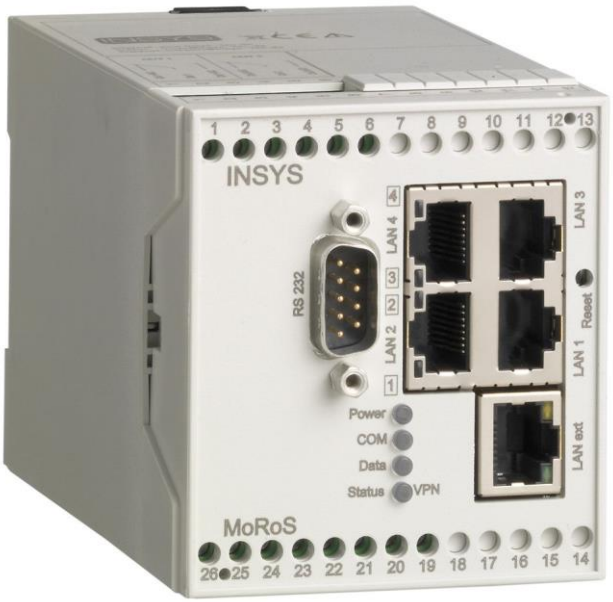
Manual

INSYS icom

Industrial Data Communication

MoRoS LAN



Trademarks

The use of a trademark not shown below is not an indication that it is freely available for use.

MNP is a registered trademark of Microcom Inc.

IBM PC, AT, XT are registered trademarks of International Business Machine Corporation.

INSYS®, VCom®, e-Mobility LSG® and e-Mobility PLC® are registered trademarks of INSYS MICROELECTRONICS GmbH.

Windows™ is a registered trademark of Microsoft Corporation.

Linux is a registered trademark of Linus Torvalds.

Publisher:
INSYS MICROELECTRONICS GmbH
Hermann-Köhl-Str. 22
D-93049 Regensburg, Germany
Phone: +49 941 58692 0
Fax: +49 941 58692 45
E-mail: info@insys-icom.com
Internet: http://www.insys-icom.com

Date: Jun-17
Item: 31-22-03.164
Version: 1.13
Language: EN

1 Preface

This manual allows for the safe and efficient use of the product. The manual is part of the product and must always be stored accessible for installation, commissioning and operating personnel.

1.1 Defects Liability Terms

A usage not according to the intended purpose, an ignorance of this documentation, the use of insufficiently qualified personnel as well as unauthorised modifications exclude the liability of the manufacturer for damages resulting from this. The liability of the manufacturer ceases to exist.

The regulations of our Delivery and Purchasing Conditions are effective. These can be found on our website (www.insys-icom.de/imprint/) under “General Terms and Conditions“.

1.2 Feedback

We are permanently improving our products and the associated technical documentation. Your feedback is very helpful for this. Please tell us what you like in particular on our products and publications and what can be improved from your point of view. We highly appreciate your suggestions and will include them in our work to support you and all our customers. We are looking forward to any of your feedback.

Please send an e-mail to support@insys-tec.de.

We'd like to know your applications. Please send us a few headwords that we know the applications you solve using products of INSYS icom.

1.3 Marking of Warnings and Notes

Symbols and Key Words

Danger!

Risk of severe or fatal injury

One of these symbols in conjunction with the key word Danger indicates an imminent danger. It will cause death or severe injuries if not avoided.

Warning!

Personal injury

This symbol in conjunction with the key word Warning indicates a possibly hazardous situation. It might cause death or severe injuries if not avoided.

Caution!

Slight injury and / or material damage

This symbol in conjunction with the key word Caution indicates a possibly hazardous or harmful situation. It might cause slight or minor injuries or a damage of the product or something in its vicinity if not avoided.

Note

Improvement of the application

This symbol in conjunction with the key word Note indicates hints for the user or very useful information. This information helps with installation, set-up and operation of the product to ensure a fault-free operation.

1.4 Symbols and the Formatting in this Manual

This section describes the definition, formatting and symbols used in this manual. The various symbols are meant to help you read and find the information relevant to you. The following text is structured like a typical operating instruction of this manual.

Bold print: This will tell you what the following steps will result in

After that, there will be a detailed explanation why you could perform the following steps to be able to reach the objective indicated first. You can decide whether the section is relevant for you or not.

⇢ An arrow will indicate prerequisites which must be fulfilled to be able to process the subsequent steps in a meaningful way. You will also learn which software or which equipment you will need.

1. ***One individual action step: This tells you what you need to do at this point. The steps are numbered for better orientation.***

   ✓ A result which you will receive after performing a step will be marked with a check mark. At this point, you can check if the previous steps were successful.

   ⓘ Additional information which you should consider are marked with a circled "i". At this point, we will indicate possible error sources and tell you how to avoid them.

   ➢ *Alternative results and steps are marked with an arrow. This will tell you how to reach the same results performing different steps, or what you could do if you didn't reach the expected results at this point.*

2 Safety

The Safety section provides an overview about the safety instructions, which must be observed for the operation of the product.

The product is constructed according to the currently valid state-of-the-art technology and reliable in operation. It has been checked and left the factory in flawless condition concerning safety. In order to maintain this condition during the service life, the instructions of the valid publications and certificates must be observed and followed.

It is necessary to adhere to the general safety instructions must when operating the product. The descriptions of processes and operation procedures are provided with precise safety instructions in the respective sections in addition to the general safety instructions.

Moreover, the local accident prevention regulations and general safety regulations for the operating conditions of the device are effective.

An optimum protection of the personnel and the environment from hazards as well as a safe and fault-free operation of the product is only possible if all safety instructions are observed.

2.1 Intended Use

The product may only be used for the purposes specified in the function overview. In addition, it may be used for the following purposes:

- Usage and mounting in an industrial cabinet.
- Switching and data transmission functions in machines according to the machine directive 2006/42/EC.
- Usage as data transmission device for a PLC.

The product may not be used for the following purposes and used or operated under the following conditions:

- Controlling or switching of machines and systems, which do not comply with the directive 2006/42/EC.
- Usage, controlling, switching and data transmission of machines and systems, which are operated in explosive atmospheres.
- Controlling, switching and data transmission of machines, which may involve risks to life and limb due to their functions or when a breakdown occurs.

2.2 Permissible Technical Limits

The product is only intended for the use within the permissible technical limits specified in the data sheets.

The following permissible limits must be observed:

- The ambient temperature limits must not be fallen below or exceeded.
- The supply voltage range must not be fallen below or exceeded.
- The maximum humidity must not be exceeded and condensate formation must be prevented.
- The maximum switching voltage and the maximum switching current load must not be exceeded.
- The maximum input voltage and the maximum input current must not be exceeded.

2.3 Responsibilities of the Operator

As a matter of principle, the operator must observe the legal regulations, which are valid in his country, concerning operation, functional test, repair and maintenance of electrical devices.

2.4 Qualification of the Personnel

The installation, commissioning and maintenance of the product must only be performed by trained expert personnel, which has been authorised by the plant operator. The expert personnel must have read and understood this documentation and observe the instructions.

Electrical connection and commissioning must only be performed by a person, who is able to work on electrical installations and identify and avoid possible hazards independently, based on professional training, knowledge and experience as well as knowledge of the relevant standards and regulations.

2.5 Instructions for Transport and Storage

The following instructions must be observed:

- Do not expose the product to moisture and other potential hazardous environmental conditions (radiation, gases, etc.) during transport and storage. Pack product accordingly.
- Pack product sufficiently to protect it against shocks during transport and storage, e.g. using air-cushioned packing material.

Check product for possible damages, which might have been caused by improper transport, before installation. Transport damages must be noted down to the shipping documents. All claims or damages must be filed immediately and before installation against the carrier or party responsible for the storage.

2.6 Markings on the Product

The identification plate of the product is either a print or a label on a face of the product. Amongst other things, it can contain the following markings, which are explained in detail here.

Observe manual

This symbol indicates that the manual of the product contains essential safety instructions that must be followed implicitly.

Dispose waste electronic equipment environmentally compatible

This symbol indicates that waste electronic equipment must be disposed separately from residual waste via appropriate collecting points. See also Section Disposal in this manual.

CE marking

By applying a CE marking, the manufacturer confirms that the product complies with the European directives that apply product-specific.

UL marking

By applying a UL marking, the manufacturer confirms that the product complies with the obligatory safety requirements.

Appliance Class II - double insulated

This symbol indicates that the product complies with Appliance Class II

2.7 Environmental Protection

Dispose the product and the packaging according to the relevant environmental protection regulations. The Waste Disposal section in this manual contains notes about disposing the product. Separate the packaging components of cardboard and paper as well as plastic and deliver them to the respective collection systems for recycling.

2.8 Safety Instructions for Electrical Installation

The electrical connection must only be made by authorised expert personnel according to the wiring diagrams.

The notes to the electrical connection in the manual must be observed. Otherwise, the protection category might be affected.

The safe disconnection of circuits, which are hazardous when touched, is only ensured if the connected devices meet the requirements of VDE T.101 (Basic requirements for safe disconnection).

The supply lines are to be routed apart from circuits, which are hazardous when touched, or isolated additionally for a safe disconnection.

An easily accessible isolation device that disconnects all lines must be installed prior to commissioning of the device to be able to isolate it completely from power supply.

2.9 General Safety Instructions

Caution!

Moisture and liquids from the environment may seep into the interior of the product!

Fire hazard and damage of the product.

The product must not be used in wet or damp environments, or in the direct vicinity of water. Install the product at a dry location, protected from water spray. Disconnect the power supply before you perform any work on a device which may have been in contact with moisture.

Caution!

Short circuits and damage due to improper repairs and modifications as well as opening of maintenance areas.

Fire hazard and damage of the product.

It is not permitted to open the product for repair or modification.

Caution!

Overcurrent of the device supply!

Fire hazard and damage of the product due to overcurrent.

The product must be secured with a suitable fuse against currents exceeding 1.6 A.

Caution!

Overvoltage and voltage peaks from the mains supply!

Fire hazard and damage of the product due to overvoltage.

Install suitable overvoltage protection.

Caution!

Damage due to chemicals!

Ketones and chlorinated hydrocarbons dissolve the plastic housing and damage the surface of the device.

Never let the device come into contact with ketones (e.g. acetone) or chlorinated hydrocarbons, such as dichloromethane.

3 Using Open Source Software

3.1 General Information

Our product MoRoS LAN contains, amongst others, so-called open-source software that is provided by third parties and has been published for free public use. The open-source software is subject to special open-source software licenses and the copyright of third parties. Basically, each customer can use the open-source software freely in compliance with the licensing terms of the respective producers. The rights of the customer to use the open-source software beyond the purpose of our product are regulated in detail by the respective concerned open-source software licenses. The customer use the open-source software freely, as provided in the respective effective license, beyond the purpose that the open-source software gets in our product. In case there is a contradiction between the licensing terms for our product and the respective open-source software license, the respective relevant open-source software license takes priority over our licensing terms, as far as the respective open-source software is concerned by this.

The use of the used open-source software is possible free of charge. We do not demand usage fees or any comparable fees for the use of the open-source software contained in our product. The use of the open-source software in our product by the customer is not part of the earnings we achieve with the contractual compensation.

All open-source software programs contained in our product can be taken from the available list. The most important open-source software licenses are listed in the Licenses section at the end of this publication.

As far as programs contained in our product are subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Clarified Artistic License or another open-source software license, which regulates that the source code must be made available, and if this software is not already delivered in source code on a data carrier with our product, we will send you this at any time upon request. If it is required to send this on a data carrier, the sending will be made against payment of a cost compensation of € 10,00. Our offer to send the source code upon request ceases automatically 3 years after delivery of our product to the customer. Requests must be directed to the following address, if possible under specification of the serial number:

INSYS MICROELECTRONICS GmbH

Hermann-Köhl-Str. 22

93049 Regensburg, Germany

Phone +49 941 58692 0

Fax +49 941 58692 45

E-mail: support@insys-icom.de

3.2 Special Liability Regulations

We do not assume any warranty or liability, if the open-source software programs contained in our product are used by the customer in a manner that does not comply any more with the purpose of the contract, which is the basis of the acquisition of our product. This concerns in particular any use of the open-source software programs outside of our product. The warranty and liability regulations that are provided by the respective effective open-source software license for the respective open-source software as listed in the following are effective for the use of the open-source software beyond the purpose of the contract. In particular, we are not liable, if the open-source software in our product or the complete software configuration in our product is changed. The warranty granted with the contract, which is the basis of the acquisition of our product, is only effective for the unchanged open-source software and the unchanged software configuration in our product.

3.3 Used Open-Source Software

Please contact our support department (support@insys-icom.de) for a list of the open-source software used in this product.

4 Device variants

This manual describes different versions of the MoRoS LAN. The router will feature increased RAM memory from version 2.2, which is of advantage for complex sandbox applications in particular. These devices are referred to as MoRoS LAN in the manual. The devices are:

- MoRoS LAN 2.1 PRO
- MoRoS LAN 2.2 PRO

If the devices are different, this will be mentioned explicitly in the respective sections.

Manuals for earlier versions of the MoRoS LAN are still available on our download page under http://www.insys-icom.com/manual/#moros.

5 Scope of Delivery

The scope of delivery includes all accessories listed below. Please check if all accessories are included in the box. If a part is missing or damaged, please contact your distributor.

- 1 MoRoS LAN
- 1 Quick Installation Guide
- 1 Monitoring App

The scope of delivery does not include optional accessories. The following parts are available from your distributor or INSYS icom:

- DIN rail power supplies
- Monitoring packages for monitoring external devices

The following related documents can be found in the download area and on the product page of the MoRoS LAN under www.insys-icom.com:

- Add-On Manual ASCII Configuration File
- Add-On Manual Automatic Update
- Add-On Manual CLI
- Add-On Manual Monitoring App

6 Technical Data

6.1 Physical Features

All specified data was measured with nominal input voltage, at full load, and an ambient temperature of 25 °C. The limit value tolerances are subject to the usual variations.

Physical Feature	Value
Operating voltage	10 V … 60 V DC (±0%)
Power consumption idle	approx. 2 W
Power consumption connection	max. 3 W
Level inputs	HIGH level = 3-12 V (contact open or voltage strength for external supply) LOW level = 0-1 V
Current consumption of an active input against GND (internal +5V)	Typically 0.5 mA (when enabling the input by connecting to GND)
Switch output, maximum switch voltage	30 V (DC) / 42 V (AC)
Switch output, maximum current load	1 A (DC) / 0.5 A (AC)
Weight	280 g
Dimensions (Width x Depth x Height)	70 mm x 110 mm 75 mm
Temperature range	-30 °C … 70 °C (max. 85 °C, s. below)
Maximum permissible humidity	95% non-condensing
IP rating	Housing IP40, Terminals IP20

Table 1: Physical Features

ⓘ Max. specification applies to occasional data transmission and use of no more than 2 LAN ports. Functional limitations (in particular for data transmission) may occur with this.

6.2 Technological Features

Technological Feature	Description
4-port Ethernet switch	10/100 Mbit/s full/half duplex auto sense; automatic detection of "crossover" or "patch" wiring.
LAN ext interface	10/100 Mbit/s full/half duplex auto sense; automatic detection of "crossover" or "patch" wiring.
RS232 interface	Max. baud rate 115,200 bit/s; hardware handshake RTS/CTS; software handshake XON/XOFF; various data formats

Table 2: Technological Features

7 Display and Control Elements

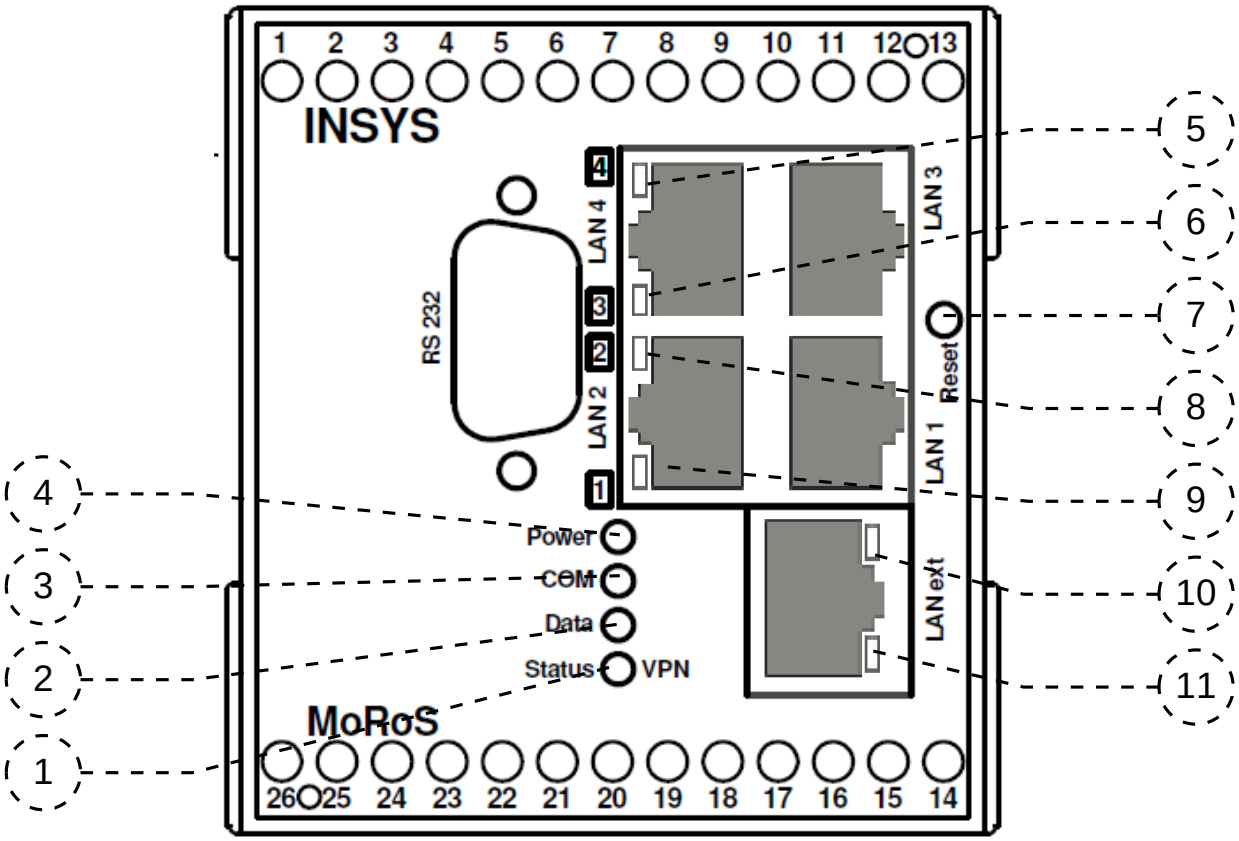


Figure 1: Display and control elements on the front of the device

Position	Description
1	Status/VPN LED
2	Data LED
3	COM LED
4	Power LED
5	Status LED for Switch LAN 4
6	Status LED for Switch LAN 3
7	Reset key
8	Status LED for Switch LAN 2
9	Status LED for Switch LAN 1
10	Status LED for Switch LAN ext
11	Status LED for Switch LAN ext

Table 3: Description of the display and control elements on the front panel of the device

7.1 Meaning of the display elements

LED	Colour	Function	off	flashing	blinking	on
Switch LAN 1-4	yellow	Link 10 Mbit/s			Data traffic	connected
	green	Link 100 Mbit/s				
Switch LAN ext	orange	Link 10 Mbit/s			Data traffic	connected
	green	Link 100 Mbit/s				
Power	green	Supply	missing			present
COM	green	PPP link	offline			establishing
	orange	PPP link				established
Data	green			PPP data traffic		
Status / VPN	green	VPN				VPN connection established
	red	Status				Initialization, FW update, fault

Table 4: Meaning of the display elements

7.2 Function of the Control Elements

Description	Operation	Meaning
Reset key	Press once for a short time.	Resets the software and restarts it. (Soft reset)
	Press for at least 3 seconds.	Resets the hardware and restarts it. (Hard reset)
	Press three times for a short time within 2 seconds.	Deletes all settings and resets the device to the factory defaults.

Table 5: Description of the functions and meaning of the control elements

8 Connections

8.1 Front Panel Connections

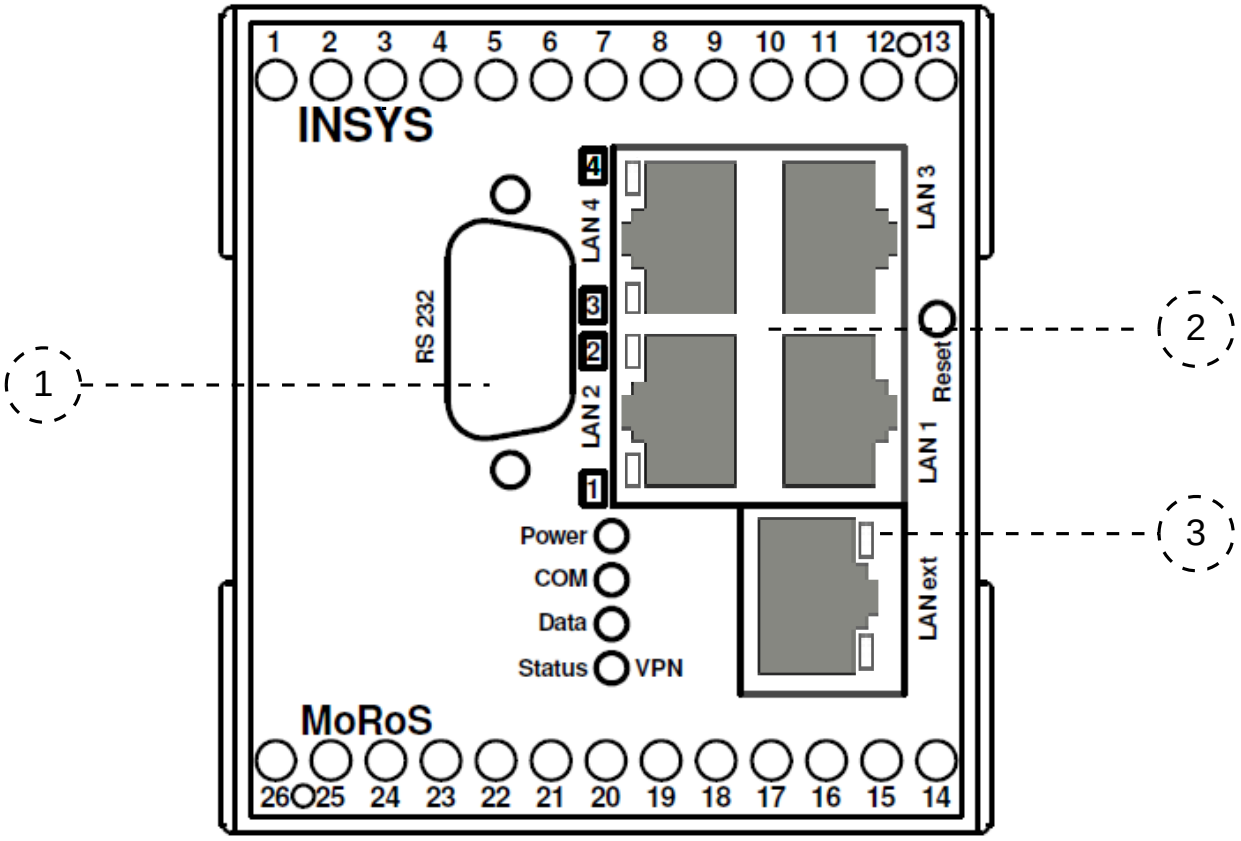


Figure 2: Connections on the front panel of the device

Position	Description
1	Serial interface (RS232 socket V.24/V.28)
2	Switch with 4 Ethernet ports (RJ45, 10/100 BT)
3	Ethernet port (RJ45, 10/100 BT)

Table 6: Description of the connections on the front panel of the device

8.2 Terminal Connections on the Top

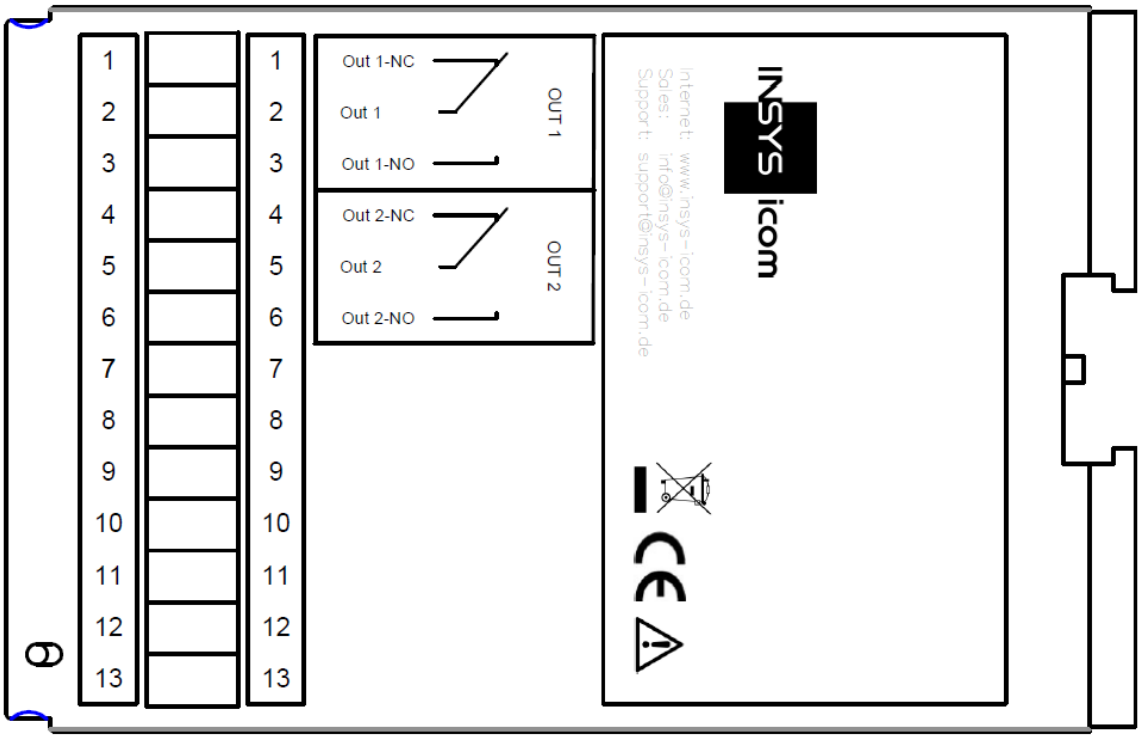


Figure 3: Connections on the top of the device

Terminal	Designation	Description
1	OUT 1-NC	Output 1 normally closed
2	OUT 1	Output 1
3	OUT 1-NO	Output 1 normally open
4	OUT 2-NC	Output 2 normally closed
5	OUT 2	Output 2
6	OUT 2-NO	Output 2 normally open

Table 7: Description of the connections on the top of the device

8.3 Terminal Connections on the Bottom

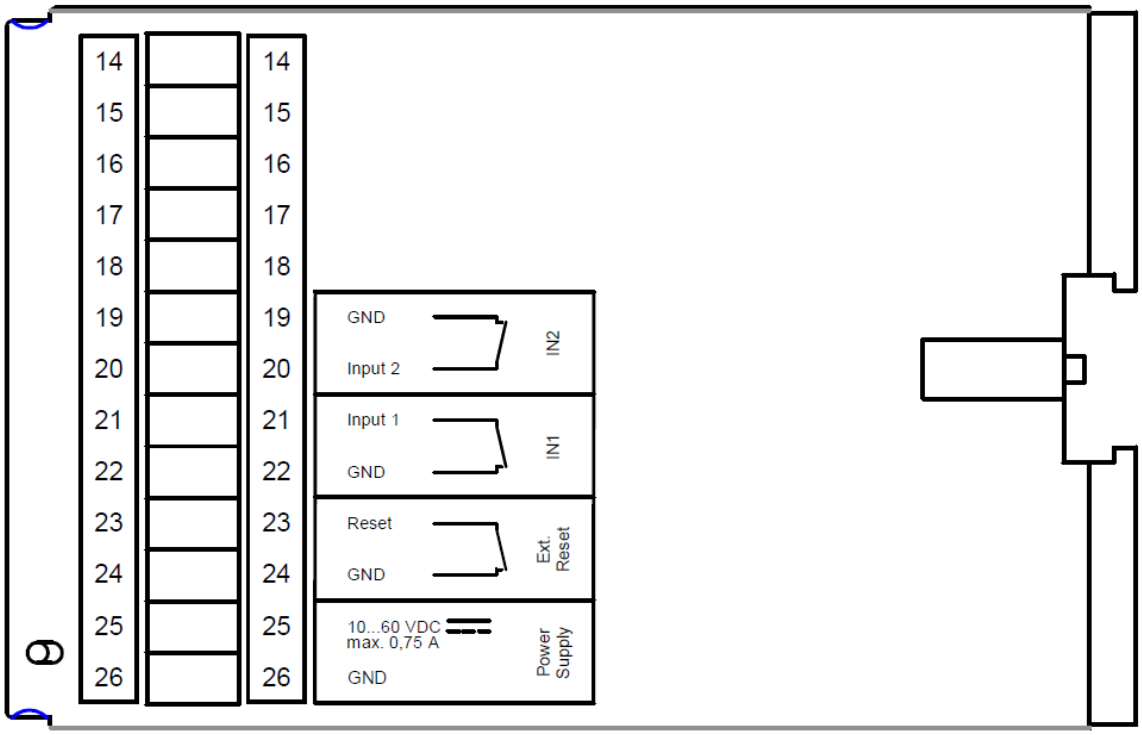


Figure 4: Connections on the bottom of the device

Terminal	Designation	Description
19	GND	Ground
20	Input 2	Input 2
21	Input 1	Input 1
22	GND	Ground
23	Reset	Reset input
24	GND	Ground
25	10 ... 60 VDC	Power supply 10 V – 60 V DC
26	GND	Ground

Table 8: Description of the connections on the bottom of the device

8.4 Pin Assignment of the Serial Interface

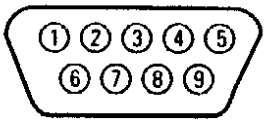


Figure 5: 9-pin D-Sub socket at the device

Pin	Signal	Description
1	DCD	Data Carrier Detect
2	RXD	Receive Data
3	TXD	Transmit Data
4	DTR	Data Terminal Ready
5	GND	Ground
6	DSR	Data Set Ready
7	RTS	Request To Send
8	CTS	Clear To Send
9	RI	Ring Indication

Table 9: Description of the pin allocation of the D-Sub socket

8.5 LAN Connection

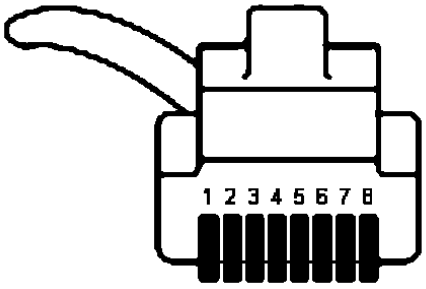


Table 10: RJ45 connector Ethernet cable

Pin	Signal	Description
1	RX+	Receive positive
2	RX-	Receive negative
3	TX+	Transmit positive
4	n/a	Not connected
5	n/a	Not connected
6	TX-	Transmit negative
7	n/a	Not connected
8	n/a	Not connected

Table 11: Description of the pin allocation of the RJ45 connector

9 Function Overview

The MoRoS LAN provides you with the following functions:

- **Configuration via web interface command line (CLI) or configuration file**

  All functions can be configured and set via a web interface or a command line interface (CLI). The access to the interface is protected with a user name and password query. The port required for this can be freely configured. Alternatively, a file (ASCII or binary), which contains the configuration, can also be uploaded.

- **Access control via radius server**

  The access to the web interface or command line interface (CLI) can be protected against unauthorised access using an optional Radius server.

- **IPv6 routing**

  Additionally to the IPv4 addresses, the interfaces have also addresses according to the IPv6 protocol. The router configures one or several IPv6 addresses for itself using SLAAC (StateLess Address Auto Configuration). If a router with router advertisement advertises IPv6 address prefixes in the LAN, the router configures itself another IPv6 address with the advertised prefix in addition to the already configured IPv6 addresses. In addition, the router can distribute its prefix to local devices (router advertisement).

- **Serial Ethernet gateway**

  It is possible to output arriving data from a certain network port at the serial interface. Also, data arriving at the serial interface are sent to an IP remote terminal. Together with the INSYS VCom® driver, the serial Ethernet gateway enables the transmission of a serial connection via a network.

- **DHCP server**

  Ethernet devices connected to the switch can retrieve their IP address automatically.

- **DHCP client**

  IP addresses from the network can be retrieved automatically at the LAN ext interface optionally.

- **Static IP address**

  A static IP address can be configured for the LAN ext interface.

- DSL leased line operation

  A permanent connection can be established and maintained via a DSL ("PPP over Ethernet") connection. A DSL modem can be connected via the LAN ext interface for this. This makes it possible to communicate with an external network via a "leased line".

- Periodic DSL connection set-up

  A DSL (PPPoE) connection can be established and also terminated time-controlled. Fixed times can be specified for the connection set-up and termination.

- Dynamic DSL connection set-up

  A DSL (PPPoE) connection can be established independently if required. The connection will be terminated again after a configurable idle time or after a configurable maximum connection time.

- Dialling filters for DSL connection set-up

  The dialling filters allow to define, which data packets lead to a PPPoE connection set-up. This helps to avoid needless connections and save costs.

- NAT and port forwarding

  The router can also forward data packets via NAT and port forwarding. According to defined rules, incoming IP packets to definable ports and port ranges will be forwarded to IP addresses and ports in the LAN.

- IP forwarding

  IP forwarding rules can be used to create additional IP addresses at the LAN ext interface. Packets to one of these IP addresses will be forwarded to the IP address in the local LAN that is assigned to it.

- OpenVPN

  The router can be used as OpenVPN server or client. This enables machines to establish a safe connection to the LAN behind the router from the outside via an unsafe network. An entire LAN can also be connected interception-proof and interference-proof via an unsafe Internet connection through a VPN tunnel to another network (e.g. the company network). The authentication when connecting to an OpenVPN server via a static key, a certificate with user name and password, or just a certificate is supported with this. An OpenVPN connection without authentication can also be established.

- **PPTP**

  The router can be used as PPTP server or client. This enables machines to establish a safe connection to the LAN behind the router from the outside via an unsafe network. An entire LAN can also be connected interception-proof and interference-proof via an unsafe Internet connection through a VPN tunnel to another network (e.g. the company network).

- **IPsec protocol**

  Two subnets can be connected with each other via an unsafe Internet connection tap- and interference-proof using an IPsec tunnel. The authentication when connecting to an IPsec terminal device via certificates or a passphrase (PSK) is supported with this. Up to 10 tunnels can be established at the same time.

- **GRE tunnel**

  GRE tunnel enable a transparent data transmission through an existing connection without changing the original packets.

- **IPT protocol**

  Support of communication via IPT (Internet-Protokoll Telemetrie). The router can connect to an IPT master as IPT slave and tunnel payload of the serial Ethernet gateway to another IPT slave.

- **Dynamic DNS update**

  The assigned IP address can be deposited at a dynamic DNS service (e.g. DynDNS) after the set-up of a PPP connection to an Internet service provider . The router can be accessed from the Internet.

- **DNS relay server**

  DNS requests can be forwarded to previously configured DNS servers in the Internet or the DNS servers passed on during PPP connection establishment.

- **Firewall (stateful firewall)**

  The firewall enables the limitation of incoming and outgoing IP connections. A flexible rule may be created for each connection and stored user. If one of these firewall rules applies to a connection through the router, this connection will be allowed, otherwise the connection is inhibited. The "Stateful Firewall" will allow connections also for protocols with special requirements, e.g. FTP.

- **Configurable Ethernet switch**

  For each port at the switch, the transmission rate, the transmission mode and the LED display for certain network events may be set individually. The settings are detected automatically in default setting. The switch can be divided in up to four VLANs.

- **Port mirroring at the Ethernet switch for analysis purposes**

  A port at the switch can reproduce a copy of the data at another network port of the switch. At these mirror ports, the transmitted data can be read for analysis purposes (e.g. for intrusion detection systems, problem analysis of end terminals), without affecting the network traffic.

- **MAC filter**

  The MAC filter allows that only those packets are accepted at the Ethernet interface that come from explicitly permitted network devices.

- **E-Mail dispatch and SNMP trap triggering on different events**

  It is possible to send an e-mail to any recipient on different events or trigger an SNMP trap. A series of pre-define events are available for this, like set-up of connections or tunnels, input signals, link condition changes, false authentication at the web interface, firewall rejection, configuration changes and other device-internal procedures.

- **SNMP agent for processing SNMP requests**

  It is possible to respond to incoming SNMP requests (SNMP Get requests) if the SNMP agent is enabled. Almost all configuration parameters can be read out with this.

- **Digital switch outputs and inputs**

  Two potential-free control outputs are available, which can be used to switch other functions in an application. Digital inputs are also available, which are used to establish PPPoE connections or to send messages via e-mail.

- **Time synchronisation via NTP**

  Synchronisation of the system time via Network Time Protocol with an NTP server in the Internet. The system time will thus always be current and the internal clock must not be set manually.

- **NTP server**

  An NTP server can respond to NTP requests in the local network.

- **HTTP and HTTPS proxy with URL filter**

  The proxy is used to limit the access to web addresses for applications in the local network of the router, and to avoid connection timeouts. The protocols HTTP and HTTPS are supported. The proxy maintains connections during the connection setup of the communication device to prevent a premature timeout. The proxy will not work as a cache for frequently accessed websites

- **Log files**

  Different log files can be downloaded as text file via the web interface.

- Downloadable configuration files

  The configuration can be downloaded as binary or ASCII file. The file can be used as backup copy for configurationafter a reset to factory defaults, or for convenient loading of the same configuration into a different router. The ASCII configuration file can be edited and offers a comfortable option for an alternative configuration.

- Firmware update via web interface

  The firmware can be updated via the web interface. An update can be performed locally or remotely.

- Automatic daily update

  A daily automatic update of firmware files, configuration files (binary and ASCII) or sandbox image files that are provided accordingly on a server is possible.

- An optional, redundant communication device may be connected.

  You can connect a second INSYS communication device via the serial interface to secure the dial-out and dial-in communication through redundancy and to increase the availability.

- Freely programmable sandbox

  A freely configurable sandbox is available. The sandbox is a kind of a virtual machine, which runs on the router and allows to start programs, collect data and offer services in the sandbox, which do not exist in the actual system.

- Debugging tools for analysing network connections

  Different tools are available to be able to analyse problems with network connections. Ping packets can be sent, routes of IP packets can be traced, DNS information can be queried and network packets can be recorded with this.

- Querying and setting objects via MCIP protocol

  The digital I/Os and a part of the LEDs can be queried or set via MCIP protocol. The MCIP protocol is available in the sandbox as well as from external devices via TCP/IP.

- Pre-installed Monitoring App

  The pre-installed Monitoring App enables the monitoring of timers, incoming SMS (cellular devices) or objects of a Siemens control of the types LOGO!™ or S7 (each subject to licence) as well as dispatching alarm messages.

10 Assembly

This section describes how to mount the MoRoS LAN to a DIN rail, connect the power supply and uninstall it again. Observe the instructions in the "Safety" section of this manual, in particular the "Safety Instructions for Electrical Installation" for that purpose unconditionally.

Caution!

Moisture and liquids from the environment may seep into the interior of the device!

Fire hazard and damage of the product.

The device must not be used in wet or damp environments, or in the direct vicinity of water. Install the device at a dry location, protected from water spray. Disconnect the power supply before you perform any work on a device which may have been in contact with moisture.

Caution!

The device could be destroyed if the wrong power supply is used!

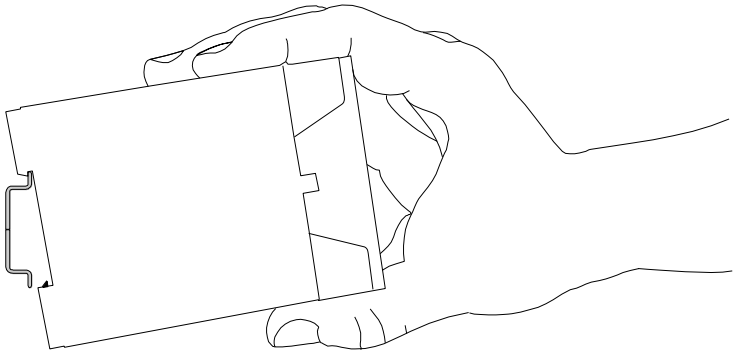
If the device is operated with a power supply that supplies a voltage exceeding the permissible operating voltage, it will be destroyed.

Make sure that you use the suitable power supply. Refer to the Technical Data section for the proper voltage range.

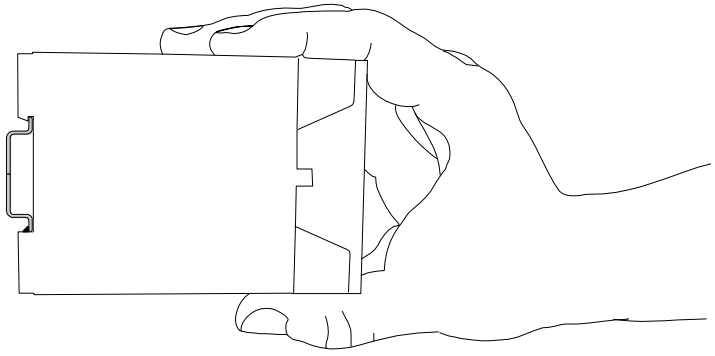
Mounting the device to the DIN rail

How to mount the MoRoS LAN to a DIN rail:

1. ***Position the device at the DIN rail as seen in the following diagram. There are two snap-in hooks at the upper and lower edge of the DIN rail groove. Hook the upper one into place behind the upper edge of the DIN rail.***



2. ***Lift the device perpendicular to the DIN rail until the two lower, flexible snap-in hooks engage in the DIN rail.***



✓ The MoRoS LAN is now readily mounted.

Connecting the power supply

⇢ The device has already been mounted to the DIN rail.

⇢ The power supply is connected and switched off.

1. ***Connect the ground lead of the power supply to the terminal "GND".***
2. ***Connect the plus pole of the power supply to the terminal for the power supply.***

✓ The MoRoS LAN is now connected to the power supply.

Disconnecting the power supply

⇢ The device is mounted to the DIN rail.

⇢ The power supply is connected and switched off.

1. ***Disconnect the ground lead of the power supply from the terminal "GND".***

2. ***Disconnect the plus pole of the power supply from the terminal for the power supply.***

✓ The MoRoS LAN is disconnected from the power supply.

Removing the device from the DIN rail

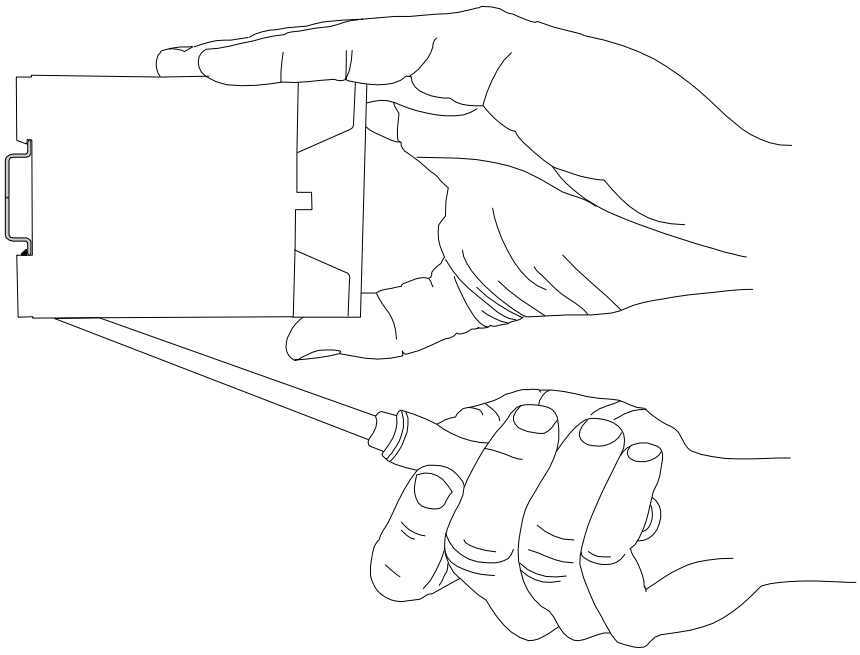
How to uninstall the MoRoS LAN from a DIN rail in a switch cabinet:

⇢ You will need a small flat-blade screwdriver.

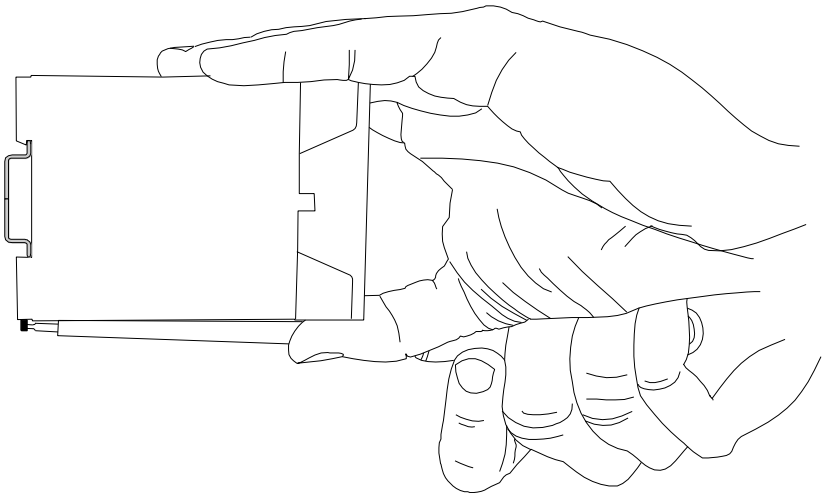
⇢ The power supply of the switch cabinet is switched off and secured against being switched on accidentally.

⇢ All cables at the device are disconnected.

1. ***Insert the flat-blade screwdriver into the groove in the bottom as shown in the following figure.***



2. Turn the flat-blade screwdriver into the direction of the device as shown in the following figure.



✓ The plastic spring of the snap-in hook is stretched.

3. While you hold the plastic spring apart with the lower snap-in hooks, pull the device away from the DIN rail.

4. Un-hook the device and take it off perpendicularly to the DIN rail.

✓ The MoRoS LAN is now removed.

11 Commissioning

This chapter describes how to activate the MoRoS LAN, i.e. how to connect it to a PC, and how to prepare it for the configuration.

Connecting to a LAN and a PC

How to connect the MoRoS LAN to a PC for configuration and an external LAN.

⇢ The power supply is disabled.

⇢ You will need a Cat 5 network patch cable

⇢ You will need a network card in the PC.

⇢ You will need a connection to your external LAN via a network cable.

1. ***Locate the RJ-45 socket of the network card at the PC.***
2. ***Plug one end of the network cable into the RJ-45 socket at the PC, and the other end into a network socket at the MoRoS LAN switch.***
3. ***Connect the network cable of the external LAN to the LAN ext socket.***

Configuring the MoRoS LAN

⇢ The device is connected to the PC.

⇢ The power supply of the device is enabled.

⇢ You have the required access rights to change the IP address of the network card to which the MoRoS LAN is connected.

1. Change the IP address of the network card to which the device is connected to an address that starts with 192.168.1.

➢ *As an alternative, you may also configure your network card to "Automatic address allocation". The integrated DHCP server of the MoRoS LAN will then allocate an address from the according address range to your network card.*

ⓘ Do not use the address 192.168.1.1. This is the factory default IP address of the device. For example, use 192.168.1.2 as IP address for the network card in your PC.

2. Open a web browser and enter the URL "http://192.168.1.1" into the address bar.

✓ The browser loads the start page of the MoRoS LAN.

➢ *If you see the message in your browser window that the page with this address cannot be found, follow the following steps: Check, whether the device is supplied with power. If yes, most probably a wrong IP address is configured in the device. Press the reset key three times within two seconds and repeat this instruction from step 2.*

✓ A dialogue will prompt you to enter a user name and password for authentication.

3. Enter the user name "insys" and the password "moros".

ⓘ User name and password are set as factory defaults. If the registration at the web interface does not work with the data entered, just reset the device to the factory defaults.
Press the reset key three times within two seconds and repeat this instruction from step 2.

✓ You should now see the start page of the web interface.

✓ The MoRoS LAN is installed successfully and ready for configuration.

12 Operating Principle

This chapter describes how to operate and configure the MoRoS LAN.

Configuration and operation are performed using a web-based interface (web interface). The web interface itself is displayed and operated using a web browser.

12.1 Operating the Web Interface

The web interface allows easy configuration using a web browser. All functions can be configured via the web interface. The operation is mostly self-explanatory. The web interface also provides an online help feature, which describes the meaning of possible settings The online help is displayed by selecting the option "Display help text" in the title bar below the language selection.

ⓘ We urgently recommend to enable online help for the first configurations to allow a quick and flawless configuration.

Configuring with the web interface

How to configure with the web interface basically.

⇢ The device is ready for operation and you have access to it (refer to Commissioning section).

1. ***Start the web browser and enter the IP address into the address bar.***

   ⓘ The factory default IP address is 192.168.1.1.

   ✓ A dialogue will prompt you to enter the user name and the password for authentication.

2. ***Enter the user name and the password and click OK.***

   ⓘ The default setting of the web interface is as follows:
   the user name is "insys", the password is "moros".

   ✓ The start page of the web interface is displayed.

3. ***Use the menu on the left side to select the menu item, in which you want to change settings.***

4. ***Enter the required settings.***

5. ***Click on the button OK on the according configuration page to save the settings.***

   ⓘ After you completed the configuration changes, always click the button OK. Otherwise the settings will not be taken over as soon as you change to another page or close the browser.

12.2 Access via HTTPS Protocol

The web interface also allows a secure configuration using the HTTPS protocol. The HTTPS protocol allows an authentication of the server (i.t. the MoRoS LAN) as well as an encryption of the data transmission.

in case of a first access via the HTTPS protocol, the browser indicates that the MoRoS LAN uses an invalid security certificate. The certificate is not trusted, because the CA (certification authority) certificate is unknown.

You can ignore this warning and (depending on browser and operating system) add an exception for this server or establish the secure connection to this server nevertheless.

We recommend to download the CA certificate CA_MoRoS.crt from the certificate page (http://www.insys-icom.com/certificate/) and import it into your browser, to approve INSYS MICROELECTRONICS as certification authority. Proceed for this as described in the documentation of your browser.

If INSYS MICROELECTRONICS is stored as certification authority in your browser and you access the device again via the HTTPS protocol, the browser indicates again that an invalid security certificate is used. The certificate is not trusted, because the Common Name of the certificate differs from your input in the address bar of the browser. The browser indicates that a different device answers under this URL. The Common Name of the certificate consists of the MAC address of the MoRoS LAN, where the colons are replaced by underscores.

You can ignore this warning and (depending on browser and operating system) add an exception for this server or establish the secure connection to this server nevertheless.

In order to avoid this browser warning as well, you must enter the Common Name of the MoRoS LAN to be accessed into the address bar of your browser. The Common Name must be connected with the IP address of the device that the URL leads to the correct device. You can find out the general name (Common Name) by downloading and viewing the certificate from the device. The proceeding for this depends on your browser. The proceeding for setting up the link depends on your operating system.

- Editing of /etc/hosts (Linux/Unix)
- Editing of C:\WINDOWS\system32\drivers\etc\hosts (Windows XP)
- Configuring your own DNS server

For further information, refer to the documentation of your operating system.

13 Functions

13.1 Basic Settings

13.1.1 Configuring Web Interface Access

The web interface is used to configure the MoRoS LAN. It will be protected against unauthorised access by requesting user name and password (alternatively also via a Radius server). The web interface can be configured for a configuration from a computer in the internal network or for remote configuration from the WAN via the HTTP or HTTPS protocol. A location can be entered for a better differentiation. You can specify the port, under which the web interface can be accessed.

Configuration via web interface (menu "Basic Settings", page "Web interface")

For a **local authentication at the device**, select the radio button "Authentication with password" and enter the access data into the respective fields.

For an **authentication at the Radius server**, select the radio button "Authentication at Radius server“.

ⓘ The Radius server must be configured for this (in the "Basic Settings" menu on the "Radius" page).

To enable an authentication via password if the **Radius server is not accessible** or does not reply, check the checkbox “Authentication with password after Radius timeout”.

In order to specify the access options (local or remote via HTTP or HTTPS) that are **permitted for the configuration**, check or uncheck the respective checkboxes.

The **web interface port** is defined in the entry field "Port for HTTP web interface" or "Port for HTTPS web interface". Port 80 (HTTP) or port 443 (HTTPS) is configured for the web interface by default.

A **description or location of the router** may be entered in the entry field "Location". This description appears in the browser window title as well as the start page of the web interface then and facilitates a differentiation if more web interface windows are open.

Save your settings by clicking "OK".

13.1.2 Setting IP Addresses

It must be possible to access the MoRoS LAN in the LAN under a certain IP address. You must assign a static IP address for this. You can enter an IPv4 and an IPv6 address here. The router can configure one or several IPv6 addresses for itself using SLAAC (StateLess Address AutoConfiguration). If a router with router advertisement advertises IPv6 address prefixes in the LAN, the router configures itself another IPv6 address with the advertised prefix in addition to the already configured IPv6 addresses.

A virtual net address can be assigned to the local network. Devices in the local network can then be addressed with the virtual address via WAN. The router replaces the network portion of the virtual IP address with the network portion of the local network and forwards the packet to the destination.

Configuration via web interface (menu "Basic Settings", page "IP address (LAN)")

In order to configure a **static IP address**, enter the **IPv4 address** of the router in the LAN as well as the **netmask**.

ⓘ When changing the local IP address, the address range of the DHCP server will be adjusted to the new network automatically, if the netmask has not changed. The DHCP server will be disabled with a changed netmask and must be configured manually. This is indicated in a notification.

The **MAC address** can be found in the entry fields for the IP address and the network mask under "MAC address" on this page.

Check the checkbox "Retrieve IPv6 address automatically (SLAAC)" that the **router configures one or more IPv6 addresses automatically**.

Enter the **IPv6 address** of the router in the LAN into the entry field "IPv6 address" or select the link "Generate new ULA" to generate a ULA (Unique Local Address).

In order to assign a **virtual net address** to the local network, check the checkbox "Activate netmapping" and enter the net address (i.e. the whole IP range) into the "Virtual net address" field (e.g. 192.168.2.0). This virtual address is only visible from the WAN or VPN side.

Save your settings by clicking "OK".

ⓘ If communication is to be restricted to one IP version only (IPv4 or IPv6) due to reasons of security, no IP address must be entered here for the version to be blocked.
If IPv6 is to be blocked, SLAAC and the router advertiser must also be disabled.
If IPv4 is to be blocked, DHCP server and client must be disabled.
The same must be done for the IP address of the LAN (ext) interface.
Moreover, the firewall for the IP version to be blocked must be activated and all firewall rules must be modified such that they do not permit any data traffic of this IP version.

13.1.3 Entering a Static Route

You can define static routes for forwarding data packets in the MoRoS LAN, which are loaded during system start.

Configuration via web interface (menu "Basic Settings", page "Routing")

In order to enter a **static route**, **enter** in the section "Add new route" the **Net address**, the **netmask** as well as the **Gateway** into the respective fields for IPv4 or IPv6. All fields must be completed that a new route for the respective IP version is taken over into the table. Save the route by clicking "OK".

In order to **delete an existing route**, check under "Existing routes" the checkbox of the route(s) to be deleted.

Save your settings by clicking "OK".

ⓘ Neither a default gateway can be entered nor NAT can be enabled or disabled here. This is configured in the menu "LAN (ext)" on the respective page "Routing".

13.1.4 Entering Host Names

You can specify the host and domain name of the MoRoS LAN here.

Moreover, a host table can be created, in which IP addresses are combined with host names. If the router is entered as DNS server at a PC, this can use the host names for addressing instead of the IP addresses.

Configuration via web interface (menu "Basic Settings", page "Host names")

In order to enter the **host name**, enter the host name.

In order to enter the **domain name**, enter the domain name.

In order to enter a new host into the host table, enter in the "Add new host" section the **IP address** and the associated **Host name** into the respective fields. Save the host in the table by clicking "OK".

In order to **delete an existing host**, check under "Existing hosts" the checkbox of the host(s) to be deleted.

Save your settings by clicking "OK".

13.1.5 Configuring MAC Filter

A MAC filter can be enabled in the MoRoS LAN. This will then only accept packets at the local Ethernet interface that come from network devices that are explicitly permitted in the filter.

ⓘ This is only effective for connections that are initiated by the device in the local LAN, not for connections that are initiated from the WAN side.

Note

Loss of availability!

If the MAC address of the computer that is used for configuration is not entered, no further configuration will be possible any more.

It is necessary that you enter the MAC address of the computer that is used for configuration into the list of allowed source MAC addresses before activating the MAC filter.

Configuration via web interface (menu "Basic Settings", page "MAC filter")

In order to **enable the MAC filter**, check the checkbox "Activate MAC filter".

In order to **enter a new source MAC address**, enter this into the "Allow new source MAC" field. The MAC address can be entered with or without colons; other formats are not supported. Save the entry by clicking "OK".

In order to **delete an existing MAC address**, check under "Allowed source MAC addresses" the checkbox of the route(s) to be deleted.

Save your settings by clicking "OK".

13.1.6 Configuring Access Protection via Radius Server

The access to the web interface or command line interface (CLI) can be protected against unauthorised access using an optional Radius server in the network. The access data for the Radius server must be configured in the MoRoS LAN for this.

Configuration via web interface (menu "Basic Settings", page "Radius")

In order to **configure access protection via a Radius server**, enter its address and port into the respective fields. Port 1812 is set by default. Enter also the "Shared Secret" (authentication key) into the respective field.

ⓘ These settings are only effective, if the authentication at the Radius server is selected in the menu "Basic Settings" on the page "Web interface" and/or the page "CLI".

Save your settings by clicking "OK".

13.1.7 Configuring Command Line Interface CLI Access

Besides the configuration via the web-interface or configuration file, a MoRoS LAN can also be configured via a CLI (Command Line Interface). It will be protected against unauthorised access by requesting user name and password (alternatively also via a Radius server). Access to the CLI can either be accomplished from the local network or remote via Telnet or SSH (encrypted). You can specify the port, under which the CLI can be accessed for Telnet and SSH. You can also configure the CLI prompt.

A detailed description of the configuration via CLI can be found in the respective add-on manual.

Configuration via web interface (menu "Basic Settings", page "CLI")

For a **local authentication at the device**, select the radio button "Authentication with password" and enter the access data into the respective fields.

For an **authentication at the Radius server**, select the radio button "Authentication at Radius server".

ⓘ The Radius server must be configured for this (in the "Basic Settings" menu on the "Radius" page).

To enable an authentication via password if the **Radius server is not accessible** or does not reply, check the checkbox "Authentication with password after Radius timeout".

In order to specify the access options (local or remote via Telnet or SSH) that are **permitted for the configuration**, check or uncheck the respective checkboxes.

You can enable or disable the **permissible configuration** using the respective checkbox.

ⓘ If none of these checkboxes is enabled, the CLI cannot be accessed!

You can specify the **Telnet port** in the "Telnet port" entry field. Port 23 is set by default.

You can specify the **SSH port** in the "SSH port" entry field. Port 22 is set by default.

You can specify the **prompt** in the "CLI prompt" entry field. "> " is set by default.

The **SSH MD5 checksum** serves for positive identification of the device for an SSH connection. The key used for this can be re-generated using the "Create new SSH key" button.

Save your settings by clicking "OK".

13.2 LAN (ext)

13.2.1 Configuring the Interface to the External Network (LAN/WAN)

The MoRoS LAN uses its router function to switch the data traffic between two IP networks, an "internal" and an "external". The LAN ext interface serves for connecting the router to the external network. This external network can be another LAN, which can be accessed via an Ethernet cable. Then, an IP address must be configured or obtained for the LAN ext interface. This IP address must be in the address range of the external LAN, into which the MoRoS LAN shall route. The router can configure one or several IPv6 addresses for itself using SLAAC (StateLess Address AutoConfiguration). If a router with router advertisement advertises IPv6 address prefixes in the LAN, the router configures itself another IPv6 address with the advertised prefix in addition to the already configured IPv6 addresses. However, the external network can also be a WAN, which is connected via an DSL connection. In this case, you must configure the interface for PPPoE operation, to enable a communication with the WAN via a DSL modem.

Configuration via web interface (menu "LAN (ext)", page "LAN (ext)")

For a connection **to a LAN**, select the radio button "static IP address". Then, enter into the entry fields "static IP address" and "Netmask" an IPv4 address as well as a netmask. The IP address must be an address from the external LAN, to which you connect the device.

Check the checkbox "Retrieve IPv6 address automatically (SLAAC)" that the **router configures one or more IPv6 addresses automatically**.

Enter the **IPv6 address** of the router in the LAN into the entry field "IPv6 address" or select the link "Generate new ULA" to generate a ULA (Unique Local Address).

In order to connect the device **via DSL to a WAN**, configure in the "LAN (ext)" menu on the "DSL" page the DSL connection first. Select the "PPPoE connection" radio button.

In order to enable the **DHCP client**, select the "DHCP-Client" radio button. The router retrieves an IP address from a DHCP server via the LAN ext interface then. In order to **obtain another IP address for each host table entry**, check the checkbox "Request an additional IP address for each entry of the host table". Another IP address is requested for each host table entry and assigned to the LAN ext interface then. The host name will be composed by the own host name and the host name of the table entry. All packets that are sent to this additional IP addresses, will be forwarded to the IP address of the host table entry.

In order to **operate the device as bridge**, select the "Bridge" radio button. Then, the LAN ext interface behaves like another switch port.

Save your settings by clicking "OK".

13.2.2 Configuring DSL

The MoRoS LAN can connect to a WAN using a DSL modem. The DSL modem is connected using the LAN ext interface. The device can communicate with the DSL modem via a PPPoE connection. You must configure the LAN ext interface for PPPoE operation for this. To be able to establish a connection to the provider via the DSL modem, you must configure the DSL connection with your access data and activate the option "Set default route".

Configuration via web interface (menu "LAN (ext)", page "DSL")

In order to **configure the DSL access**, connect the DSL modem to the LAN ext interface. Then, enter your user name and your password for the DSL access into the entry fields "User name" and "Password".

Enter an **optional idle time** into the entry field "Idle time" in seconds, after which the connection is terminated, if no data is transferred any more. If you enter "0", the connection remains established for an unlimited time.

Enter an **optional maximum connect time** into the entry field "Maximum connect-time" in seconds, after which the connection will be terminated. Enter "0" to disable the time-controlled connection termination.

In order to **adjust the MTU** (maximum permissible number of bytes in a packet to be transmitted), change the entry in the entry respective field.

In order to **adjust the MRU** (maximum permissible number of bytes in a packet to be received), change the entry in the respective field.

ⓘ The default settings of MTU and MRU are suitable for most applications and do not need to be modified usually.

If your DSL access requires **to add VLAN tags to Ethernet packets over the PPPoE connection**, this can be entered into the respective field.

ⓘ If the DSL modem achieves a sync, but cannot establish a PPPoE connection, a missing or wrong VLAN tag may be the cause. Refer to your provider for more information about this.

In order to **retrieve the IPv6 prefix from the DSL provider** after retrieving an IPv6 address, check the checkbox "Get IPv6 address and prefix". The router assigns itself a local IPv6 address from this network.

Check the checkbox "Request DNS server address" that the **IP addresses of the name servers are retrieved from the DSL provider**.

Save your settings by clicking "OK".

In order to **configure a default route**, check in the menu "LAN (ext)" on the page "Routing" the checkbox "Set default route to gateway". The device cannot switch the data traffic between the internal network at the switch and the DSL connection without the default route to the DSL modem.

Save your settings by clicking "OK".

13.2.3 Configuring Leased Line Operation

You can configure the MoRoS LAN to permanently maintain the previously configured DSL connection. The connection will immediately be established the connection after system start in this operating mode. The device checks the connection for its function periodically. The connection check can be performed either via a DNS request of a host name or via PING at a host.

Configuration via web interface (menu "LAN (ext)", page "DSL")

In order to **configure a leased line**, check the checkbox "Connect immediately and hold connection".

If necessary, enter another time in minutes for the **connection check** into the entry field "Interval for checking connection". The default setting is 5 minutes. If a closed connection is determined after this time, the MoRoS LAN will attempt to re-establish the connection after one minute. If the attempt fails, there will be another attempt after 5 minutes. The next attempt will take place after 30 minutes; if this attempt fails as well, the device will attempt to re-establish the connection every 60 minutes.

Select the **method for connection check** using the radio buttons behind "Type to check the connection" and enter a host name or an "IP address". If the checkbox "Renegotiate PPP connection in case of failure" is checked, a failed ping or DNS request causes that a possibly existing connection will be closed. It will be attempted to establish a connection again afterwards in any case.

Save your settings by clicking "OK".

13.2.4 Configuring a Periodical DSL Connection Establishment

The MoRoS LAN can establish and terminate the previously configured DSL connection time-controlled. The DSL connection is established and terminated daily at a certain time.

This function initiates individual events, regardless whether other times have already been defined for the connection termination. Example: If you already configure a daily connection termination at 14:00 and a daily connection establishment at 16:00, other settings and events can also initiate a connection establishment within this period, e.g. a packet, that complies with the dialling filter. The connection is also terminated, if the configured "Idle time" has expired, for example.

Configuration via web interface (menu "LAN (ext)", page "DSL")

In order to **establish a daily connection at a certain time**, check the checkbox "Connect automatically once a day at" and enter a time for the connection setup into the entry fields for hours and minutes.

In order to **terminate a daily connection at a certain time**, check the checkbox "Disconnect automatically once a day at" and enter a time for the disconnection into the entry fields for hours and minutes.

Save your settings by clicking "OK".

13.2.5 Routing

Routing is the core function of the MoRoS LAN. Routing means that incoming data packets are routed to certain network devices according to certain rules defined by you.

The routes determine where to packets are forwarded. A net address and netmask are used to distinguish, whether a route is applied to an IP packet or not. If a packet comes in, that has a destination with an existing route, the device forwards the packet to the gateway address defined in the route.

You can specify a default route. All incoming packets, which cannot be assigned to a route, are sent to this gateway. If you have connected a DSL modem to the LAN ext interface, you can set the default route to the DSL modem.

Moreover, Network Address Translation is supported. If NAT is enabled, the device replaces the source address of the packets of an outgoing connection with its own. The device stores the actual source address in its NAT table. If it receives a reply packet of the remote terminal of this connection, it replaces the destination address of the packet with the address of the original source.

ⓘ Due to the "stateful firewall" it is possible that changes to these functions will not become effective immediately. This may happen if connections or connection attempts have already been made.

Configuration via web interface (menu "LAN (ext)", page "Routing")

In order to **configure an IPv4 default route**, check the checkbox "Set default route to gateway" and enter the default gateway behind. The entry field is not visible in DSL operation.

In order to **configure an IPv6 default route**, check the checkbox "Set IPv6 default route to gateway" and enter the default gateway behind. The entry field is not visible in DSL operation.

In order to **disable NAT for incoming packets**, uncheck the checkbox "Activate NAT for incoming IPv4 packets". This may be useful in LAN operation if the routed packets must not be changed.

In order to **disable NAT for outgoing packets**, uncheck the checkbox "Activate NAT for outgoing IPv4 packets". This may be useful in LAN operation if the routed packets must not be changed.

ⓘ The router will unblock own services (e.g. DNS, VPN, NTP, etc.) automatically with enabled firewall. If you uncheck the checkbox "Activate NAT for outgoing IPv4 packets", the services must be permitted manually in the firewall.

In order to **add a new route**, enter in the section "Add new route" the "net address", the associated "netmask" and a gateway into the respective fields for IPv4 or IPv6. All fields must be completed that a new route for the respective IP version is taken over into the table. Save the route by clicking "OK".

In order to **delete an existing route**, check under "Existing routes" the checkbox of the route(s) to be deleted.

Save your settings by clicking "OK".

13.2.6 Setting up a Dialling Filter

The dialling filter can restrict the network traffic which could trigger a connection establishment. All packets with external destination initiate a connection establishment without dialling filter. If the dialling filter is enabled, only the packets, which are permitted by the rules, can initiate a connection establishment.

Configuration via web interface (menu "LAN (ext)", page "Dial filters")

In order to enable the dialling filter, check the checkbox "Activate Dial-Out filters for LAN (ext) interface".

In order to **permit connections via a certain protocol**, select in the field "Create new rule" the permitted protocol in the drop-down list "Protocol".

In order to **permit connections of certain IP addresses**, enter the permitted source IP address into the entry field "Source IP address".

In order to **permit connections to certain ports**, enter the permitted destination port into the entry field "Destination port".

In order to **permit connections to certain IP addresses**, enter the permitted destination IP address into the entry field "Destination IP address".

Optionally, you can use the checkbox "Allow DNS requests from source IP address to initiate a connection" to **allow that DNS requests** of the defined source IP addresses are allowed to **initiate a connection establishment**.

Save your settings by clicking "OK".

In order to **disable individual dialling filter rules temporarily**, uncheck in the section "These data packets are allowed to initiate a Dial-Out" the checkbox in the column "active". Click on "OK" to confirm the settings.

In order to **delete one or more rules**, check in the section "These data packets are allowed to initiate a Dial-Out" the checkbox in the column "delete". Click on "OK" to confirm the settings.

13.2.7 Creating or Deleting a Firewall Rule

A firewall is available for all connections via the LAN ext interface. It is used to prevent unauthorized data traffic. The logic of the firewall states that any data traffic is forbidden, which is not explicitly permitted through a rule. If you enable the firewall for the connection type "Dial-Out", only connections will be possible which are authorised by the firewall rules. All other connections will be blocked.

ⓘ Due to the "stateful firewall" it is possible that changes to these functions will not become effective immediately. This may happen if connections or connection attempts have already been made.

Configuration via web interface (menu "LAN (ext)", page "Firewall")

In order to **enable the firewall for IPv4 connections via the LAN ext interface**, check the checkbox "Activate firewall for LAN (ext) interface".

In order to **enable the firewall for IPv6 connections via the LAN ext interface**, check the checkbox "Activate IPv6 firewall for LAN (ext) interface".

ⓘ It is strongly recommended to keep the firewall for IPv6 always enabled, even if IPv6 is not used.

In order to **create a rule for a permitted IP connection**, proceed as follows.

Select in the section "Allow new connection" in the drop-down list field "Data direction" a **data direction** for the rule.

Define the **protocol of the permitted connection** in the drop-down list field "Protocol".

Select the **IP version** for which the rule shall apply in the drop-down list "IP version".

Enter the further specifications of the connections permitted by the router into the entry fields "**Source IP address**", "**Destination IP address**" and "**Destination port**". Only rules can be created, which are not valid for individual machines (hosts), but for whole networks. In this case, the netmask must be entered following the "/".

Save your settings by clicking "OK".

In order to **temporarily disable firewall rules**, uncheck in the section "Allowed connections ..." the check box in the column "active" in the firewall rule overview. Click on "OK" to confirm the settings.

In order to **delete one or more rules**, check the checkbox in the column "delete" in the firewall rule overview. Click on "OK" to confirm the settings.

13.2.8 Creating or Deleting an IP Forwarding Rule

IP forwarding rules create additional IP addresses at the LAN (ext) interface, if "static IP address" has been selected on the "LAN (ext)" page. Packets to one of these IP addresses will be forwarded to the IP address in the local LAN that is assigned to it.

ⓘ The firewall is also effective for these additional IP addresses. Therefore, these additional IP addresses must be permitted in the "LAN (ext)" menu on the "Firewall" page, if the firewall is enabled. Otherwise, all packets that are not directed to these IP addresses would be discarded.

Configuration via web interface (menu "LAN (ext)", page "IP forwarding")

In order to **enable IP forwarding**, check the checkbox "Activate IP forwarding".

In order to **create an IP forwarding rule**, in the "Create new rule" section the additional IP address with netmask into the "LAN (ext) IP address" field and the destination address into the "Destination IP address" field. The packets to the additional address will then be forwarded to this address. Save the entry by clicking "OK".

In order to **delete an existing rule**, check under "Existing rules" the checkbox of the rule(s) to be deleted.

Save your settings by clicking "OK".

13.2.9 Creating or Deleting a Port Forwarding Rule

If port forwarding is enabled, the router forwards packets coming in from the WAN to the machines in the LAN, which have been specified in the port forwarding rules.

Only the WAN IP address of the MoRoS LAN is accessible from the WAN, if NAT is enabled for packets going into the WAN. The local terminal devices in the network of the device can still be accessed with this IP address using port forwarding. Packets from the WAN sent to the WAN IP address at a port x, can be forwarded to a machine with the IP address Y at the port y. If a whole port range is specified alternatively, the packets will be forwarded to the same ports of the destination IP address. It is possible to define the rules such that they apply only to WAN connections, only to OpenVPN connections or always.

ⓘ Due to the "stateful firewall" it is possible that changes to these functions will not become effective immediately. This may happen if connections or connection attempts have already been made.

Configuration via web interface (menu "LAN (ext)", page "Port forwarding")

In order to **enable port forwarding**, check the checkbox "Activate port forwarding for LAN (ext) interface".

In order to **create a port forwarding rule**, select in the field "Create new rule" the protocol and specify the port or port range, for the incoming packets at the MoRoS LAN. Enter an IP address for the routing destination in the entry field "to IP address" and a port in the entry field "to port"; this is the address and the port where the packets are routed to. If a port range is specified, no destination port is necessary since this corresponds always to the port range in the WAN. Select in the drop-down list “apply”, whether the rule shall apply always, only for WAN connections or only for OpenVPN connections.

In order to **disable an existing rule**, disable the checkbox "active" of the respective rule and then click on "OK".

In order to **delete an existing rule**, check the checkbox "delete" of the respective rule and then click on "OK".

The rules in the list are processed from top to bottom. If two rules contradict each other (for example, the same port is used twice), only the rule which is further up in the list will be processed.

13.2.10 Defining the Exposed Host

All packets which do not comply with any port forwarding rule, can be forwarded to a predefined computer in the LAN, also called "Exposed Host" (for example, for diagnostic purposes) optionally. The exposed host contains all packets which have not been requested by the local network of the MoRoS LAN or which have not been forwarded to a participant in the local network by a port forwarding rule. If no exposed host is configured, these incoming packets are discarded.

Configuration via web interface (menu "LAN (ext)", page "Port forwarding")

In order to **define** an **exposed host**, enter in the entry field "Exposed host" the IP address of a computer in the LAN, which shall be accessible from outside via all ports.

Save your settings by clicking "OK".

13.3 VPN

13.3.1 VPN General

A VPN (virtual private network) is used to connect IP end devices or entire networks with each other, in a safe way. The data is transmitted tamper-proof to a destination and cannot be read by third parties.

You can configure the MoRoS LAN for an OpenVPN, PPTP IPsec or GRE connection.

The exact proceeding for creating a certificate structure and configuring a VPN participant is described in a series of configuration guides. These are available from our website (http://www.insys-icom.com/cg/) or our support team (support@insys-icom.de).

13.3.2 OpenVPN General

You can use the MoRoS LAN as OpenVPN server or OpenVPN client.

Figure 6 shows a sample configuration for an OpenVPN connection. One MoRoS LAN is configured as OpenVPN server and a second as OpenVPN client here. Both, client as well as server can be replaced by any OpenVPN-capable devices. In the example, a WWAN connection between the two devices exists. Via this WWAN connection, an OpenVPN connection is established.

As soon as a WAN connection has been established, IP connections between both networks can be established. OpenVPN uses an existing WAN connection to establish a VPN tunnel. A tunnel consists of an IP connection, which transports all packets to be tunnelled in its payload. OpenVPN will make a virtual network card available for sending data traffic.

Figure 6: OpenVPN connection and IP addresses in the sample configuration

In the sample configuration, the end points of the OpenVPN connection will have the IP addresses 10.1.0.1 and 10.1.0.2. The VPN tunnel will be established within an already existing WAN connection. The OpenVPN clients and servers must also know which network is located behind the according tunnel ends. In the sample configuration, this is the network 192.168.200.0/24 on one side. On the other side, this is the network 192.168.1.0/24. As soon as the tunnel is established, data for these target networks is sent through the OpenVPN tunnel. If only data with a target in the network behind the tunnel end are to be transmitted via the WAN interface, it is recommended to enable the firewall after successful configuration. This will limit the communication to the port at which the OpenVPN tunnel is established (default setting: UDP port 1194).

The MoRoS LAN supports several authentication methods when establishing the VPN tunnel:

Authentication type	Usage	Characteristics
None	For testing purposes and to connect networks without encryption.	No encrypted connection. It is not possible to log in several clients at the server at the same time.
Static key	For encrypted connections of one client and one server each in small applications	Encrypted connection. It is not possible to log in several clients at the server at the same time.
User name/password and common CA certificate (can only be configured at the OpenVPN client)	For encrypted connections from one or more clients to an OpenVPN server.	Flexible application for several clients. Cannot be used with the MoRoS LAN as OpenVPN server.
Certificate-based; each participant has an individual certificate and key.	For encrypted connections from one or more clients to an OpenVPN server.	Solution for maximum security, but the configuration is more complicated. This is the recommended operating mode.

Table 12: Authentication methods for OpenVPN

For detailed information and troubleshooting, we also recommend the OpenVPN web site: http://openvpn.net/howto.html

13.3.3 Setting Up an OpenVPN Server

You can use the MoRoS LAN as OpenVPN server, if you want to send confidential data via an unsecured network, for example. This section describes the set-up of an OpenVPN server. The basic settings are reasonable factory defaults, which you may change in certain circumstances. Here, you define which port of the MoRoS LAN is used to create the OpenVPN tunnel and if the OpenVPN transmission is performed with the UDP or the TCP protocol. Moreover, you can specify here, whether the clients are informed about the server network, the remote terminal may change its IP address, LZO compression is used, packets are masked before tunnelling, which encryption algorithm is used during transmission, how big the tunnel packets are to be, and in which time intervals the OpenVPN server sends VPN pings. In addition, you will have the option to display the OpenVPN status, to display the current configuration file, to create a configuration for an OpenVPN remote terminal, and to display a log of the last connection. You can use the generated configuration file to create an OpenVPN configuration file for exampple, which can be used as basis for the operation of an OpenVPN instance on a client PC. The OpenVPN packet for Windows clients can be downloaded from the INSYS icom web site (www.insys-icom.com/driver).

This program is used as remote terminal, if you want to establish an OpenVPN connection from a Windows PC.

Configuration via web interface (menu "LAN (ext)", page "OpenVPN server")

In order to use **the OpenVPN server for a connection**, check the checkbox "Activate OpenVPN server".

In order to **display the state of the OpenVPN server**, select the link "OpenVPN server state".

In order to **display the messages of the last connection**, select the link "Display log of last connection".

In order to **display the configuration file of the router as OpenVPN server**, select the link "Display configurations file".

In order to **display a sample configuration for an OpenVPN client**, select the link “Create sample configuration file for remote terminal”.

In order to **define the local port at the MoRoS LAN as well as the port at the remote terminal**, enter a value for the required port into the entry fields "Tunnelling over port (local / remote)" (default setting 1194).

The **OpenVPN transmission protocol** is selected with the radio buttons "UDP" or "TCP". We recommend using UPD to minimise latency.

In order to **inform the clients about the route to the network behind the server**, check the checkbox "Inform clients about server network". If this setting is disabled, a communication can only be initiated from the network of the server.

In order to **enable remote OpenVPN terminals to change its IP during a connection** ("**Floating**"), check the checkbox "Remote terminal is allowed to change its IP address (float)". This setting is activated by default.

In order to **enable or disable LZO compression**, check or uncheck the checkbox "Activate LZO compression". If already strongly compressed data (e.g. jpg) is transmitted, the compression will have hardly any effect; however, if compressible data (e.g. text) is transmitted, the compression may significantly reduce the transmitted volume of data. Switch the compression off, if the remote terminal does not support LZO compression.

In order to **mask the packets with the virtual tunnel IP address**, check the checkbox "Masquerade packets before tunnelling". The recipient of the packets sees the IP address of the tunnel end as sender then, not the address of the original sender.

In order to **use a different encryption method** than the preset method for the OpenVPN connection, select one of the encryption types in the drop-down list "Cipher algorithm". Blowfish 128 Bit, DES 64 Bit, DES EDE 128 Bit, DES EDE3 192 Bit, DESX 192 Bit, CAST5 128 Bit, IDEA 128 Bit, RC2 128 Bit, RC2 40 Bit, RC2 64 Bit, AES 128 Bit, AES 192 Bit, AES 256 Bit and no encryption are available.

In order to **use a different hash algorithm** than the preset one for the OpenVPN connection, select one of the hash algorithms in the drop-down list "Hash algorithm". SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 and no hash algorithm are available.

In order to configure the **detail level of the messages in the connection log**, enter the detail level into the field "Log level", where "0" disables the log record completely and "9" records the most detailed information.

In order to define a certain **fragmenting size for the OpenVPN tunnel packets** in bytes, use the entry field "Fragment packets". Enter the required maximum packet size in bytes here. If you don't enter a value, the OpenVPN packets will have a maximum size of 1.500 bytes. The actually transmitted amount of user data is lower, because OpenVPN creates a "protocol overhead", which means that the protocol information that is transmitted as well is a part of the packet size.

In order to **adjust the interval up to the key renegotiation**, use the entry field "Interval for renegotiation of data channel key". This interval configures the time in seconds, which must expire before new keys are created.

In order to adjust the **VPN ping interval**, use the entry field "Ping interval". Enter the interval in the amount of seconds, in which the OpenVPN server of the MoRoS LAN sends ping packets to the remote VPN terminal. The frequent ping is used to keep the connection open via several routers and gateways, which may participate in the connection and would close the channel in case there was no communication.

In order to adjust the **ping restart interval**, use the entry field "Ping restart interval". The ping restart interval configures the time in seconds after which the tunnel is to be established again, if no ping from the remote terminal has arrived during the complete time. The value "0" prevents the tunnel to be terminated, even if no ping is received any more.

ⓘ The ping interval and the ping restart interval must be adjusted to each other. Typical values are 30 and 60 (default). The ping interval should not exceed half of the ping restart interval. We recommend for poor WAN connections to reduce the ping interval and, if required, increase the ping restart interval.

In order to **configure the authentication with certificates**, select the radio button "Authentication based on certificate". It is indicated under the option here, whether the individual certificates and keys are present (green checkmark) or not (red cross). Present certificates can also be downloaded (blue arrow) or deleted again (red cross on white box). The private key can only be deleted. Check the checkbox " Activate tls-auth" to use a static key as well in addition to the certificates. The static key stored in the "Authentication with preshared key" section will then be used. Optionally, a direction can be specified in the "Use direction of key" drop-down list (refer to the note in the following for this). Check the checkbox "Allow communication between clients" to enable a communication between the clients as well. Define the IP address pool for the clients in the fields "IPv4 address pool / Netmask" or "IPv6 address pool / Netmask". In order to create a new route to a client network, enter in the section "Create new route to a client network" the Common Name of the client into the field "Name in certificate" as well as its net address and netmask into the fields "IPv4 net address / netmask" or "IPv6 net address / netmask". Optionally, enter the VPN IPv4 address for the tunnel end of a client into the field "VPN IPv4 address". One IPv4 and one IPv6 address will always be assigned to each tunnel end, even if the tunnel of one IP version is not used at all. Click on "OK" to take over the new route. You can delete existing routes by checking the checkbox in the column "delete" of the respective route and clicking on "OK".

ⓘ If tls-auth is used, it is possible to specify that the static key can only be used for a certain direction. It is important here that this setting is harmonised with the remote VPN terminal, i.e. no direction is configured for bot or the settings are complementary (0/1 or 1/0).

ⓘ A link of a network address with "DEFAULT" as "Common Name" may be created as "Standard route". It is always used as route, when a client registers with a certificate, for whose "Common Name" no other link has been entered.

In order to **configure the authentication with static key**, select the radio button "No authentication or authentication with preshared key". It is indicated under the option here, whether the static key is present (green checkmark) or not (red cross). A present key can also be downloaded (blue arrow) or deleted again (red cross on white box). If no key exists, the remote terminal will neither be authenticated nor the data traffic through the OpenVPN tunnel will be encrypted. You can also generate a new static key using the "Generate a new static key" link. This static key must then be downloaded and also uploaded to the remote terminal. Both OpenVPN remote terminals must have the same static key that a tunnel is functional with this authentication type. Enter the IP address or the domain name of the remote terminal into the "IP address or domain name of remote site" field. You can enter the IP address or the domain name of an alternative remote terminal into the "Alternative remote site" field. Enter the IP address of the local tunnel end into the "IPv4 tunnel address local" or "IPv6 tunnel address local" field and the IP address of the remote tunnel end into the "IPv4 tunnel address remote" or "IPv6 tunnel address remote" field. Enter the address as well as the associated netmask of the network behind the OpenVPN tunnel into the "IPv4 net address behind the tunnel" or "IPv6 net address behind the tunnel" and "IPv4 netmask behind the tunnel" or "IPv6 netmask behind the tunnel" fields.

In order to **confirm all settings** made above, click on "OK".

In order to **upload a certificate or key**, click in the section "Upload key or certificates" on the "Browse..." button (button depends on the used browser). Then, select in the "Upload file" window the desired file on the respective data carrier and click on the "Open" button. If the file is encrypted, you must also enter the password into the "Password (only with encrypted file)" field. Click on "OK" then to upload the file.

13.3.4 Setting Up an OpenVPN Client

You can use the MoRoS LAN as OpenVPN client, if you want to connect to an OpenVPN server via an unsecured network. This section describes the set-up of an OpenVPN client. The basic settings are reasonable factory defaults, which you need to adjust to the VPN which will be connected to the MoRoS LAN. Here, you define with which IP address or domain and via which ports the OpenVPN tunnel is established, and if the OpenVPN transmission is performed with the UDP or the TCP protocol. If the remote terminal can only be accessed via a proxy server, this can be configured accordingly. Moreover, you can specify here, whether a default route is set, the local address and the port are fixed, the remote terminal may change its IP address, LZO compression is used, packets are masked before tunnelling, which encryption algorithm is used during transmission, how big the tunnel packets are to be, and in which time intervals the OpenVPN client sends VPN pings to the server. In addition, you will have the option to display the OpenVPN status, the current configuration file, a configuration for an OpenVPN remote terminal (the OpenVPN sever) and a log of the last connection.

Configuration via web interface (menu "LAN (ext)", page "OpenVPN client")

In order to use **the OpenVPN client for a connection**, check the checkbox "Activate OpenVPN client".

In order to **display the state of the OpenVPN client**, select the link "OpenVPN client state".

In order to **display the messages of the last connection**, select the link "Display log of last connection".

In order to **display the configuration file of the router as OpenVPN client**, select the link "Display configurations file".

In order to **display a sample configuration for an OpenVPN server**, select the link “Create sample configuration file for remote terminal”.

In order to define the **IP address or the domain name of the remote terminal**, which you use to have the router establish the OpenVPN connection, enter an IP address or a domain name in the field "IP address or domain name of remote site".

Optionally, an **alternative remote terminal can be defined**, which will be used to establish the VPN connection, if the remote terminal configured above is not available. Enter an IP address or domain name into the "Alternative remote site" field for this.

In order to **define the local port at the MoRoS LAN as well as the port at the remote terminal**, enter a value for the required port into the entry fields "Tunnelling over port (local / remote)".

The **OpenVPN transmission protocol** is selected with the radio buttons "UDP" or "TCP". We recommend to use UDP to minimize latency.

If the remote terminal can only be accessed via a **proxy server**, enter its IP address or domain name into the "IP address or domain name of proxy server" field, select its type using the "HTTP" or "SOCKS5" radio buttons and enter its port into the "Port" field. If the proxy server requires an authentication, enter the access data into the "User name" and "Password" fields.

In order to **set a default route**, check the checkbox "Set default route (redirect-gateway)". The complete data traffic will be routed through the tunnel then.

It is not obligatory to provide the **local port and the IP address of the OpenVPN connection**. If you want to leave the use of ports and the IP address free, uncheck the checkbox "Bind to local address and port".

In order to **enable remote OpenVPN terminals to change its IP during a connection** ("**Floating**"), check the checkbox "Remote terminal is allowed to change its IP address (float)". This setting is activated by default.

In order to **enable or disable LZO compression**, check or uncheck the checkbox "Activate LZO compression". If already strongly compressed data (e.g. jpg) is transmitted, the compression will have hardly any effect; however, if compressible data (e.g. text) is transmitted, the compression may significantly reduce the transmitted volume of data. Switch the compression off, if the remote terminal does not support LZO compression.

In order to **mask the packets with the virtual tunnel IP address**, check the checkbox "Masquerade packets before tunnelling". The recipient of the packets sees the IP address of the tunnel end as sender then, not the address of the original sender.

In order to **use a different encryption method** than the preset method for the OpenVPN connection, select one of the encryption types in the drop-down list "Cipher algorithm". Blowfish 128 Bit, DES 64 Bit, DES EDE 128 Bit, DES EDE3 192 Bit, DESX 192 Bit, CAST5 128 Bit, IDEA 128 Bit, RC2 128 Bit, RC2 40 Bit, RC2 64 Bit, AES 128 Bit, AES 192 Bit, AES 256 Bit and no encryption are available.

In order to **use a different hash algorithm** than the preset one for the OpenVPN connection, select one of the hash algorithms in the drop-down list "Hash algorithm". SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 and no hash algorithm are available.

In order to configure the **detail level of the messages in the connection log**, enter the detail level into the field "Log level", where "0" disables the log record completely and "9" records the most detailed information.

In order to define a certain **fragmenting size for the OpenVPN tunnel packets** in bytes, use the entry field "Fragment packets". Enter the required maximum packet size in bytes here. If you don't enter a value, the OpenVPN packets will have a maximum size of 1.500 bytes. The actually transmitted amount of user data is lower, because OpenVPN creates a "protocol overhead", which means that the protocol information that is transmitted as well is a part of the packet size.

In order to **adjust the interval up to the key renegotiation**, use the entry field "Interval for renegotiation of data channel key". This interval configures the time in seconds, which must expire before new keys are created.

In order to **adjust the VPN ping interval**, use the entry field "Ping interval". Enter the interval in the amount of seconds, in which the OpenVPN client of the MoRoS LAN sends ping packets to the remote VPN terminal. The frequent ping is used to keep the connection open via several routers and gateways, which may participate in the connection and would close the channel in case there was no communication.

In order to adjust the **ping restart interval**, use the entry field "Ping restart interval". The ping restart interval configures the time in seconds after which the tunnel is to be established again, if no ping from the remote terminal has arrived during the complete time. The value "0" prevents the tunnel to be terminated, even if no ping is received any more.

In order to **send a ping via ICMP protocol** to a domain or an IP address additionally, enter this into the entry field "Additional ICMP Ping to". It is recommended to enter a domain name or IP address, which can only be connected via the tunnel, here. If the ping is not successful, a possibly existing tunnel will be terminated, and a new tunnel will be established. The ping interval is 15 minutes.

In order to **configure the authentication with certificates**, select the radio button "Authentication based on certificate". It is indicated under the option here, whether the individual certificates and keys are present (green checkmark) or not (red cross). Present certificates can also be downloaded (blue arrow) or deleted again (red cross on white box). The private key can only be deleted. Alternatively, or in addition to the usage of a client certificate and a private key, an user name/password combination can be used for the authentication with the OpenVPN server (however, the CA certificate is required in any case, which must be possessed by every participant of this VPN). Enter a user name into the field "User name" as well as the associated password into the field "Password" for this. In order to check the certificate type of the remote terminal, check the checkbox "Check remote certificate type". Check the checkbox " Activate tls-auth" to use a static key as well in addition to the certificates. The static key stored in the "Authentication with preshared key" section will then be used. Optionally, a direction can be specified in the "Use direction of key" drop-down list (refer to the note in the following for this).

ⓘ If tls-auth is used, it is possible to specify that the static key can only be used for a certain direction. It is important here that this setting is harmonised with the remote VPN terminal, i.e. no direction is configured for bot or the settings are complementary (0/1 or 1/0).

In order to **configure the authentication with static key**, select the radio button "No authentication or authentication with preshared key". It is indicated under the option here, whether the static key is present (green checkmark) or not (red cross). A present key can also be downloaded (blue arrow) or deleted again (red cross on white box). If no key exists, the remote terminal will neither be authenticated nor the data traffic through the OpenVPN tunnel will be encrypted. You can also generate a new static key using the "Generate a new static key" link. This static key must then be downloaded and also uploaded to the remote terminal. Enter the IP address of the local tunnel end into the "IPv4 tunnel address local" or "IPv6 tunnel address local" field and the IP address of the remote tunnel end into the "IPv4 tunnel address remote" or "IPv6 tunnel address remote" field. Enter the address as well as the associated netmask of the network behind the OpenVPN tunnel into the "IPv4 net address behind the tunnel" or "IPv6 net address behind the tunnel" and "IPv4 netmask behind the tunnel" or "IPv6 netmask behind the tunnel" fields.

In order to **confirm all settings** made above, click on "OK".

In order to **upload a certificate or key**, click in the section "Upload key or certificates" on the "Browse..." button (button depends on the used browser). Then, select in the "Upload file" window the desired file on the respective data carrier and click on the "Open" button. If the file is encrypted, you must also enter the password into the "Password (only with encrypted file)" field. Click on "OK" then to upload the file.

13.3.5 PPTP General

PPTP (Point-to-Point Tunnelling Protocol) is a VPN (virtual private network) that is not recommended for new installations. A recent alternative is OpenVPN.

PPTP establishes a WWAN connection via a tunnel set-up with the GRE protocol. To establish the tunnel, it is essential that the GRE (Generic Routing Encapsulation) protocol is routed without restrictions between the two PPTP participants and a TCP connection with port 1723 is possible. The TCP port 1723 is fix and cannot be modified. The GRE protocol is not always routed directly in the Internet. In this case, NAT can prevent to establish a tunnel, if performed.

We strongly recommend to use as long as possible passwords with special characters and the encryption method MPPE-128 Bit.

13.3.6 Setting up a PPTP Server

The settings for the MoRoS LAN as PPTP server are configured here. A maximum of 5 PPTP clients can log on to this server at the same time. However, it is possible to create more users, but only 5 tunnels can be active at the same time.

Configuration via web interface (menu "LAN (ext)", page "PPTP server")

For an operation as **PPTP server**, check the checkbox “Activate PPTP server”.

In order to **display the messages of the last connection**, select the link "Display log of last connection".

In order to **select the authentication method for the PPTP client at the server**, select this from the drop-down list “Authentication”". If the data traffic is to be encrypted via the PPTP connection using MPPE, the authentication type MS-CHAP-v2 is mandatory. PAP, CHAP, MS-CHAP or no encryption are also available.

In order to **select the encryption for the PPTP connection**, select this from the drop-down list “Encryption”. The same encryption must also be configured for the client. MPE 40, MPE 128 or no encryption are available.

In order to **adjust the MTU** (maximum permissible number of bytes in a packet to be transmitted), change the entry in the entry respective field.

In order to **adjust the MRU** (maximum permissible number of bytes in a packet to be received), change the entry in the respective field.

ⓘ The default settings of MTU and MRU are suitable for most applications and do not need to be modified usually.

Enter the **IP address of the local tunnel end** into the field "IPv4 tunnel address local". If no explicit address is specified, the PPTP server will use the IP address 192.168.0.1. If this address is already reserved, another address can be specified here.

Define the **available IP address pool for the tunnel ends of the PPTP clients** in the fields “IP address pool”. This pool must be in the network of the LAN. The PPTP clients address their destination directly with IP addresses in the LAN of the MoRoS LAN.

In order to **add a new user**, that is permitted for the connection of PPTP clients, enter a user name and a password into the respective fields for this. Click on "OK" to take over the user. You can delete existing users by checking the checkbox in the column "delete" of the respective user and clicking on "OK".

In order to **confirm all settings for the loaded tunnel** made above, click on "OK".

13.3.7 Setting Up a PPTP Client

The settings for the PPTP client are configured here. All packets through the PPTP tunnel are masked by the MoRoS LAN with its tunnel address.

Configuration via web interface (menu "LAN (ext)", page "PPTP client")

In order to use the MoRoS LAN as **PPTP client**, check the checkbox “Activate PPTP client”.

In order to **display the messages of the last connection**, select the link "Display log of last connection".

In order to define the **IP address or the domain name of the remote terminal**, to which the VPN connection is to be established, enter an IP address or a domain name in the field “IP address or domain name of remote site”.

Enter the **user name and the password** of the PPTP client for login to the server into the respective fields.

In order to **select the encryption for the PPTP connection**, select this from the drop-down list “Encryption”. The encryption that is also used by the PPTP server must be selected. MPE 40, MPE 128 or no encryption are available.

In order to **set the default route to this PPTP tunnel**, check the checkbox “Set default route”. The complete data traffic will be routed through the tunnel then. However, this is only possible, if no preferential default route has been set before.

If no default route to the tunnel is set, the **local subnet behind the tunnel must be defined**. Enter this network with respective netmask into the field "Remote subnet". Only that way, packets into the network behind the PPTP tunnel will be routed through the tunnel.

In order to **adjust the MTU** (maximum permissible number of bytes in a packet to be transmitted), change the entry in the entry respective field.

In order to **adjust the MRU** (maximum permissible number of bytes in a packet to be received), change the entry in the respective field.

ⓘ The default settings of MTU and MRU are suitable for most applications and do not need to be modified usually.

In order to configure a **connection check using a ping via ICMP protocol** to a domain or an IP address, enter this into the entry field “Additional ICMP ping to” to". It is recommended to enter a domain name or IP address, which can only be connected via the tunnel, here. If the connection check is not successful, a possibly existing tunnel will be terminated, and a new tunnel will be established. The ping interval is 15 minutes.

ⓘ If a tunnel aborts, this will not be re-established automatically, but the establishment will only be made after a new WAN connection establishment. Therefore, the condition of the tunnel should be checked using an ICMP ping in any case.

In order to **confirm all settings for the loaded tunnel** made above, click on "OK".

13.3.8 Setting Up IPsec

IPsec (Internet Protocol Security) is a security protocol for the safe communication via IP networks and can be used to set-up virtual private networks (VPN). Two subnets can be connected together using two suitable routers (e.g. INSYS MoRoS 2.1) via a secure tunnel. It is possible to configure up to 10 different tunnels.

A tunnel can also be used as fall back tunnel for another active tunnel. The active tunnel will always be started when establishing the WAN connection. If the additional ICMP ping is not successful, the active tunnel will be closed and the fall back tunnel will be started. If the connection check via ICMP ping fails for a fall back tunnel, the fall back tunnel will be closed and the active tunnel will be started.

Configuration via web interface (menu "Dial-In"/"Dial-Out"/"LAN (ext)", page "IPsec")

In order to use **IPsec for a connection**, check the checkbox "Activate IPsec".

In order to **display the current state of the IPsec tunnels**, select the link "IPsec current state".

In order to **display the messages of the last connection**, select the link "Display log of last connection".

In order to **configure NAT traversal**, use the drop-down list "NAT-Traversal" to select the desired option. If you select "activate" (default setting), all ESP (Encapsulating Security Payload) packets are additionally packed into a UDP packet and sent using the UDP port 4500, if a NAT router is detected. If you select "force", this behaviour will be enforced without checking for a NAT router (the remote terminal must also have NAT traversal enabled in this case). If you select "deactivate", a UDP data encapsulation will be prevented, what might lead to problems in operation with a NAT router. This setting applies for all tunnels.

In order to **configure the interval of the keep alive packets**, which are sent, if NAT traversal is used, enter the time in seconds into the field "Keep alive interval". This can prevent that e.g. a stateful firewall blocks the connection after an extended inactivity period.

In order to **select the tunnel, whose settings are to be edited**, select the desired tunnel from the drop-down list "Tunnel name" and click on the button "load to edit" then. If settings are made to the currently loaded tunnel, these must be taken over before using the button "OK", before a new tunnel is loaded to prevent that these settings get lost. Loading a tunnel does not save settings that have been made!

In order to **activate the loaded tunnel**, select the option "active" in the drop-down list "Activate tunnel".

In order to **specify the loaded tunnel as fallback tunnel for an active tunnel**, select the option "Fallback for ..." in the drop-down list "Activate tunnel".

In order to **assign a descriptive name to the loaded tunnel**, enter it into the field "Tunnel name". This makes the assignment of messages in the log or status view easier.

In order to **specify the remote terminal, to which the tunnel is to be established**, enter the IP address or the domain name of the remote terminal into the field "IP address or domain name of remote site". If no remote terminal is specified, incoming connection requests from all remote terminals are accepted, but no connection can be initiated. In this case, the "Action on dead peer" of the dead peer detection must be set to "hold", since no new incoming connection request can be accepted any more in case the existing connection has been terminated.

In order to **define a network behind the switch of the MoRoS LAN to be tunnelled**, enter this network with according netmask into the field "Local subnet". This does not have to be the actual local subnet, but can also be behind further gateways. In such a case it must be observed that the required routing rules are entered correctly. If this field is not completed, the local subnet is used automatically.

In order to **define the local subnet behind the remote terminal**, enter this network with according netmask into the field "Remote subnet". Only data, which is addressed to this network, is packed in ESP packets.

In order to **specify the ID of the remote terminal**, enter it into the field "Remote ID". The respective IP address is used as ID by default. If the actual IP address differs from the received ID (e.g. due to NAT routers in between) or is unknown, the ID of the remote terminal can be specified explicitly (a self-defined string, which must contain an "@"). When using certificates, the DN (Distinguished Name) is used as ID by default. The domain name of the remote terminal can also be used as ID, because it is resolved by a DNS lookup.

In order to **adjust the own ID**, enter it into the field "Local ID". This is only necessary, if the default ID can or shall not be used.

In order to **permit only a certain protocol and a certain port for the local tunnel end**, enter the IANA protocol number and the port (if the protocol supports ports) into the fields "Local protocol and port". If protocol and/or port are not specified here, all protocols or ports are permitted.

In order to **permit only a certain protocol and a certain port for the remote tunnel end**, enter the IANA protocol number and the port (if the protocol supports ports) into the fields "Remote protocol and port". If protocol and/or port are not specified here, all protocols or ports are permitted.

In order to **specify the authentication mode**, select it in the drop-down list "Authentication mode". The main mode is more secure, because all authentication data is transmitted encrypted. The aggressive mode is quicker, because it does not use encryption and the authentication is preformed via a passphrase.

In order to **define encryption and hash algorithms as well as the Diffie-Hellman group for the IKE key exchange**, select these from the drop-down lists "IKE algorithms". DES EDE3, AES 128/192/256 as well as SHA1 or MD5 and DH 768/1024/1536 are available.

In order to **define encryption and hash algorithms for the IPsec connection**, select these from the drop-down lists "IPsec algorithms". DES EDE3, AES 128/192/256 as well as SHA1 or MD5 are available.

In order to **enter the maximum number of connection attempts**, which must be exceeded that a remote terminal is considered as not available, enter this into the field "Maximum retries". A value of "0" means an infinite number of attempts here.

In order to **mask the received packets with the local IP address of the MoRoS LAN**, check the checkbox "Mask packets through tunnel". The recipient of the packets will see the local IP address of the MoRoS LAN as sender than, not the address of the original sender from the local net of the remote terminal.

In order to **configure the dead peer detection**, enter the interval, which is used to send requests to the remote terminal, in seconds into the field "Dead peer detection interval" and the maximum time, in which these requests must be replied, in seconds into the field "Dead peer detection timeout". Select the behaviour for a connection, which is considered as interrupted, in the drop-down list "Action on dead peer". If you select "restart" (default setting) here, the connection will be restarted, for "clear", it will be terminated, and for "hold", it will be held.

In order to **enable perfect forward secrecy**, check the checkbox "Activate perfect forward secrecy". This can prevent that the next key can be discovered more quickly from a hacked encryption. Both remote terminals must have matching settings to be able to establish the connection.

In order to **configure the interval for the IKE SA key renegotiation**, enter the value in seconds into the field "Interval for renegotiation of IKE SA". The minimum value is 3600 seconds (1 hour). The regular renewal of the used keys can ensure the security of the IPsec connection for a longer period.

In order to **configure the interval for the IPsec SA key renegotiation**, enter the value in seconds into the field "Interval for renegotiation of IPsec SA". The minimum value is 3600 seconds (1 hour). The regular renewal of the used keys can ensure the security of the IPsec connection for a longer period.

in order to **send an additional ping via ICMP protocol to an IP address**, enter this address, which must be located in the local subnet of the remote terminal, into the field "Additional ICMP ping to". If the ping is not successful, a possibly existing tunnel will be terminated, and a new tunnel will be established. The ping interval is 15 minutes. An additional second IP address as ping target can be specified behind the first separated by a "#".

In order to **configure the authentication for an IPsec connection**, select either the radio button "Authentication based on certificates" or the radio button "Authentication with pre shared key (PSK)“. The authentication with certificates can be used for the main mode. It is indicated under the option here, whether the individual certificates and keys are present (green checkmark) or not (red cross). Present certificates can also be downloaded (blue arrow) or deleted again (red cross on white box). The private key can only be deleted. The authentication with passphrase can be used for main mode and aggressive mode. The passphrase, which must be used by all IPsec participants, must be entered into the field below the option for this.

In order to **confirm all settings for the loaded tunnel** made above, click on "OK".

In order to **upload a certificate or key**, click in the section "Upload key or certificates" on the "Browse..." button. Then, select in the "Upload file" window the desired file on the respective data carrier and click on the "Open" button. If the file is encrypted, you must also enter the password into the "Password (only with encrypted file)" field. Click on "OK" then to upload the file.

13.3.9 Configuring a GRE Tunnel

The Generic Routing Encapsulation protocol allows to transmit data transparently through an existing connection without changing the original packets.

Configuration via web interface (menu "Dial-In"/"Dial-Out"/"LAN (ext)", page "GRE")

In order to **enable a GRE tunnel**, check the checkbox "Activate GRE tunnel".

Enter the **remote tunnel terminal** as IP address or domain name into the "IP address or domain name of remote site" field.

Enter the **own IP address** that is to be used as tunnel end point into the "Own IP address" field. This may be the WAN, VPN or local LAN address for example.

Enter the **IP address of the local tunnel end** into the field "Tunnel address local". A netmask can be specified optional here. In this case, an appropriate route to this network will be created automatically, which enables to access the tunnel address of the remote terminal for example.

In order to **adjust the MTU** (maximum permissible number of bytes in a packet to be transmitted), change the entry in the entry respective field.

ⓘ The default settings of MTU is suitable for most applications and does not need to be modified usually.

If you want to **specify a TTL (Time to Live)**, enter this into the "TTL (Time to live)" field. If no TTL is specified, the TTL value from the tunneled packet is used for the GRE packet.

In order to **add a new route**, enter in the section "Add new route" the "IPv4 net address" and the "Netmask" as well as the "Gateway" into the respective fields. All fields must be completed that a new route is taken over into the table. Save the route by clicking "OK".

In order to **delete an existing route**, check under "Existing routes" the checkbox of the route(s) to be deleted.

Save your settings by clicking "OK".

13.4 Inputs and Outputs

13.4.1 Querying the Condition of the Inputs

The MoRoS LAN has digital inputs, which may trigger a PPP connection set-up, a message dispatch via e-mail, an OpenVPN tunnel set-up, a PPTP tunnel set-up, an IPsec tunnel set-up, or the set-up of a serial Ethernet connection. The inputs are closed when connected to GND. They are opened when there is no connection to GND. The conditions of the two inputs can be queried via the web interface.

ⓘ Input 1 is used to dispatch messages (see Messages section) and Input 2 is used to establish connections (see Configuring the Function of the Inputs).

Configuration via web interface (menu "In-/Outputs", page "Inputs")

In order to **query the conditions of the inputs**, click on the "Refresh" button. After the page has been reloaded, the conditions of the inputs are displayed next to "Input 1:" and "Input 2:".

13.4.2 Configuring the Function of the Inputs

The MoRoS LAN can establish a pre-configured dial-out connection, an OpenVPN tunnel, a PPTP tunnel, an IPsec tunnel or a serial Ethernet gateway connection, as soon as input 2 is closed for at least 4 seconds, i.e. connected to "GND". When activating the input, a dial-out or tunnel or connection set-up is performed as configured in the according menu. The connection will remain as long as the connection configuration allows.

Configuration via web interface (menu "In-/Outputs", page "Inputs")

In order to **configure the function of input 2**, select either the option "none", "Dial-Out automatically", "Establish OpenVPN tunnel", "Establish IPsec tunnel", or "Establish outgoing serial Ethernet connection".
The respective Dial-Out or OpenVPN/IPsec functions must be configured, to be triggered by the input.

In order to **trigger a Dial-Out connection only with input 2**, check the checkbox "Exclusively (dial-on-demand is deactivated)".

In order to **terminate a Dial-Out connection by opening input 2**, check the checkbox "Cancel if no longer connected with GND".

In order to **trigger an OpenVPN tunnel only with input 2**, check the checkbox "Establish exclusively via input (not automatically after Dial-Out)".

In order to **terminate an OpenVPN tunnel by opening input 2**, check the checkbox "Cancel if no longer connected with GND".

In order to **trigger a PPTP tunnel only with input 2**, check the checkbox "Establish exclusively via input (not automatically after Dial-Out)".

In order to **terminate a PPTP tunnel by opening input 2**, check the checkbox "Cancel if no longer connected with GND".

In order to **trigger an IPsec tunnel only with input 2**, check the checkbox "Establish exclusively via input (not automatically after Dial-Out)".

In order to **terminate an IPsec tunnel by opening input 2**, check the checkbox "Cancel if no longer connected with GND".

In order to **terminate an outgoing serial Ethernet connection by opening input 2**, check the checkbox "Cancel if no longer connected with GND".

Save your settings by clicking "OK".

13.4.3 Switch Outputs

The MoRoS LAN has digital outputs, whose condition can be queried and changed via the web interface.

The outputs can also be operated daily at a certain time. Moreover, it is possible to operate the outputs by establishing a PPP connection, an OpenVPN tunnel, a PPTP tunnel, or a serial Ethernet connection.

Configuration via web interface (menu "In-/Outputs", page "Outputs")

The **condition of the outputs** is displayed in the section "Manual switching of outputs" by the radio buttons next to the text "Output 1/2".

In order to **change the condition of the outputs**, select in the section "Manual switching of outputs" for the respective output "Idle condition" or "Operated condition" using the radio buttons and click "OK".

In order to **switch an output to operated condition daily at a certain time**, check in the section "Switching times Output 1/2" the checkbox "Switches to operated condition at" and enter into the following field the time for operating the respective output.

In order to **switch an output to idle condition daily at a certain time**, check in the section "Switching times Output 1/2" the checkbox "Switches to idle condition at" and enter into the following field the time for releasing the respective output.

In order to **configure output 1 for an operation with the presence of a PPP connection**, select under "Function of output 1" the option "Switches to operated condition if a PPP connection is established".

In order to **configure output 2 for an operation with the presence of an OpenVPN tunnel**, select under "Function of output 2" the option "Switches to operated condition if an OpenVPN tunnel is established".

In order to **configure output 2 for an operation with the presence of an PPTP tunnel**, select under "Function of output 2" the option "Switches to operated condition if an PPTP tunnel is established".

In order to **configure output 2 for an operation with the presence of an IPsec tunnel**, select under "Function of output 2" the option "Switches to operated condition if an IPsec tunnel is established".

In order to **configure output 2 for an operation with the presence of a serial Ethernet connection**, select under "Function of output 2" the option "Switches to operated condition if a serial Ethernet connection is established".

Save your settings by clicking "OK".

13.5 Configurable Switch

13.5.1 Querying Configuration and Status of the Switch Ports

The switch of the MoRoS LAN is configurable. This means that you can determine for each switch port individually which transmission rate should be used or if it is supposed to be operated in half-duplex or full-duplex mode. You may also control via the web interface, to which switch port a cable is connected and if a physical connection exists.

Configuration via web interface (menu "Server services", page "Port configuration")

You can **see the current configuration of the individual switch ports** next to the port list.

The coloured fields indicate **whether a cable is connected to the switch**. These fields indicate the four switch ports. The boxes are green if there is a network cable connected, and red if there is no cable connected or if no physical connection exists to the network.

13.5.2 Configuring Switch Ports

You can determine, which switch port is operated with which transmission rate and if it is operated in half-duplex or full-duplex mode. You can also determine if the auto negotiation (the recognition of the network cabling) is available at each port. These settings may be required if end devices have problems with the automatic recognition of the connection parameters. You can determine how the events at the network and the states of the switch ports are displayed at the switch port status LEDs.

Configuration via web interface (menu "Server services", page "Port configuration")

In order to enable or disable the respective switch port, use the checkbox "active" of the respective switch port.

In order to enable or disable auto negotiation, use the checkbox "Auto negotiation" of the respective switch port.

In order to define the transmission rate of a switch port, use the radio buttons "10 Mbit/s" and "100 Mbit/s".

To operate a switch port in full-duplex or half-duplex mode, use the radio buttons "Half-duplex" and "Full-duplex".

Save your settings by clicking "OK".

Note

Loss of availability!

The configuration will immediately be transferred to the switch after clicking on "OK". This may result that the device cannot be accessed any more.

Do not disable the switch port that is used to connect the configuration PC with the router.

13.5.3 Configuring the LED Display of the Switch Ports

You can determine how the events at the network and the states of the switch ports are displayed at the switch port status LEDs. We recommend not to change the basic settings and to change the displays only temporarily for diagnosis purposes.

Configuration via web interface (menu "Server services", page "LED configuration")

Select for the **respective network event or the state of the port the colour of the LED display** of the switch port status LED via the radio buttons.

Save your settings by clicking "OK".

13.5.4 Configuring VLAN

The switch of the MoRoS LAN can be divided in up to four VLANs. The VLANs are described as VLAN A, VLAN B, VLAN C, and VLAN D. The ports 1 to 4 are the switch ports accessible from outside. The device itself is connected to the 4-port switch via an internal port. The belonging of a port to a VLAN can be defined. The device can also belong to a VLAN. Each Ethernet packet that belongs to a VLAN will be marked by an identifier (tag). The VLAN tag contains the VLAN ID amongst others. Each port that belongs to a VLAN, will insert the VLAN tag automatically for the received packets, if it not already contained in the packet.

Configuration via web interface (menu "Switch", page "VLAN configuration")

In order to **enable VLAN configuration**, check the checkbox "Activate VLAN configuration".

In order to **assign a port or the router to a VLAN**, check the respective checkbox in the configuration matrix.

In order to **specify a VLAN ID for a >VLAN**, enter it into the field "VLAN ID".

In order to **specify for a port that belongs to a VLAN, whether it shall insert a VLAN tag into every received packet, or remove a possibly already existing one**, use the radio buttons "Insert VLAN tag" or "Remove VLAN tag" for the respective port. If a port shall belong to several VLANs, the VLAN tag must not be removed. The device connected to this port must be able to interpret these VLAN tags. The VLAN tags will always be removed for packets to the router.

Save your settings by clicking "OK".

Note

Loss of availability!

The configuration will immediately be transferred to the switch after clicking on "OK". This may result that the device cannot be accessed any more.

Therefore, configure the set VLAN on your locally connected device accordingly.

13.5.5 Configuring Port Mirroring

With port mirroring, you can copy the data traffic of a switch port to a definable, other switch port, called the sniffer port. This enables you to read the network traffic for analysis purposes. The transmitting and receiving packets (TX/RX) of certain ports can be mirrored separately to a sniffer port, where the network traffic can be read.

Configuration via web interface (menu "Server services", page "Port mirroring")

To use a port as sniffer port, select the according port in the drop-down list "Sniffer port".

Select in the drop-down list "TX mirroring to sniffer port" the port, **whose TX line data you want to copy to the sniffer port**.

Select in the drop-down list "RX mirroring to sniffer port" the port, **whose RX line data you want to copy to the sniffer port**.

Save your settings by clicking "OK".

13.6 Serial Ethernet Gateway

13.6.1 Setting up the Serial Ethernet Gateway

The serial Ethernet gateway enables the addressing of serial end devices from the local network of the MoRoS LAN or via the WAN interface, which are connected to the serial interface. The data which is sent to a configurable network port of the MoRoS LAN is output at the serial interface. The connection to the serial Ethernet gateway can either be maintained permanently (leased line mode) or set-up if required (connection on request).

The serial Ethernet gateway can be made dependent of the status of input 2 in the menu "In- / Outputs" on the page "Inputs".

Configuration via web interface (menu "Serial Ethernet", page "Serial Ethernet")

In order to enable the **serial Ethernet gateway**, check the checkbox "Activate serial Ethernet gateway".

In order to **display the current state of the serial Ethernet gateway**, click on the link "Serial Ethernet gateway current state".

In order to **display the log of the serial Ethernet gateway**, click on the link "Serial Ethernet gateway log".

In order to **configure the display of the serial Ethernet gateway log**, enter on the page "Serial Ethernet gateway log" into the field "Refresh after“ the update interval of the log in seconds as well as into the field "show last … lines" the number of lines to be displayed and select "OK".

In order to configure the **operation mode of the serial Ethernet gateway** , select either the radio button "Leased line mode" or "Connection on request".

In order to use an **IPT connection**, check the checkbox "Use IPT". In this case, the IPT slave must also be configured and enabled in the menu "Server services" on the page "IPT".

In order to increase the **time between connection attempts** in leased line mode, check the checkbox "increase reconnection interval". In this case, the interval between the connection attempts will increase (1, 5, 15, 30, 60 minutes). Otherwise, the MoRoS LAN will try to establish a connection every minute, if this is interrupted.

In order to enable **incoming connections**in "Connection on request" mode as well, select in the "Accept incoming connection" section either the radio button "TCP" or "Modbus TCP" and enter the port, on which the serial Ethernet gateway reacts on incoming connections, into the "Port" field. If "TCP" is selected, the serial Ethernet gateway monitors the port for incoming connections for transparent data transmission. This port is not necessary if IPT is used. Every incoming IPT connection will then be accepted. It is possible to allow outgoing and incoming connections simultaneously. If an incoming or outgoing connection is active in this case, the other is not available until the active connection is closed. If "Modbus TCP" is selected, the serial Ethernet gateway operates as Modbus TCP to RTU gateway. It accepts incoming Modbus TCP connections at the configured port (e.g. standard Modbus port: 502). It acts like a Modbus TCP Slave in doing so. All incoming requests are output at the serial interface as Modbus RTU requests and the replies from the Modbus RTU Slave are sent back to the Modbus TCP Master. All outgoing connections are disabled in this mode.

In order to **limit incoming connections to the local network**, check the checkbox “only local connections permitted”. No connections will then be accepted via the WAN interface.

In order to specify that the connection is only accepted, if an **UDP or TCP authentication of an INSYS VCom®** has been performed before, select in the "VCOM® authentication" section for "incoming" either the radio button "UDP" or "TCP". An existing connection will be terminated by a VCom® authentication during the existing connection. This setting is ignored if IPT is used.

In order to specify that an **ATD dialling command triggers an outgoing connection**, select in the "Outgoing connection" section the radio button "triggered by dialling command ATD". Then, the serial interface will be operated in AT command mode and a connection must be initiated by an ATD or ATDT command. The Serial Ethernet Gateway expects the dialling command ATD or ATDT via the serial interface with the destination as IP address or domain name, followed by the TCP port (e.g.: ATD192.168.1.1:1234 or ATD"name.company.com":1234. When using IPT, only the IPT number is specified here (e.g.: "ATD12345").

In order to specify that a **character on the serial interface triggers an outgoing connection**, select in the "Outgoing connection" section the radio button "triggered by serial character". Then, a connection will be established as soon as the serial interface receives a character. A destination must be specified in this operation mode. Enter the IP address or the domain name of the target into the "IP address or domain name" field as well as the port into the "Port" field. Alternatively, enter for an IPT connection the IPT number into the "IPT dial number" field. A secondary target can be entered optionally, to which a connection will be established if the primary target is not available. If the connection set-up fails, a new connection set-up cannot be performed before 5 minutes have expired.

In order to specify a **set-up of an outgoing connection by an active WAN connection**, select in the "Outgoing connection" section the radio button "triggered by active WAN connection". Then, a connection will be established as soon as a WAN connection is established. A destination must be specified in this operation mode. Enter the IP address or the domain name of the target into the "IP address or domain name" field as well as the port into the "Port" field. Alternatively, enter for an IPT connection the IPT number into the "IPT dial number" field. A secondary target can be entered optionally, to which a connection will be established if the primary target is not available.

In order to **establish a connection in leased line mode**, it is also necessary, to enter the IP address or the domain name of the target as well as the port or the IPT dial number. A secondary destination can be entered optionally.

In order to **establish an outgoing connection via input 2**, it is also necessary, to enter the IP address or the domain name of the target as well as the port or the IPT dial number. A secondary destination can be entered optionally. The function itself can be enabled in the menu "In- / Outputs" on the page "Inputs".

In order to use **authentication via TCP or UDP** at an INSYS VCom® for outgoing connections, select in the "VCom® authentication" section for "outgoing" either the radio button "UDP" or "TCP". This authentication will also be used in leased line mode or when establishing a connection via an input. This setting is ignored if IPT is used.

Save your settings by clicking "OK". The serial Ethernet gateway will be restarted with this. Existing serial Ethernet gateway connections will be terminated.

13.6.2 Configuring the Serial Ethernet Gateway Interface

The serial Ethernet gateway of the MoRoS LAN allows a comprehensive configuration of the serial interface and the packing of the data arriving there into TCP packets. It is also possible to use the Telnet protocol. RFC 2217 is also supported with this, which allows to modify the serial interface parameters during the operation via a Telnet connection.

Configuration via web interface (menu "Serial Ethernet", page "Interfaces")

In order to configure the **serial interface speed**, select the speed in the drop-down list "Speed (in Bit/s)".

Configure the **data format of the serial interface** in the drop-down lists "Data bits / Parity bits / Stop bits".

Select the **data flow control** (Hardware, i.e. RTS/CTS or Software i.e. XON/XOFF) in the drop-down list "Flow control". If the connected serial device does not support the respective data flow control, you must not use this.

In order to use the **control lines** DCD and DTR, check the checkbox "Use modem control lines".

In order to **reset the control lines after the connection is terminated**, check the checkbox "Reset modem control lines after connection termination".

In order to **set the control line DTR for signalling an established connection**, check the checkbox “Set DTR line on connection”.

In order to specify the **maximum block size**, from which the serially received data are packed to a TCP packet and sent when reached, enter the value into the field "Maximum block size".

In order to specify the **maximum time until packing a TCP packet**, enter the time into the field "Aggregation timeout" in milliseconds. If this time has expired, the serially received data will be packed to a TCP packet and sent, even if the maximum block size has not yet been reached. This timer will only be restated if the RS232 input buffer is empty and the first character is received. The subsequent characters do not reset the timer.

In order to **close the serial Ethernet connection automatically, if no data is transmitted** any more, enter a timeout value in seconds into the field "Idle time". If no data transfer takes place as long as specified here, the connection will be closed. To ensure that the connection is never closed, set the value to "0". The value "0" is the default setting.

In order to enable **sending keep alive packets**, enter the sending interval of the packets in seconds into the field "Keep alive interval". This function is disabled by entering "0". If the serial Ethernet gateway receives no reply to a keep alive packet for three consecutive times, the connection will be considered as interrupted and the serial Ethernet gateway terminates the connection.

In order to **use the Telnet protocol**, check the checkbox "Use Telnet protocol". In this case, the serial Ethernet gateway filters all Telnet commands from the incoming TCP data and replies them. Additionally, the serial and the TCP data stream are adjusted to transmit Telnet control characters error free.

Enter the **maximum connect time** to limit the duration of a connection. If you enter a maximum connection time, the connection will be closed after this time period has expired. To keep the connection open without any time restrictions (until the connection is terminated for other reasons), enter the value "0" in the field "Maximum connect-time".

Save your settings by clicking "OK".

13.6.3 Modem Emulator

The serial Ethernet gateway can emulate a modem. It provides a series of AT commands for this. A modem will be emulated for each connection type with this function. If an outgoing connection has been triggered by the ATD command, the modem emulator will always be used, even if it is disabled. The following AT commands are supported:

AT command	Description
ATA	Manual acceptance of an incoming TCP connection (via evaluation of the serial RING message)
ATD<IP>:<port> ATD“<domain>“:<port> ATDT<IP>:<port> ATDT“<domain>“:<port>	Connection set-up to <IP>:<port> or <domain>:<port> Following this, the serial Ethernet gateway is in data mode
ATDL ATDTL	Redialling of the last dialled connection (only possible as long as the serial Ethernet gateway has not been restarted)
ATH	The serial Ethernet gateway closes the serial Internet connection
ATE<n>	Configuring the echo behaviour ATE0 Echo disabled ATE1 Echo enabled (default)
+++	Puts the serial Ethernet gateway into command mode (a pause of at least one second is necessary before and after the string)
ATO	Change from command mode into data mode
ATQ<n>	Configuring the quiet behaviour ATQ0 Messages are sent (default) ATQ1 No messages are sent
ATV<n>	Configuring the message format ATV0 Messages in short format, i.e. only the error number ATV1 Messages in long format, i.e. the error text (default)
ATS0=<n>	Automatic call acceptance after <n> ring tones (<n> = 0 for disabling the automatic call acceptance)

AT command	Description
AT+FDIS AT+FDT	Puts the serial Ethernet gateway into fax mode. Then, the Modem emulation waits for a dialling command (ATD or ATDT) for 10 seconds. The dialling command hands over the phone number, but dialling will not yet be started. A CONNECT does not take place as well. Dialling will only be initiated if the command AT+FDT is received within 10 seconds.

Table 13: List of the AT commands supported by the serial Ethernet gateway

ⓘ Moreover, a reply to the ATI command is defined in the default AT answer file.

Configuration via web interface (menu "Serial Ethernet", page "Modem emulator")

In order to **enable the modem emulator**, check the checkbox “Activate modem emulator”.

In order to **enable the echo function using the ATE command** in the modem emulator, check the checkbox “Enable echo (ATE)”.

In order to **disable the answers using the ATQ command** in the modem emulator, check the checkbox “Disable answers (ATQ)”.

In order to **enable the verbose answers using the ATV command** in the modem emulator, check the checkbox “Enable verbose answers (ATV)”.

In order to configure the **number of ring tones until call acceptance**, enter the number of ring tones into the field “Number of rings until connection is answered (ATS0)”.

In order to configure the **default answer for unknown commands**, enter this into the field “Default answer for unknown commands”. If nothing is entered here, the message "ERROR" is returned in case of an unknown or invalid AT command.

The **modem message when establishing a connection** can be set in the “Message on connection” field to be able to emulate certain modems correctly. “CONNECT” is entered as standard message.

In order to allow the remote terminal to **close a connection with ATZ**, check the checkbox “Close connection on ATZ”.

In order to **download the current AT answer file**, click on the link “Download current AT answer file”.

In order to **upload an AT answer file**, click on the “Browse…” button and locate the respective file. The file will be uploaded after clicking on "OK". This file must be a text file, which defines an associated answer for each desired AT command. Each line in this text file defines an "command-answer-pair" in the form <i="Serial Ethernet Gateway Version 1.0">. The part preceding the "=" indicates the command (here "i" for ati; the "at" must be removed) and the part following in quotation marks indicates the associated answer (here "Serial Ethernet Gateway Version 1.0"). In this case, the message "Serial Ethernet Gateway Version 1.0" would be replied on the ati command. A multi-line answer within the quotation marks is possible. Capitalization is ignored. Moreover, the order of the entries must be observed. If an answer for the atxy command and the atx command is defined for example, the entry for the atxy command must be entered before the entry for the atx command, because otherwise the entry for the atx command would be found first and processed after entering the atxy command, before looking for a aty command, which does not exist.

In addition, a mapping for convertig phone numbers to IP addresses can be entered into the AT answer file. This allows for example that a connected analogue device can establish a connection to an IP address by dialling a phone number. Below the separator "--- ATD ---", the mappings follow in the text file in the form <phone number>=<IP address>:<port> or <phone number>="<domain name>":<port>. The characters 0-9, + and , are permissible for the phone number.

Save your settings by clicking "OK".

13.7 Messages

13.7.1 Configuring the Message Dispatch

The MoRoS LAN can send an e-mail or an SNMP trap to any recipient on different. A series of pre-define events are available for this, like signals or pulses at input 1 or set-up of connections or VPN tunnels for example.

Configuration via web interface (menu "Messages", page "Configuration")

In order to enable to **send an e-mail**, you must enter the necessary data for the e-mail account in the section "E-mail". Enter the e-mail address into the field "E-mail address" for this. Enter the first and last name of the person holding the e-mail account (or any text) into the field "Real name". Enter the domain name or the IP address of the SMTP server into the field "SMTP server" as well as the port, at which the SMTP server receives e-mails, into the field "SMTP port" (usually port 25). Enter the user name for the e-mail account into the field "User name" as well as the associated password into the field "Password". Check the checkbox "Use SSL/TLS" to send the e-mails encrypted.

In order to enable to **send an SNMP trap**, you must specify the SNMP version in the section "SNMP traps". In order to use SNMP v2c, select the radio button "SNMP v2c". Moreover, the community string must be entered into the field "Community". In order to use SNMP v3, select the radio button "SNMP v3". Moreover, the community string must be entered into the field "Community". In order to use an optional SNMP v3 authentication, select the authentication method in the drop-down list field "Authentication" and enter the password for the authentication (at least 8 characters) into the respective field. In order to use an optional SNMP v3 encryption, select the encryption method in the drop-down list field "Encryption" and enter the password for the encryption (at least 8 characters) into the respective field. An authentication is pre-condition for an encryption.

Save your settings by clicking "OK".

13.7.2 Configuring E-Mail Dispatch

The MoRoS LAN can send an e-mail to any recipient on different, pre-defined events. An attachment, which can be selected from different log files, can be attached to every e-mail. Moreover, it is possible to attach the status page of the web interface to the message text. It is possible to create and manage a series of different combinations of recipient, event, attachment, and text.

The signals at input 1 are distinguished between a long, at least 4 seconds long pulse and single pulses, which last between 200 milliseconds and 2 seconds with a pause between the pulses with the same time slot. The long pulse triggers the message for the simple alarm. The short pulses trigger the dispatch of messages for the according number of pulses.

Sending an e-mail is only possible if the access data for the e-mail account are entered correctly in the menu "Messages" on the page "Configuration".

Configuration via web interface (menu "Messages", page "E-mail")

In order to **enable e-mail dispatch**, check the checkbox "Activate e-mail messages".

In order to **create an e-mail message**, you have to define this in the section "Create new e-mail". Enter the e-mail address of the recipient into the field "Recipient" for this. Select from the drop-down list "Event" the respective event for triggering the e-mail dispatch. Select from the drop-down list "Attachment" the respective log file to be attached to the e-mail. If this file is not present on the MoRoS LAN, the e-mail will be sent without attachment. Check the checkbox "Attach current status to message text", if the status page of the web interface is to be attached to the message text. Enter the message text into the field "Text".

Save your settings by clicking "OK".

In order to **temporarily switch off e-mail messages**, uncheck in the section "Existing e-mails" the check box in the column "active" in the e-mail message overview. Click on "OK" to confirm the settings.

In order to **delete one or more e-mail messages**, check in the section "Existing e-mails" the check box in the column "delete" in the e-mail message overview. Click on "OK" to confirm the settings.

13.7.3 Configuring SNMP Trap Dispatch

The MoRoS LAN can dispatch an SNMP trap to any recipient on different predefined events. It is possible to create and manage a series of different combinations of recipient and event. The SNMP traps are described in the MIB (Management Information Base).

The signals at input 1 are distinguished between a long, at least 4 seconds long pulse and single pulses, which last between 200 milliseconds and 2 seconds with a pause between the pulses with the same time slot. The long pulse triggers the message for the simple alarm. The short pulses trigger the dispatch of messages for the according number of pulses.

Dispatching an SNMP trap is only possible if the settings for the SNMP traps are configured correctly in the menu "Messages" on the page "Configuration".

Configuration via web interface (menu "Messages", page "SNMP traps")

In order to enable **dispatching of SNMP traps**, check the checkbox "Activate SNMP traps".

In order to **download the private MIB**, click on the link "Download private MIB".

In order to **create an SNMP trap**, you have to define this in the section "Create new SNMP trap". Enter the IP address or the domain name and the associated port of the recipient into the fields "IP address or domain name" and "Port" for this. Select from the drop-down list "Event" the respective event for triggering the SNMP trap.

Save your settings by clicking "OK".

In order to **temporarily switch off SNMP traps**, uncheck in the section "Existing SNMP traps" the check box in the column "active" in the SNMP trap overview. Click on "OK" to confirm the settings.

In order to **delete one or more SNMP traps**, check in the section "Existing SNMP traps" the check box in the column "delete" in the SNMP trap overview. Click on "OK" to confirm the settings.

13.8 Server Services

13.8.1 Setting up DNS Forwarding

You may use the MoRoS LAN as DNS relay server. If it is configured as DNS server at the locally connected network devices, it will either forward the DNS requests to the previously configured DNS servers in the Internet, or will use the DNS server sent during the connection establishment. If IP addresses are combined with host names in the local host table ("Basic Settings" menu, "Host names" page), these will be processed first.

Configuration via web interface (menu "Server services", page "DNS")

In order to **disable the DNS relay**, uncheck the checkbox "Activate DNS relay".

In order to **specify further optional DNS servers**, enter the IP addresses of the according name servers in the entry fields "First DNS server address" or "First IPv6 DNS server address" and "Second DNS server address" or "Second IPv6 DNS server address".

Save your settings by clicking "OK".

13.8.2 Dynamic DNS Update

The MoRoS LAN can forward the IP address, which it was allocated during the dial-in into the Internet, to a DynDNS provider, so it can be reached from the Internet with a domain name. This means that the network behind the router can always be reached with the same domain name from the Internet, also for dynamically allocated IP addresses (if incoming connections are not blocked by the provider). The IP address connected to the domain name at the DynDNS provider will be updated for this during each dialup. For this function, you will need an account with a DynDNS provider.

Alternatively or additionally to the DynDNS protocol, it is possible to update up to five further DNS entries with the IP address of the router with the provider FreeDNS.

Configuration via web interface (menu "Server services", page "Dyn. DNS update")

In order to **configure the dynamic DNS update**, check the checkbox "Activate dynamic DNS update".

Select a **DynDNS provider** from the drop-down list "DynDNS provider".

In order to **define an own DynDNS server**, select in the drop-down list "DynDNS provider" the entry "Userdefined DynDNS" and enter a DynDNS server in the entry field "Userdefined DynDNS server".

Enter the **domain name to be updated** into the entry field "Domain name".

Enter **user name and password** of your DynDNS account into the entry fields "User name" and "Password".

In order to **use a DNS entry of FreeDNS**, enter the hash value generated by FreeDNS into one of the "Hash" fields.

ⓘ This hash value will be generated automatically when creating a domain to be updated. It can be taken from "quick cron example" or read out from the curl or wget scripts offered for download. It will be generated from user name, password and the domain to be updated and looks like this for example:
azVRU6MzSaVRcWc0WWs193c4MImQ6vTA37fDIz1Dc=

In order to **register the IPv6 address with FreeDNS**, check the checkbox "IPv6" behind the respective hash entry.

Save your settings by clicking "OK".

13.8.3 Setting up the DHCP Server

On request, the DHCP server of the MoRoS LAN can automatically allocate other devices in the LAN an address. This automatically allocated, dynamic IP addresses are only valid for a certain time. The validity of the IP addresses allocated by the DHCP server are controlled via the "Lease time". If there is already a DHCP server in the network, in which the MoRoS LAN is used, this function must absolutely be disabled in the device. Otherwise, clients would let their IP address be assigned by a wrong DHCP server.

IP addresses, which are in the IP pool and for which a connection to a MAC address exists, are exclusively reserved for this DHCP client. The IP address is thus not in the IP pool anymore. No IP addresses should be selected from the IP pool for this MAC IP address connections. The pool should only be available for the DHCP clients, for which no MAC address is known or is to be considered.

Configuration via web interface (menu "Server services", page "DHCP")

In order to setup the **DHCP server**, check the checkbox "Activate DHCP server".

Enter into the entry fields "First and last IP address" the **first IP address** and the **last IP address** of the address range, from which the DHCP server of the device allocates addresses in the LAN. The IP address range of the DHCP server must be located in the same network as the IP address of the MoRoS LAN.

Enter into the entry field "Lease Time" a **validity period** in seconds enter a Validity period for the **IP addresses** to be allocated by the DHCP server. The default value is 3.600 seconds.

In order to **inform the DHCP clients about a special DNS server**, enter its IP address into the entry field "Alternative DNS server address". If the field is empty, the local IP address of the router and the IP addresses of the fixed configured DNS servers are communicated to the clients.

In order to **specify an alternative gateway**, enter its IP address into the "Alternative default gateway address" field. If the field is empty, the IP address of the router will be proposed to the clients as gateway.

Save your settings by clicking "OK".

In order to view the IP addresses allocated by the DHCP server and their "Lease Time" (validity period), use the link "Display DHCP lease times".

You can define fix allocations in the section "Add new allocation of MAC address and IP address" in order to **allocate always the same IP address to DHCP clients**. For this, enter the MAC address of the respective DHCP client into the entry field "MAC address" and the IP address, to which the DHCP client is to be connected, into the field "IP address". The MAC address can be entered with or without colons; other formats are not supported. Save the allocation by clicking "OK".

In order to **delete one or more allocations**, check in the section "Fixed allocation of IP addresses to MAC addresses“ the checkbox in the column "delete" and click then "OK" to accept the setting.

13.8.4 Configuring the Router Advertiser

IPv6 prefixes can be advertised in the local LAN with the router advertiser. Machines connected to the LAN can configure one or several IPv6 addresses (SLAAC) independently using these received prefixes.

In order to support the configuration of the prefixes to be distributed, it will be displayed, which prefix is set in the MoRoS LAN and which prefixes are indicated at the LAN (ext) interface.

Configuration via web interface (menu "Server services", page "Router advertiser")

In order to enable the **router advertiser**, check the checkbox "Activate router advertiser".

Select the **Preference** in the drop-down list field "Preference". It specifies the importance to be used by the machines in the LAN for handling the received routes. If several router advertisers that distribute default routes are in the LAN, the preference decides, which default route is used by the machine in the end.

In order to **add a new prefix**, enter in the section "Add new prefix" the IPv6 net address and the netmask into the respective fields. Save the prefix by clicking "OK".

In order to **delete an existing prefix**, check under "Existing prefixes" the checkbox of the prefix(es) to be deleted.

Save your settings by clicking "OK".

13.8.5 Configuring a Proxy Server

The MoRoS LAN provides a proxy server. This does **not** serve as a cache for frequently accessed websites. It is used to delay the connection timeouts for connections that load slowly and to filter undesired URLs (e.g. www.xyz.xx).

The proxy supports the HTTP and HTTPS protocols.

Configuration via web interface (menu "Server services", page "Proxy")

In order to **enable the proxy server**, check the checkbox "Activate proxy server".

Enter in the entry field "**Port of proxy server**" the port, which you want to use to access the proxy server from the internal network at the IP address of the MoRoS LAN.

In order to **terminate connections,which seem to be inactive, after a certain time**, you can configure the time in seconds in the entry field "Timeout for inactive connections".

In order to **avoid overloading**, you can restrict the number of clients which can connect at the same time. Enter the maximum number of simultaneously authorized clients in the entry field "Maximum amount of allowed clients".

In order to **increase the availability** of the proxy, you can define a minimum number of proxy server processes. Enter the desired number of proxy server processes that are always running into the entry field "Minimum amount of free proxy servers".

In order to **avoid overloading with proxy requests**, you can define a maximum number of proxy server processes. An individual proxy server process is started on the MoRoS LAN for each client request. Enter the desired maximum number of simultaneous proxy server processes in the entry field "Maximum amount of free proxy servers" for this. If more requests are received than proxy servers are available, the additional requests are rejected.

Save your settings by clicking "OK".

13.8.6 Configuring an URL Filter

With the help of the URL filter, the proxy server can restrict possible URLs, which can be accessed by computers from the internal network of the MoRoS LAN. This will allow only access to URLs which are entered in the filter list. All other URLs are blocked. To allow access to the Internet only via the proxy, the firewall must be activated. Without the firewall, the access to any URLs would be possible just by bypassing the proxy.

The IP address and the port of the proxy must be defined at the clients (e.g. a web browser on a PC), which establish connections via the proxy.

Configuration via web interface (menu "Server services", page "Proxy")

In order to **enable the URL filter**, check the checkbox "Activate filter".

In order to **enter an allowed URL**, which is accessible from the internal network, enter the desired URL in the entry field "Allowed URLs".

In order to **delete an URL from the list**, delete the text of the URL from the list.

Save your settings by clicking "OK".

13.8.7 Configuring IPT

The MoRoS LAN also allows data transfer via an IPT channel. It can act as IPT slave here.

Configuration via web interface (menu "Server services", page "IPT")

In order to **enable IPT**, check the checkbox "Activate IPT slave".

In order to **display the current state of the IPT slave**, click on the link "IPT current state".

In order to **display the messages of the IPT slave**, click on the link "IPT log". This helps to draw conclusions on the failure cause in case of an unsuccessful connection attempt.

In order to configure the **connection to the IPT master**, enter its IP address or domain name into the entry field "IP address or domain name". Enter the port on which the IPT master accepts the connection into the entry field "Port". Enter the access data for registering at the IPT master into the entry fields "User name" and "Password". These data must be entered for the primary IPT master. A secondary IPT master can be entered optionally that will be used following an unsuccessful connection attempt to the primary IPT master.

In order to specify the **IPT device identifier**, enter it into the entry field "IPT device identifier". By default, a combination of the string "INS" and the MAC address of the MoRoS LAN is entered.

In order to increase the **time between connection attempts**, check the checkbox "Increase reconnection interval". In this case, the interval between the connection attempts will increase (1, 5, 15, 30, 60 minutes). Otherwise, the MoRoS LAN will try to establish a connection every minute.

In order to specify the **maximum time between IPT request and IPT response** that must be exceeded that the connection to the IPT master will be disconnected and re-established again, enter this time in seconds into the field "Timeout between request and response".

In order to specify the **maximum time between two characters of an IPT command** that must be exceeded that the connection to the IPT master will be disconnected and re-established again, enter this time in seconds into the field "Timeout between characters".

In order to enable **scrambling of the IPT connection**, check the checkbox "Use scrambling". If scrambling is used, a challenge and a fix scramble key must be specified. The fix scramble key encrypts the registration with the IPT master and the challenge scramble key is used for encryption following the successful registration. While the challenge scramble key is transferred from the slave to the master, the fix scramble key must be configured identically at the master and at the slave. Both keys must have the fix length of 32 bytes that must be specified hexadecimal with 64 digits for the configuration.

Save your settings by clicking "OK". The IPT slave will be restarted with this. Existing IPT connections to the master or existing IPT data tunnels will be closed before.

13.8.8 Configuring the SNMP Agent

The MoRoS LAN provides an SNMP agent that responds to incoming SNMP Get requests. All parameters that exist in the ASCII configuration file, can be read via SNMP Get requests (except user name and password of the web interface authentication). These parameters are described in the MIB (Management Information Base).

Configuration via web interface (menu "Server services", page "SNMP agent")

In order to **enable the SNMP agent**, check the checkbox "Activate SNMP agent".

In order to **download the private MIB**, click on the link "Download private MIB".

In order to permit SNMP Get requests **only from the local network** and send responds only to the local network, check the checkbox "Exclusively allow SNMP local".

In order to specify the **port**, on which the SNMP agent receives UDP messages, enter the port into the field "Port".

In order to specify a **contact information** for the SNMP agent, you can enter this into the field "Contact information".

In order to specify a **description** for the SNMP agent, you can enter this into the field "description".

In order to use the **SNMP agent**, you must specify and configure the SNMP versions to be used. In order to use SNMP v1 or SNMP v2c, check the checkbox "Use SNMP v1/v2c" and enter the community string into the field "Community". In order to use SNMP v3, check the checkbox "Use SNMP v3" and enter the SNMP user name into the field "User name". In order to use an SNMP v3 authentication, select the authentication method in the drop-down list field "Authentication" and enter the password for the authentication (at least 8 characters) into the respective field. In order to use an SNMP v3 encryption, select the encryption method in the drop-down list field "Encryption" and enter the password for the encryption (at least 8 characters) into the respective field. An authentication is pre-condition for an encryption.

Save your settings by clicking "OK".

13.8.9 Configuring MCIP

MCIP (Management Control and Information Protocol) is a minimalist protocol for exchanging short telegrams between an MCIP server and MCIP device drivers based on TCP. Device drivers register with the MCIP server and inform it about the Object IDs (OIDs) which can be addressed by it. An OID can be assigned to the objects contained in the router so that they can be addressed in MCIP telegrams. The state of the objects can be set and/or queried via the device drivers.

Configuration via web interface (menu "Server services", page "MCIP")

In order to enable **device drivers to register with the MCIP server via TCP**, check the checkbox "Accept incoming TCP connections on port" and specify the TCP port in the field behind.

In order to **limit MCIP connections to the local network**, check the checkbox "Exclusively allow MCIP local". No MCIP connections will then be accepted via the WAN interface.

Assign an **Object ID** to the objects contained in the MoRoS LAN by entering this into the field behind the respective object. An OID is a number between 1001 and 65534.

Save your settings by clicking "OK".

13.9 System Configuration

The MoRoS LAN displays system data such as firmware version, serial number, hardware revision or firmware checksum, together with short system messages about events and errors in the menu "System" on the page "System data". This information is helpful and should be known together with the configured IP address if you contact the support. Furthermore, several links enable to display system states and connection logs.

13.9.1 Displaying the System Log

The MoRoS LAN allows to display the detailed system log in the menu "System" on the page "System data". The number of displayed lines and the update interval can be configured.

Configuration via web interface (menu "System", page "System data")

In order to **view the detailed system messages via the web interface**, click on the link "Show the extensive system log".

In order to **configure the display of the system log**, enter on the page "System log" into the field "Refresh after“ the update interval of the log in seconds as well as into the field "show last … lines" the number of lines to be displayed and select "OK".

13.9.2 Displaying the Last System Messages

The MoRoS LAN displays short system messages about events and errors in the menu "System" on the page "System data". For analysis purposes, you can dispaly the last messages on the web interface.

Configuration via web interface (menu "System", page "System data")

In order to **display the last system messages**, click on the link "Show the last system messages".

13.9.3 Setting Time and Time Zone

The MoRoS LAN has an internal clock to control time-controlled events. This clock must be set to ensure that time-controlled events are processed precisely to the desired time, and that system messages are dated correctly.

The clock can be updated automatically via an NTP server from the Internet. During each connection establishment, it will be tried to synchronize the time from the specified NTP server. In contrast to the time, the time zone must be manually adjusted to the location. An NTP server for the local network can be started on the router itself. In this case, it is recommended that the router synchronises its clock via a WAN connection regularly, that the inaccuracies of the internal clock is compensated by a regular synchronisation to avoid that an inaccurate time will be broadcast in the network.

The time will be buffered internally for several hours in case of a power supply interruption.

Configuration via web interface (menu "System", page "Time")

In order to **configure time and date**, enter the values for day, month, year as well as hours and minutes into the entry fields "DD MM YYYY hh mm".

Configure the **time zone of the operation location** by selecting it from the drop-down list field "Timezone".

In order to **synchronise time and date via NTP server**, check the checkbox "Clock synchronization with" and enter the name of an NTP server or its IP address into the entry field.

In order to **synchronise time and date via NTP server daily at a defined time**, check the checkbox "Additionally every day at" and enter the time for the daily synchronisation into the entry field.

In order to **synchronise time and date via NTP server immediately**, check the checkbox "Update time now". Then, it will be tried to establish a one-time connection with the NTP server to synchronise the time with saving the settings. This enables an immediate test of the NTP server settings.

In order to **act as an NTP server itself**, check the checkbox "Activate local time server". Local NTP requests will then be responded at UDP port 123.

Save your settings by clicking "OK".

13.9.4 Reset

You can reset the MoRoS LAN via the web interface or by pressing the reset key on the front of the device. A software reset can be initiated by briefly pressing the reset key once. Pressing the reset key for at least three seconds initiates a hardware reset. A restart will be made in both cases. Pressing the reset key briefly three times within two seconds loads the factory defaults (see Section Display and Control Elements – Function of the Control Elements).

Configuration via web interface (menu "System", page "Reset")

In order to **restart**, select the radio button "Reset". Click on "OK" to execute the reset.

In order to **restart and load the default settings**, select the radio button "Load default configuration and reset". Then, click on "OK" to execute the restart and reset the device to default settings.

In order to **configure a daily restart at a defined time**, check the checkbox "Daily restart at" and enter the time for the daily restart into the entry field.

Save your settings by clicking "OK".

13.9.5 Update

You can update the MoRoS LAN with a new firmware or provide a new configuration using the web interface. A detailed description about these processes can be found in the following sections "Updating the Firmware" and "Uploading the Configuration File" of this manual.

Moreover, a daily automatic update of firmware files, configuration files (binary and ASCII) or sandbox image files is possible. These must be provided on a server accordingly for this.

Note

Loss of availability!

Upon changing the configuration,it may happen that your MoRoS LAN cannot be accessed for a further configuration (e.g. by changing the IP address).

Check critical settings, like IP address or access data (user name, passwords) very carefully.

Configuration via web interface (menu "System", page "Update")

In order to **enable the automatic update**, check the checkbox "Activate automatic daily update".

In order to **select the file transmission protocol**, select the radio button "HTTP" or "FTP".

In order to **specify the storage location of the update files**, enter the IP address or the domain name of the server into the "Server" field and the respective port into the "Port" field. It is also possible to specify sub-directories of the server that are to be searched for the files.

In order to **define a fix, MAC-depending time for the daily update**, select under "Update time" the radio button "depending on MAC".

In order to **define a user-defined time for the daily update**, select under "Update time" the radio button "fix" and enter the time for the update.

In order to **perform the daily update directly upon WAN connection establishment**, select under "Update time" the radio button "every time after connecting to WAN".

If the **file access is to be protected by an authentication**, enter the respective access data into the fields "User name" and "Password".

In order to **initiate the automatic update immediately**, check the checkbox "Search for updates now".

Save your settings by clicking "OK".

In order to **upload a firmware or configuration file (binary or ASCII)**, click in the section "Manual update" on the "Browse..." button. Then, select in the "Upload file" window the desired image file on the respective data carrier and click on the "Open" button. Click on "OK" then to upload the file.

13.9.6 Updating the Firmware

You can update the firmware of the MoRoS LAN manually. The firmware is a combination of operating system and programs, in which the device functions are implemented. You'll find the latest firmware under www.insys-icom.com/firmware.

Note

Function loss due to faulty update!

A connection failure during the update and a following restart may cause a loss of function of the MoRoS LAN.

As long as the red Status LED is illuminated, you are not permitted to perform any actions at the web interface, you must not pull the power plug and you must not perform a reset.

After a failed update, do not restart the device; contact the support of INSYS icom.

Complete update of the firmware

The following steps must be performed to update the firmware.

- ⇢ You have access to the web interface.
- ⇢ If you access the web interface via a dial-up connection, the connection must be maintained long enough to perform the uploads. The option "Maximum connect-time" should be set to "0" for the update, also the "Idle time".
- ⇢ You have ensured that the power supply cannot be switched off during the update procedure.
- ⇢ You have the firmware files with the names "system_<rev>" and "data_<rev>". The files can be located on the PC from which you want to perform the update.

1. ***In the menu "System", switch to the page "Update".***
2. ***Click on Browse... in the "Manual update" section and select the file "system_<rev>".***
3. ***Click on OK to start the update.***

   ✓ A page with a security query is displayed. Compare the displayed MD5 checksum with the MD5 checksum of the file (e.g. using the md5sum.exe tool). If they match, the file has been transferred correctly and you can proceed with the update. The time until the file is completely transmitted varies, depending on the firmware size.

4. ***Confirm the query with Yes.***

✓ The update process starts. The browser waits. During the update, the Status/VPN LED lights up red.

✓ After the completed update, a page is displayed which confirms the successful update procedure. Do not perform any action at the web interface until this page is displayed.

ⓘ An update of the file "data_<rev>" is not always necessary. You'll find further information about this in the PDF file contained in the firmware package.

5. ***In order to update the file "data_<rev>" also, proceed with the second file "data_<rev>" as with the first file, without performing a restart before. Repeat the steps from step 1. An automatic restart takes place following the upload.***

6. ***If you have only uploaded the file "system_<rev>", change in the "System" menu to the "Reset" page, select "Reset" and click on*** ***OK***.

✓ The new firmware is now active.

Note

Disabling the sandbox!

If a firmware update is performed, a possibly running sandbox will be disabled before.

Observe for your application that a running sandbox will be disabled, if a firmware update will be performed.

13.9.7 Uploading the Configuration File

You may upload a previously downloaded or edited configuration file to the MoRoS LAN, to replace the current configuration by the settings in the file.

Uploading the Configuration File

⇢ You have a configuration file for your version of the MoRoS LAN.

1. ***In the web interface under "System", switch to the page "Update".***
2. ***Click on Browse... in the "Manual update" section and select the configuration file (e.g. configuration.bin).***
3. ***Click on OK to start the upload.***

   ✓ A page with a security query is displayed.

4. ***Confirm the query with Yes.***

   ✓ The upload process of the configuration starts.

   ✓ After the completed upload, a page is displayed which confirms the successful update procedure.

5. ***In the menu "System", switch to the page "Reset", select "Reset" and click on OK.***

   ✓ The new configuration is now active.

13.9.8 Download

You can download the complete configuration file of the MoRoS LAN in binary, encoded form via the web interface. With this file, you can configure other, identical devices, or safely store a working configuration.

Moreover, it is possible to download an ASCII text file of the configuration or an "empty" configuration file (ASCII template). A description of the ASCII configuration file can be found in the respective add-on manual.

Downloading the different log files is also possible. Different log files are available depending on the version. The current log file is always available for download. If this log file exceeds a size of 1 MByte, it will be provided with a timestamp and saved as bzip2-compressed archive file. Up to four of the last archive files are available for download.

It is possible to download a support packet for support cases. This contains the status of the running device and the complete configuration and thus all data to provide a good troubleshooting basis when using the support of the manufacturer. The support packet will be encrypted so that the secret passwords or keys contained in it cannot be read out unauthorised in case of an insecure dispatch of the support packet.

Configuration via web interface (menu "System", page "Download")

In order to **download the binary configuration file**, click on the link "Binary". The name of the last uploaded configuration file is also displayed in the link. The browser will prompt you to save the file.

In order to **download the ASCII configuration file**, right-click on the "ASCII" link and select in the context menu "Save target as…". Then, save the file.

In order to **download an empty ASCII configuration file**, right-click on the "ASCII template" link and select in the context menu "Save target as…". Then, save the file.

In order to **download the log files**, right-click on the respective link and select in the context menu "Save target as…". Then, save the file.

In order to **download the support packet**, click on the link "Create new support packet". Click on the link that appears hereupon to save the support packet.

13.9.9 Sandbox

The MoRoS LAN provides a freely programmable sandbox. The sandbox is a kind of a virtual machine, which runs on the device. It is possible to start programs, collect data and offer services in the sandbox, which do not exist in the system of the actual device. Moreover, the MoRoS LAN can be configured out of the sandbox using an ASCII configuration file. A current configuration can be imported into the sandbox in addition. Refer to the add-on manual for the ASCII configuration file for further details.

You'll find further information about the sandbox and their use under http://www.insys-icom.com/Sandbox.

Configuration via web interface (menu "System", page "Sandbox")

In order to **enable the sandbox**, check the checkbox "Activate sandbox".

In order to configure the **password for the user "user"**, enter the desired password into the field "New password" (the default password is "user"). The user name itself cannot be changed. Permissible are only the characters 0 to 9, a to z, A to Z and the special characters ! " # $ % : ' ( ) * + , - . / ; < = > ? @ [ ] \ ^ _ { } | ~. The ampersand "&" is not permissible.

The file name of the currently **stored sandbox image** is indicated behind "Stored sandbox image:" together with its MD5 checksum.

The file name of the currently **installed sandbox image** is indicated behind "Installed sandbox image:" together with its MD5 checksum.

In order to **install a stored sandbox image**, the checkbox "Install stored sandbox image" must be checked. The image will then be installed after storing the settings with "OK".

ⓘ If an installed sandbox image cannot be started any more (if important files have been deleted unintentionally for example), a re-installation of the default image can recover the original state of the sandbox.

In order to **reserve the RS232 interface for the sandbox**, the checkbox "Reserve RS232 interface for sandbox" must be checked.

In order to **allow a configuration out of the sandbox without authentication**, the checkbox "Allow ASCII configuration without authentication from within the sandbox" must be checked. In this case, the sandbox will be searched for the file /var/spool/ascii_config.txt once a minute. If it exists, the MoRoS LAN will be configured using this ASCII file. Afterwards, the file will be deleted in the sandbox.

In order to **install a new sandbox image with automatic update**, the checkbox "Install new sandbox image on automatic update" must be checked. Otherwise, it will only be stored and must be installed manually.

Note

Unauthorised access to the device!

If the configuration out of the sandbox without authentication is allowed, the configuration can be tampered with to gain unauthorised access.

Ensure that only authorised users have access to the sandbox! By unauthorised access to the sandbox, the configuration can be modified using this function, so that the invader gets access to the configuration and thus to further confidential information, like VPN keys or passwords for example.

In order to **upload a new sandbox image**, click in the section "Upload new sandbox image" on the "Browse..." button. Then, select in the "Upload file" window the desired image file on the respective data carrier and click on the "Open" button. Click on "OK" then to upload the file.

Save your settings by clicking "OK".

13.9.10 Debugging

Various tools of the MoRoS LAN enable to analyse problems with network connections.

The "PING" tool allows to send ICMP pings (ping packets). This enables to test, whether a specific machine is available in the network, easily. The "TRACEROUTE" tool shows the route of an IP packet to its destination. The "DNS LOOKUP" tool allows to request DNS information via an IP address or a domain name. The "TCPDUMP" tool allows to record network packets.

Configuration via web interface (menu "System", page "Debugging")

In order to **send a ping packet**, select the tool "PING" for IPv4 pings or "PING6" for IPv6 pings in the drop-down list field, enter the IP address, to which you want to send the ping packet, or the domain name into the field "Parameter" and click on "OK". Optionally, you may enter additional parameters before, like -s 300 (sends 300 bytes as payload in ICMP ping) or -c 3 (sends subsequent 3 pings) for example. The reply will be displayed on the bottom of the page.

In order to **trace the route of an IP packet**, select the tool "TRACEROUTE" for IPv4 packets or "TRACEROUTE6" for IPv6 packets in the drop-down list field, enter the IP address, to which you want to send the IP packet, or the domain name into the field "Parameter" and click on "OK". Optionally, you may increase the standard number of 3 hops by increasing the number of hops to 5 for example using the parameter "-m 5" before. The reply will be displayed on the bottom of the page.

In order to **query DNS information**, select the tool "DNS LOOKUP" in the drop-down list field, enter the IP address or domain name to be queried into the field "Parameter" and click on "OK". If no DNS server has been configured or assigned by an external provider or router, this query may take up to 40 seconds.

In order to **start recording of network packets**, select the tool "TCPDUMP" in the drop-down list field, specify at least the network device using the parameter "-i" in the field "Parameter" (e.g. "-i br0" for the LAN interface) and click on "OK". The available network devices can be identified by selecting the link "Show current system state" in the menu "System" on the page "System data". After starting, the recording will continue until it is stopped manually, the logged network interface is closed (e.g. the cellular radio interface), or has reached a size of 1 MB. The recording will be displayed in text format immediately after stopping and can be downloaded as a file using the link "TCPDUMP recording"that will then be displayed. It can be viewed on an external machine using "tcpdump" or "wireshark". The recording will not be stored in case of a restart of the device.

13.10 Monitoring

The Monitoring App of the MoRoS LAN is displayed in a separate browser window upon selecting the menu item "Monitoring". It is a software application that runs on the device and is configured independently from the device.

It must be kept in mind that the functionality of the monitoring application can be affected by settings at the device (e.g. interface reservations for the sandbox).

The function and configuration is described in the Add-On Manual for Monitoring App. The add-on manual can be downloaded on the documentation page (www.insys-icom.com/manual) under the respective router.

14 Maintenance, Repair and Troubleshooting

14.1 Maintenance

The product is maintenance-free and does not require special regular maintenance.

14.2 Troubleshooting

If a failure occurs during the operation of the product, you will find troubleshooting tips in the "Knowledge Base" on our web site (http://www.insys-icom.de/knowledge/). If you need further support, please contact your reseller or INSYS icom. You can contact our support team via e-mail under support@insys-tec.de.

14.3 Repair

Send defect devices with detailed failure description to the source of supply of your device. If you have purchased the device directly from INSYS icom, send the device to: INSYS MICROELECTRONICS GmbH, Hermann-Köhl-Str. 22, 93049 Regensburg.

Before dispatching the device:

- Remove any inserted SIM cards.
- Backup the configuration on the device and any other stored data if required.
- Backup any sandbox applications running on the device.

Caution!

Short circuits and damage due to improper repairs and modifications as well as opening of products.

Fire hazard and damage of the product.

It is not permitted to open the product for repair or modification.

15 Waste Disposal

15.1 Repurchasing of Legacy Systems

According to the new WEEE guidelines, the repurchasing and recycling of legacy systems for our clients is regulated as follows:

Please send those legacy systems to the following address, carriage prepaid:

Frankenberg-Metalle
Gaertnersleite 8
D-96450 Coburg
Germany

This regulation applies to all devices which were delivered after August 13, 2005.

ⓘ Please consider possible stored passwords or security certificates before disposing the device. It is recommended to block possible existing access rights for the device (e.g. on your VPN server) and reset the device to default settings (if possible), before passing it on or disposing it.

16 Declaration of Conformity

Hereby, INSYS Microelectronics GmbH declares that herein described device types are in compliance with Directives 2014/30/EU and 2011/65/EU. The full text of the EC Declaration of Conformity is available under the following Internet address: www.insys-icom.com/manual

17 FCC Statement

Note: This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment under FCC rules.

18 Export Restriction

Note

Export restriction!

Possible violation of export regulations.

This device uses encryption technology and is therefore subject to export control as per German (AL classification 5A002) and European law (EG-DUAL-USE VO 428/2009). The export from Germany requires a permission of the Bundesamt für Wirtschaft und Ausfuhrkontrolle (Federal Office of Economics and Export Control).

This device may contain components with US origin. Possible export conditions as per US law (ECCN classification) will be mentioned explicitly on receipts.

19 Licenses

The software technologies and programs of the firmware used in the MoRoS LAN are partly bound to the following licenses. The source code of the firmware components of the MoRoS LAN which are bound to these licenses may be obtained from INSYS MICROELECTRONICS on request.

19.1 GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
>
> c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and

so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR

THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

19.2 GNU LIBRARY GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming

the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) The modified work must itself be a software library.
- b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestrict-

ed, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

- b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

- c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

- d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any

work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A

FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

19.3 Other Licenses

OpenVPN license:

Copyright (C) 2002-2005 OpenVPN Solutions LLC <info@openvpn.net>

OpenVPN is distributed under the GPL license version 2 (see below).

Special exception for linking OpenVPN with OpenSSL:

In addition, as a special exception, OpenVPN Solutions LLC gives permission to link the code of this program with the OpenSSL library (or with modified versions of OpenSSL that use the same license as OpenSSL), and distribute linked combinations including the two. You must obey the GNU General Public License in all respects for all of the code used other than OpenSSL. If you modify this file, you may extend this exception to your version of the file, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.

LZO license:

LZO is Copyright (C) Markus F.X.J. Oberhumer, and is licensed under the GPL.

Special exception for linking OpenVPN with both OpenSSL and LZO:

Hereby I grant a special exception to the OpenVPN project (http://openvpn.net/) to link the LZO library with the OpenSSL library (http://www.openssl.org).

Markus F.X.J. Oberhumer

OpenSSL License:

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in

the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

20 Glossary

This describes the most important terms and abbreviations of this manual.

APN: Access Point Name, computer name that provides cellular subscribers of the GPRS network with Internet access.

AT command: Commands to devices such as modems to set up this device.

Broadcast: Data packet that is sent to all participants of a network.

Caller ID: Phone number transmitted by the caller that can be evaluated by the called device.

Client: Device that requets services from another device (server).

CLIP: Calling Line Identification Presentation is a service feature for incoming calls in analogue and ISDN telephone networks as well as cellular radio. The caller ID of the caller is transmitted to the recipient.

CHAP: Challenge Handshake Authentication Protocol; an authentication protocol often used for PPP connections.

DHCP: Dynamic Host Configuration Protocol; DHCP servers can dynamically design an IP address and other parameters to DHCP clients on request.

Dial-in: The device can be called via a dial-in connection and then create a connection to the LAN.

Dial-out: The device can use a dial-up connection to make calls and establish Internet connections, for example.

DFÜ: Datenfernübertragung (remote data transmission); data can be exchanged between computers over considerable distances. The transmission is often realised with modems and the PPP protocol.

DNS: Domain Name System; service used for the translation of domain names into IP addresses.

Domain name: The domain is the name of an Internet site (e.g. insys-icom). It consists of the name and an extension (Top Level Domain, e.g. .com), (e.g. insys-icom.com).

EDGE: Enhanced Data Rates for GSM Evolution designates a technology for increasing the data rate in GSM cellular networks by introducing an additional modulation process. EDGE enhances GPRS to E-GPRS (Enhanced GPRS) and HSCSD to ECSD.

Firewall: Network rules that block in particular data packets to certain sources or destinations.

Gateway: This is a machine that works like a -> Router. In contrast to the router, a gateway can also route data packets from different hardware networks.

GPRS: General Packet Radio Service; advancement of the -> GSM cellular network to achieve higher data transmission rates.

GSM: Global System for Mobile communications; cellular network for voice and data transmission.

ICMP: Internet Control Message Protocol; protocol that is often used to control a network. The program "ping" uses ICMP for example.

IP address: Internet Protocol address; The IP address of a device in a network under which it can be accessed. It consists of four bytes and is indicated decimal, (e.g. 192.168.1.1)

ISP: Internet Service Provider; an ISP can be called using a dial-up connection (e.g. with an analogue modem or ISDN-TA). The ISP will then provide access to the Internet via this dial-up connection.

LAN: Local Area Network; a network of computers which are located relatively close to each other.

MAC address: Media Access Control Address. A MAC is a part of an Ethernet interface. Each Ethernet interface has a unique global number, the MAC address.

MSN: Multiple Subscriber Number. Devices that are active on an So bus require an answerback code in form of a terminal device number.

Netzmask: Defines a logical group of IP addresses in net address and device addresses.

Net address: Consists of the overlap of IP address and netmask. It always ends with "0". The netmask (e.g. 255.255.255.0) is applied in binary form to an IP address (e.g. 192.168.1.1); the still "visible" part of this overlapping (masking) is the net address (here: 192.168.1.0).

Network rules: You decide how the different data packets are handled in a network device. You can block or redirect data packets to or from certain network participants for example.

PAP: Password Authentication Protocol; an authentication protocol often used for PPP connections.

Port: (1) Socket at the switch for connecting Ethernet devices.
(2) Part of a socket for data connections

Port forwarding: Network rules that redirect data packets from certain senders to special recipients of a network.

PPP: Point to Point Protocol; a protocol, which connects two machines via a serial line to enable the exchange of TCP/IP packets between those two machines.

PPPoE: Point to Point Protocol over Ethernet; a protocol, which connects two devices via an Ethernet line to enable the exchange of TCP/IP packets between those two machines.

Router: This is a machine in a network, which is responsible for the incoming data of a protocol to be forwarded to the planned destination or sub network.

SCN: Service Center Number, phone number of the computer that accepts short messages (->SMS) via the GSM network and forwards them to the recipients.

Server: Device that provides services, e.g. web server, to other devices (client).

SMS: Short Message Service; short messages can be sent via the GSM cellular network.

Socket: Data connections that are established using ->TCP or ->UDP use sockets for addressing. A socket consists of an IP address and a port (cf. address: street name and number)

Switch: A device that can connect several machines with the Ethernet. In contrast to a hub, a switch will "think" by itself, i.e. it can remember the MAC addresses connected to a port and directs the traffic more efficiently to the individual ports.

TCP: Transmission Control Protocol; a transport protocol to enable data exchange between network devices. It operates "connection-based", i.t. the data transmission is protected.

UDP: User Datagram Protocol; a transport protocol to enable data exchange between network devices. It operates "without connection", i.t. the data transmission is not protected.

UMTS: Universal Mobile Telecommunications System stands for the third generation cellular standard (3G) that allows significantly higher data transmission rates (384 kbit/s to 7,2 Mbit/s) than the second generation cellular standard (2G), the GSM standard (9,6 kbit/s to 220 kbit/s).

URL: Uniform Resource Locator; this is the address used by a service to be found in the web browser. In this manual, an URL is mostly entered as the IP address of the device.

VPN: Virtual Private Network; logical connections (so-called tunnels) are established via existing unsafe connections. The end points of these connections (tunnel ends) and the devices behind can be considered as an independent logical network. A very high degree of tap- and tamper-resistance can be achieved with the encryption of the data transmission via the tunnels and the previous two-way authentication of the partcipants at this logical network.

WAN: Wide Area Network; a network consisting of computers, which are located far away from each other.

21 Tables and Diagrams

21.1 List of Tables

21.2 List of Diagrams

22 Index