network Under Microsoft Windows, the dial-up network forms a link between Internet applications and the modem or ISDN card. An Internet connection can be established via the dial-up network.

DTE **D**ata **T**erminal **E**quipment – Termination devices that are always installed at the start 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. Direct connection of two DTE devices can only be implemented using crossed cables.

E

Ethernet Network standard developed by Intel, DEC, and Xerox, which has been widely used, especially in LANs, since 1976. The Ethernet standard contains specifications on the network architecture (bus or star topology), hardware (e.g., cabling with coaxial or twisted pair cables), transmission and access methods.

Ethernet address See MAC address

F

Fast Ethernet Fast Ethernet is operated using Category 5 copper cables or fiber optics, the data transmission rate is 100 Mbps.

File Transfer Protocol See FTP

Firewall Special computer used in company computer networks that enables employees to access the Internet, but blocks external unauthorized access. Firewall programs are also available for privately used computers.

Firmware Internal software that runs on the relevant devices and thus enables the devices to operate.

FL standard See 10Base-FL

Flash ROM See ROM

Flow control Method that controls data flow between two devices; it prevents data being lost when a device buffer is full.

FO **F**iber **O**ptics

FO port Fiber optic connection.

F-SMA connector Fiber optic connector for POF and HCS fibers, secured with a cap nut, easy connection thanks to fast connection technology.

FTP The File Transfer Protocol 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 into the server, an access ID and corresponding password must be entered. By default upon delivery the password for read-only access is "public" and the password for read/write access is "private".

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

FX standard See 100Base-FX

G

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

Gateway address See Standard gateway

H

Half duplex In half duplex mode, transmission is possible in one direction or in the other direction, but not both simultaneously.

Half duplex port A half duplex port can only send and receive data at different times, while a full duplex port can send and receive data simultaneously.

Hardware handshake Handshake via signal lines. For V.24 (RS-232) usually indicated with CTS/RTS or DTR/DSR.

See CTS, RTS, DTR, DSR

HCS Hard Clad Silica – Fiber optic mixed fiber, glass core + plastic sheath, 200/230 µm diameter, easy to assemble with fast connection connector.

Header The start of a data packet is referred to as the header. It contains information about the packet size and the sender and recipient address.

HTML Hypertext Markup Language – HTML is not a programming language, but a standardized page description language for web pages. So that HTML documents can be displayed by all popular computers, operating systems, and browsers, they only contain ASCII text. "Formatting" and "commands" are placed in angular brackets so that the browser can distinguish them from the actual content. The HTML standard was introduced by the World Wide Web Consortium (W3C) in Geneva, Switzerland.

HTTP Hypertext Transfer Protocol – Protocol (transmission standard) that controls the exchange of data between a web server and a web client. HTTP is based on TCP/IP.

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

I

IEEE The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers defines standards. The Ethernet system is described in IEEE 802.xx, where xx stands for the various parts of the standard.

Interface Defined limit between two hardware components, two software components or between hardware and software components, which separates the technical functions and/or administrative responsibilities of technical devices. Examples of interfaces include the transitions from computers to data transmission devices or between communication devices.

Internet The Internet is the world's largest network, which can be used in conjunction with TCP/IP platform-independent services such as e-mail, TFTP, HTTP, etc.

Internet Explorer Internet Explorer is the browser from Microsoft.

Intranet A closed network within which typical Internet services can be used.

IP **I**nternet **P**rotocol – Enables the connection of devices that are located in different networks.

IP address An IP address is a unique device address in Ethernet. It is a numerical code made up of four numbers between 0 and 255 separated by dots (dotted decimal notation). The IP address is assigned by the network administrator.

J

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

Java Java was developed by Sun Microsystems. This object-oriented, platform-independent programming language was designed specifically for the Internet. Java is integrated into web pages using Java applets (small application modules) or JavaBeans (Java

programming blocks). The Java Virtual Machine is required in order to execute Java programs. In order for your Internet browser to use Java, it must be activated (usually already set by default).

Java applet

Small program written in Java, which is downloaded from the Internet and interpreted and executed in the user's Java-compatible browser. Java commands are integrated into HTML pages and implemented when the page is downloaded. Java applets run in a "sandbox", the Java Virtual Machine (JVM), and thus do not have access to local resources on the computer. From time to time errors occur in the implementation of the JVM, which means that Java applets can in fact access local files. Therefore you should only allow Java when calling "trusted" sites, e.g., www.t-online.de.

JavaScript

JavaScript is a script language (not a programming language) developed by Netscape, which is used to make web pages dynamic or interactive. JavaScript is integrated directly in the HTML code and is interpreted via the browser. However, there is no "sandbox" to prevent access to files and programs on the computer running JavaScript. The Microsoft-specific version of JavaScript is called JScript. In order for your Internet browser to use Java, it must be activated (usually already set 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 implemented when the page is downloaded. Java programs (Java applets) run in the closed environment of the JVM, which usually does not allow access to local resources on the computer. The JVM is also known as a "sandbox". From time to time errors occur in the implementation of the JVM, which means that Java applets can in fact access local files.

L

LAN

Local **A**rea **N**etwork – Network of computers, which share applications, data, printers, and other services. The physical expansion is limited to a local area, i.e., a building or a group of buildings.

Line (1:1) cable

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

Link status

The device sends regular link status pulses to the ports of connected partner devices to monitor the validity of the connection with these partner devices. A valid connection is indicated by a green LED.

M

MAC address

Globally unique ID for a network component that comprises eight bytes and a manufacturer ID.

Manchester code

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

Master/slave network

A group of several communication devices. A master in the system controls all communication in the network. The master is always involved in communication. Slave/slave communication can only be established by using the master as a relay station.
See Multi-master network

MDI	**M**edia **D**ependant **I**nterface – Ethernet connection, which can be connected directly to other infrastructure components without the need for special crossover cables. These connections are often referred to as "uplinks".
MDI-X	**M**edia **D**ependent **I**nterface **Cross**over – Ethernet connection, which can be connected directly to termination devices such as PCs or PLCs.
Media converter	Converter from wired Ethernet to fiber optic technology.
MIB	**M**anagement **I**nformation **B**ase – Database which contains all the data (objects and variables) required for network management via SNMP.
Modem	Derived from the term "**mo**dulator/**dem**odulator", which indicates the function of a modem: converting analog signals into digital data and vice versa. A modem can be used to connect your computer to the Internet.
Mono-mode	See Single mode
Multicast address	Telegrams with a multicast address can be received by several devices, which are ready to receive for this address.
Multi-master network	A group of several communication devices. All devices have the same rights to establish, maintain, and terminate communication. In principle, every device can communicate directly with every other device.
Multi-mode	Large-core fiber optic cable, which can hold several modes; see also Single mode.
N	
Network	A group of computers, which share files, data, and resources.
Network address	See MAC address
Network management	Network management is carried out by the administrator using software (e.g., Factory Manager from Phoenix Contact). The network can be configured, optimized, and monitored. In the event of an error, the cause can be determined.
Network spy	Function which searches specific IP address areas for active devices. You can specify the start and stop IP address of the area to be searched.
NIC	**N**etwork **I**nterface **C**ard – Adapter card, which is integrated in a PC and provides the necessary software/hardware for communication via an Ethernet network.
NRZ	**N**on **R**eturn to **Z**ero – Describes the data code in which there is no edge change if multiple bits of the same type are transmitted in sequence. See Manchester code
O	
OSI	**O**pen **S**ystem **I**nterconnect

P

Packet	Group of bits, which contain data, monitoring information, source and destination address, and are secure for data transmission.
PAP	**P**assword **A**uthentication **P**rotocol – Authentication mechanism for a PPP connection. The password is not encrypted, i.e., it is sent to the communication partner in plain text for checking. The password is checked once during connection establishment. A password error during connection establishment leads to an immediate connection abort.
Parity	Bit in asynchronous data transmission, which 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 when the number of bits of data is an even number. Similarly, with odd parity it is set for an odd number.
Peer-to-peer connection	Communication where both partners are equally responsible for initiating, maintaining, and terminating the session. P2P (peer-to-peer) networks are an option for serial cabling via the network.
Permanent line	Special telephone or other telecommunications line in which the connection is permanently active. This means there is no need to establish a connection before exchanging data. These lines are used, for example, by companies to communicate with their branches or for a connection to an Internet Service Provider.
Ping	**P**acket **In**ternet **G**roper – A ping is used to measure the reliability of a network connection and the response time of a server. A client contacts a server at its ping port. As soon as the server responds, the client calculates the elapsed time in milliseconds. The function also determines whether pings (small data packets) are lost. To achieve realistic results, pings with different byte sizes can be sent (Factory Manager supports sizes from 1 to 32 bytes).
POF	**P**olymer **O**ptical **F**iber, see Polymer fiber.
Point-to-point connection	Communication between only two devices on a cable, see also Master/slave network and Multi-master network.
Polymer fiber	Optical fiber made from 100% plastic, easy assembly with F-SMA fast connection connectors, 980/1000 µm diameter.
Port (I)	Interface for data transfer to a PC. The Internet address and the associated port are required to access an Internet service. Some defined services have fixed port numbers, e.g., port 80 for web servers or port 21 for FTP servers.
Port (II)	Ethernet interface (fiber optic or copper) of Factory Line devices.
PPP	**P**oint-to-**P**oint-**P**rotocol – Successor to the SLIP protocol. Enables data transmission via permanent and dial-up line connections in analog and digital fixed-line and mobile phone networks. Used when the PC is connected to the Internet via telephone lines.
PPPoE	Point-to-Point Protocol over Ethernet
PROM	**P**rogrammable **ROM** – Read-Only Memory, the contents of which can be modified.
Protocol	Convention for data exchange between computers in a network. Protocols specify the structure, configuration, and encoding of data packets.

Q

R

RARP — **R**everse **A**ddress **R**esolution **P**rotocol – Indicates the IP address assigned to a specific MAC address.

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

RFC — **R**equest **F**or **C**omments – Standardization document from the Internet research and development group, e.g., for the definition of protocols or services.

RIP — **R**outing **I**nformation **P**rotocol – Protocol for the exchange of routing information between routers.

RJ45 — The most commonly used connector for Ethernet and ISDN connections. Often also referred to as a Western connector.

ROM — **R**ead-**O**nly **M**emory – Memory that stores data permanently (even in the event of a voltage failure). An extension is the Flash ROM, which can be rewritten by the user. This enables firmware to be updated.

Router — Routers connect different networks together. The IP address is used to determine which network an IP packet should be forwarded to.

RTS — **R**equest **T**o **S**end – In the hardware handshake, signal of the V.24 (RS-232) interface.

RTS/CTS control — See Hardware handshake

S

SC duplex connector — Plastic fiber optic connector (which can usually be divided) for multi-mode and single mode fibers. The connector is locked to transmit/receive components using a push/pull mechanism.

Serial transmission — Data transmission method in which the bits of a data character are transmitted sequentially via a single data channel.

Server — In terms of hardware, this is a computer in a network, which provides services to other devices. In terms of software, this is a program on a server computer, which provides specific services.

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

See Client/server principle

Single mode — Fiber optic cable in which only a single mode can propagate for the operating wavelength of the fiber optic cable. The core diameter is around 9 µm for a wavelength of 1300 nm.

SLIP — **S**erial **L**ine **I**nternet **P**rotocol – An old protocol for establishing a TCP/IP connection via serial connections. Has been replaced by PPP.

SNMP

Simple **N**etwork **M**anagement **P**rotocol – Manufacturer-independent standard for Ethernet management.

Socket

Refers to the combination of the IP address and the communication port, which ensures a unique connection assignment.

Software handshake

Handshake using specified characters. Not suitable for binary transmissions without transmission protocol because the data could also contain reserved handshake characters. The most common characters are XON/XOFF.

See XON, XOFF

Source code

Program code that is not compiled or assembled.

Spanning Tree

The Spanning Tree algorithm is a method for suppressing loops in (redundant) connected networks. The physically redundant network structures are determined and a loop-free structure is created by disconnecting specific ports. This measure reduces the active connection paths in any meshed structure. The resulting tree structure has two key features:

– All networked points (ports) are only connected together by a single path.
– All networked points can be reached from all other networked points.

The algorithm is implemented in the relevant devices, and each switch uses defined quality criteria to calculate the path to the root switch. Possible quality criteria include distance, capacitance, cost, load, etc.

Start bit

Bit used in asynchronous transmission, which indicates the start of a data word. Always logic "0".

ST connector

See B-FOC connector, registered trademark of AT&T

Stop bit

One or two bits in asynchronous transmission, which indicate the end of a data word. Always logic "1".

STP

Shielded **T**wisted **P**air – Shielded data cable in which the relevant data wires are twisted together.

Subnet mask

The subnet mask specifies 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 is the IP address of the subnetwork. The IP address is 207.142.2.1, which means the subnet address is 207.0.0.0 and the device address is 142.2.1.

Switch

LAN switches are used in local networks. They connect areas of the network, which for example operate at different speeds (10 or 100 Mbps) or keep areas with very large volumes of traffic (data flow over time) separate from other areas of the network. The switch can determine the area of the network to which data packets are addressed and only forwards them to another segment if required. This increases the useful total bandwidth of the network.

Synchronous connection

Connection in which a clock signal is transmitted with the user data, which means that the start and stop bits used in an asynchronous connection are not required. Transmission is therefore faster.

System reserve

Optical safety reserve. In order to provide long-term compensation for the technical aging of transmitter diodes, this must be taken into account when configuring fiber optic paths (typically 3 dB).

T

TCP/IP
Transmission **C**ontrol **P**rotocol – TCP uses IP and ensures that data is correct and data packets are transmitted in the right order.

TCP/IP stack
Part of the operating system or a driver, which provides all the drivers and functions required to support the IP protocol.

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

Telnet
Termina**l** over **Net**work – Standard protocol which is used to establish an interactive connection to other devices via Ethernet. Telnet uses TCP/IP as its transmission and data link protocol.

Terminal program
Simple communication program for the transmission of ASCII and binary data. Implemented as standard in PC operating systems, e.g., Windows HyperTerminal.

Termination resistor
A termination resistor (terminator) is not required with 10Base-T/100Base-TX. With 10Base-5 or 10Base-2 coaxial network topologies, 50 Ohm termination resistors are required.

Terminator
A termination resistor (terminator) is not required with 10Base-T/100Base-TX. With 10Base-5 or 10Base-2 coaxial network topologies, 50 Ohm termination resistors are required.

TFTP
Trivial **F**ile **T**ransfer **P**rotocol – The protocol is suitable for the transmission of entire files. It uses a minimum number of commands and UDP as the transmission protocol.

TFTP server
Server from which Factory Line components can download new firmware/configurations via TFTP.

Topology
The topology refers to the physical positions and connections of network devices. A distinction is made between ring, bus, star or tree topologies.

TP
See Twisted pair

Trap
Traps are SNMP alarm and event messages, which are transmitted with maximum priority to various addresses (if required) and can then be displayed by the management station in plain text.

Trap targets
Trap targets are the targets, which evaluate traps (alarm or event messages).

Twisted pair
Data cable in which pairs of data wires are twisted together. Twisting the forward and return lines greatly reduces the crosstalk ratio. A distinction is made between STP (Shielded Twisted Pair) and UTP (Unshielded Twisted Pair).

U

UART
Universal **A**synchronous **R**eceiver and **T**ransmitter – Integrated circuit, which converts between serial and parallel signals. It offers transmission clocking and stores data in a buffer, which is sent to or from a computer.

UDP

User **D**atagram **P**rotocol – UDP is a connectionless protocol, which is based on IP but does not use any security measures. UDP supports higher speeds for data transmission.

UTP

Unshielded Twisted Pair – Unshielded data cable with twisted wire pairs.

V

V.24 (RS-232) interface

The V.24 (RS-232) interface is defined in the American standard EIA-232 and in the international standard CCITT V.24. This serial interface carries out data exchange between two devices in full duplex mode (point-to-point connection). The maximum transmission speed is 115.2 kbps, and the maximum transmission length is 15 m.

See DCE, DTE

W

WAN

Wide **A**rea **N**etwork – A network which uses conventional transmission mechanisms. The network extends over a large geographical area such as a country or continent.

WBM

Web-based management – In WBM, HTML pages for device diagnostics and configuration are loaded to the web browser.

WINSOCK

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

X

XON/XOFF

Name of the start and stop bits in software handshake mode for a V.24 (RS-232) connection.

Y

Z

B Appendix

B 1 List of Figures

Section 2

Section 3

Section 4

Section 5

Section 6

B 2 List of Tables

Section 1

Section 2

Section 4

C Help and support

C 1 Hotline

Should problems occur that cannot be resolved with the help of this documentation, please contact our hotline:


+49 - 52 81 - 94 62 88 8


factoryline-service@phoenixcontact.com

SCATTERGOOD & JOHNSON LTD
ELECTRICAL ENGINEERING & FLUID CONTROL DISTRIBUTORS
Est.1899

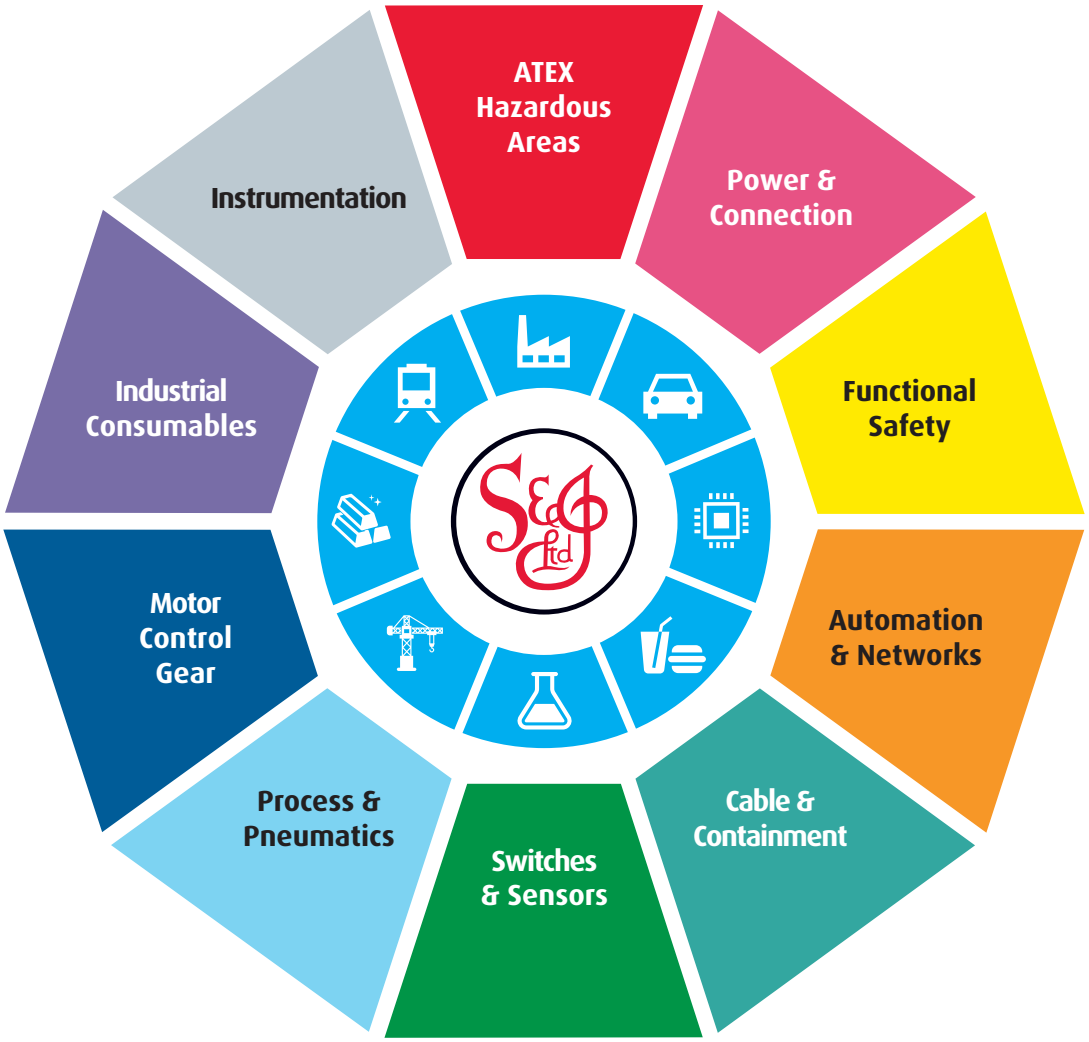
At Scattergood & Johnson Ltd, we pride ourselves on being a technical distributor to specialist industries.

Working with a range of quality product suppliers across a number of specialist markets, we are not your average 'box shifter' - we are your technical and supply chain partner.

We fully support every product we sell - for free! Our internal team and external sales engineers can answer any product or application question, no matter the complexity.

Backing up this technical ability is a range of 50,000+ products available from stock for nationwide next day delivery (same day if required!), or you can collect what you need from any of our trade counters around the UK.

Select your specialist interest below to learn more about how we can help.



Online, In Branch and On the Road - Scattergood & Johnson Ltd, there when you need us.

www.scatts.co.uk