

mbNET[®]

MANUAL V5.1.6 EN

MDH800 – MDH859

June 4th, 2019



MDH800, MDH802, MDH803, MDH804, MDH810, MDH811, MDH812, MDH813, MDH814, MDH815, MDH816, MDH817, MDH818, MDH819, MDH830, MDH831, MDH832, MDH832, MDH833, MDH834, MDH835, MDH841, MDH848, MDH849, MDH850, MDH855, MDH858, MDH859



Copyright © MB connect line GmbH 2007 – 2019

No part of this document and its contents may be reproduced, used or distributed without the express permission of MB Connect Line GmbH. Damages will be claimed in the event of infringement. All rights reserved.

By purchasing the **mbNET** router, you have chosen a product *made in Germany*.

Our products are produced exclusively in Germany, which guarantees the highest quality and safe-guards jobs in Europe.

This user manual (please read carefully and keep safely) describes the functions and use of the **mbNET** router MDH800 – MDH59.

The latest information and updates can be found on our homepage www.mbconnectline.com.

We welcome comments, suggestions for improvement or constructive criticism at any time.

Trademarks

The use of any trademark not listed herein is not an indication that it is freely available for use.

No part of this document and its contents may be reproduced, used or distributed without our express permission.

Damages will be claimed in the event of infringement.

All rights reserved.

MB Connect Line hereby confirms that the device **mbNET** (MDH8xx) complies with the basic requirements and all other relevant regulations of the European Directive 2014/30/EU resp. 2014/53/EU. You can view the Declaration of Conformity at: www.mbconnectline.com

Issued by:

MB connect line GmbH
Fernwartungssysteme
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY

Phone: +49 (0) 700 MBCONNECT
+49 (0) 700 62 26 66 32

Website: www.mbconnectline.com

1. Table of contents	
1. Table of contents.....	3
2. General.....	8
2.1 Purpose of this documentation	8
2.2 Validity of this documentation	8
2.3 Brief description	8
2.4 Features	8
2.5 Prerequisites/components:	8
2.6 Releas notes:	9
3. Safety Instructions (English and France)	10
4. Using Open Source Software.....	12
4.1 General Information.....	12
4.2 Special Liability Regulations	12
4.3 Used Open-Source Software.....	12
5. Technical specification.....	13
5.1 Dimensional drawing.....	13
5.2 Datasheet.....	14
5.3 General approvals	16
6. What is included in the package.....	17
7. Displays, controls and connections.....	18
7.1 Front panel view.....	18
7.2 Top, bottom and back panel views	19
8. Interfaces	20
8.1 Pinout of top panel terminal blocks X1 and X2	20
8.2 Pinout of bottom panel RJ11 jack	20
8.3 Pinout of front panel serial interfaces COM1 and COM2	20
8.4 Pinout of front panel LAN / WAN ports	21
8.5 Pinout front panel USB port	21
9. First time operation.....	22
9.1 Router installation.....	22
9.1.1 Mounting position / minimum distances	22
9.1.2 DIN rail mounting	22
9.2 Connecting the router to the power supply and switching on	23
9.3 Connecting the router to a configuration PC.....	24
10. Router configuration prerequisites	24
10.1 How to set computer address (IP address) and subnet mask in Windows 7.....	25
10.2 How to set computer address (IP address) and subnet mask in XP	26
11. Access the web interface of the router	27
11.1 Cloudserver	28
11.1.1 External Router	29
11.1.2 External DSL Modem	30
11.1.3 WLAN.....	31
11.1.4 Cloudserver	32
11.1.5 Start screen of the mbNET	33
11.2 Classic router	34

11.3	Configuration screen of the mbNET	35
12.	Basic configuration of the router using the web interface	36
12.1	Web interface home page	36
12.2	Icons, buttons and fields.....	37
12.3	System > CTM (Configuration Transfer Manager)	38
12.4	System > Settings.....	39
12.5	System > WEB.....	41
12.6	WLAN Configuration.....	43
13.	Description of different connection scenarios	46
13.1	General.....	46
13.2	Configuring the industrial router for connection over the telephone network	48
13.2.1	Connecting and configuring the router	49
13.2.1.1	Connecting the router	49
13.2.1.2	Configuring the router using the web interface.....	50
13.2.2	Configuring a client (PC) to access the router	53
13.2.3	Establishing a connection between the client PC and the industrial router.....	55
13.2.4	Displaying and verifying connection status	55
13.3	Configuring the industrial router for connection via the Internet	56
13.3.1	Connection and configuration of the router.....	56
13.3.1.1	Connecting the router	56
13.3.1.2	Configuring the router – client connection over the telephone network.....	57
13.3.2	Router Internet dial-in	62
13.3.3	Displaying the Internet connection	62
13.4	Configuring the industrial router for connection to the Internet using a DSL modem	63
13.4.1	Connecting and configuring the router	63
13.4.1.1	Connecting the router	63
13.4.1.2	Configuring the router using the web interface.....	64
13.4.2	Establishing a connection between client PC and router	66
13.4.3	Displaying connection status	66
13.5	Configuring the industrial router for connection to the Internet via an existing router	67
13.5.1	Connecting the router	67
13.5.2	Configuring the router using the web interface	67
13.6	Configuring the industrial router for VPN connection to a client	71
13.6.1	Connecting and configuring the router	72
13.6.1.1	Connecting the router	72
13.6.1.2	Adding VPN dial-in users	72
13.6.1.3	Configuration of the router (VPN-Server)	72
13.6.2	Configuring a client PC for a VPN connection to the router	75
13.6.3	Setting up a VPN connection between client PC and router	77
13.6.3.1	Router Internet dial-in.....	77
13.6.3.2	Setting up a VPN connection from client to router.....	77
13.6.3.3	Additional settings.....	77
13.7	Configuring a connection between two routers via VPN PPTP	78
13.7.1	Settings for connecting two industrial routers – PPTP – server	79
13.7.2	Settings for connecting two industrial routers - PPTP-Client	81
14.	Creating certificates and revocation lists using XCA.	83
14.1	Certificates overview	83
14.2	Creating certificates.....	84
14.2.1	Creating a root certificate.....	85
14.2.1.1	Root certificate source	85
14.2.1.2	Root certificate subject	86
14.2.1.3	Root certificate extensions.....	88

14.2.1.4	Root certificate key usage.....	90
14.2.2	Creating a client certificate	91
14.2.2.1	Client certificate source	92
14.2.2.2	Client certificate subject	93
14.2.2.3	Client certificate – Extensions.....	94
14.2.2.4	Client certificate – Key usage.....	95
14.2.2.5	Client certificate – Netscape.....	96
14.3	Generating CRL-Files (Certificate Revocation Lists)	98
15.	Importing certificates in Windows XP	100
16.	System settings.....	102
16.1	System – Users	102
16.1.1	General.....	102
16.1.2	Editing users	102
16.1.3	Adding users.....	103
16.1.4	Deleting Users	104
16.2	System – Certificates	105
16.2.1	Personal Certificates.....	105
16.2.2	Root certificate (CA)	107
16.2.3	Peer certificates (IPSec).....	108
16.2.4	CRL.....	109
16.3	System - USB	110
16.4	System – Logging	111
16.5	System – Configuration	112
16.6	System – Firmware	113
16.6.1	Upgrade via USB	113
16.6.2	Upgrade via Network	114
17.	Network	115
17.1	Network – LAN	115
17.2	Network – WAN	116
17.3	Network – Modem	118
17.3.1	Network – Modem –Incomming	118
17.3.2	Network – Modem – Outgoing.....	120
17.3.3	Menu Settings SIM	122
17.3.4	Network – Modem – Callback	124
17.3.5	Network – Modem – SMS	125
17.3.6	Remote service control commands using SMS	126
17.4	Network – Internet.....	127
17.4.1	Network – Internet – Internet Connections.....	127
17.4.2	Network – Internet – Internet Settings	128
17.4.3	Internet failover connection	130
17.5	Network – DHCP	133
17.6	Network – DNS server	134
17.7	Network – Hosts	135
17.8	Network – DynDNS.....	135
17.8.1	General.....	135
17.8.2	How to set up DynDNS configuration	135
18.	Serial interfaces.....	137
18.1	General.....	137
18.1.1	RS232/485 serial interfaces.....	137
18.1.2	MPI/PROFIBUS Interface	139
18.2	Redirecting serial interfaces to your PC (VCOM LAN2).....	141

18.2.1	Settings for Simatic Manager.....	142
18.3	Enabling RFC1006 on the mbNET.....	142
18.3.1	Settings for NETPro Step 7.....	143
18.3.2	Create subnets.....	143
18.3.3	Add PC station.....	144
18.3.4	Configure PC station.....	145
18.3.5	Add PC/PG station.....	146
18.3.6	Configure mbNET PC station.....	149
18.3.7	Routing.....	151
18.4	Connecting to S7 using the mbNET S7 driver.....	152
19.	Security.....	154
19.1	Firewall General.....	154
19.2	WAN > LAN.....	156
19.3	LAN > WAN.....	158
19.4	Forwarding.....	160
19.5	NAT.....	162
19.5.1	SimpleNAT.....	162
19.5.2	1:1 NAT.....	163
20.	VPN.....	164
20.1	VPN-IPSec.....	164
20.1.1	Configuring a VPN-IPSec connection with two routers.....	164
20.1.1.1	Connection settings.....	165
20.1.1.2	Network Settings.....	166
20.1.1.3	Authentication.....	167
20.1.1.4	Protocol settings.....	168
20.1.1.5	L2TP Server Configuration.....	169
20.2	VPN - PPTP.....	170
20.2.1	Server settings.....	170
20.2.2	Client settings.....	171
20.3	VPN – OpenVPN.....	172
20.3.1	Basics about OpenVPN.....	172
20.3.2	Connection scenarios.....	173
20.3.2.1	Client – router.....	173
20.3.2.2	Configuring an OpenVPN Windows client.....	177
20.3.3	Router-Router.....	180
20.3.3.1	Using the connection wizard.....	180
20.3.3.2	Server – no authentication or static key.....	182
20.3.3.3	Server – authentication with certificates.....	183
20.3.3.4	Client authentication: No or static key.....	185
20.3.3.5	Client authentication: With certificates.....	186
20.3.4	Authentication.....	187
20.3.4.1	No authentication.....	187
20.3.4.2	Authentication with static key.....	187
20.3.4.3	Authentication with certificates.....	189
20.3.5	Inactivity settings.....	193
20.3.6	Protocol options.....	194
21.	I/O Manager.....	196
21.1	Configuring the connection.....	197
21.1.1	Creating the PLC connection.....	198
21.1.1.1	Creating the tags.....	199
21.2	Configuring the logging function.....	200
21.3	Tag status.....	201

21.4	Diagnostic.....	201
22.	Alarm management	202
22.1	General.....	202
22.2	Digital inputs	202
22.2.1	Multiplex inputs	203
22.3	Digital outputs.....	205
23.	Status messages	207
23.1	General.....	207
23.2	Status – Interfaces	207
23.3	Status - Network.....	208
23.3.1	Firewall	209
23.3.1.1	IN / OUT / FORWARD	209
23.3.1.2	NAT	210
23.4	Status – Modem	211
23.5	Status – Internet.....	214
23.6	Status – DHCP.....	215
23.7	Status – DNS Server	216
23.8	Status – DynDNS.....	216
23.9	Status – NTP	217
23.10	Status – VPN-IPSEC.....	218
23.11	Status – VPN-PPTP.....	219
23.12	Status – VPN OpenVPN.....	220
23.13	Status – Diagnostics.....	221
23.14	Status – USB	222
23.15	Status – Alarmmanagement	222
23.16	Status – System	223
24.	Extras	224
24.1	LUA.....	224
24.2	Toolbox	225
25.	Firmware update directly via USB	226
26.	Importing the portal configuration into an <i>mbNET</i> via USB	227
27.	Factory settings on delivery	228
27.1	Username and password	228
27.2	IP address of the router	228
28.	Loading the factory settings	228
29.	Restart the mbNET router	229
29.1	Via webinterface	229
29.2	Via reset button.....	229
30.	Initializing the modem.....	230
	General information on the AT commands	230
30.1	Analog modem commands	230
30.2	ISDN terminal adapter (TA) commands	232
31.	Appendix	233
31.1	Country codes for analog devices	233

2. General

2.1 Purpose of this documentation

This user manual describes the functions and use of the mbNET router MDH800 – MDH859. Please read carefully and retain this information.

2.2 Validity of this documentation

This manual is valid for the router mbNET MDH800, MDH802, MDH803, MDH804, MDH810, MDH811, MDH812, MDH813, MDH814, MDH815, MDH816, MDH817, MDH818, MDH819, MDH830, MDH831, MDH832, MDH832, MDH833, MDH834, MDH835, MDH841, MDH848, MDH849, MDH850, MDH855, MDH858, MDH859 from firmware version V 5.1.6

2.3 Brief description

The **mbNET** industrial router offers you optimum flexibility and security, making remote communication with your systems both easy and secure. Thanks to its compact design, the **mbNET** router will fit into any switch cabinet, and with its multiple interfaces and drivers, is the perfect solution for integrating different control systems. The **mbNET** router is configurable using a web interface.

2.4 Features

- Fully configurable using web interface via locally connected computer, or remotely.
- Deployable worldwide using different modem connections, (ISDN, analog, mobile broadband) plus access via LAN and Internet.
- Secure connection using an integrated firewall with IP filter, NAT and port forwarding, VPN with AES, DES/3DES/DESX, Blowfish or RC2 encryption, and authentication via pre-shared key (PSK), static key or certificate (X.509).
- Alarm management:
 - Fully configurable digital inputs and outputs, and the ability to send via email, SMS or Internet dial-up.
 - Via remote output switching in the event of a fault or with an active Internet connection.
- Integrated server secures all settings, keys and certificates and allows data sharing within the network via connected USB flash or hard drive.
- Variable RS232, RS485, RS422 RS interface or optional MPI/PROFIBUS for connecting control systems.

2.5 Prerequisites/components:

RSP mbCONNECT24 from firmware V 2.4
mbCONNECT24 from firmware V 1.7
mbDIALUP* from firmware V 3.8
mbCHECK* from firmware V 1.1.2
mbNET* from firmware V 5.0

* The latest version can be downloaded from www.mbconnectline.com.

2.6 Releas notes:

Version	Date	
V 5.0	01.10.2017	
Comment		
<p>Previous version: V 3.3.5 DR 05 (23.03.2017)</p> <p>Changes:</p> <p>Chapter 11.1.4 Cloudserver Here, for the purpose of hardening the system, the verification via certificates was additionally added.</p> <p>Chapter 12.4 System > Settings > Time Settings The following functions have been added:</p> <ul style="list-style-type: none"> • „NTP Server Interval“ and • „NTP Server Defaulttime“ <p>Chapter 12.4 System > Settings > ... The "System Services" area has been added here and the functions (security features)</p> <ul style="list-style-type: none"> • „Disable Network Configuration (Conftool)“ and • „Enable Manufacturer System Access“. <p>Chapter 12.5 System > WEB > HTTP or HTTPS Access from Network A selection field (http or https) has been added here.</p> <p>Chapter 12.5 System > WEB > ... Here, as an additional security feature, the "Services" area has been added, including the functions</p> <ul style="list-style-type: none"> • „Disable complete Web-GUI (only recoverable with Factory Reset!)“ • "Disable Factory Webservice " • "Disable Communication Webservice (SMS/Email) " <p>Chapter 16.3 System > USB Changing the access function (access to USB only via SFTP).</p> <p>Chapter 18.1.1 RS232/485 serial interfaces and 18.1.2 MPI/PROFIBUS interface For additional hardening of the system, the function "Disable Service" has been added.</p> <p>Chapter 19.1 Firewall General Fundamental revision of the firewall.</p> <p>Chapter 19.2 WAN > LAN The "WAN Interface" selection field has been extended and a "LAN Interface" selection field for the target interface has been added. You can now enter ranges or enumerations in the fields IP and Port.</p> <p>Chapter 19.3 LAN > WAN Here, a selection field "LAN Interface" has been added and the existing selection field "WAN Interface" has been extended. You can now enter ranges or enumerations in the fields IP and Port.</p> <p>Chapter 19.4 Forwarding Change the interface target for forwarded packets from a checkbox to a selection field. You can now enter ranges or enumerations in the fields IP and Port.</p> <p>Chapter 19.5 NAT The menu has been extended by the "SimpleNAT" function.</p> <p>Chapter 22.3 Digital outputs Here the selection field "Function" was expanded by the option "On by any User -Cloudserver-connection".</p> <p>Added / inserted:</p> <p>Chapter 25 Firmware update directly via USB Chapter 26 Importing the portal configuration into an mbNET via USB</p>		

Version	Date	Comment
V 5.0 DR01	18. 07. 2018	Chapter 25. Firmware update directly via USB: Additional information.
V 5.0 DR01-1	13. 12. 2018	Chapter 25. Firmware update directly via USB: error correction <ul style="list-style-type: none"> • Now push and hold down the Dial Out button ① until LED Fc3 flashes ②. <p>“...until LED FC3 flashes...” is wrong, it has to be Fc2.</p>
V 5.1.6	08. 04. 2019	In chapter 19.1 Security > Firewall General the function SNAT (WAN) has been added. Correction of the description in chapters 19.2 - 19.4 "Input of ranges" in the input fields for IP addresses and "Input of ranges or enumerations" in the input fields for ports.
	04. 06. 2019	Updating the company logo

3. Safety Instructions (English and France)

- Only qualified specialist personnel may install, start up, and operate the router. The national safety and accident prevention regulations must be observed.
- The router is built to the latest technological standards and recognized safety standards (see Declaration of Conformity).
- The router is only intended for operation in the control cabinet and with SELV according to IEC 60950/EN 60950/VDE 0805.
- The router is for indoor use only.
- Never open the router chassis. Unauthorized opening and improper repair can pose a danger to the user. Unauthorized modifications are not covered by the manufacturer's warranty

Opening up the device voids the warranty!

- The router must be disposed of in line with European regulations and German legislation on electronics and electronic device (WEEE), and not as general household waste
- The router may only be connected to devices, which meet the requirements of EN 60950.



ADVICE:

- The unit should be connected and operated on a telephone switchboard only. The unit is not intended to be direct connected to a public telephone system.



NOTE:

Electrostatic discharge!

Observe the necessary safety precautions when handling components that are vulnerable to electrostatic discharge (EN 61340-5-1 and IEC 61340-5-1)!

Consignes de sécurité

- Le routeur est construit selon l'état actuel de la technique et les règles techniques reconnues en matière de sécurité (voir la déclaration de conformité).
- Le routeur doit être monté à un endroit sec. Aucun liquide ne doit pénétrer dans le routeur, car cela pourrait occasionner des chocs électriques ou des courts-circuits.
- Le routeur est uniquement prévu pour l'utilisation dans des bâtiments et non pas à l'extérieur.
- Ne jamais ouvrir le boîtier du routeur. L'ouverture du routeur ou des réparations non adaptées peuvent mettre en danger l'utilisateur du routeur. Le fabricant n'assure aucune garantie concernant les modifications arbitraires.

La garantie devient caduque en cas d'ouverture de l'appareil !

- Conformément aux prescriptions européennes et à la loi allemande relative à l'électronique et les appareils électroniques, il est interdit de mettre au rebut l'appareil avec les déchets domestiques normaux. L'appareil doit être éliminé dans le respect des prescriptions.

AVERTISSEMENT:

Les modèles MDH830, MDH820, MDH800, MDH810 et MDH815 doivent être utilisés et raccordés uniquement via des centrales téléphoniques. Il est interdit de les faire fonctionner directement sur le réseau téléphonique public.

4. Using Open Source Software

4.1 General Information

Our products contain, 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 products 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 products. In case there is a contradiction between the licensing terms for one of our products 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 products. The use of the open-source software in our products by the customer is not part of the earnings we achieve with the contractual compensation.

All open-source software programs contained in our products 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 products are subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), the Berkeley Software Distribution (BSD), the Massachusetts Institute of Technology (MIT) 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:

MB connect line GmbH
Fernwartungssysteme
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY

Tel. +49 (0) 98 51 / 58 25 29 0
Fax +49 (0) 98 51 / 58 25 29 99
info@mbconnectline.com

4.2 Special Liability Regulations

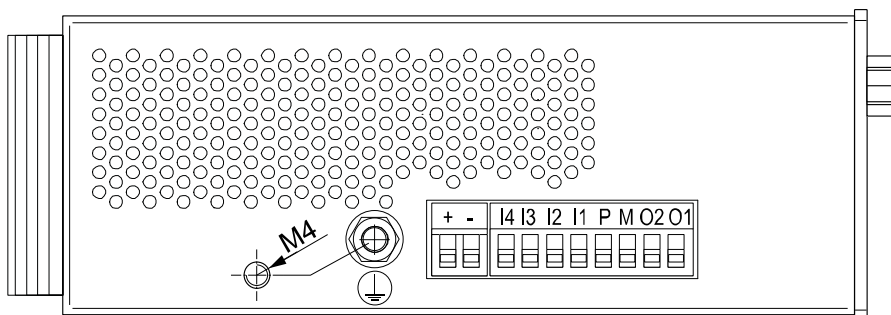
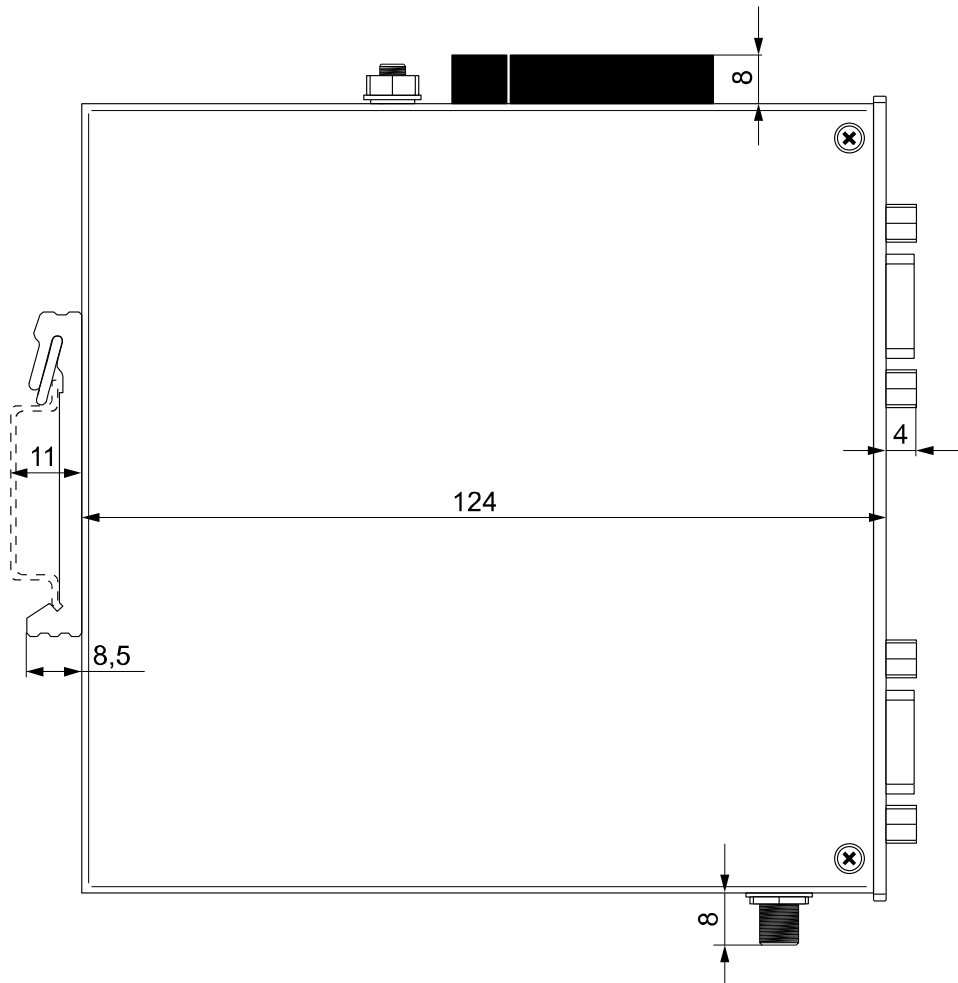
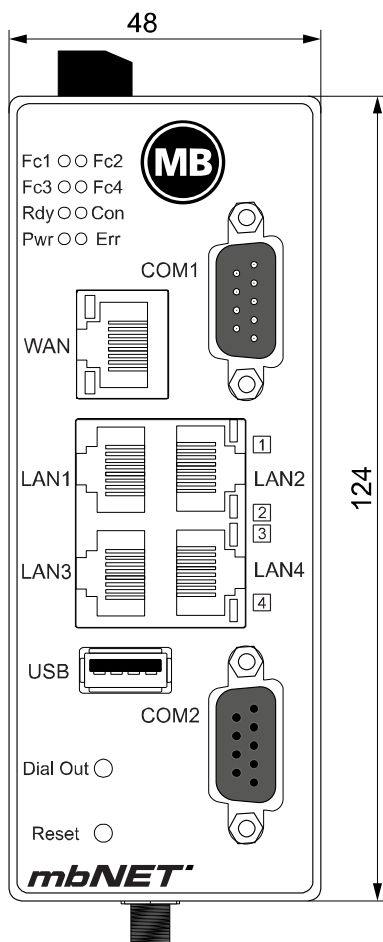
We do not assume any warranty or liability, if the open-source software programs contained in our product are used by the customer in a manner that does not comply any more with the purpose of the contract, which is the basis of the acquisition of our product. This concerns in particular any use of the 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.

4.3 Used Open-Source Software

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

5. Technical specification

5.1 Dimensional drawing



5.2 Datasheet

General data

Voltage $\text{---} \text{ V (DC)}$	10 – 30V DC (external Power Supply or other SELV Power Supply Source, rated 10-30V DC, max. 40A)
Power consumption	max. 1300 mA @ 24 V
IP protection class	IP 20
Area of application	Dry environments
Operating temperature	0 – 50 °C
Storage temperature	-20 – 60 °C
Humidity	0 – 95% (non condensing)
Dimensions (max.)	48 mm x 137 mm x 140 mm (W x D x H)
Weight (max.)	650 g
Housing (material)	Metal with plastic front
Mounting	DIN rail mounting (based on DIN EN 50022)

I/Os and standard interfaces

Digital inputs	4 pcs. digital inputs (10-30V) (fuse-protected), (Low 0-3,2 V DC, High 8-30 V DC)
Digital outputs	2 pcs. digital outputs (200mA max. / output), 200 mA @ 12 V DC / 100 mA @ 24 V DC
LAN interfaces	4 pcs. 10/100 Mbit/s full and half duplex operation, autodetection patch cable / crossover cable
USB interface	USB Host 2.0

VPN

VPN protocol	IPsec/PPTP/OpenVPN, 64 tunnel	Item no.: 8810-UL, 8811-UL, 8812-UL, 8813-UL, 8814-UL, 8830-UL, 8831-UL, 8833-UL, 8834-UL, 8850-UL-EU, 8850-UL-AT&T, 8855-UL-EU, 8855-UL-AT&T
Encryption method	Blowfish, AES, DES/3DES	
VPN protocol	OpenVPN, 1 tunnel	Item no.: 8815-UL, 8816-UL, 8817-UL, 8818-UL, 8819-UL, 8835-UL*, 8841-UL, 8849-UL, 8858-UL-EU, 8858-UL-AT&T, 8859-UL-EU, 8859-UL-AT&T
Encryption method	Blowfish	
Encryption algorithm	MD5, SHA1	
Authorization	Pre-Shared-Key, X.509	
*can only be operated with mbCONNECT24, mymbCONNECT24.hosted, -.virtual, -.mini, -.midi or -.maxi		

Network / Security


Firewall	1:1 NAT, IP-Filter, Port forwarding, stateful inspection
IP-Router	NAT-IP, TCP/IP routing, IP forwarding
Services	DHCP server, DHCP client, DNS server, NTP client, PPP server, DynDNS
Time synchronization	NTP server

Optional interfaces


WAN interface	10/100 Mbit/s full and half duplex operation, autodetection patch cable / crossover cable
Interface 1 (COM1)	RS-232/485 (using software switchable)
Interface 2 (COM2) depending on the device	RS-232/485 (using software switchable) or MPI/PROFIBUS - 12 Mbit/s
SIM card slots	2 pcs. SIM card reader with ejector (for mini-SIM)

Communication

Devices with analog modem (Item no.: 8810-UL, 8815-UL, 8830-UL)	
Target region	240 countries
Modulation type	V.21, V.22, V22bis, V.23, V.32, V.32bis, V.34
Data compression	V.42bis, MNP5
Error correction	MNP 2-4, V.42 LAPM
Dialing method	MFV/IWV
Modem connector	RJ11 socket
FCC	Part 15 & Part 68

Devices with UMTS (3G) modem (Item no.: 8814-UL, 8819-UL, 8834-UL, 8849-UL)	
Target region	Global
GSM / GPRS / EDGE	850, 900, 1800, 1900 MHz; downlink max. 296 kbps, uplink max. 236.8 kbps
HSxPA	800/850, 900, AWS 1700, 1900, 2100 MHz; downlink max. 21 Mbps, uplink max. 5.76 Mbps
Antenna connector	SMA socket 
FCC	FCC ID: R17HE910

Devices with UMTS (3G) modem (Item no.: 8813-UL, 8818-UL, 8833-UL)	
Target region	EMEA (Europe, the Middle East and Africa), Australia APAC (East Asia, Southeast Asia, Australia and Oceania) LATAM (Latin America)
GSM / GPRS / EDGE	850, 900, 1800, 1900 MHz; downlink max. 296 kbps, uplink max. 236,8 kbps
HSxPA	800/850, 900, AWS 1700, 1900, 2100 MHz; downlink max. 7.2 Mbps, uplink max. 5.76 Mbps

Devices with LTE (4G) modem (Item no.: 8850-UL-EU, 8855-UL-EU, 8858-UL-EU, 8859-UL-EU)	
Target region	EMEA (Europe, the Middle East and Africa), Australia
GSM /GPRS / EDGE	850, 900, 1800, 1900 MHz; max. 236 kbps
HSxPA	850, 900, 1900, 2100 MHz; downlink max. 42 Mbps, uplink max. 5.76 Mbps
LTE	800, 900, 1800, 2100, 2600 MHz; downlink max. 100 Mbps, uplink max. 50 Mbps
Antenna connector	SMA socket 
FCC	FCC ID: N7NMC7304

Devices with LTE (4G) modem - AT&T (Item no.: 8850-UL-AT&T, 8855-UL- AT&T, 8858-UL- AT&T, 8859-UL-AT&T)	
Target region	AMER (North and South America)
CDMA 1XRTT / EV-DO REV A	800 (BC0), 1900 PCS (BC1), Secondary 800 (BC10) MHz; max. 236 kbps
GSM / GPRS / EDGE	850, 900, 1800, 1900 MHz; max. 236 kbps

Communication

HSxPA	2100 (B1), 1900 (B2), AWS (B4), 850 (B5), 900 (B8) MHz CDMA EVDO/1x: BCO, BC1, BC10; downlink max. 42 Mbps, uplink max. 5.76 Mbps
LTE	1900 (B2), AWS (B4), 850 (B5), 700 (B13), 700 (B17), 1900 (B25) MHz; downlink max. 100 Mbps, uplink max. 50 Mbps
Antenna connector	SMA socket
FCC	FCC ID: N7NMC7355

Devices with WiFi modem (Item no.: 8811-UL, 8831-UL, 8841-UL) - not currently UL listed -	
WiFi	IEEE802.11b/g & 802.11n (1T1R mode), up to 150 Mbit/s
WiFi specification	<ul style="list-style-type: none"> · EU (2.412 GHz-2.472 GHz, 1-13 Channel) · USA (2.412 GHz-2.462 GHz, 1-11 Channel) · WPA/WP2, 64/128/152bit WEP, WPS · 802.11b: 1,2,5.5,11 Mbps · 802.11g: 6,9,12,18,24,36,48,54 Mbps · 802.11n: (20 MHz) MCS0-7, up to 72 Mbps · 802.11n: (40 MHz) MCS0-7, up to 150 Mbps
Antenna connector	RP-SMA socket
FCC	FCC ID: YWTWFXM05

5.3 General approvals




General approvals	EN 61000-6-4, interference emission for industrial enterprises EN 61000-6-2, immunity for industrial enterprises	
--------------------------	---	--




 I. T. E. E358792	The following models are UL listed
	MDH800, MDH802, MDH803, MDH804, MDH810, MDH812, MDH813, MDH814, MDH815, MDH816, MDH817, MDH818, MDH819, MDH820, MDH822, MDH823, MDH824, MDH830, MDH832, MDH833, MDH834, MDH835, MDH848, MDH849, MDH850, MDH855, MDH858, MDH859


Certificates (CE, UL etc.) can be downloaded from www.mbconnectline.com.

6. What is included in the package

First, check that the following parts are in the product package:

All devices		
		
mbNET router	Quick Start Guide	Straight-through Ethernet cable

Router variants with analog modem		Router variants with GSM modem (3G, 4G)
		
RJ11 plug	RJ10 to TAE adapter	GSM antenna (SMA male)

Router variants with WiFi modem

Wifi / Bluetooth antenna (2.5 m cable length) (SMA female)

Should any of these parts are missing or damaged, please contact the following address:

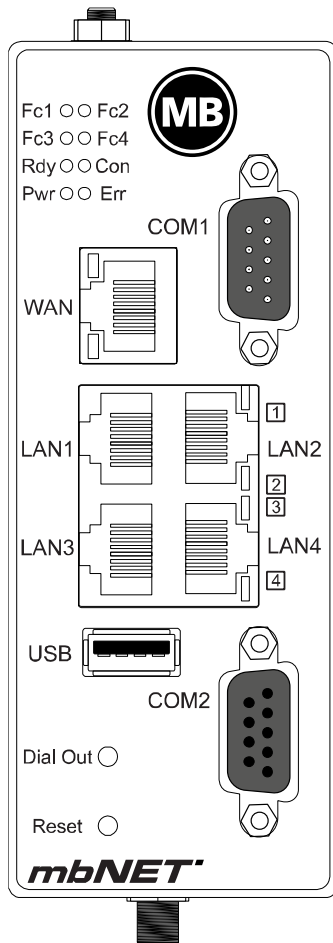
MB connect line GmbH
 Winnettener Str. 6
 91550 Dinkelsbühl
 GERMANY

Tel.: +49 (0)9851/282529-0
 Fax: +49 (0)9851/282529-99

Please keep the original box and the original packaging in case you need to send the device for repair at a later date.

7. Displays, controls and connections

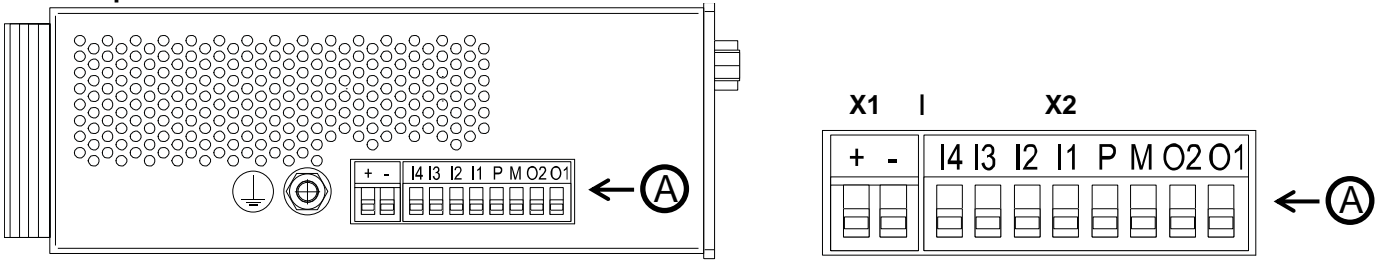
7.1 Front panel view



Label	Status	Description
Fc1 (Function 1)	LED off	Serial interface COM1 not receiving data.
	LED on	Serial interface COM1 receiving data.
Fc2 (Function 2)	LED off	Serial interface COM1 not sending data.
	LED flashing	Serial interface COM1 sending data.
Fc3 (Function 3)	LED off	Serial interface COM2 not receiving data.
	LED flashing	Serial interface COM2 receiving data. On if MPI: bus communication OK
Fc4 (Function 4)	LED off	Serial interface COM2 not sending data.
	LED flashing	Serial interface COM2 sending data. If MPI: bus transferring data
Rdy (Ready)	LED flashing	The Ready LED does this for approx. 35 seconds when the device is switched on. After this, flashing indicates boot sequence. This may take up to 90 seconds depending on the type of device.
	LED solid	The router is ready
Con (Connect)	LED off	No connection to Internet or VPN
	LED on	Connection to Internet
	LED flashing (1,5Hz)	VPN connection active
	LED flashing (3 Hz)	Internet or VPN connection is being established
Pwr (Power)	LED off	Router power source is switched off or router is not connected to power source / power pack.
	LED on	Power source is connected to terminal block and switched on.
Err (Error)	LED off	Router working without errors
	LED on	Router error. Diagnostics under System Status(see Status – System)
WAN	–	Router WAN port (customer network, DSL modem ...).
WAN LED	green light up	Network connection available
	flashing orange	Network data transfer active
LAN 1 – 4	–	Local network ports (e.g. machine network)
LAN LED 1 – 4 (Dual LED)	green light up	Network connection available
	flashing orange	Network data transfer active
USB	–	Portable USB drive port
Dial out	–	Among other things, this button establishes an Internet or VPN connection (hold down the button until the Con LED starts to flash).
Reset	–	Pushing this button restarts the router (so-called cold start).
COM1	–	COM1 port for connecting to devices with RS232 / RS485, RS422 interface.
COM2	–	COM2 port is for either connecting to devices with MPI interface or to devices with RS232 / RS485, RS422 interface. This depends on your device type.

7.2 Top, bottom and back panel views

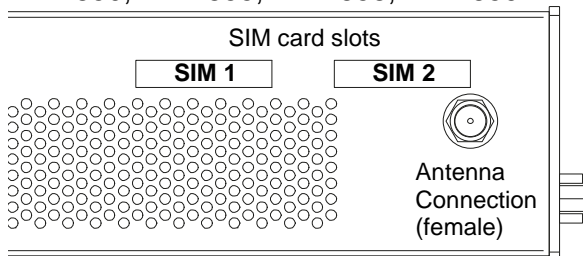
Top view



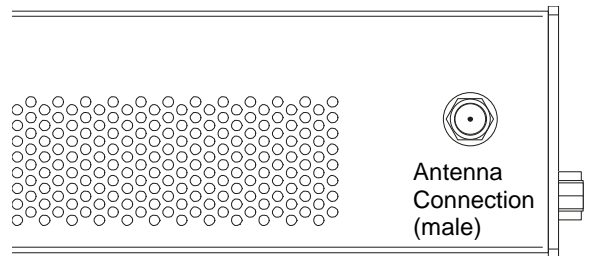
X1	+	Power supply connection 10-30V DC
	-	0V DC connection
X2	4	Digital input I4 (10-30V)
	3	Digital input I3 (10-30V)
	2	Digital input I2 (10-30V)
	1	Digital input I1 (10-30V)
	P	Fuse-protection 10-30V DC
	M	0V DC connection
	O2	Digital output A2
	O1	Digital output A1

Bottom view

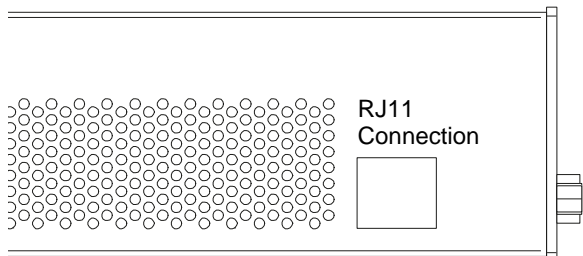
MDH814, MDH819, MDH834, MDH849,
MDH850, MDH855, MDH858, MDH859



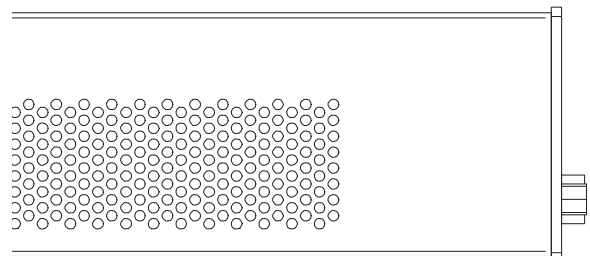
MDH811, MDH831, MDH841



MDH810, MDH815, MDH830



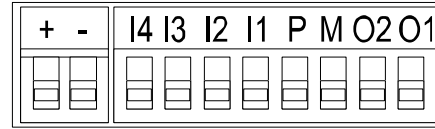
MDH816, MDH835



8. Interfaces

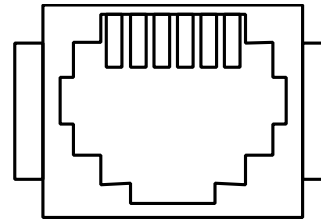
8.1 Pinout of top panel terminal blocks X1 and X2

X1	+	Power supply connection 10 – 30V DC
	-	0V DC connection
X2	1	Digital input I1 (10 – 30V)
	2	Digital input I2 (10 – 30V)
	3	Digital input I3 (10 – 30V)
	4	Digital input I4 (10 – 30V)
	P	Fuse protection 10 – 30V DC
	M	0V DC connection
	02	Digital output A2
	01	Digital output A1



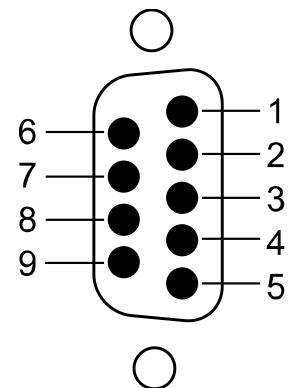
8.2 Pinout of bottom panel RJ11 jack

Pin	ISDN	Analog
1	Not connected	Not connected
2	TX+	Not connected
3	RX+	Lb/b
4	RX-	La/a
5	TX-	Not connected
6	Not connected	Not connected



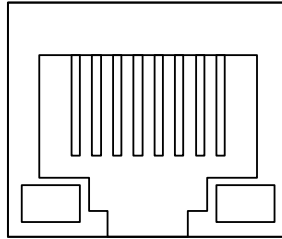
8.3 Pinout of front panel serial interfaces COM1 and COM2

Pin	RS 232	RS 485	MPI
1	COM1 / COM2 DCD Data Carrier Detect	Not connected	Not connected
2	RxD Receive Data	RxD – Receive Data	GND 24V
3	TxD Transmit	TxD + Transmit Data	Data circuit B
4	DTR Data Terminal Ready	+5Volts (only in 4-wire operation)	Send request
5	Ground signal	Ground signal	GND 5V(200mA)
6	DSR Data Set Ready	Not Connected	5V output
7	RTS Request to Send	TxD – Transmit Data	24V supply input
8	CTS Clear to Send	RxD+ Receive Data	Data circuit A
9	RI Ring Indicator	Not connected	Send request



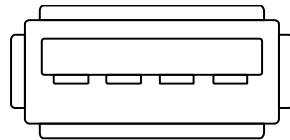
8.4 Pinout of front panel LAN / WAN ports

	Signal
	1 2 3 4 5 6 7 8
1	TX+
2	TX-
3	RX+
4	Not connected
5	Not connected
6	RX-



8.5 Pinout front panel USB port

	Signal
1	VCC (+5V)
2	- Data
3	+Data
4	GND



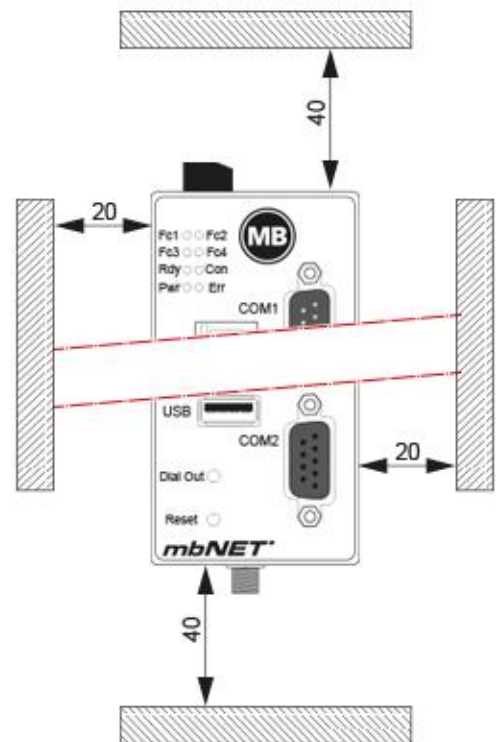
9. First time operation

9.1 Router installation

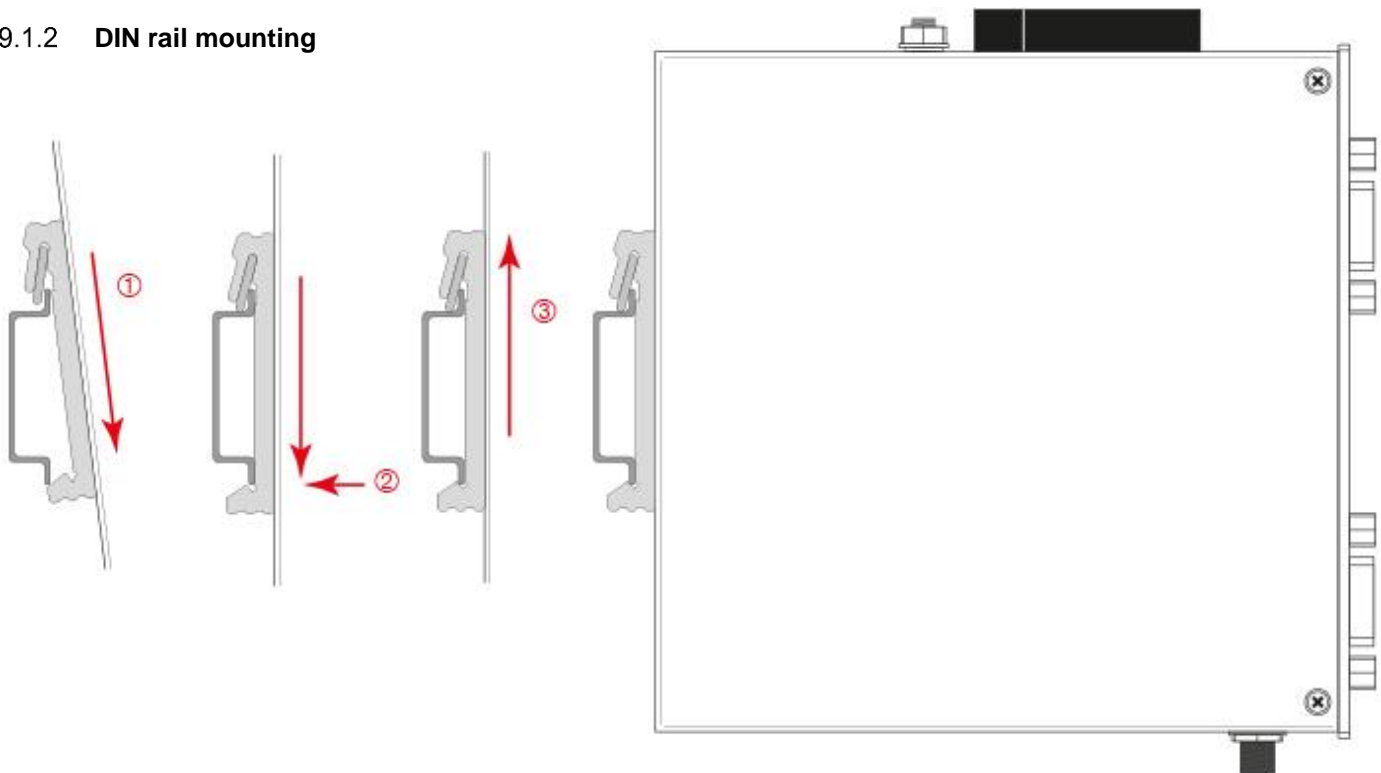
9.1.1 Mounting position / minimum distances

The **mbNET** router is designed for mounting on DIN rails (in accordance with DIN EN 50 022) and is intended for switchgear installation. Installation and mounting must be carried out in accordance with VDE 0100 / IEC 364. The router may only be installed in vertical position as described.

Failure to observe the minimum distances can destroy the device at high ambient temperatures!



9.1.2 DIN rail mounting



Insert the router into the DIN rail. To do this, position the upper guide on the rail and then press the router downwards against the rail until fully inserted.

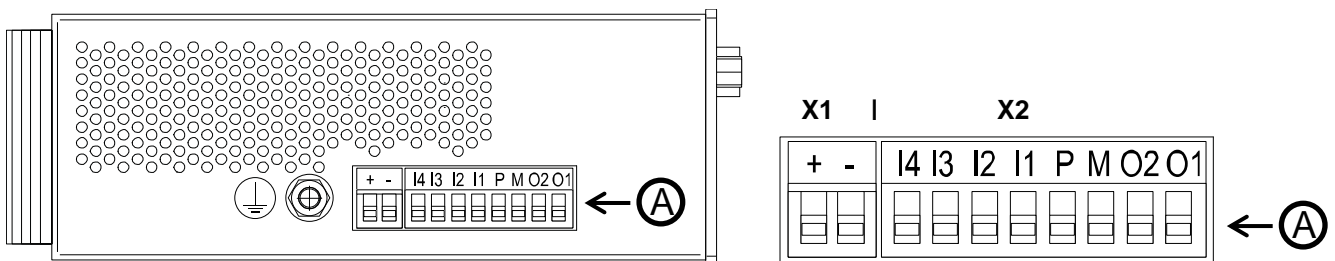
9.2 Connecting the router to the power supply and switching on

ADVICE

Before connecting the router to a network or PC, first ensure that it is properly connected to a power supply, otherwise it may cause damage to other equipment. You should therefore follow the instructions given below

IMPORTANT

Connect equipotential bonding to the grounding lug on the router's top panel!



- Connect the (10-30V DC) power supply to the **X1 terminal** of the router.
- Ensure correct polarity reversal!**
- Now switch on the power supply. The green **Power** LED should light up immediately. After approx. 90-110 seconds (depending on device model) the **Ready** LED should be solid. The device is now ready for operation.



For further support on the mbNET industrial router, visit our online support forum at www.mbcconnectline.de

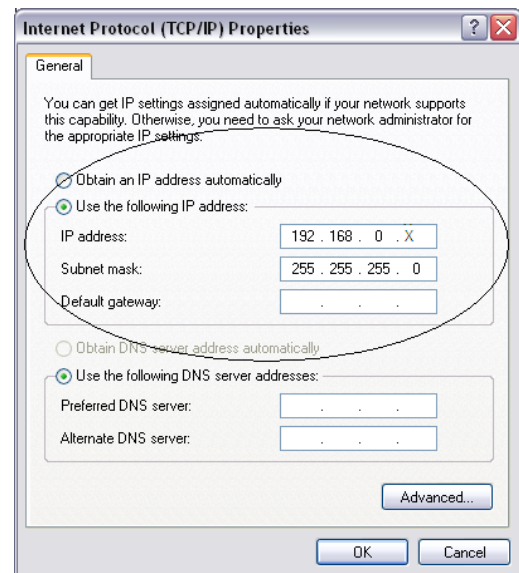
9.3 Connecting the router to a configuration PC

- ❑ Before configuring the router, connect it to the computer using the crossover cable supplied (1). To do this, connect one end of the cable to the router port labeled **LAN**, and the other end to your computer's network card.



10. Router configuration prerequisites

- ❑ a PC with a network card
- ❑ an Internet browser (HTML5-compatibility)
- ❑ The required settings on your PC are as follows:
 - the computer's IP address must be set to **192.168.0.X** where **X** is variable
 - the subnet mask must be **255.255.255.0**



For instructions on how to create the required settings on a PC, please see the next page. If you already know how to set the IP address and subnet mask, set them as described above and then proceed with configuration as described in Initial Configuration

10.1 How to set computer address (IP address) and subnet mask in Windows 7

To set the IP address, proceed as follows:

- ❑ First, select “Start” (1) then Control Panel from the Windows Start menu (2) and then click on Network Connections (3). Click on Network Center (4) then Change Adapter Settings (5).
- ❑ Right-click on **Local Area Connection (6)** and select **Properties**.
- ❑ In the next window, double-click on **Internet Protocol (TCP/IP)**
- ❑ In the next window, enter the appropriate IP address. An appropriate IP address would be e.g. **192.168.0.2**.



Please note:
the Internet IP address must be **192.168.0.X** and is not allowed to be already in use by another network subscriber.

- ❑ In Subnet mask, enter **255.255.255.0** and in Default gateway, enter the router IP address as shown in the section on [Router IP address](#).
- ❑ Where a DNS server is in use, there is an option to select “**Obtain DNS server address automatically**”.
- ❑ To save and close the settings, click **OK** on each of the open windows.

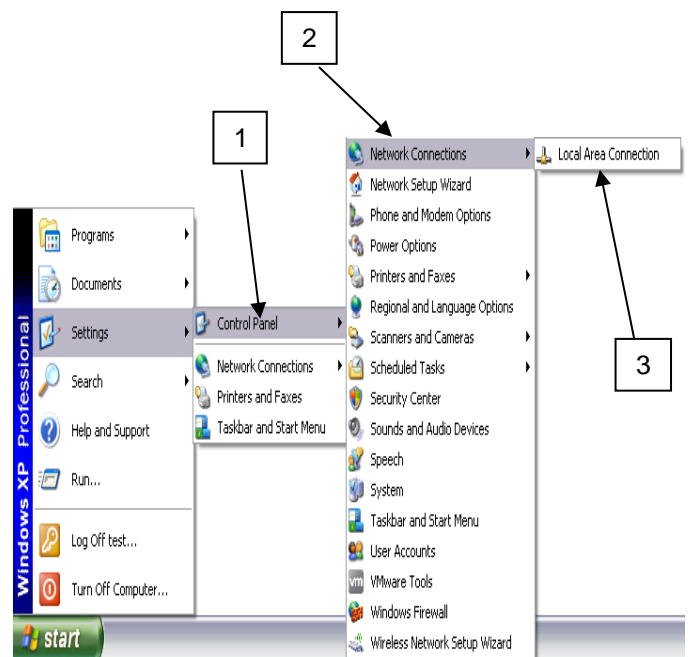
The screenshots illustrate the following steps:

- Clicking on the Start button.
- Clicking on Control Panel in the Start menu.
- Clicking on Network and Internet in the Control Panel.
- Clicking on Network Center in the Network and Internet window.
- Clicking on Change Adapter Settings in the Network Center.
- Right-clicking on Local Area Connection in the Network Connections window and selecting Properties.
- Clicking on Internet Protocol (TCP/IP) in the Local Area Connection Properties window.
- Clicking on the radio button for 'Folgende IP-Adresse verwenden' in the Internet Protocol (TCP/IP) Properties window.
- Entering the IP address '192.168.0.X' and the Subnetmaske '255.255.255.0'.

10.2 How to set computer address (IP address) and subnet mask in XP

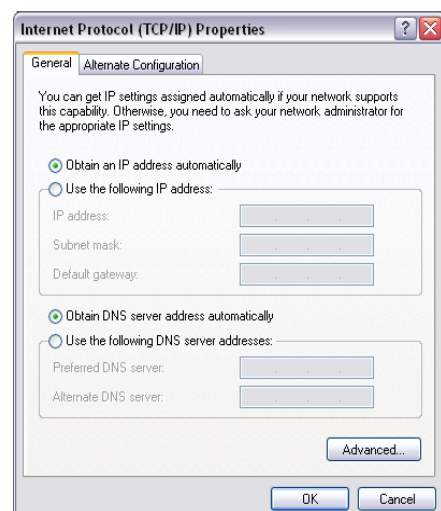
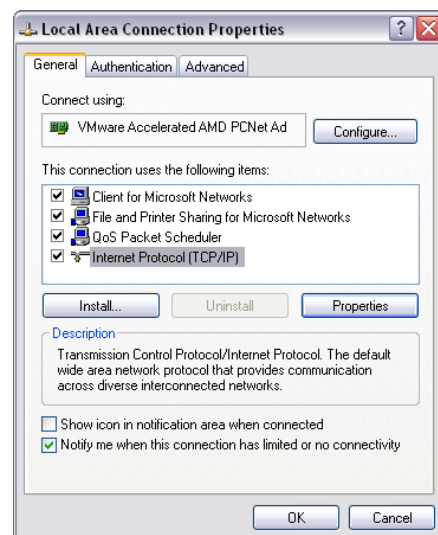
To set the IP address, proceed as follows:

- ❑ First, select Control Panel from the Windows Start menu (1) and then double-click on Network Connections (2).
- ❑ Right-click on **Local Area Connection (3)** and select **Properties**.
- ❑ In the next window, double-click on **Internet Protocol (TCP/IP) (4)**.
- ❑ In the next window, enter the appropriate IP address. An appropriate IP address would be e.g. **192.168.0.2**.



Please note:
the Internet IP address must be 192.168.0.X and is not allowed to be already in use by another network subscriber.

- ❑ In Subnet mask, enter **255.255.255.0** and in Default gateway, enter the router IP address as shown in the section on [Router IP address](#).
- ❑ Where a DNS server is in use, there is an option to select “**Obtain DNS server address automatically**”.
- ❑ To save and close the settings, click **OK** on each of the open windows.

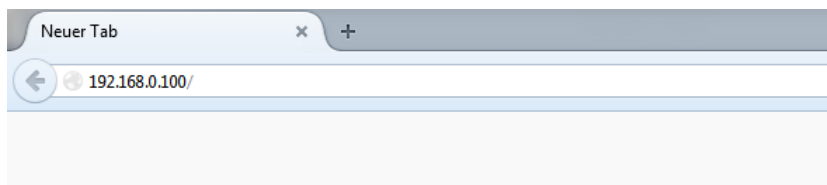


11. Access the web interface of the router

Proceed as follows:

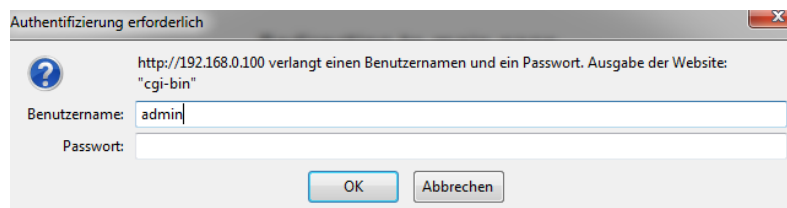
Open your browser and enter the router's IP address in the address bar:

The factory setting is: **192.168.0.100**



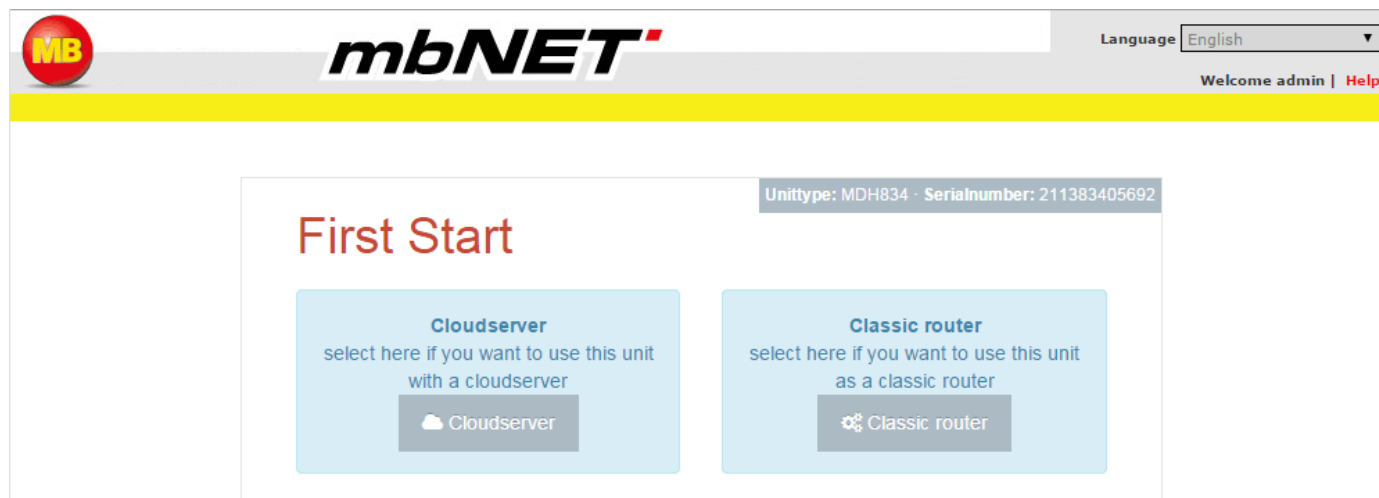
Log into the router using the following login data:

- Username:** admin
- Password:** no password required



First Start on the Web interface.

Here you can select between the adjustment “Cloudserver” and “Classic router”



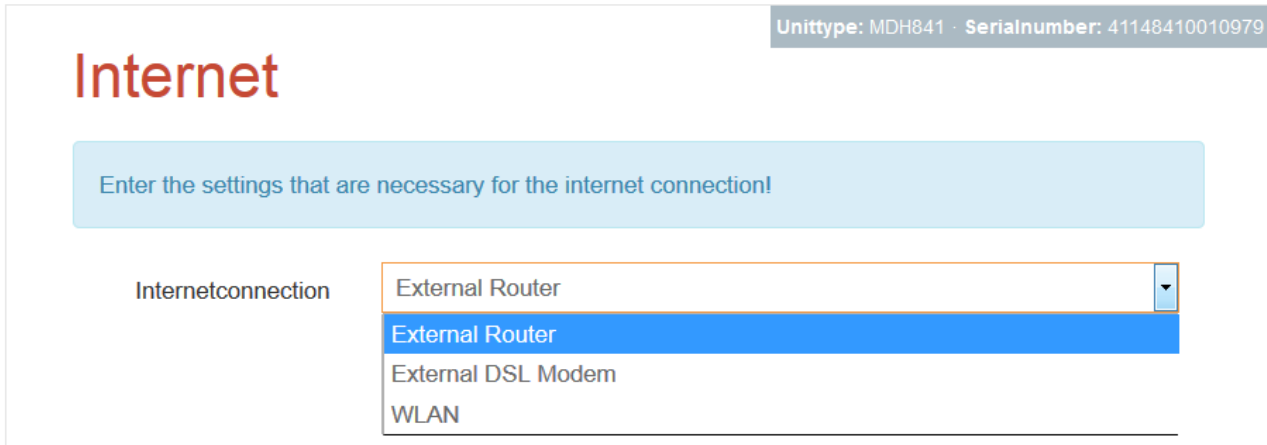
With the setting “Cloudserver”, you can connect to the portal mbCONNECT24 and synchronize your configuration via CTM (Configuration Transfer Manager) to the device.

If you selected the adjustment “Classic router”, you can create a router without a connection to the portal mbCONNECT24, but you can create a VPN-connection on your own.

11.1 Cloudserver



If you selected “Cloudserver“, you can synchronize your configurations per CTM to your device. The following page will appear.



11.1.1 External Router

If you selected **External Router**, you will be redirected to the WAN-Settings.

WAN Settings

Enter your WAN Settings for the ethernet<>internet connection

WAN Typ	DHCP
Gateway	192.168.1.1
DNS Server	8.8.4.4
Use Proxy	<input type="checkbox"/>

Label	Description
WAN Typ	<p><u>DHCP:</u> The router obtains his connection information like the IP address and the subnetmask via DHCP (Dynamic Host Control Protocol). The router will obtain connection information such as IP address and subnet mask using DHCP. Gateway and DNS servers can be specified as an option.</p> <p><u>Static IP:</u> Set the connection information manually. There will appear the following two input fields, enter your required data here.</p> <p><u>IP address:</u> Specify an IP address.</p> <p><u>Netmask:</u> Specify the netmask for the IP address</p>
Gateway	Enter the IP address of the Gateway.
DNS Server	Enter the IP address of the DNS Server.
Use Proxy	Check the checkbox if you need to use a proxy.

Click "Next"

11.1.2 External DSL Modem

If you selected DSL-Modem then you will be redirected to PPP-Settings.

PPP Settings

On this Page you can enter your PPP Configuration!

PPP Type	<input type="text" value="PPPoE"/>
User	<input type="text" value="User"/>
Password	<input type="text" value="Password"/>
Password Confirmation	<input type="text" value="Password Confirmation"/>

Label	Description
PPP Type	<p><u>PPPoE:</u> Activate Point-to-Point Protocol over Ethernet. Used Protocol for connections over ADSL.</p> <p><u>PPTP:</u> Activate Point-to-Point Tunneling Protocol. Protocol used for a transmission method with tunneling.</p>
User / Password	<p>Please enter your username and the password for your Point-to-Point Connection. You receive these information from your ISP (Internet Service Provider).</p> <p>Please Note: Important criterion: If you use this setting, then the router expects that a DLS-Modem is connected direct to the WAN slot.</p>
Label	Description
PPP Type	<p><u>PPPoE:</u> Activate Point-to-Point Protocol over Ethernet. Used Protocol for connections over ADSL.</p> <p><u>PPTP:</u> Activate Point-to-Point Tunneling Protocol. Protocol used for a transmission method with tunneling.</p>
User / Password	<p>Please enter your username and the password for your Point-to-Point Connection. You receive these information from your ISP (Internet Service Provider).</p> <p>Please Note: Important criterion: If you use this setting, then the router expects that a DLS-Modem is connected direct to the WAN slot.</p>

Click "*Next*"

11.1.3 WLAN

If you have selected „WLAN“, you will see this screen.

Unittyp: MDH841 · Seriennummer: 41148410010979

WLAN Settings

Enter your WLAN Settings for the WLAN-<>internet connection

WLAN Typ	<input type="text" value="DHCP"/>
Gateway	<input type="text" value="192.168.2.1"/>
DNS Server	<input type="text" value="DNS Server"/>

Label	Description
WLAN type	<p><u>DHCP:</u> The router obtains his connection information like the IP address and the subnet-mask via DHCP (Dynamic Host Control Protocol). The router will obtain connection information such as IP address and subnet mask using DHCP. Gateway and DNS servers can be specified as an option.</p> <p><u>Static IP:</u> Set the connection information manually. There will appear the following two input fields, enter your required data here.</p> <p>IP address: Specify an IP address.</p> <p>Netmask: Specify the netmask for the IP address</p>
Gateway	Enter the IP address of the Gateway.
DNS Server	Enter the IP address of the DNS Server.

Click “Next”

Unittyp: MDH841 · Seriennummer: 41148410010979

WLAN Settings

Enter your WLAN Settings for the connecting to the Accesspoint

SSID	<input type="text" value="SSID"/>
Authentication Mode	<input type="text" value="WPA2PSK"/>
Encrypt Mode	<input type="text" value="AES"/>
Key	<input type="text" value="Key"/>
Use Proxy	<input type="checkbox"/>

Label	Description
SSID	Enter the name of your WLAN-router or AP
Authenticationmode	Enter your kind of authentication
ciphering method	Enter the kind of ciphering your router has
Key	Enter the WLAN key
Use a proxy	Hook the field to activate a proxy-server

Click “Next”

11.1.4 Cloudserver

Unitytype: MDH834 (4.5.15) · Serialnumber: 211383405693

Cloudserver

Cloudserver settings

Cloudserverlist:

Cloudserver address/name:

Session-Key:

Cloudserver certificate: No file selected.

Label	Description
Cloudserverlist	You can choose between: <ul style="list-style-type: none"> Europe USA/Canada rsp.mbconnect24.net (EU) rsp.mbconnect24.us (US/CAN) User Defined
Cloudserver address/name	The Cloudserver to be used is displayed / entered here.
Session-Key	If you have set a session key on the upload of the configuration file, then you have to enter this session key here.
Cloudserver certificate	If you select "User Defind" under Cloudserlist , you can select a CA certificate here. Self-issued certificates must first be integrated in the router's Setup menu.

Now click on **"Next"** and in the next site click on **"Apply"**.

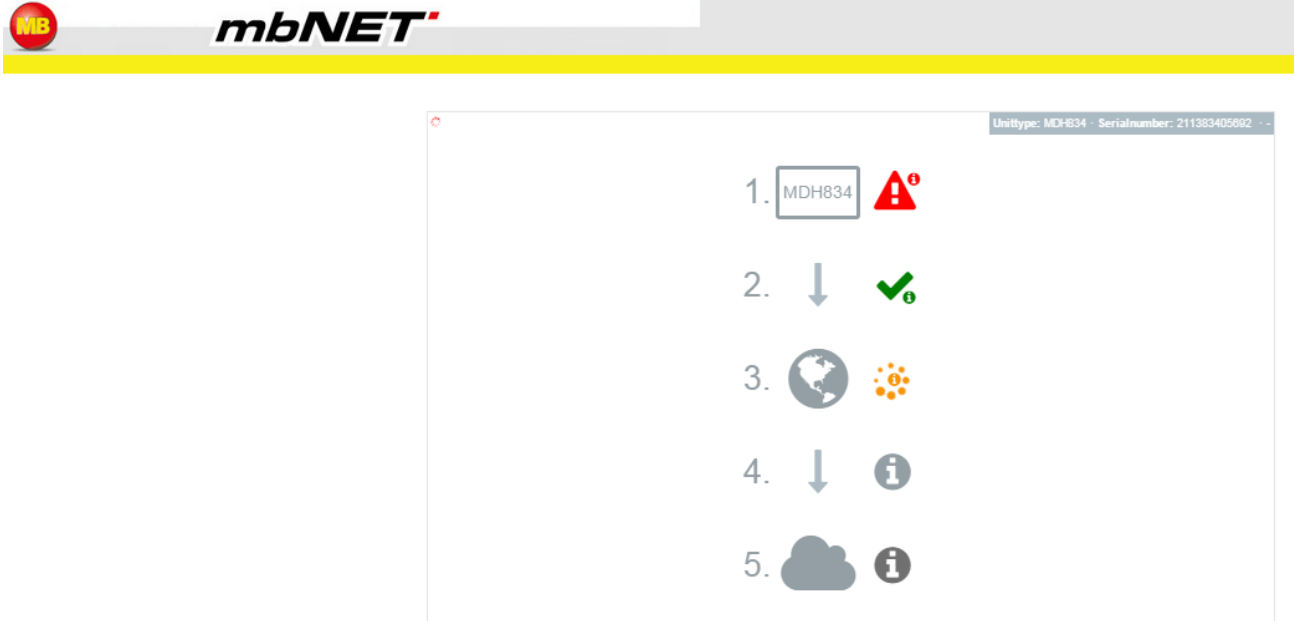
Unitytype: MDH841 · Serialnumber: 41148410010979

Finish

Click on Apply to Save and Enable the Settings on the Device.

11.1.5 Start screen of the mbNET

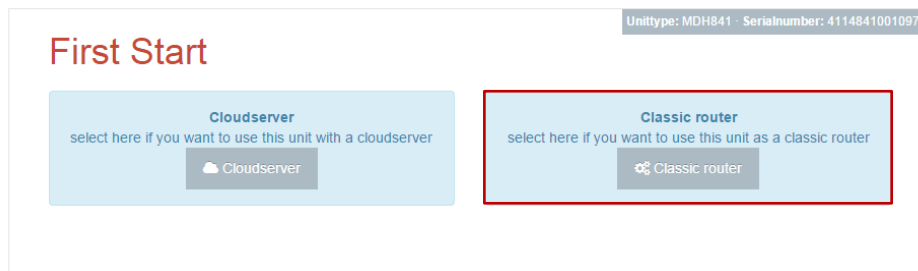
If you search for your mbNET in your web browser you get this screen. Here you can see the connection or network-problems of the mbNET. To see more detailed information click on the "i".



Click on "Setup" to go to the configuration menu.



11.2 Classic router

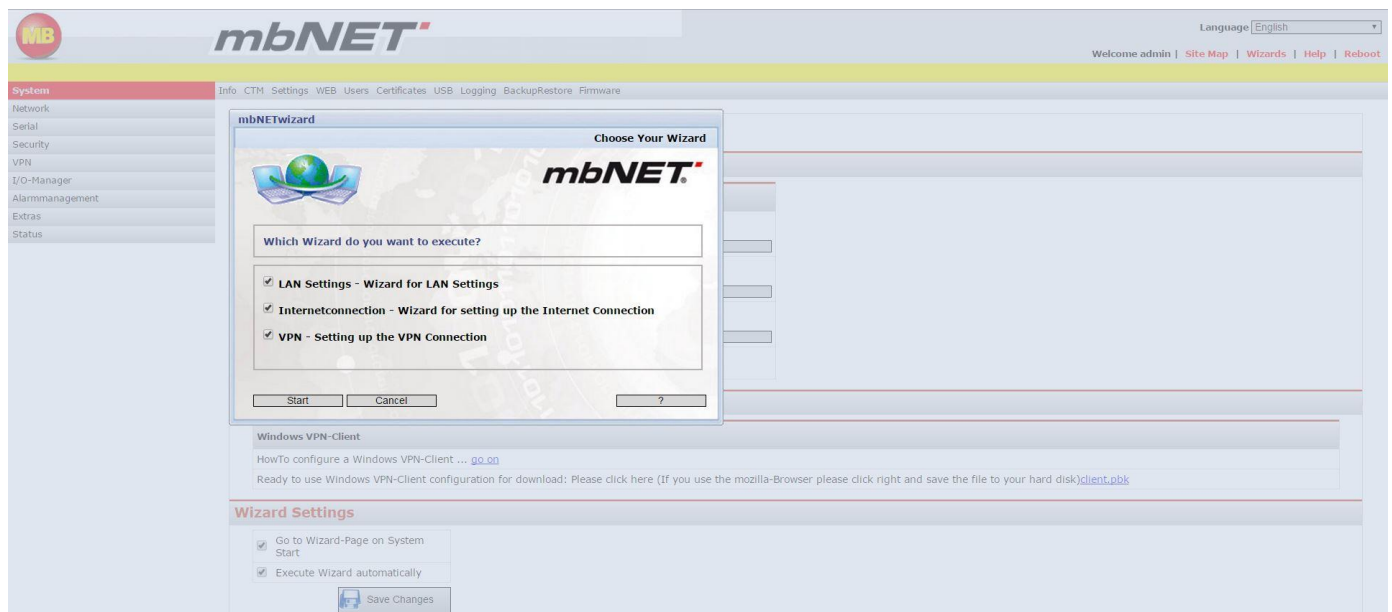


If you selected this option then you will be directed to the following page. A wizard appears which helps you to configure your **mbNET** router.

If you have selected “Classic router” a connection wizard will launch, simplifying network, Internet and VPN connection set up. The wizard is easy to use and takes you through the configuration process step by step. You can also launch the wizard manually. To do this, click on "Wizards" at the top right of your browser window.



If you have selected „Classic router”, your router doesn’t connect to the portal. If you want to use your router in the portal you have to set the configuration manually or restore the device to the factory settings.



11.3 Configuration screen of the mbNET

On successful log in you will be taken to the **configuration interface home page**.

The screenshot shows the mbNET Administration web interface. The browser address bar displays '192.168.0.100/cgi-bin/'. The page header includes the mbNET logo, a language dropdown set to 'English', and navigation links: 'Welcome admin | Site Map | Wizards | Help | Reboot | Logout'. A sidebar on the left lists menu items: System, Network, Security, VPN, I/O-Manager, Alarmmanagement, Extras, and Status. The main content area is titled 'System Information' and contains the following sections:

- System Information:** A table with system details:

Unittyp	MDH834
Serialnumber	211383405693
Firmware version	4.5.14 -- 2017-07-25-07:39:37
Hostname	mbNET

 Below this table is a warning icon and the text: 'Last error: [Jul 25 13:25:00] > (none) GSM-Modem: There is no SIM Card inserted. Please insert a SIM Card'.
- Network:** A table showing network interface status:

Interface	Cable	IP	MAC
LAN	<input checked="" type="radio"/>	172.16.20.241	70:B3:D5:2C:F1:CA
WAN	<input type="radio"/>		70:B3:D5:2C:F1:CB
WLAN	<input checked="" type="radio"/>		7C:DD:90:6A:ED:04

 Below this is another table for wireless settings:

SSID	Active	Link Quality	Frequency
	<input type="radio"/>	10 (%)	2.412 GHz (Channel 1) (GHz)

 Further down are sections for 'Internet-Connection' and 'Modem-Connection', both showing 'Active' status with radio buttons for 'IP local' and 'IP remote'.
- Serial:** A table showing serial interface configurations:

Interface	RS-Typ	Driver	Port
COM1	RS232	AllenBradley - Allen Bradley 19200 - V1.1	7001
COM2	MPI/PROFIBUS	MPI/PROFIBUS	7002
- USB:** A section showing a green indicator and the text 'usb connected'.

12. Basic configuration of the router using the web interface



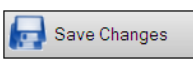
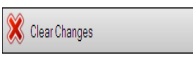










12.1 Web interface home page

The home page is designed to provide you with an at-a-glance view of the most important information on **mbNET** router access or status. The side (1) and top (2) navigation bars will provide the support you need when configuring the router. The navigation bar at the top (2) displays the submenu for each of the main menu items listed in the navigation bar at the side (1).

Pos.	Label	Description
3	System	System information such as device model, device name, current firmware version and serial number of the router.
4	Network	<p>Interface: LAN – WAN: Displays which network connections are currently connected to the existing network via the respective ports. A green icon indicates an existing connection.</p> <p>SSID: Here you will find information about the WiFi network name (SSID), the connection status (if a connection is active, this is indicated by the green LED symbol), the signal strength of the connection quality (%) and the values for the frequency and the selected WiFi channel.</p> <p>Internet connection: A currently active Internet connection (or connections) is indicated by a green dot. If there is no currently active Internet connection, the circle is solid gray.</p> <p>Modem connection: Only incoming modem connections are shown here. A green dot means that a modem connection is established. The display also shows which user is connected to the modem.</p>
5	Serial	This shows the current configuration of interfaces COM1 and COM2 .
6	USB	Information on connected USB storage devices. A connected storage device (e.g. flash drive or external hard drive) is indicated by a green dot.

12.2 Icons, buttons and fields

In the rest of these operating instructions you will repeatedly encounter specific icons. These are listed and explained on the next page.

No.	Icon and field types	Description
1	 	<p>Gray LED: connection inactive / cable or USB device disconnected. / Green LED: connection active / cable or USB device connected.</p>
2		<p>This button appears wherever there are settings that can be changed. It saves the current configuration temporarily, i.e. if the router is re-started, any changes to settings will be lost. To save settings permanently, click button no.5</p>
3		<p>If you saved your settings temporarily (see no.2), you can undo the changes by clicking on this button.</p>
5		<p>This permanently stores and applies all saved changes.</p>
6		<p>This is a check box. Clicking on a box enables/disables the option associated with it.</p>
7		<p>If input is required in a field that looks like this, it must be entered manually.</p>
8		<p>Clicking on a checked box will present the available options as a drop-down field.</p>
9		<p>Clicking on this field allows you to change (edit) settings in the associated row.</p>
10		<p>To reverse changes made to the associated row, click on this button.</p>
11		<p>Use this to do a temporary save of the settings that you are currently working on. To save changes to the router permanently, click button no.5.</p>
12		<p>This inserts additional input rows The currently displayed row must contain values or data before you click on this button. If not, an error message will appear at the top of the open configuration page.</p>
13		<p>This deletes the input of the row that you are currently working on.</p>
14		<p>This enables you to change the order of rules.</p>

12.3 System > CTM (Configuration Transfer Manager)

The CTM allows the transmitting of the configuration via internet connection, or respectively the device receives his configuration as soon as it gets online. CTM has to be activated on the device, to ensure the transmitting of the configuration.

ADVICE: The CTM function is only relevant if you are using the router in the mbCONNECT24 portal. A description of this function can be found in the mbCONNECT24 online help.

The screenshot shows the 'CTM (Config Transfer Manager)' settings page. The 'Information' tab is active, displaying:

- CTM is: inactive
- Host address or DNS: ctm.mbconnect24.net

 Below this, there are sections for 'Loggings' and 'Control'. A 'CTM connect' button is visible at the bottom of the control section.

The screenshot shows the 'CTM (Config Transfer Manager)' settings page with the 'Settings' tab active. The configuration fields are:

- Active:
- Host address or DNS: ctm.mbconnect24.net
- Session-Key: (empty text field)
- Enable connection through a HTTP proxy: no

 A 'Save Changes' button is located at the bottom right of the settings area.

Settings	
Active	Activate / Deactivate CTM.
Host address or DNS	Enter the Host address or the Name of your DNS-Server.
Session-Key	Enter the generated session key from the portal.
Enable connection through a HTTP proxy	Yes / No

12.4 System > Settings

Before you configure the mbNET industrial router specifically for your application, you should first make certain basic settings. To do this, proceed as follows:
 On the navigation bar at the top bar on the web interface home page, click **System** and **Settings**. This will display the system settings screen shown below. Now proceed as described on the following pages.


The screenshot displays the 'System Settings' page in the mbNET web interface. The top navigation bar includes 'System', 'Info', 'CTM', 'Settings', 'WEB', 'Users', 'Certificates', 'USB', 'Logging', 'BackupRestore', and 'Firmware'. The left sidebar lists various system functions: Network, Security, VPN, I/O-Manager, Alarmmanagement, Extras, and Status. The main content area is titled 'System Settings' and is organized into three distinct sections:

- System Settings:** Contains input fields for 'Hostname' (mbNET), 'Host Description' (mbNET), and 'System Reboot after ... [h]'.
- Time Settings:** Displays 'Date Time (UTC)' as Tue Jul 25 10:26:13 UTC 2017 and 'Locale Date Time' as Tue Jul 25 12:26:13 CEST 2017. It includes a 'Set local Date Time' field, a 'Timezone' dropdown menu set to 'Berlin, Germany', and several NTP server configuration options (Enable, Address, Interval, Defaulttime).
- Mail Settings:** Features a dropdown for 'Activate automatic Mail' set to 'no', and fields for 'SMTP-Server', 'SMTP-Port' (25), 'E-Mail Address', 'SMTP requires Authentication', 'User', and 'Password'.
- System Services:** Includes two checkboxes: 'Disable Network Configuration (Conftool)' and 'Enable Manufacturer System Access', both currently unchecked.

A 'Save Changes' button with a floppy disk icon is positioned at the bottom right of the settings area.

You can find the description on the next page.

System Settings	
Hostname	Assign a name to the router.
Host Description	To identify the device within a network, provide a meaningful description here.
System Reboot after ... [h]	Enter a period of time (in hours), after which the device performs an automatic reboot. ADVICE: The time interval is not linear to the operating time of the router, but counts every full hour. That is, if you enter 2 hours, a device reboot is performed every second hour. Exception: If you enter 24 hours , the device is rebooted every time at 00:00 .

Time Settings															
Date Time (UTC)	Displays the current system time in UTC (Coordinated Universal Time).														
Local Date Time	Displays the time based on local time zone.														
Set local Date Time [JJJJ.MM.TT-HH:MM:SS]	Enter the time here in case there is no NTP server installed, or in case it is unavailable. Example: 2007.10.30-13:33:48 <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Format</th> <th style="text-align: left;">Meaning</th> </tr> </thead> <tbody> <tr> <td>YYYY</td> <td>Year e.g. 2007</td> </tr> <tr> <td>MM</td> <td>Month e.g. 10</td> </tr> <tr> <td>DD</td> <td>Day e.g. 30</td> </tr> <tr> <td>HH</td> <td>Hour e.g. 13</td> </tr> <tr> <td>MM</td> <td>Minute e.g. 33</td> </tr> <tr> <td>SS</td> <td>Seconds e.g. 48</td> </tr> </tbody> </table>	Format	Meaning	YYYY	Year e.g. 2007	MM	Month e.g. 10	DD	Day e.g. 30	HH	Hour e.g. 13	MM	Minute e.g. 33	SS	Seconds e.g. 48
Format	Meaning														
YYYY	Year e.g. 2007														
MM	Month e.g. 10														
DD	Day e.g. 30														
HH	Hour e.g. 13														
MM	Minute e.g. 33														
SS	Seconds e.g. 48														
Timezone	Choose from the selection field the time zone in which you are located or, if different, the time zone in which the mbNET is operated. The preset time zone is: Berlin, Germany														
NTP Server Enable	Checkbox for activating / deactivating the NTP function.														
NTP Server Address	Enter the NTP server here (preset address: 0.de.pool.ntp.org). You can enter a time server IP address instead of a name. If you enter a name, there must be a DNS server entered in the network settings, or an existing Internet connection. The NTP server simply needs to be available.														
NTP Server Interval	Enter the value (in hours) for the NTP polling interval here. Input => natural numbers [h] > 0.  If you leave this blank or enter "0", there will be no time calibration.														
NTP Server Default time [JJJJ.MM.TT-HH:MM:SS]	The default time setting is required if access to the NTP server fails and the firmware date is younger than the default time.														

Mail Settings	
Activate automatic Mail	Selection field (yes / no) for activating / deactivating the automatic mail settings. If you select "yes", the router uses the MB connect line mail server with fixed specifications. If "no", you must enter the information of your mail server (for further information, please contact your service provider).
SMTP-Server	The SMTP server is needed for the router to send emails.
SMTP-Port	The port over which emails will be sent should be entered here. Usually this is port 25.
E-Mail Address	Enter the appropriate sender address for emails from the router here.

SMTP requires Authentication	The box should be checked or unchecked depending on ISP. Ask your ISP for the correct setting.
User Password	A user name and password are required for SMTP server authentication, i.e. if the router wants to send an email to the SMTP, it must first authenticate itself if necessary.

System Services	
Disable Network Configuration (Conftool)	<p>Checkbox for activating / deactivating this function.</p> <p>ADVICE: The function "Disable Network Configuration (Conftool)" is only relevant if you are using the router in the mbCONNECT24 portal. A description of this function can be found in the mbCONNECT24 online help.</p>
Enable Manufacturer System Access	<p>Checkbox for activating / deactivating this function.</p> <p>ADVICE: This function is disabled by default. Activate the function if, in the support case, you want to allow the device manufacturer to access the mbNET via SSH. Activation starts the SSH server for the ROOT access to the mbNET, which is handled via PKI.</p>

12.5 System > WEB

HTTP oder HTTPS Access from Network	
Protocol	<p>Selection field for the connection type, how to access the web server.</p> <ul style="list-style-type: none"> • HTTP (accessible via http: //; standard port: 80) • HTTPS (accessible via https://.....; standard port: 443)
HTTP Port	<p>Here you can change the default port, via the HTTP / HTTPS server can be reached.</p> <p>ADVICE: When you change the default port, you must specify the new port in the browser's address line (e.g., 192.168.0.100:84).</p>

Services

Disable complete Web-GUI (only recoverable with Factory Reset!)	Checkbox for activating / deactivating this function. If the function is activated, the web server of the mbNET is completely switched off. That is, the web interface of the mbNET is no longer accessible via the web.
Disable Factory Webservice	Checkbox for activating / deactivating this function. The "Factory Webservice" function serves the manufacturer during producing the mbNET.
Disable Communication Web-service (SMS/Email)	Checkbox for activating / deactivating this function. If the function is activated, neither an SMS nor an e-mail from the device (mbNET) can be sent.

12.6 WLAN Configuration

Network > WLAN

The screenshot shows the 'WLAN Configuration' page with the 'Interface' tab selected. The 'Interface Type' is set to 'DHCP'. A 'Save Changes' button is visible at the bottom right.

Interface	
Interface Type:	DHCP: Settings are received with DHCP. Static IP: You can set the settings manually.

The screenshot shows the 'WLAN Configuration' page with the 'Settings' tab selected. The configuration fields are as follows:

- SSID: [Empty text box]
- Authentication Mode: WPA2PSK
- Encrypt Mode: AES
- Key: [Empty text box]
- Operating Frequency: Channel 1-13
- Operating Band: Band 36, 40, 44, 48, 52, 56, 60, 64, 100, 104
- Operating Band: 11BGN mixed
- Channel: 1
- B/G Protection: Auto
- RTS Threshold: 2347
- Frag Threshold: 2346
- WMM Capable: Enable WMM

A 'Save Changes' button is located at the bottom right of the settings area.

Settings	
SSID	Define your SSID.
Authentication Mode	<p><u>OPEN</u> At this authentication method, every mobile Station is able to connect with the Access Point if the SSID matches. Some wireless clients know the option ALL or ANY, which allows to make a connection with every access point independently of the SSID. Assuming he is configured as "Open System".</p> <p><u>SHARED</u> In this authentication, the access point and the mobile station must have the same WPA2 password. If the entered password does not match with the set password, then the access point denies the authentication of the station. A connection cannot be established if this is the case.</p> <p><u>WPAUTO</u> The setting is not unique. Depending on the manufacturer or the access point, it may have different impacts. Additionally you have to make specifications about the encryption, the code and eventually about the encryption strength.</p> <p><u>WPAPSK</u> WPA-PSK is an encryption method that sends data through a pattern which changes the signal completely. It can only be readed again, if you put the same pattern with the key (Code/Key) which you can determine by yourself, above it</p> <p><u>WPA2PSK</u> WPA2-PSK is the implementation of a high safety standards in accordance with the WLAN standards. It is the successor of WPA and one of the safest methods of encryption.</p> <p><u>WPANONE</u> No authentication</p>
Encrypt Mode	<p><u>AES</u> The AES decryption requires necessarily that the same steps must be run as at the encryption. But just in reverse order. It is a weakness of AES.</p> <p><u>WEP</u> Warning! WEP is considered as outdated and is known to be unsafe.</p> <p>WEP is an encryption method based on a RC4 encryption. For this purpose, a secure key is stored in each wireless terminal of anyone known and should not be traceable. For this WEP provides functions for packet encryption and authentication.</p> <p><u>TKIP</u> TKIP uses the same algorithm as WEP. TKIP also ensures, that every data package gets his own key. Packet who are no fitting into the algorithm, are dropped.</p> <p><u>NONE</u> No Encryption.</p>
Key	Select a WLAN-key and enter it in this field.
Operating Frequency	<p>Select this setting depending on how many devices and base stations, are sharing the frequency spectrum. You can divide the frequency spectrum of 2.4 GHz with the channel settings.</p> <p><u>Channel 1-11</u> - The channels 1-11 are considered.</p> <p><u>Channel 1-13</u> - The channels 1-13 are considered.</p> <p><u>Channel 10,11</u> - The channels 10 and 11 are considered.</p> <p><u>Channel 10-13</u> - The channels 10 and 13 are considered.</p> <p><u>Channel 3-9</u> - The channels 3-9 are considered.</p> <p><u>Channel 5-13</u> - The channels 5-13 are considered.</p>
Settings	

<p>Operating Band</p>	<p>Select the operating band defined under IEEE 802.11 standard.</p> <div style="border: 1px solid gray; padding: 5px;"> <p>Operating Band Band 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108 ▾</p> <p style="background-color: #e0e0e0;">Band 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165 ch</p> <p>Band 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 ch</p> <p>Band 36, 40, 44, 48, 52, 56, 60, 64 ch</p> <p>Band 52, 56, 60, 64, 149, 153, 157, 161 ch</p> <p>Band 149, 153, 157, 161, 165 ch</p> <p>Band 149, 153, 157, 161 ch</p> <p>Band 36, 40, 44, 48 ch</p> <p>Band 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165 ch</p> </div>
<p>Operating Band</p>	<p><u>Legacy 11 B only</u> This is the oldest standard for radio networks. If your WLAN-adaptor supports newer standards like 802.11g, then you should use them instead.</p> <ul style="list-style-type: none"> • <i>Max. speed:</i> up to 11Mbit/s • <i>Frequency:</i> 2.4 GHz • <i>Bandwidth:</i> 22 MHz • <i>Range:</i> Indoor -> 35m / Outdoor -> 120m <p><u>Legacy 11 G only</u> This WLAN-standard is used most at the present. It ensures a broad compatibility to a variety of WLAN-devices.</p> <ul style="list-style-type: none"> • <i>Max. speed:</i> max. 54Mbit/s • <i>Frequency:</i> 2.4 GHz • <i>Bandwidth:</i> 20 MHz • <i>Range:</i> Indoor -> 38m / Outdoor -> 140m <p><u>11 N only</u> This standard ensures high transmission speeds and ranges. Modulation methods and antenna techniques like MIMO (Multiple Input, Multiple Output) are using the available frequency band more effectively then older standards.</p> <ul style="list-style-type: none"> • <i>Max. speed:</i> max. 54 – 600 Mbit/s • <i>Frequency:</i> 2.4 / 5 GHz • <i>Bandwidth:</i> at 2.4GHz -> 20MHz at 5GHz -> 40MHz • <i>Range:</i> Indoor -> 70m / Outdoor -> 250m <p><u>11GN mixed</u> The standards 802.11 g and 802.11 n are mixed.</p> <p><u>11BGN mixed</u> The standards 802.11 b, 802.11 g and 802.11 n are mixed.</p> <p><u>legacy 11 b/g mixed</u> The standards 802.11 g and 802.11 b are mixed.</p>
<p>Channel</p>	<p><u>Auto:</u> The channel is selected automatically. <u>1-13:</u> Select a Channel between 1 and 13.</p>
<p>B/G Protection</p>	<p><u>Auto</u> <u>Always on</u> <u>Always off</u></p>
<p>RTS Threshold</p>	<p>Request-to-send: The RTS is a handshake-protocol for avoidance of data collision. If the device recognizes a slower device, then he asks before sending the packet. This process can slow down the data rate. A value of 500 is recommended.</p>
<p>Frag Threshold</p>	<p>The fragmentation affects the data rate. You can specify the size of the packets here. Do not select a too high value.</p>
<p>WMM Capable</p>	<p><u>Active WMM:</u> WMM certification active <u>Inactive WMM:</u> WMM certification inactive</p>

13. Description of different connection scenarios

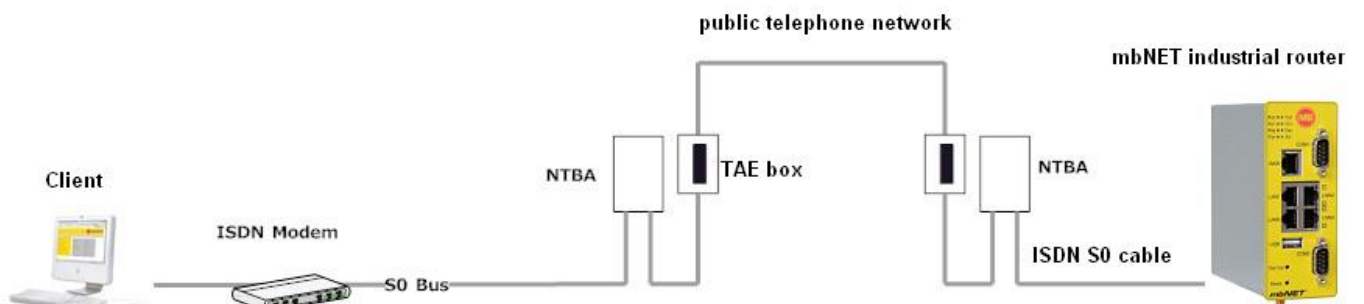
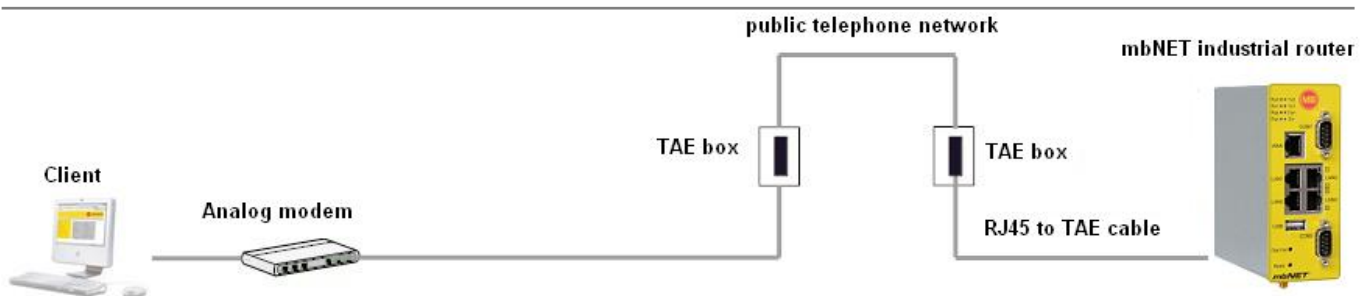
13.1 General

Now that you have completed basic configuration of the router (see previous pages), it needs to be connected via the appropriate connection type, and configured using the web interface.

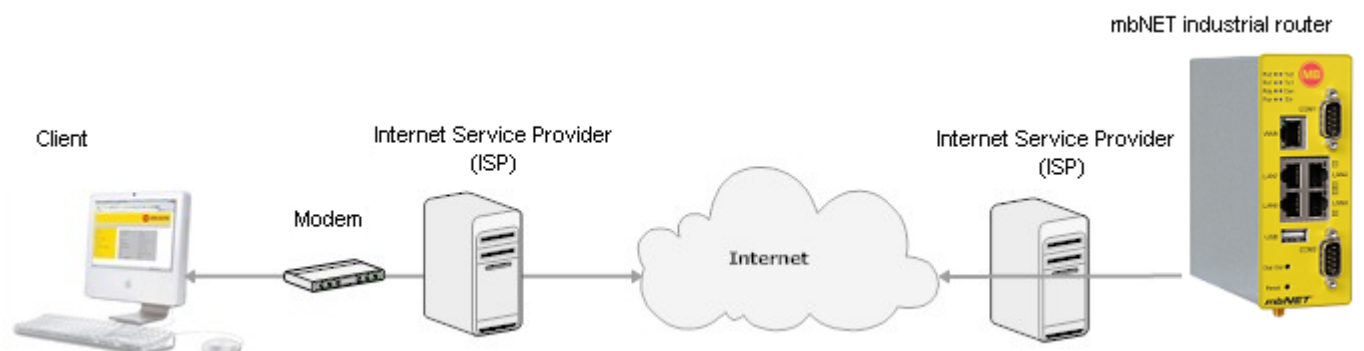
A description of some basic connection scenarios follows.

Choose the connection scenario that best applies to you and follow the instructions in the relevant section.

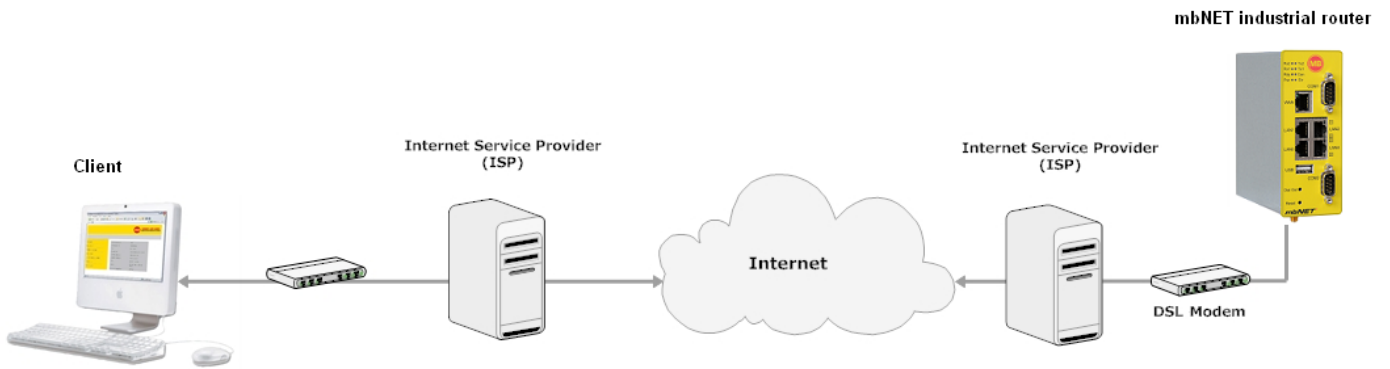
Configuring the **mbNET** industrial router's integrated modem for connection with a client PC via the public telephone network (PPP dial-up, dial-up networking) (see [section 9.2](#))



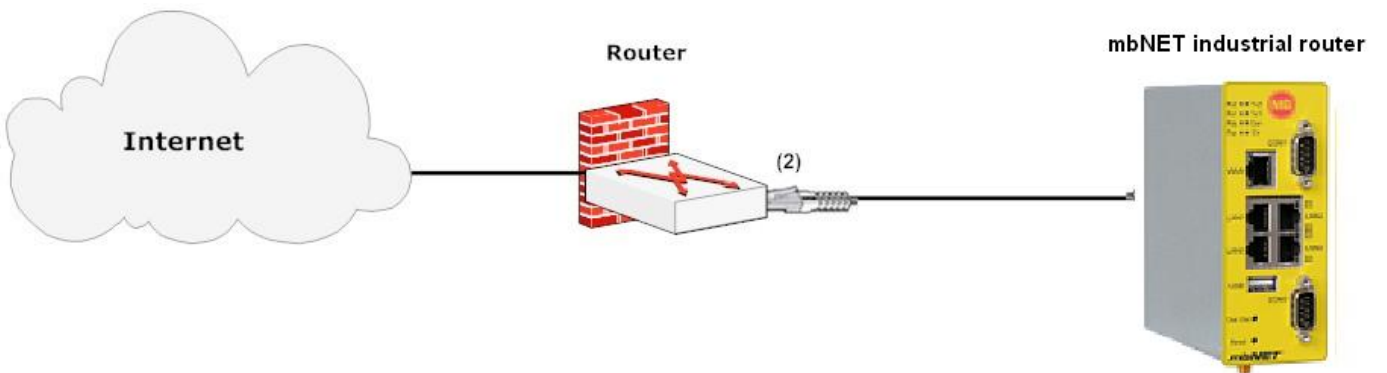
Configuring the **mbNET** industrial router's integrated modem for connection with a client PC via the Internet (see [section 9.3](#))



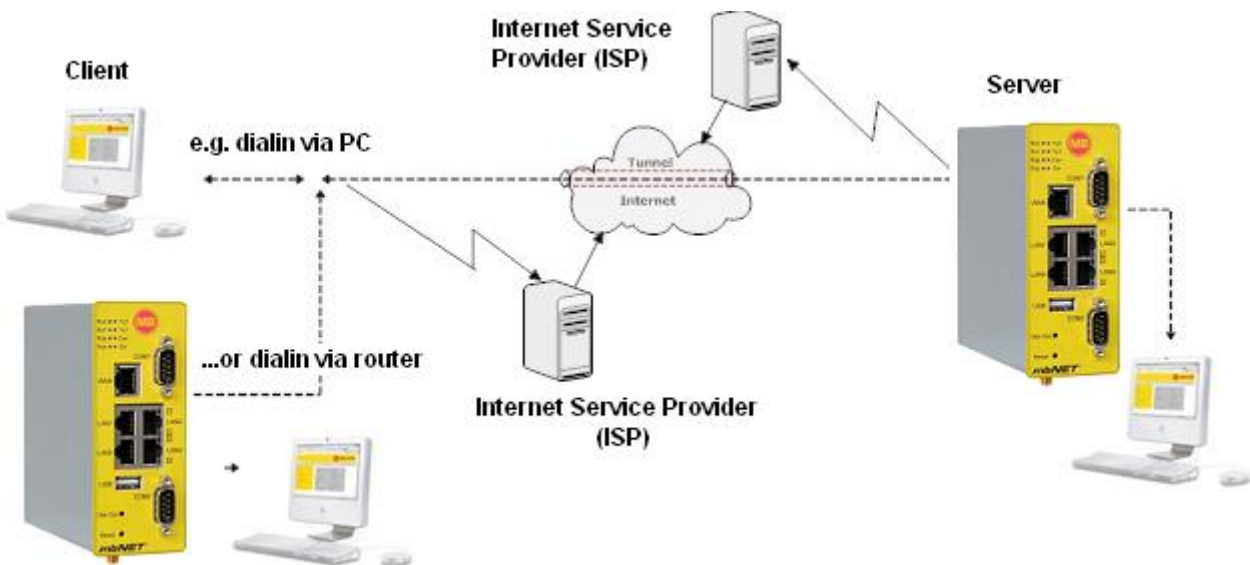
Configuring the **mbNET** router for connection with a client PC via DSL Internet access, using a DSL modem (see [section 9.4](#))



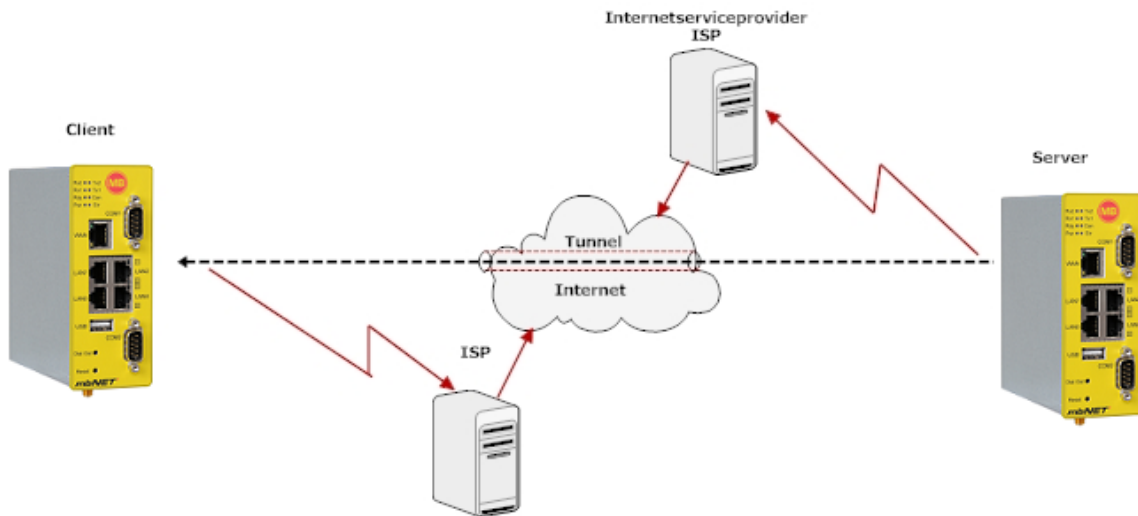
Configuring the **mbNET** industrial router for connection to the Internet using another router (see [section 9.5](#))



Configuring the **mbNET** industrial router for VPN connection with a client (client – router) (see [section 9.6](#))



Configuring an **mbNET** industrial router for VPN connection to another **mbNET** router (router – router) (see [section 9.7](#))

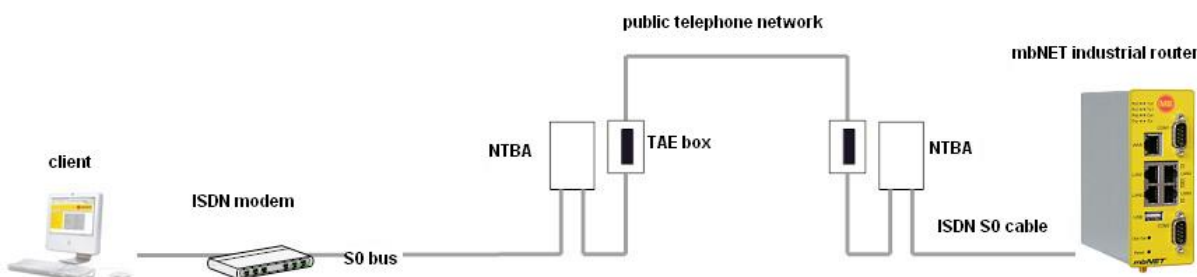
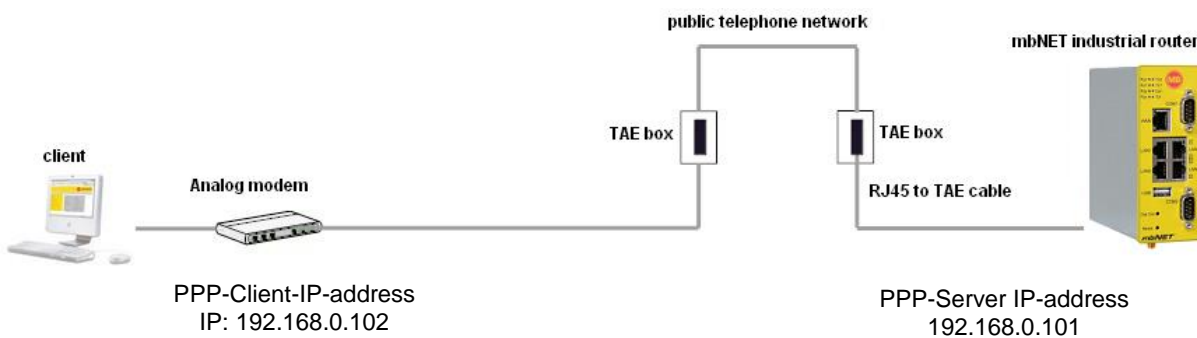


13.2 Configuring the industrial router for connection over the telephone network

The following diagram shows how to connect the industrial router to a client over the **public telephone network**.

Using this type of connection, the industrial router can be accessed over the telephone network via its serial interfaces (see [Serial Interfaces](#)) and LAN interface.

In the following example, the client is a PC with a modem connection.



13.2.1 Connecting and configuring the router

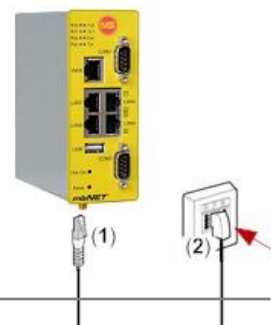
Before you begin:

- The router should be connected to a suitable power source, and the Power and Ready LEDs should be solid green.

13.2.1.1 Connecting the router

Analog connection (applies to device models MDH xx0)

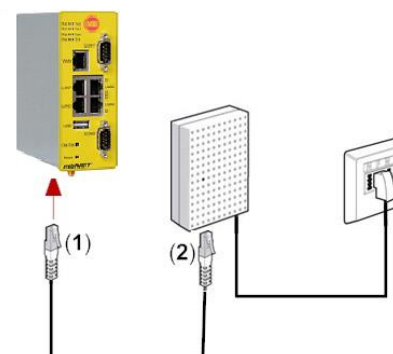
- Connect TAE adapter to analog cable.
- Plug one end of the supplied cable into the RJ12 jack (1) on the bottom of the router, and the other end into the TAE jack (2).



ISDN connection

(applies to device models MDH xx2)

- With an existing **ISDN connection**, plug one end of the ISDN cable into the jack (1) on the bottom of the router and the other end into the (2) **NTBA**.



GSM connection:

(applies to device models MDH xx3 and MDH xx4)

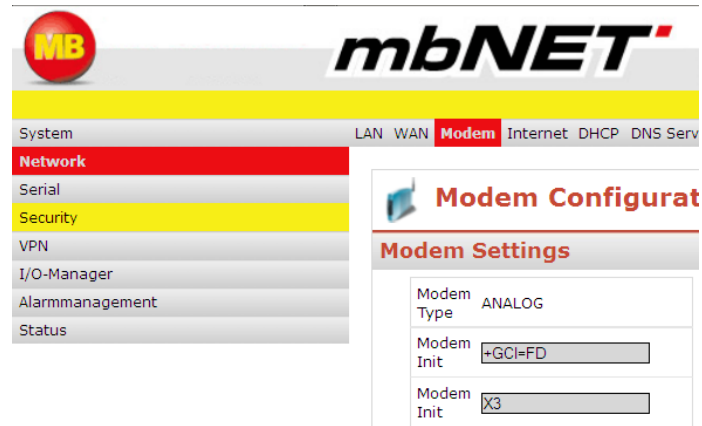
- With an existing **GSM connection**, plug the end of the GSM antenna cable into the jack on the bottom of the router.



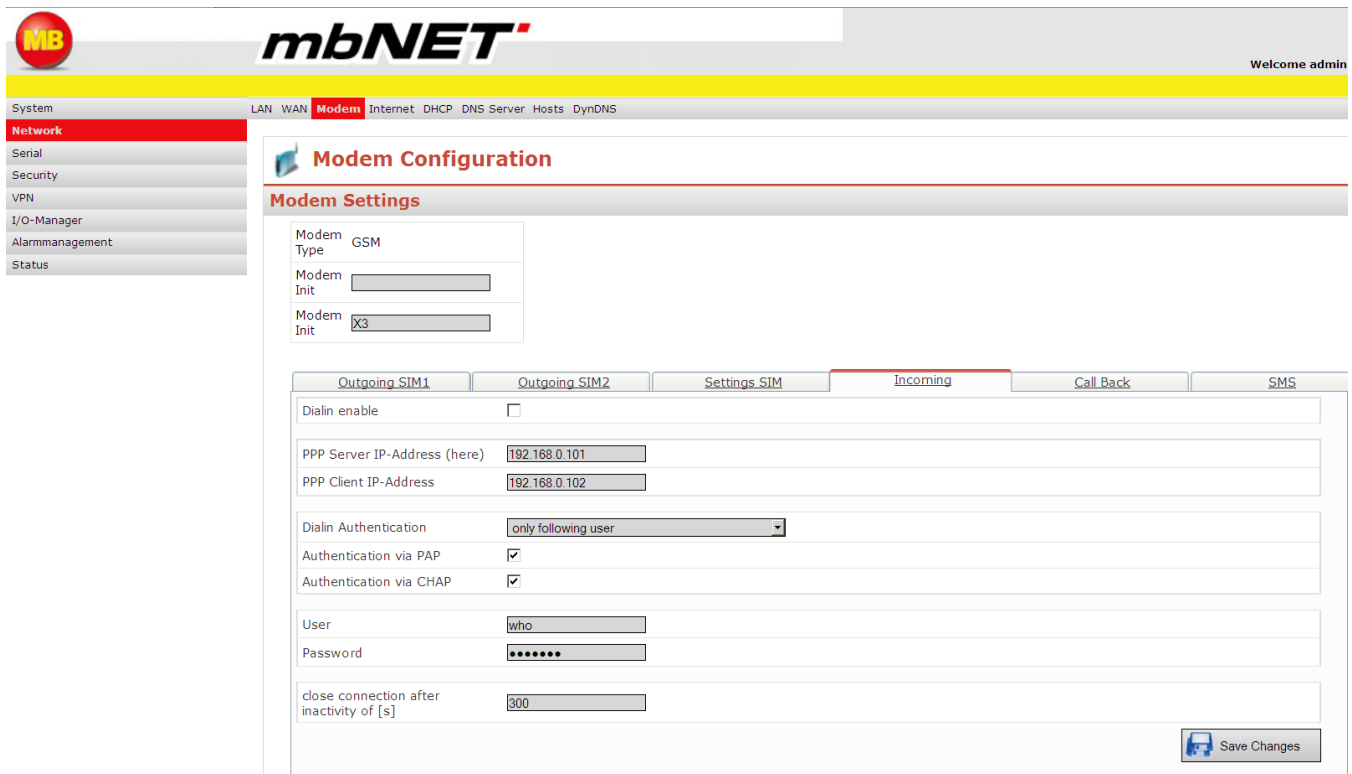
13.2.1.2 Configuring the router using the web interface

On the web interface home page, click on **Network – Modem**.

Note: Not possible at *mbNET variant with WLAN* (FW 4.1).



Configuring the router – client connection over the telephone network

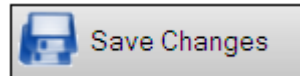
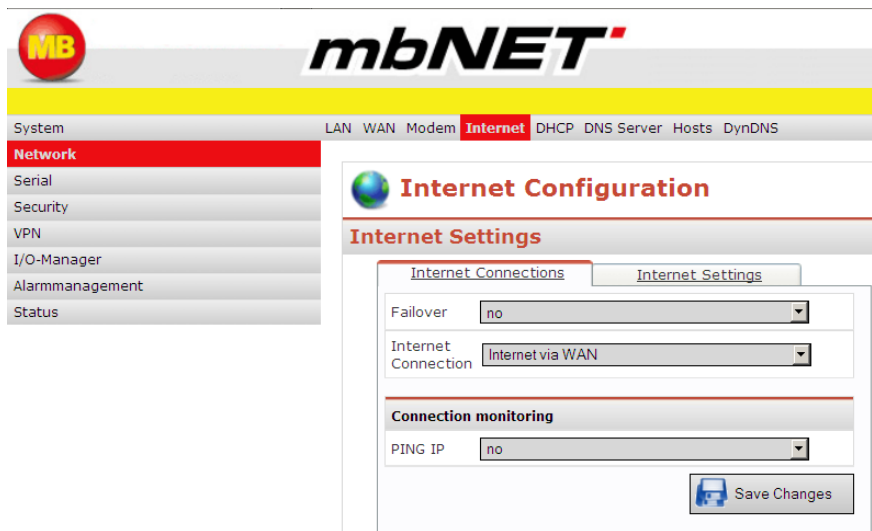


For more detailed information, please see section [Network – Modem](#)

Label	Description
Modem Init	<p>ANALOG: if using an analog device, enter the command +GCI=country code (for country codes, see Country codes for analog devices) here, and in the second row, the command X3 (do not wait for dial tone).</p> <p>ISDN: if using an ISDN device, you need to enter your MSN (multiple subscriber number) with the command AT#Z=n (n= MSN number) If you enter “n” as “*”, every call will be accepted.</p> <p>GSM: if using a GSM device, you can either keep the preset X3 command, or use the +GCI=country code command.</p>

SIM PIN (GSM only)	If required, you can enter the SIM card PIN here. However, the device will also work without SIM card PIN protection
Provider (GSM only)	You can select your mobile broadband provider here. If it does not appear, select "Other"
Provider name (GSM only)	If your provider was not shown, you can also manually enter the APN (Access Point Name) here. You can obtain details of the APN from your mobile broadband provider or from our website at http://www.mbconnectline.de/gsm/grps/mobilfunk.html
Incoming	
Dial-in enable	Click on the check box to check it and enable a client computer to connect to the mbNET via a dial-up connection.
PPP Server IP address (here)	Enter the IP address of the PPP server. In this case: 192.168.4.100 This sets this address as the mbNET address for client computers dialing in
PPP Client IP address	Enter the IP address that you want the client to receive. In this case: 192.168.4.101
Dial-in Authentication	From the drop-down field, select only following user (as shown here in the example), or every User with dialin rights This determines whether any user registered under System – User, or only one specific user, can dial in to the mbNET .
Authentication via PAP	Authentication protocol that transfers your login credentials (P assword A uthenticat I on P rotocol). However, we recommend using the more secure CHAP variant alongside this, as PAP sends your credentials unencrypted.
Authentication via CHAP	Authentication protocol that transfers your login credentials securely (C hallenge H andshake P rotocol)

- Now save your changes by clicking **Save Changes**.
- Now click on **Network** – **Internet** and enter the following settings.

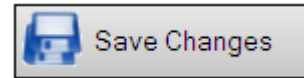
For a detailed description of the **Network** – **Internet** settings, please see section [Network – Internet](#)

Label	Description
Internet connection	Select either Internet via modem or Internet via WAN .

- ❑ Save your changes by clicking **Save Changes**

- ❑ Click on **System** – **User** and add a user with dial-in rights. For further notes on adding users and assigning specific rights, please see section [Adding users](#)

- ❑ Finally, to save your changes permanently to the industrial router, click **Apply Changes**.



For devices to be able to communicate with the LAN interface, they must be configured using the **mbNET** LAN interface IP address as the device gateway. Communication is not via PPP addresses, but via the **mbNET** LAN interface IP address and the IP addresses of connected devices.

Configuring the router – client connection over the telephone network (continued)

13.2.2 Configuring a client (PC) to access the router

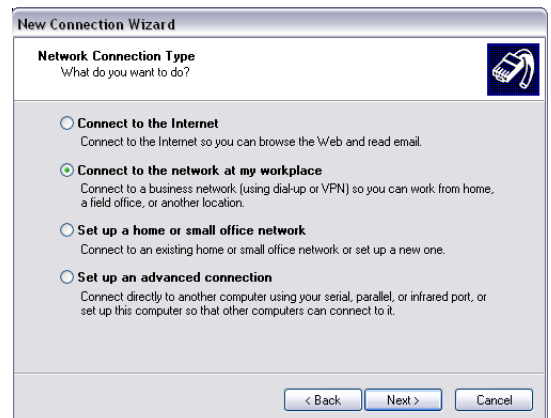
You can connect directly to the router, and to a remote network, using a telephone line. Router access must first be correctly configured as described above. Then you need to set up a suitable dial-up connection on the computer, as follows.

- ❑ Click on START and then Control Panel.
- ❑ Click on NETWORK CONNECTIONS and then NEW CONNECTION WIZARD. This launches the connection wizard which will make all the necessary settings.

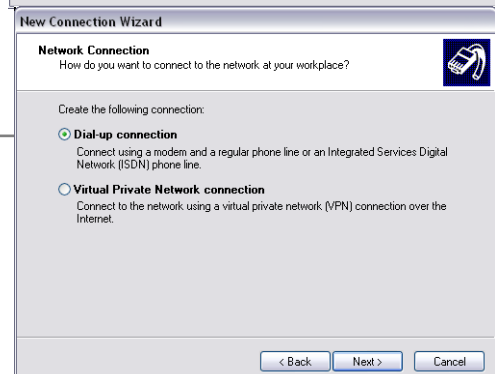
The welcome screen of the connection wizard will appear. Click **NEXT**.



- ❑ In Network Connection Type, choose the second option, **Connect to the network at my workplace** and then click **NEXT**.



- ❑ Choose **Dial-up connection** and the modem that you wish to use to set up a connection with the industrial router.



Configuring the router – client connection over the telephone network (continued)

- ❑ Now you need to give your connection a name, then click **NEXT**.

The screenshot shows the 'New Connection Wizard' window. The title bar reads 'New Connection Wizard'. The main heading is 'Connection Name' with a sub-heading 'Specify a name for this connection to your workplace.' There is a telephone icon in the top right corner. Below the heading, it says 'Type a name for this connection in the following box.' followed by 'Company Name' and a text input field. A note below the field says 'For example, you could type the name of your workplace or the name of a server you will connect to.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- ❑ Enter the telephone number of your remote station (the number that accesses the industrial router)

The screenshot shows the 'New Connection Wizard' window. The title bar reads 'New Connection Wizard'. The main heading is 'Phone Number to Dial' with a sub-heading 'What is the phone number you will use to make this connection?' There is a telephone icon in the top right corner. Below the heading, it says 'Type the phone number below.' followed by 'Phone number:' and a text input field. A note below the field says 'You might need to include a "1" or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

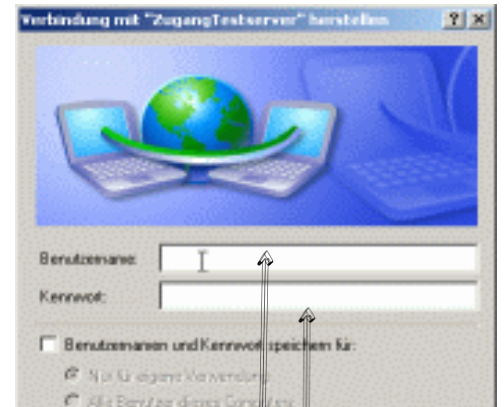
- ❑ Click **Finish**.

The screenshot shows the 'New Connection Wizard' window. The title bar reads 'New Connection Wizard'. The main heading is 'Completing the New Connection Wizard'. There is a telephone icon in the top left corner. The text says 'You have successfully completed the steps needed to create the following connection:' followed by 'Dial-up connection' and a bullet point '• Share with all users of this computer'. Below this, it says 'The connection will be saved in the Network Connections folder.' followed by a checkbox 'Add a shortcut to this connection to my desktop'. At the bottom, it says 'To create the connection and close this wizard, click Finish.' There are three buttons: '< Back', 'Finish', and 'Cancel'.

Configuring the router – client connection over the telephone network (continued)

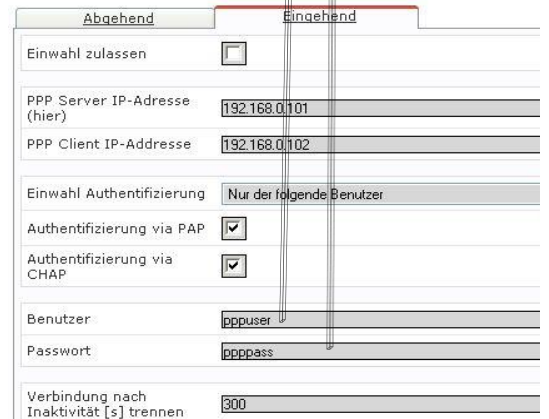
13.2.3 Establishing a connection between the client PC and the industrial router

- ❑ Double-click on the connection that you created using the instructions in the previous section.
- ❑ In this window, enter the **user name** and **password** that you created previously when configuring the modem. If you selected the option “every User with dial in rights”, you can enter the user name and password of a user who has dial-in rights.



The default settings for **Authentication via CHAP** and **Authentication via PAP** must be the same as those on the router, otherwise no connection can be established.

- ❑ Click **Connect**.
 ✓ You have established a connection to the router.



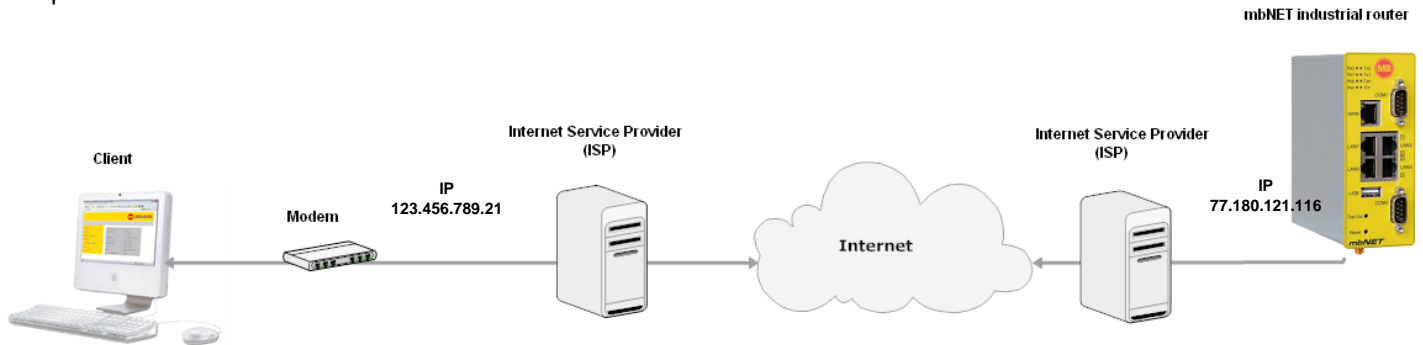
13.2.4 Displaying and verifying connection status

On a computer connected to the router’s LAN interface, clicking on **Status – Modem** shows whether a user has dialed in to the router, and where there is an established connection, who has dialed in.



13.3 Configuring the industrial router for connection via the Internet

The following diagram shows how to connect the industrial router to a client computer via the Internet. The client is a computer with a modem connection.



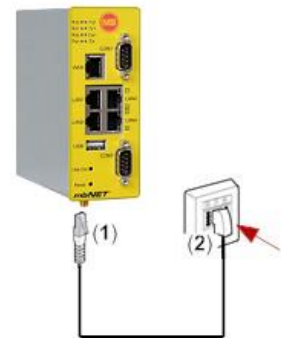
13.3.1 Connection and configuration of the router

Before you start make sure that the router is connected to a suitable power source and the **Power** and **Ready** LEDs are shining solid green.

13.3.1.1 Connecting the router

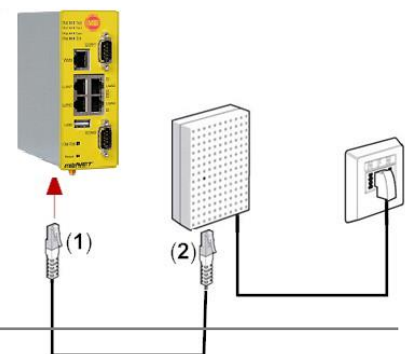
Analog connection only (applies to device models MDH xx0)

- Connect TAE adapter to analog cable.
- Plug one end of the supplied cable into the RJ12 jack (1) on the bottom of the router, and the other end into the TAE jack (2).



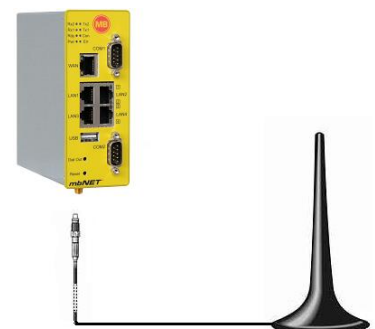
ISDN connection only (applies to device models MDH0x2)

- Plug one end of the supplied cable into the jack (1), and the other end into (2) the **NTBA**.



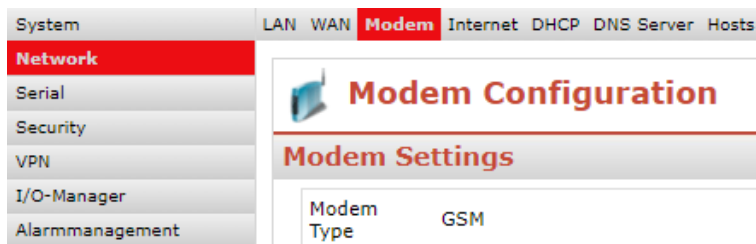
GSM connection only (applies to device models MDHxx3 and xx4)

- With an existing **GSM connection**, plug the end of the GSM antenna cable into the jack on the bottom of the router.

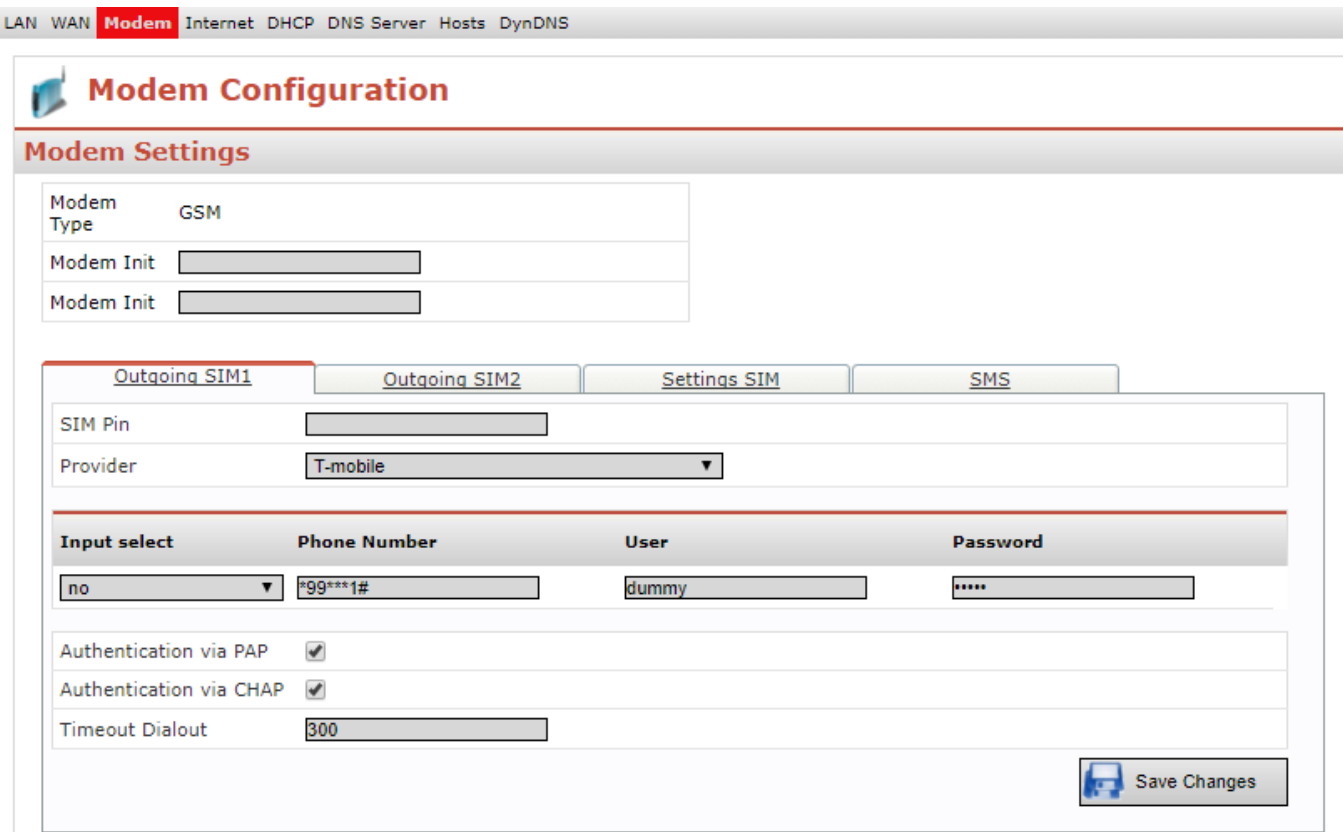


13.3.1.2 Configuring the router – client connection over the telephone network

- On the web interface home page, click on **Network** – **Modem** and then click the **Outgoing SIM1** tab when a SIM card is in the SIM card Slot1.



The following screen is displayed.

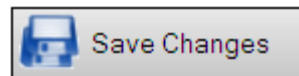


Follow the descriptions on the following pages.

For a detailed description of the **Network – Modem** settings, please see section **Network – Modem**

Label	Description
Modem Init	<p>ANALOG: If using an analog device, enter the command +GCI=country code (for country codes, see Country codes for analog devices) here, and in the second row, the command X3 (do not wait for dial tone).</p> <p>ISDN: If using an ISDN device, you need to enter your MSN number with the command AT#Z=n (n= MSN number) If you enter “n” as “*”, every call will be accepted.</p> <p>GSM: if using a GSM device, you must use the preset X3 command. The +GCI=country code may not be used.</p>
SIM PIN (GSM only)	If required, you can enter the SIM card PIN here.
Provider (GSM only)	You can select your provider here. If your provider is not shown, you can enter the APN (Access Point Name) yourself. You can obtain information on the APN from our website at http://www.mbconnectline.de/gsm/grps/mobilfunk.html or from your mobile broadband provider.
Provider name	If you do not see your provider listed, you can enter your APN manually. Ask your provider what details to enter for the APN, or visit our website at http://www.mbconnectline.de/gsm/grps/mobilfunk.html
Phone number	Enter the telephone number of the relevant provider. For example, the dial-up number for an analog data call: 019193384 See comment below table. For GSM Modems the dial-up number always uses the format *99***1#
User	Enter user name (refer to your mobile broadband provider’s network details) In example shown: any For GSM modems you can obtain the necessary information at e.g. http://www.mbconnectline.de/gsm/grps/mobilfunk.html (In most cases, any user name can be used).
Password	Enter password (from provider details). In example shown: any For GSM modems you can obtain the necessary information at e.g. http://www.mbconnectline.de/gsm/grps/mobilfunk.html (In most cases, any password can be used).
Authentication via PAP	Use the default setting for the authentication protocol. This is set by default when a dial-up connection is set up.
Authentication via CHAP	Use the default setting for the authentication protocol. This is set e.g. when a dial-up connection is set up.
Timeout dialout in [s]	Enter a time of 300 (=5 minutes in the example shown here), after which dialing attempts will stop.

Now save your changes by clicking **Save Changes**.





Please Note: The internet-by-Call providers are changing their prices often. MB connect line cannot be made responsible for any price changes.

- ❑ Now click on **Network** – **Internet** and enter the following settings.



Internet Connections

LAN WAN Modem **Internet** DHCP DNS Server Hosts DynDNS

Internet Configuration

Internet Settings

Internet Connections
Internet Settings

Failover no ▼

Internet Connection Internet via WAN (external router, fixed line) ▼

Connection monitoring

PING IP no ▼

Internet Connections	
Label	Description
Failover	The Failover feature allows you to switch between different Internet connections. If this function is activated, the Internet interfaces can be entered in the desired priority depending on the device type.
Internet Connection	From the drop-down field, select the setting Internet via Modem

Internet Settings

Internet Settings	
Label	Description
Connection Mode	Select “keep connection” here.
lock connection by	Using the drop-down field you can decide whether the Internet connection should be closed when one of the inputs receives a signal (internally-generated, between 10 and 30V).
broadcast IP-Adress via email	Enable this setting. Select whether the IP address should be sent to the email address listed.
email	Enter the email address to which the IP address is to be sent here.

Internet Settings > Settings

Settings	
Connect on traffic	<input checked="" type="checkbox"/>
Ignore traffic on LAN	<input type="checkbox"/>
Ignore traffic from internal services	<input type="checkbox"/>
Connect on "Dial-Out"	<input checked="" type="checkbox"/>
Connect on Sign 1 at Input	don't connect
close connection after inactivity of [s]	100
Save Changes	

Internet Settings > Settings	
Connect on traffic	Activate the checkbox if a connection to the Internet, initiated by data packets sent, is to be established.
Ignore traffic on LAN	If this check box is activated, no connection that differs from the setting under "Connection Mode" can be established. For example, a component connected to the LAN uses the device (router) as a gateway.
Ignore traffic from internal services	If this check box is activated, no connection that differs from the setting under "Connection Mode" can be established. For example, if an e-mail is to be sent by the device (router) or an automatic time synchronization is to be executed.
Connect on "Dial-Out"	If the connection to the Internet is to be triggered by pressing the Dial Out button on the device front, activate this checkbox.
Connect on Sign 1 at Input	<ul style="list-style-type: none"> don't connect Select this option if you do not want to set up an Internet connection, triggered by a digital signal at one of the inputs. Input 1, Input 2, Input 3, Input 4 Select this option if an Internet connection is to be established by a signal at the corresponding input.
close connection after inactivity of [s]	This is used to set the time for the existing Internet connection to be disconnected as soon as data packets are no longer sent by the router. No input turns off this function.

For a detailed description of the **Network** – **Internet** settings, please see **section Network – Internet**

Save your changes by clicking **Save Changes.**

Click on **System** – **User** and add a user with dial-in rights. For further notes on adding users and assigning specific rights, please see **section Adding users**

Finally, to save your changes permanently to the industrial router, click **Apply Changes.**

Configuring for connection over the Internet (continued)

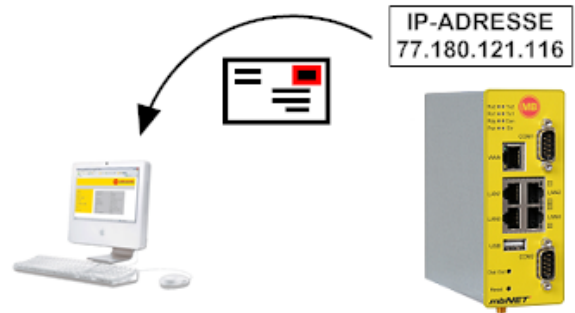
13.3.2 Router Internet dial-in

In the screen shown above, the router is configured to establish an Internet connection as soon as it is restarted

For other methods of Internet dial-in, please see section [Network – Internet](#)

Transmit IP address:

For the client to be able to access the router, it must know the router's IP address. Under the configuration settings made previously, the IP address is sent to the email address that was provided. This allows you to access the router via the IP address.



As the router IP address changes each time it dials in to the Internet, there is an alternative, which is to use our **DynDNS service**. For information on setting up and using the MB Connect Line DynDNS service, please see section [Network – DynDNS](#)

13.3.3 Displaying the Internet connection

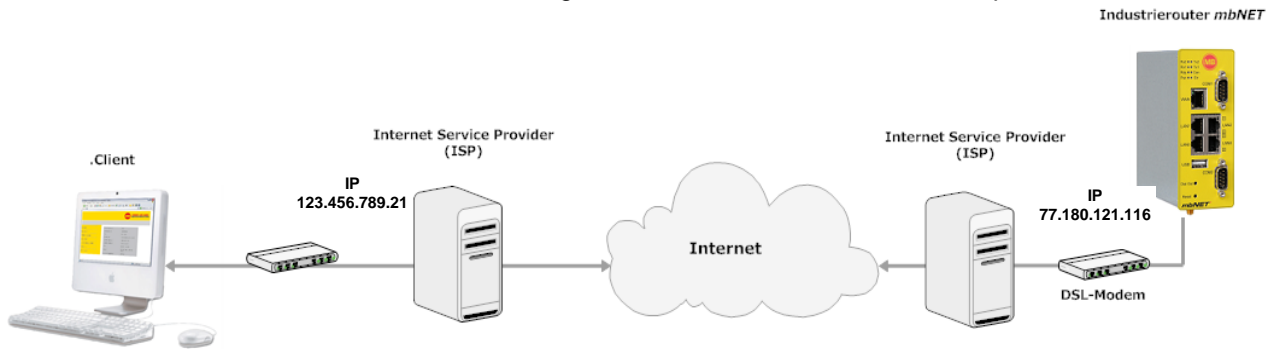
Assuming that you can access the router, you can see information on the status of the Internet connection by clicking **Status – Internet**.



For more detailed information on status messages, please see section [Status Messages](#)

13.4 Configuring the industrial router for connection to the Internet using a DSL modem

The picture below shows how to connect the **mbNET** industrial router to a client PC over the Internet, using a DSL modem. The client needs to use an existing Internet connection, or to set one up.

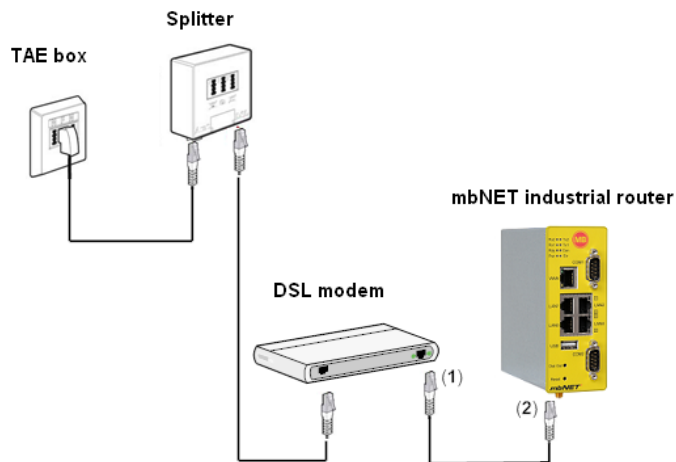


13.4.1 Connecting and configuring the router

Before you begin:
 The router must already be connected to a suitable power source and the **Power** and **Ready** LEDs must both be solid green.

13.4.1.1 Connecting the router

- Connect the router to the DSL modem as shown in the diagram on the right.
- Plug one end of the straight-through Ethernet cable into the LAN connector **(1)** of the DSL modem and the other end **(2)** into the WAN connector on the router.



13.4.1.2 Configuring the router using the web interface

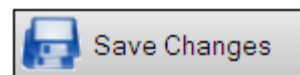
- ❑ **The connection wizard** helps you to configure your connections quickly and easily. To access the wizard, click on the Wizards link at the top right of your browser. If you have disabled the autolaunch function for wizards, click on the Start button for the Internet connection wizard.
- ❑ Now select the option for External DSL modem.
- ❑ Enter your Internet login details. You can obtain these from your Internet Service Provider.
- ❑ You can also choose whether the **mbNET** should send you an email, use a dynamic DNS service, or be accessible over the Internet via MB Connect Line's DynDNS.
- ❑ Confirm and save your entries. Finally, the **mbNET** must be restarted to fully implement the settings.

From the home page of the configuration interface, click **Network – WAN** and then the Outgoing tab. This will display the screen shown below. Follow the instructions below.

For a detailed description of **Network – WAN** settings, please see section “**Network – WAN**”

Label	Description
Interface Type	Select DSL here.
Connection Type	If you are in Germany, select PPPoE (most commonly used protocol in Germany). PPTP is most common in Austria.
PPP User Login	Enter your Internet access user name. Use the name provided by your ISP.
PPP User Pass	Enter your Internet access password. Use the password provided by your ISP.

- ❑ Save your changes by clicking **Save Changes**.



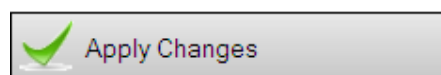
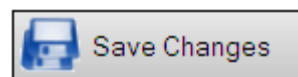
Configuring for connection over the Internet (continued)

- From the web interface home page, click **Network** – **Internet**
- The following site should be displayed.

For a detailed description of the **Network** – **Internet** settings, please see section “*Network – Internet*”

Label	Description
Internet connections	Here, select to connect over Internet via WAN .
Connection Mode	Select Connect immediately . The connection will be established whenever you restart the router.
Lock connection by	You can interrupt the Internet connection by means of a signal to one of the digital inputs.
Send IP address via email	Check the box by clicking on it, to have the router’s IP address sent to the email address that you will enter below.
Email	When an Internet connection has been established, an email message will be sent to the email address entered here.

- Save your changes by clicking **Save Changes**.
- Finally, to save your changes permanently to the router, click **Apply Changes**.
- To finish, **restart the router**.



13.4.2 Establishing a connection between client PC and router

- ❑ **Router Internet dial-in.** Depending on the router settings (see Internet Configuration), you need to either restart the router, or push the Reset button.

For further Internet dial-in settings, please see section [Network – Internet](#)



- ❑ Client PC Internet dial-in. Dial the client PC into the Internet.

- ❑ **Transmit IP address:**

For the client to be able to access the router, it must know the router's IP address. The option to transmit the IP address is selected during router configuration. The IP address is identified by sending it to the email address specified during configuration.



As the router IP address changes each time it dials up to the Internet, a helpful alternative is to use our **DynDNS service**.

For information on setting up and using the MB Connect Line DynDNS service, please see section [Network – DynDNS](#)

13.4.3 Displaying connection status

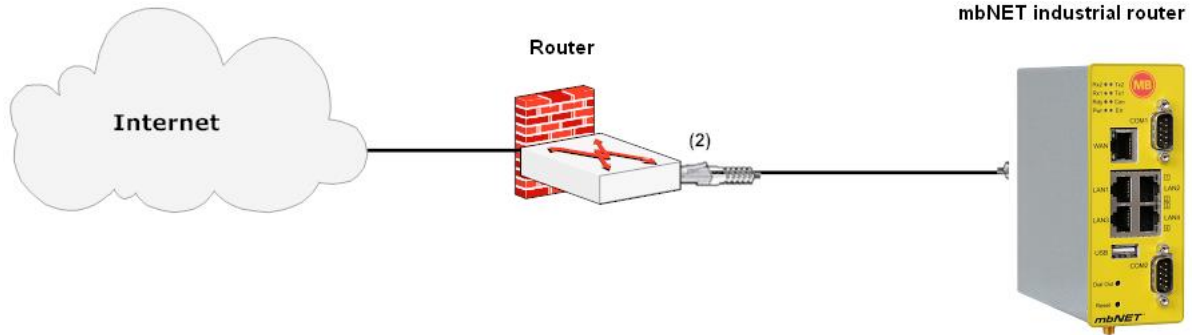
Go to **Status – Internet** to check if there is an internet connection.



For further information about the status messages, read the chapter: [Status messages](#)

13.5 Configuring the industrial router for connection to the Internet via an existing router

The diagram below shows how to link the industrial router up to a network which already has a router that is set up for connection to the Internet. The existing router must first be assigned the right settings. This operating mode is particularly useful if you need to set up a connection between the **mbNET** industrial router and a VPN gateway.



13.5.1 Connecting the router

- Connect the router to the existing router as shown in the picture at top of the page.
- To do this, plug one end of the crossover cable (1) into the (1) **WAN** connector on the **mbNET** router, and the other end into the **LAN** connector (2) of the existing network router.

13.5.2 Configuring the router using the web interface

- The connection wizard** helps you to configure your connections quickly and easily. To access the wizard, click on the Wizards link at the top right of your browser. If you have disabled the autolaunch function for wizards, click the Start button for the Internet connection wizard.
- Now select the option “External router (Firewall)”.
- At this point you have a choice between automatic recognition of your network and interface details, or entering them manually.
- Read through the information and after clicking “Next”, you can complete the wizard by clicking “Finish”. A restart is required to complete the process.
- From the home page of the configuration interface, click **Network – WAN – Interface**. This will display the screen shown below.



Configuring the router for connection to the Internet via an existing router

For a detailed description of the **Network – WAN** settings, please see section “**Network – WAN**”

Label	Description
Interface Type	As in the example shown, select Static IP . This setting also requires a DNS server (see Network – DNS server).
WAN IP address	Here, enter the IP address of the mbNET connected to the WAN port. In the example: 192.168.1.100
Netmask	Enter the subnet mask. In this case: 255.255.255.0
Default Gateway	Enter details of the gateway that connects you to the Internet, i.e. the IP address of the existing router. In this case: 192.168.1.1

Configuring the router for connection to the Internet via an existing router

- On the web interface home page, click on **Network – Internet**.
- The following screen will be displayed.
Follow the instructions on the subsequent pages.

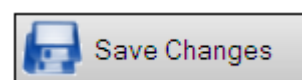
For a detailed description of the **Network – Internet** settings, please see section “Network – Internet”



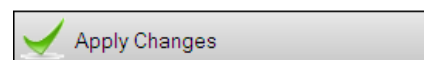
Label	Description
Internet connection	From the drop-down field, select connect to Internet via WAN (external router, fixed line) , so that the Internet connection will be made by the existing router.

This option means “no Internet connection” because the *mbNET* itself is not connecting to the Internet.

- Save your changes by clicking **Save Changes**.



- Finally, to save your changes permanently to the router, click **Apply Changes**.





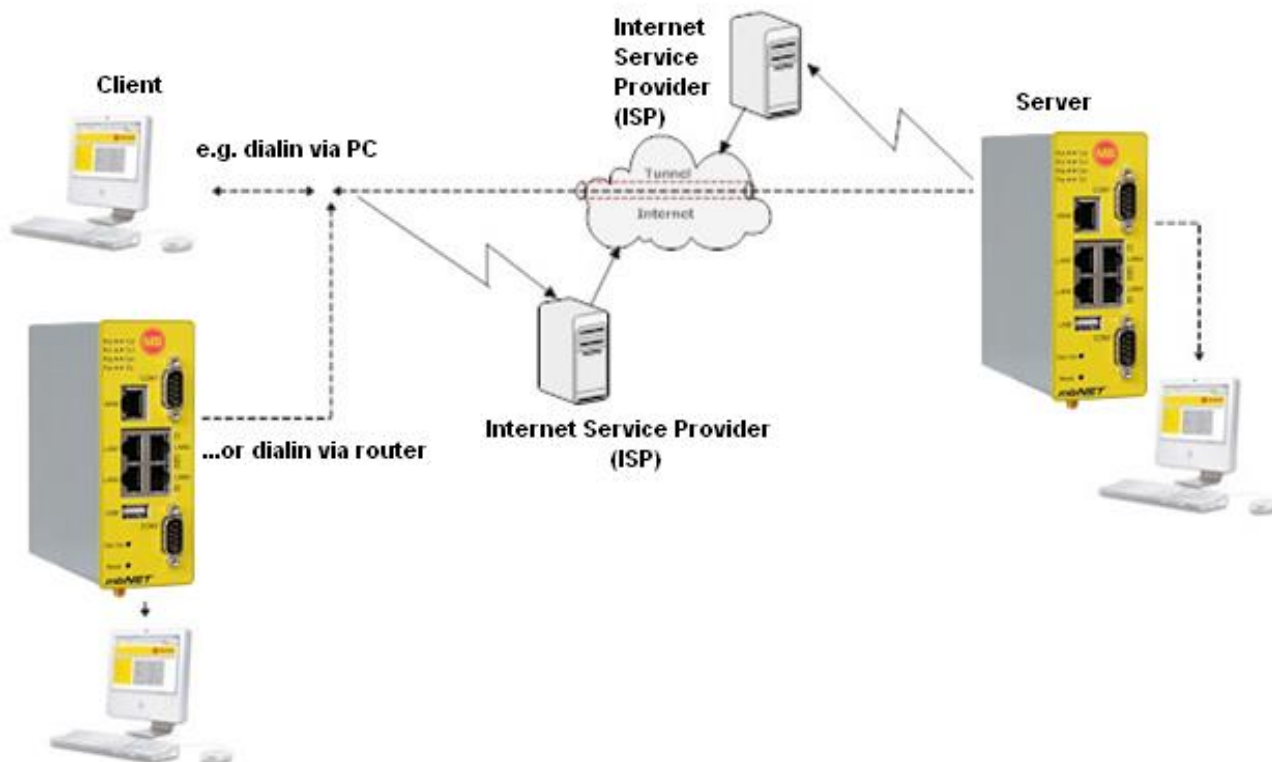
After applying the changes, please restart the router.

13.6 Configuring the industrial router for VPN connection to a client

Setting up a virtual network reduces the cost of a fixed connection between two or more LANs and ensures secure data transfer over the non-secure Internet. Using a tunneling protocol sets up a secure connection called a VPN tunnel.

In the connection scenarios described in 9.3 and 9.4, a client can only access the router's serial interfaces (for a description of serial interfaces, see **Serial Interfaces**). This does not allow for access to the LAN interface via the Internet. Using a VPN connection however, it is possible to reach or access subscribers connected to the LAN interface, such as panel PCs.

The diagram below represents a VPN connection. The client can be e.g. a PC or another industrial router, pre-configured for Internet access.



Configuring the router for VPN connection to a client

13.6.1 Connecting and configuring the router

13.6.1.1 Connecting the router

A VPN connection first requires that the router has an Internet connection in place. For instructions on how to configure the router for connection to the Internet, you can refer to the connection scenarios already described above, based on the connection mode required. As a basic principle, the router must be accessible via a public IP address.

13.6.1.2 Adding VPN dial-in users

- ❑ For a client to be able to dial into the industrial router via a VPN, a user must be added and have VPN dial-in rights assigned under user management. For instructions on exactly how to add a user with specific rights, please see section [System – Users](#).



IPSEC and PPTP

PPTP and IPSEC are the available protocols for a VPN connection tunneling protocol. The diagram below shows a VPN configuration using PPTP.

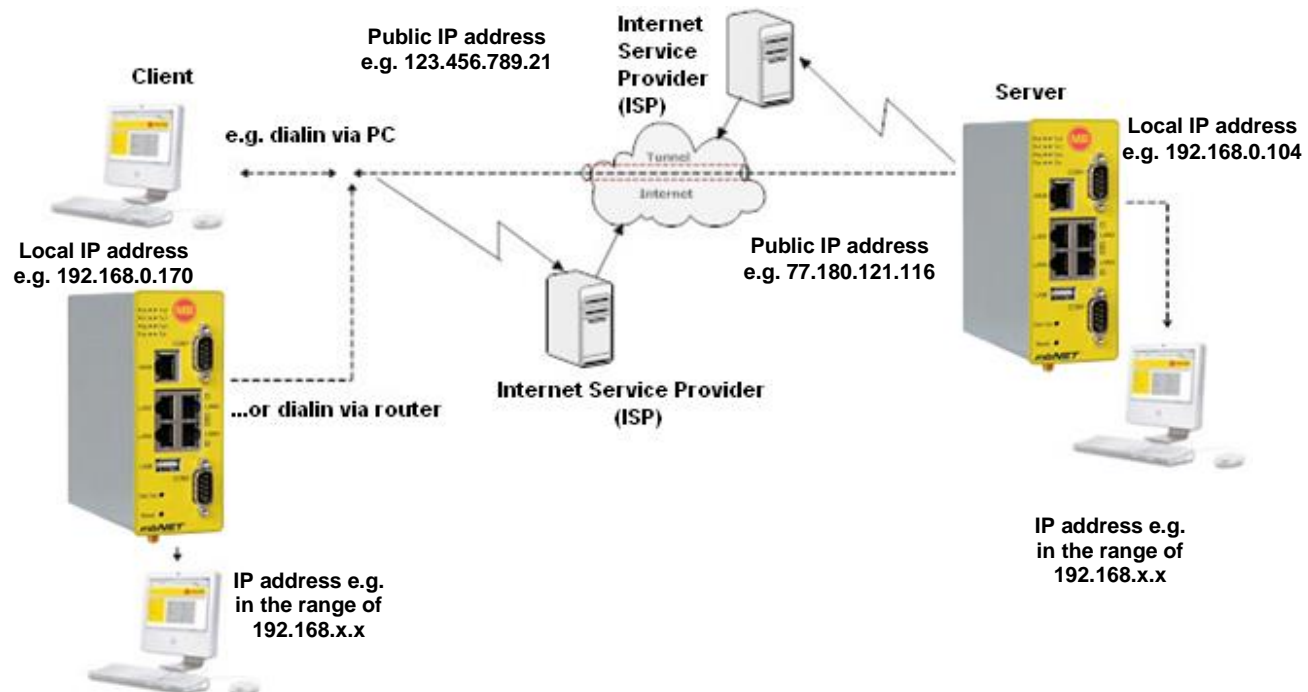
13.6.1.3 Configuration of the router (VPN-Server)

Go to **VPN** -> **PPTP**



Not possible with mbNET variant with WLAN (FW 4.1), because only OpenVPN.

The following screenshot shows the description of the various configuration settings.



13.6.1.3.1 Connection-Wizard

The connection wizard helps you to configure your connections quickly and easily. To launch the wizard, click on the Wizards link at the top right of your browser. If you have disabled the autolaunch function for wizards, click on the Start button for the VPN connection wizard. Otherwise, check “VPN – set up a VPN tunnel” and ensure that everything else is unchecked.

Important: if you configured your Internet connection manually, the VPN wizard will display a warning. If you have not yet set up an Internet connection for the **mbNET**, please cancel the VPN wizard and set up an Internet connection first. Otherwise, check the box and click “Next”.

Please note that with firmware versions 2.0 and higher, to enable IPsec configuration on the wizard page you first need to click on IPsec below the Start button for the VPN wizard, then on Save Changes, and Apply Changes.

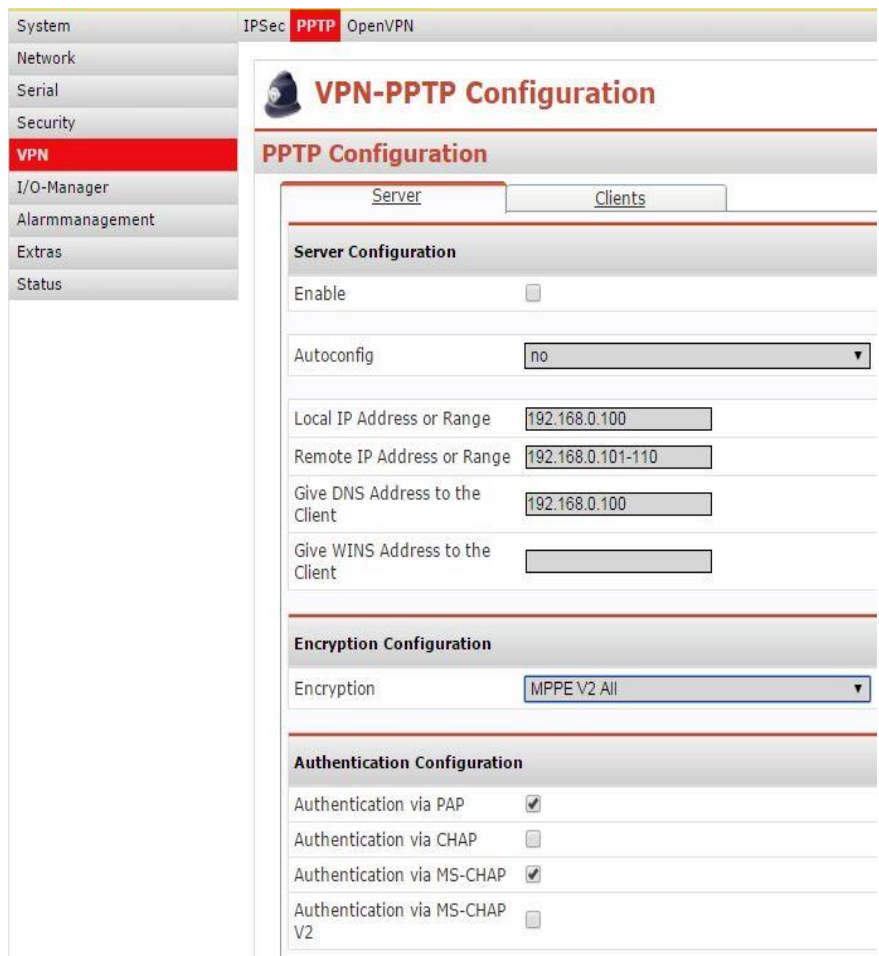
- Here, select “Connection between Networkclient and **mbNET**” and click “Next”.
- Type in your key (PSK) and click “Next”. Note that you should not use any special characters, and that your client must receive the key via a secure path.
- Now you can download a ready configured Windows VPN connection for your computer from the **mbNET**.

13.6.1.3.2 Manual configuration

- To configure manually, proceed as follows:

On the home page, click on **VPN** in the navigation bar on the left and on **PPTP** in the navigation bar at the top, then on the tab marked **Server**.

For a detailed description of the **VPN – PPTP** settings, please see section [VPN – PPTP](#)



The screenshot displays the 'VPN-PPTP Configuration' web interface. On the left is a navigation menu with 'VPN' highlighted. The main area shows the 'PPTP Configuration' page with 'Server' and 'Clients' tabs. The 'Server Configuration' section includes:

- Enable:
- Autoconfig: no
- Local IP Address or Range: 192.168.0.100
- Remote IP Address or Range: 192.168.0.101-110
- Give DNS Address to the Client: 192.168.0.100
- Give WINS Address to the Client: (empty field)

 The 'Encryption Configuration' section shows:

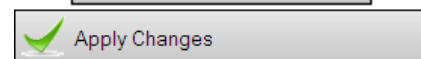
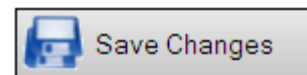
- Encryption: MPPE V2 All

 The 'Authentication Configuration' section shows:

- Authentication via PAP:
- Authentication via CHAP:
- Authentication via MS-CHAP:
- Authentication via MS-CHAP V2:

Label	Description
Enable	To enable the connection, check the box by clicking on it.
Auto config	If you select “yes” here, the PPTP server will be configured using the mbNET 's LAN address. This setting needs to be tried out first. You should only enter your PPTP server settings manually if there is an address conflict.
Local IP address or Range	Enter any local address in this input field. In the example it is: 192.168.10.100 Note: You can also use the router's LAN IP address. You should only re-host your PPTP server in a different address space if there is an address conflict.
Remote IP address or Range	Enter the remote addresses here. In the example: 192.168.10.160-170 This assigns the IP addresses of the connected clients within the range of 192.168.10.160 – 192.168.10.170. Important It is essential that the address or address range entered here is in the same address space as the local IP address chosen above
Give DNS address to the client	Enter the DNS server address. In this case: 192.168.0.100 (router IP address)
Encryption	Use the default setting (MPPE V2 All)
Authentication	Use the default setting (via CHAP and MS-CHAP V2).

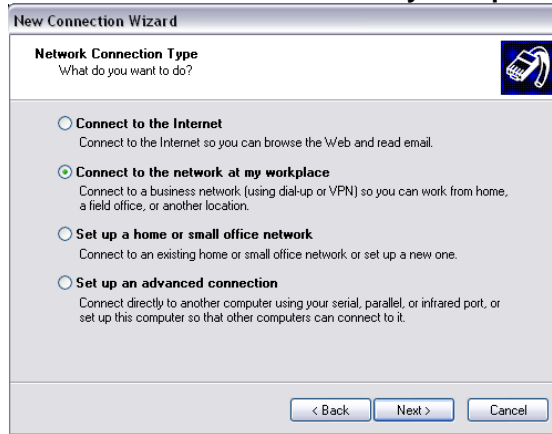
- Save your changes by clicking **Save Changes**.
- Finally, to save your changes permanently to the router, click **Apply Changes**.



Setting up the router for a VPN connection (continued)

13.6.2 Configuring a client PC for a VPN connection to the router

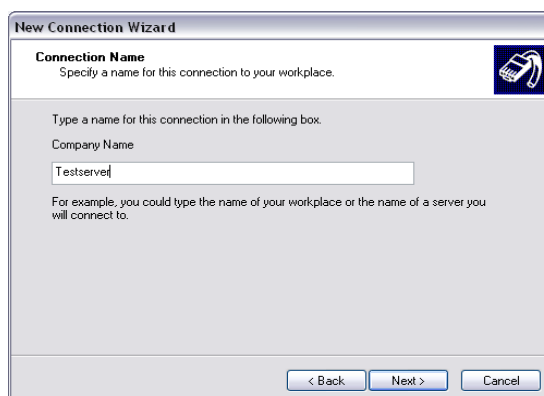
- ❑ To proceed with set up, the client PC must have an existing Internet connection. For information on setting up a client PC please see section [Configuring a client \(PC\) for router access](#)
- ❑ In Windows Control Panel, click on **Network Connections** and then on **Create a new connection**.
- ❑ Now a wizard should appear, select **Connect to the network at my workplace**.



- ❑ On the next screen, select **VPN connection**.



- ❑ Now enter a name for the **VPN connection**.

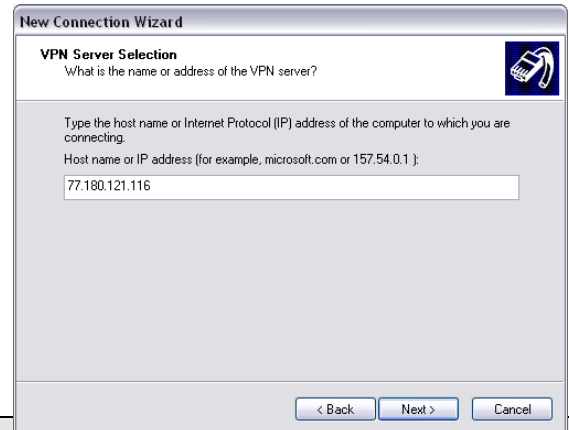


Setting up the router for a VPN connection (continued)

- Here, enter either the DynDNS service forwarding name, or the current **IP address** of the router.

Note:

- *The example in Figure 86 uses an IP address assigned by the ISP.*



For information on setting up and using the MB Connect Line DynDNS service, please see section [Network – DynDNS](#)

When entering the router’s IP address, make sure that you always enter the current IP address (the IP address changes every time the router connects to the Internet).

- Now you can select if the connection should be created for all users or only for the current user.
- Now add a desktop shortcut to the connection.
- ✓ **The VPN connection is now set up.**



Setting up the router for a VPN connection (continued)

13.6.3 Setting up a VPN connection between client PC and router

13.6.3.1 Router Internet dial-in

- Depending on the connection mode, the router must be configured for Internet access, connected to the Internet, and accessible via the IP address.

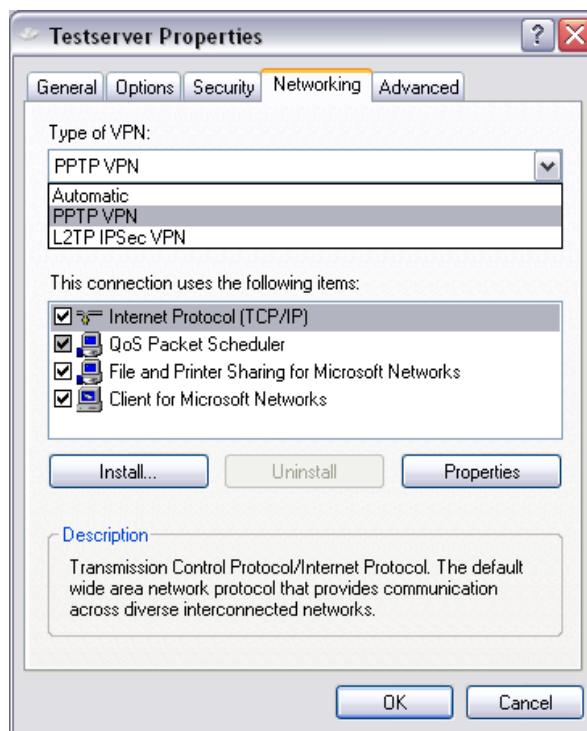
13.6.3.2 Setting up a VPN connection from client to router

- Double-click on the VPN connection icon and in the next screen, enter the user name and password to which you assigned VPN dial-up rights in the router’s user management settings.



13.6.3.3 Additional settings

- Double-click on the VPN connection icon and then click Properties. In the “Networking” menu tab you can set the VPN type to LT2P or PPTP. Select „PPTP VPN“.



Setting up the router for a VPN connection (continued)

- The client PC will display a flashing screen icon the router is connected. You can display the connection properties by right-clicking on the icon

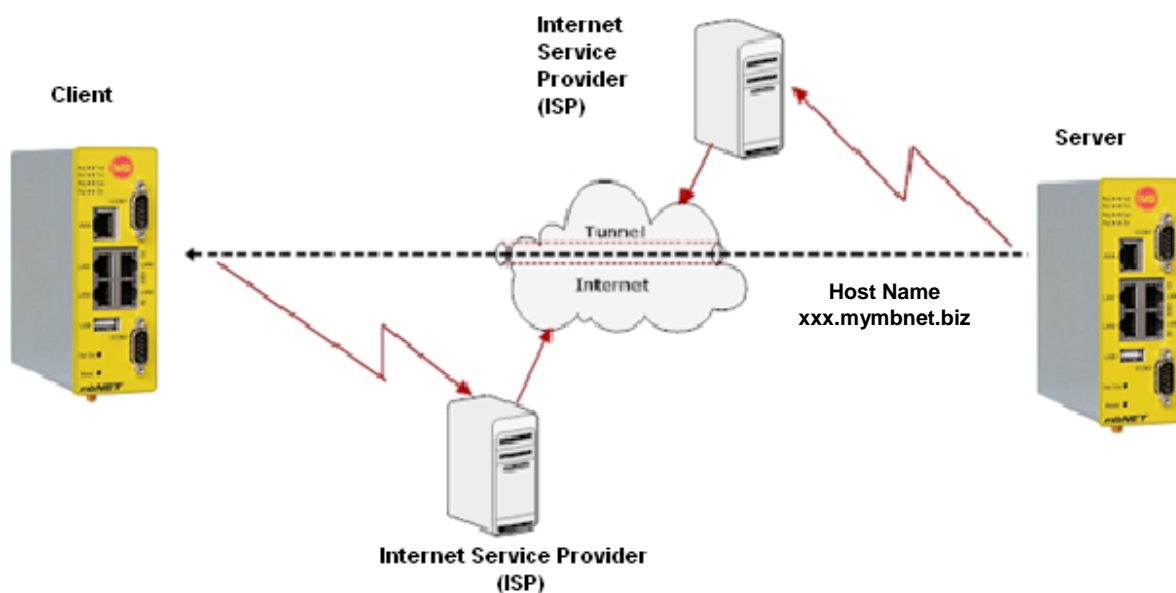
On a PC connected to the router, clicking **Status** on the sidebar and **VPN-PPTP** on the navigation bar at the top will show you information on the current status of the VPN connection, such as users currently dialed in, or current connection status.



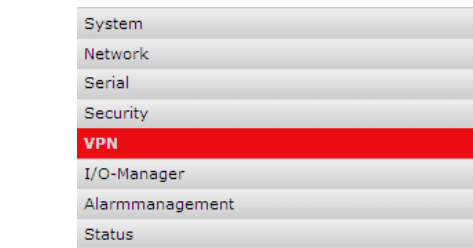
Where an industrial router has been set up as a client, please see the next section for settings that will allow it to access another remote industrial router.

13.7 Configuring a connection between two routers via VPN PPTP

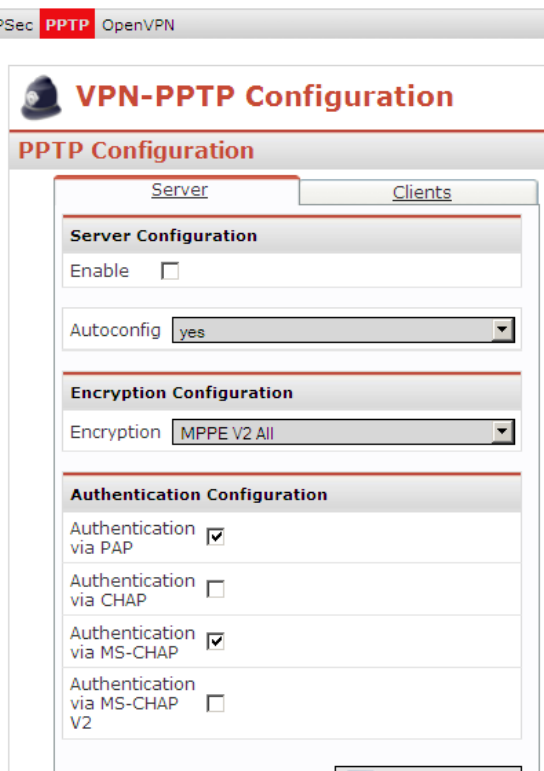
- ❑ Instead of a client PC, you can also configure another router as a client. As a client, a router must be configured such that the router on the other end of the connection is its VPN server. Both routers need an Internet connection. For details of configuring the industrial router as a VPN server, please see the previous section [Configuring the industrial router for a VPN connection with a client.](#)
- ❑ The following example should clarify the configuration.



13.7.1 Settings for connecting two industrial routers – PPTP – server

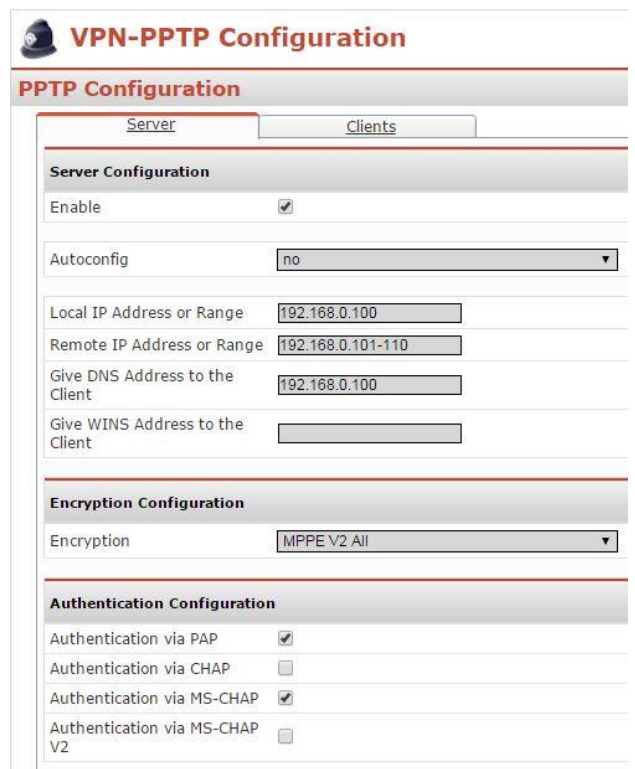


- From the home page navigation bar on the left, click **VPN** and on the navigation bar at the top click **PPTP**.
- This will display the screen below.



If you now set the "Enable" box and save this setting, your server is live. It will then provide dial-in clients with addresses from its local network and use its LAN address as the PPTP server address.

If you wish to use other addresses, set the "Autoconfig" option to **NO** and you will see the picture on the right:



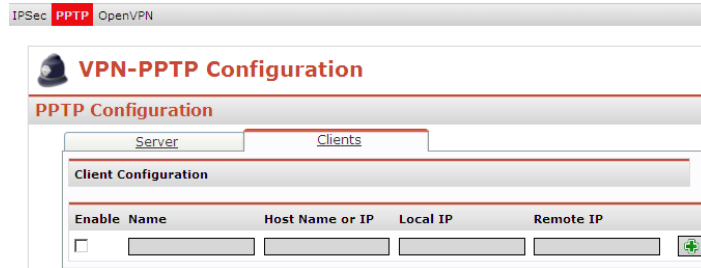
Label	Description
Enable	To enable the connection, check the box by clicking on it.
Autoconfig	Selecting “yes” means that the mbNET 's local network range and IP address will be used. By selecting „no“, you can enter this information manually.
Local IP address or Range	This is the PPTP server address
Remote IP address or Range	Enter the address or address range of dial-up clients here.
Give DNS address to the client	Here, enter the address of the server currently providing name resolution. Usually, you can enter the PPTP server address here.
Give WINS address to the client	The WINS server IP address can also be entered here for compatibility with older Microsoft operating systems.
Encryption	<p>This option selects the type of data encryption.</p> <ul style="list-style-type: none"> <input type="checkbox"/> MPPE V2 All <input type="checkbox"/> MPPE V2 128 <input type="checkbox"/> MPPE V2 40 <input type="checkbox"/> None <p>You should only select “none” if it is for test purposes. The data will not be transferred securely.</p>
Authentication via PAP, CHAP, MS-CHAP, MS-CHAP V2	You can select which authentication methods your PPTP server will support here. Place a check next to your chosen methods and click on Save Changes. Make sure that the client is also using one of the supported authentication methods, otherwise it will not be able to connect.



Note that when using MPPE encryption,
You must ALWAYS use MS-CHAP or MS CHAP v2 as the authentication method.

For more detail on **VPN – PPTP** please see section **VPN – PPTP**

13.7.2 Settings for connecting two industrial routers - PPTP-Client



➤ Clicking on the green plus sign on the far right will open the following configuration screen.



- Name:** Enter a name of your choice for the connection.
- Host Name or IP:** Enter the public address or DynDNS name for the PPTP server.
- Local IP:** You can use the PPTP server address. Generally speaking, this field should be left blank, as the PPTP server sends its address when it establishes a connection.
- Remote IP:** You can enter a single address or a whole network. We recommend using the settings shown in the screenshot on the right, and entering a network address. This makes the network accessible to all subscribers.

Please note that the network address must be in CIDR notation as shown in the screenshot on the right (192.168.0.0/24)

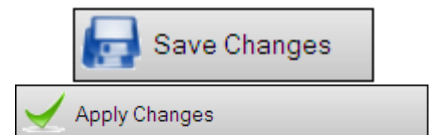
- Authentication:** Choose one of the methods supported by the PPTP server. You can see what they are on the PPTP server's web page, under VPN-PPTP.
- Encryption:** Use the same type of encryption as the server. Please note that when using MPPE encryption, you must always enable MS-CHAP or MS-CHAP V2 authentication.
- User / Password:** For the User and Password fields, the user must have been added to the PPTP server (e.g. standard user name ADMIN, without password). However you can add a new user to the server (to do this you need to change the

user on the server web page under System Users).

- Start Connection on:** allows you to choose which events the client should connect for. The following options are available:
 - Connect immediately
 - Connect on traffic
 - Connect on signal high at input 1-4

Now save your settings by clicking on the „Save Changes“ button.

Click on „Apply Changes“ to save this configuration permanently.



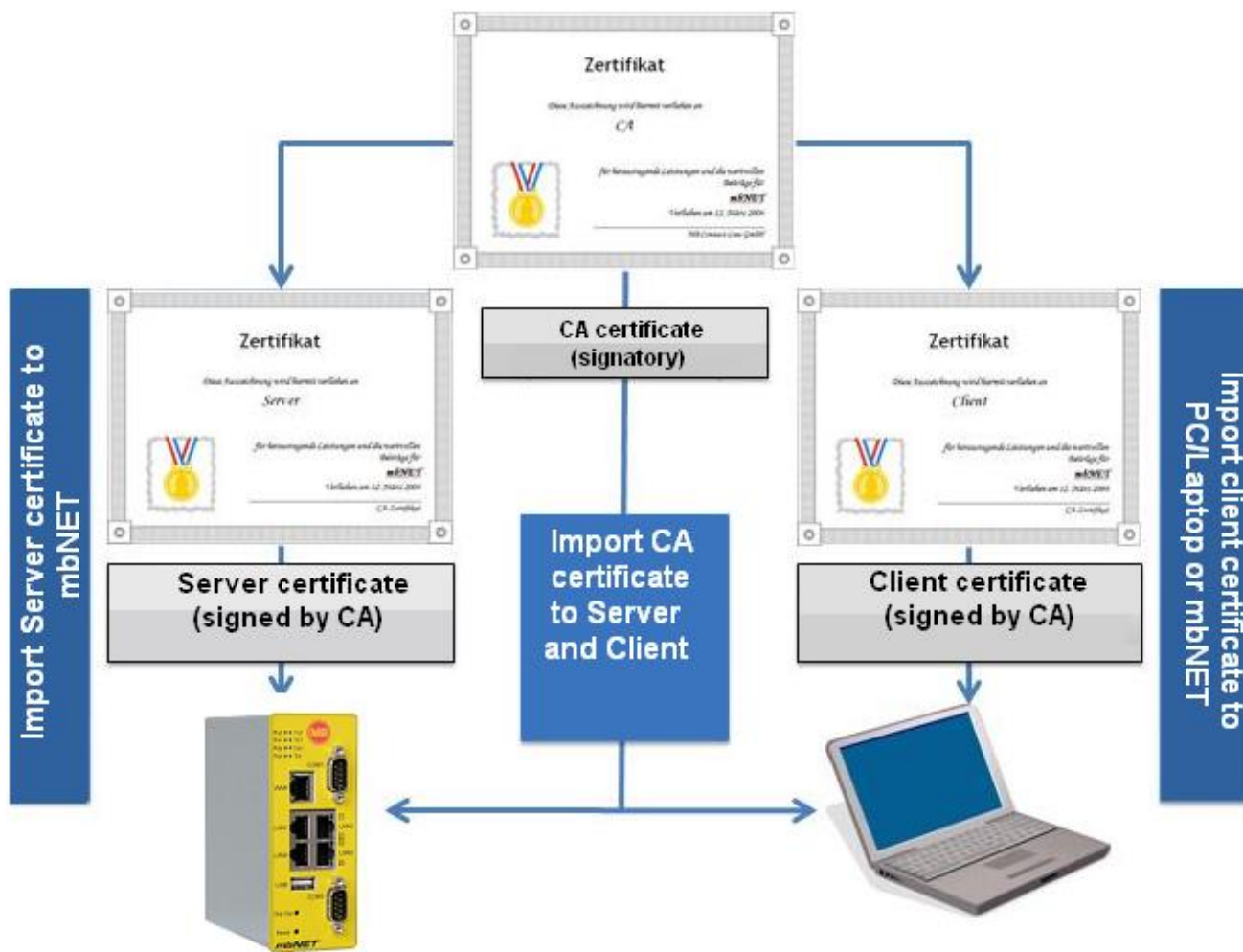
For more information on **VPN – PPTP** settings, please see section [VPN – PPTP](#)

Label	Description
-------	-------------

Enable	To enable the connection, check the box by clicking on it.
Name	Assign a name to the client. In the example we used: PPTPclientConnection
Host name or IP	Here, enter the name or IP address that the client uses to contact the server. In the example, this is: 123456789@mbNET.mymbnet.biz
Local IP	The server address can be entered here. Generally speaking, this field can be left blank.
Remote IP	Enter the address of the remote station, or the address for a whole network. We recommend entering a network address. In the example: 192.168.0.0/24. Note the CIDR notation (/24 after the network address)
Authentication	Select an authentication method that is also enabled in the server settings.
Encryption	We recommend selecting MPPE V2 encryption. Note that if you select "none", your data will NOT be sent securely.
User & Password	Enter the user name and password of a user who has been added to the PPTP server as a system user (e.g. ADMIN, without password).
Start connection on	Select Keep connection . A connection will be established on restart or boot up. It is also possible to start the connection only for specified events.

14. Creating certificates and revocation lists using XCA.

14.1 Certificates overview



Any subscriber communicating over a VPN connection needs 2 certificates. One certificate must be signed by a CA (Certificate Authority). Each subscriber must have the CA certificate plus a “server” or “client” certificate. In our case:

- **The server** may be the **mbNET** or a separate server.
- **The client** is either a computer or another **mbNET**.

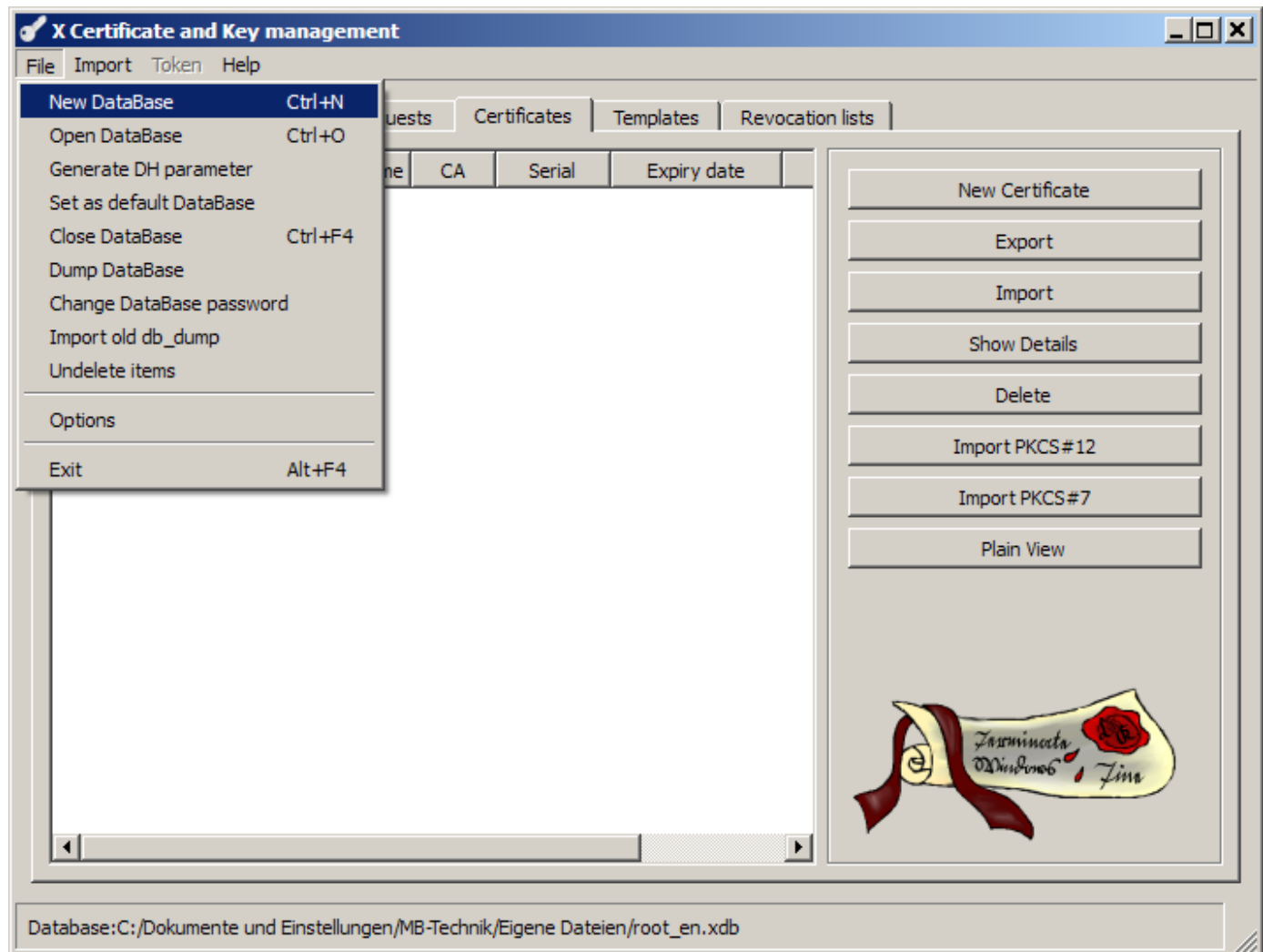
The certificates are required to set up a secure VPN tunnel and are used to authenticate the VPN subscriber. If the subscriber has no certificate, or an invalid certificate, no VPN tunnel can be established between the two devices if the authentication setting on the **mbNET** is “**X.509**”. To understand how to create certificates, please read the following pages.

14.2 Creating certificates

Christian Hohnstädt's XCA freeware program is useful for creating certificates. Using this program makes it easy to create X.509 certificates as well as the necessary private keys.

You can download the program from <http://sourceforge.net/projects/xca> free of charge, and install it in Windows in the usual way (run the .exe file).

When you launch XCA for the first time, a new database has to be created to manage the certificates. To do this, click „**File**“ and then „**New DataBase**“

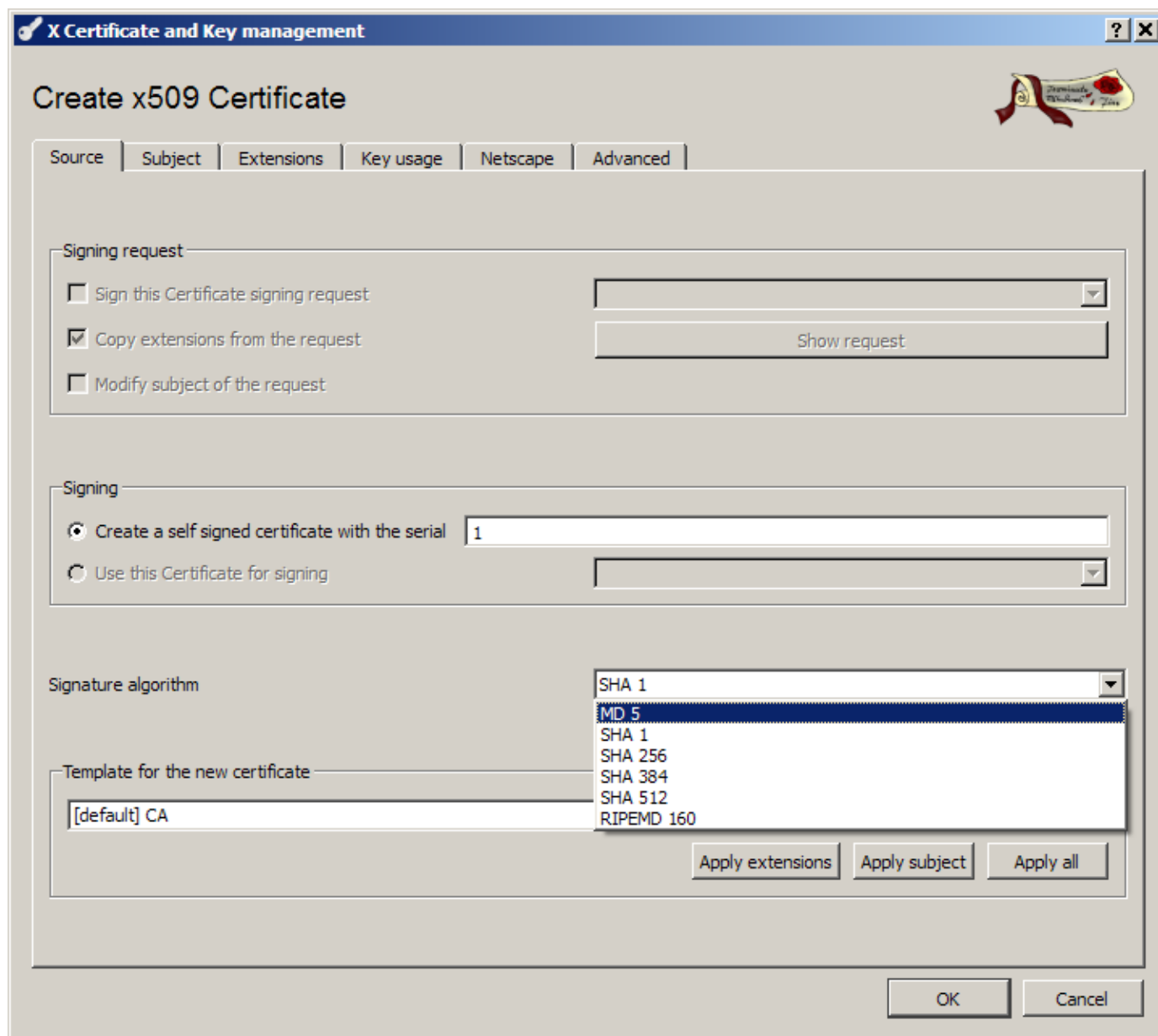


- After choosing a name, file save location and password for the database, you can open it and start creating a root (CA) certificate.

14.2.1 Creating a root certificate

- To create a root certificate, click on the “Certificates” tab and open the following dialog box by clicking “New Certificate”.

14.2.1.1 Root certificate source



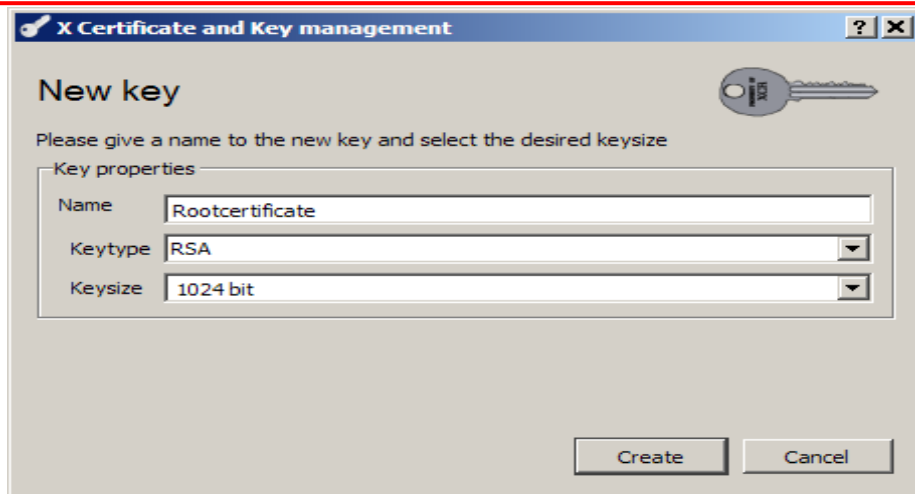
- First, change the Signature algorithm to MD5 so that the certificate is compatible with the **mbNET**. Then you can go straight to the “Subject” tab and create the certificate.

14.2.1.2 Root certificate subject

In the *“Subject”* tab, fill in the fields from “Internal Name” through “email address”. For VPNs using IPsec, Subject settings can later be used as an ID (cf. section **Authentication**)
 Next, create a private key by clicking on *“Generate a new key”*.



Please do not use accents (e.g. ü, ä, ö)
 (Example: Write Dinkelsbuehl instead of Dinkelsbühl in the locality field)



- ❑ Select key type RSA. You can select any key size and of course, any name. The longer the key, the more secure the encryption but also the more processing power required.

14.2.1.3 Root certificate extensions

In the “Extensions” tab you will find the settings for certificate type and validity.

Basic constraints

Type = Certificate Authority (CA)
 Check the box labeled Critical

and Key identifier

Check the box labeled Subject Key Identifier

Validity

You can enter a specific start and end date in the relevant fields or use the adjacent Time Range field.

Time Range

In the dialog boxes to the right, enter the number of days, months or years. The list below specifies how long individual certificates should be valid for:

- Personal certificates should be valid for 1 year.
- Server (SSL) certificates, 1 year.
- Router certificates should be valid for 1 year (external routers) or 10 years (internal routers).
- CA certificates should have an extended lifespan (e.g. >10 years).

Click “Apply” to confirm the **Time Range** values.

Subject alternative name

The subject alternative name is a list of alternative names for the certificate holder. These can be RFC822 names (email), DNS names, X.400 addresses, EDI names, URIs or IP addresses. In principle, any structured naming system is applicable. If using PKIX, this extension is essential when the certificate subject field is empty.

Issuer alternative name

For issuer alternative names, the same applies as for subject alternative names.

CRL distribution point

To be able to use a public access point for certificate revocation lists, you need to enter the LDAP or HTTP address of the list. The address should always be prefixed with a **URI** (universal resource indicator) (e.g. URI:http://de.wikipedia.de). For the field separator, use a colon. If you hold local revocation lists, this option is not relevant.

Authority Info Access

This PKIX extension defines how to access additional information and services from the issuer of the certificate. It can then provide more information about the CA (additional guidelines, root certificates ...) or online verification services (e.g. OCSP). Primarily, where certification applications like secure mail (S/MIME) do not return the entire certification path, using this extension in the end certificate is helpful for showing the verifying application where to retrieve the next higher level CA certificate.

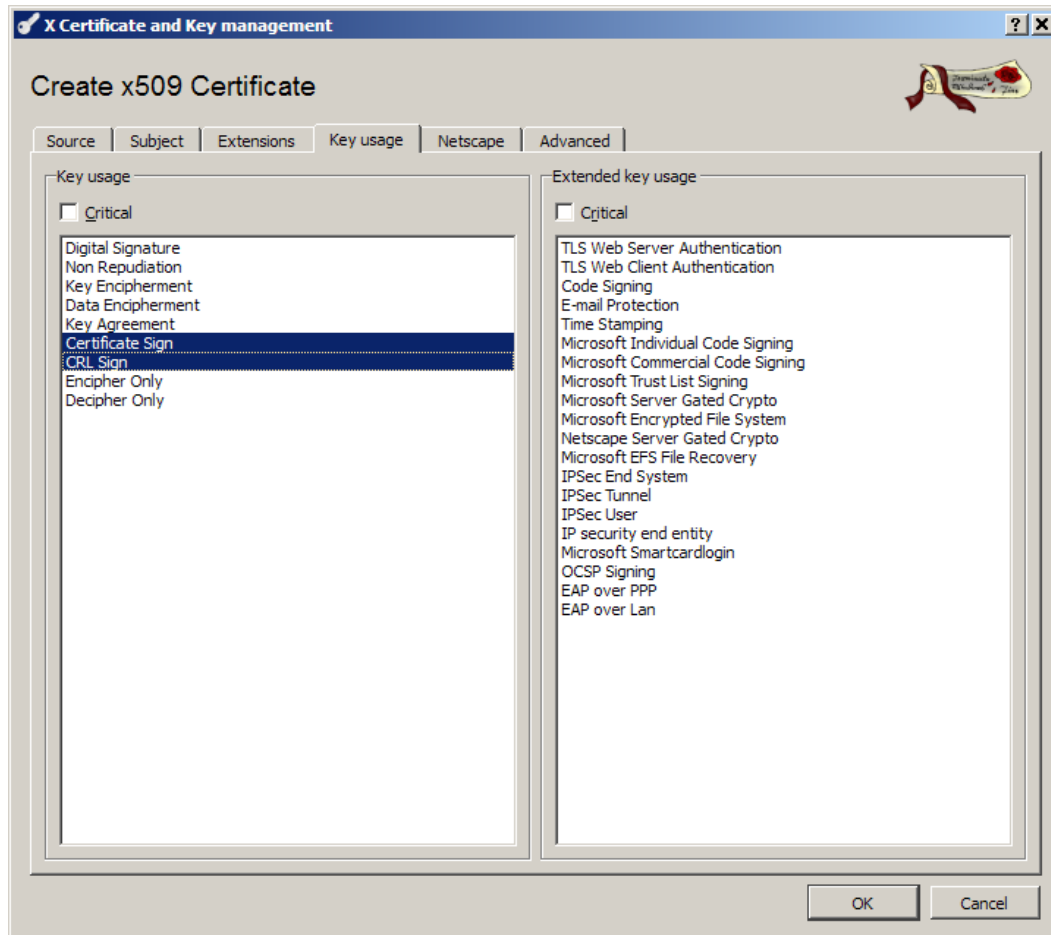
14.2.1.4 Root certificate key usage

In the “*Key usage*” tab you will find key usage and extended key usage options. Neither key should be critical i.e. you should leave the boxes marked Critical unchecked.

To create a root certificate, please select the following values in the left hand column:

- Certificate Sign
- CRL Sign

Selecting these options means that your root certificate can sign the client certificate and revocation lists.

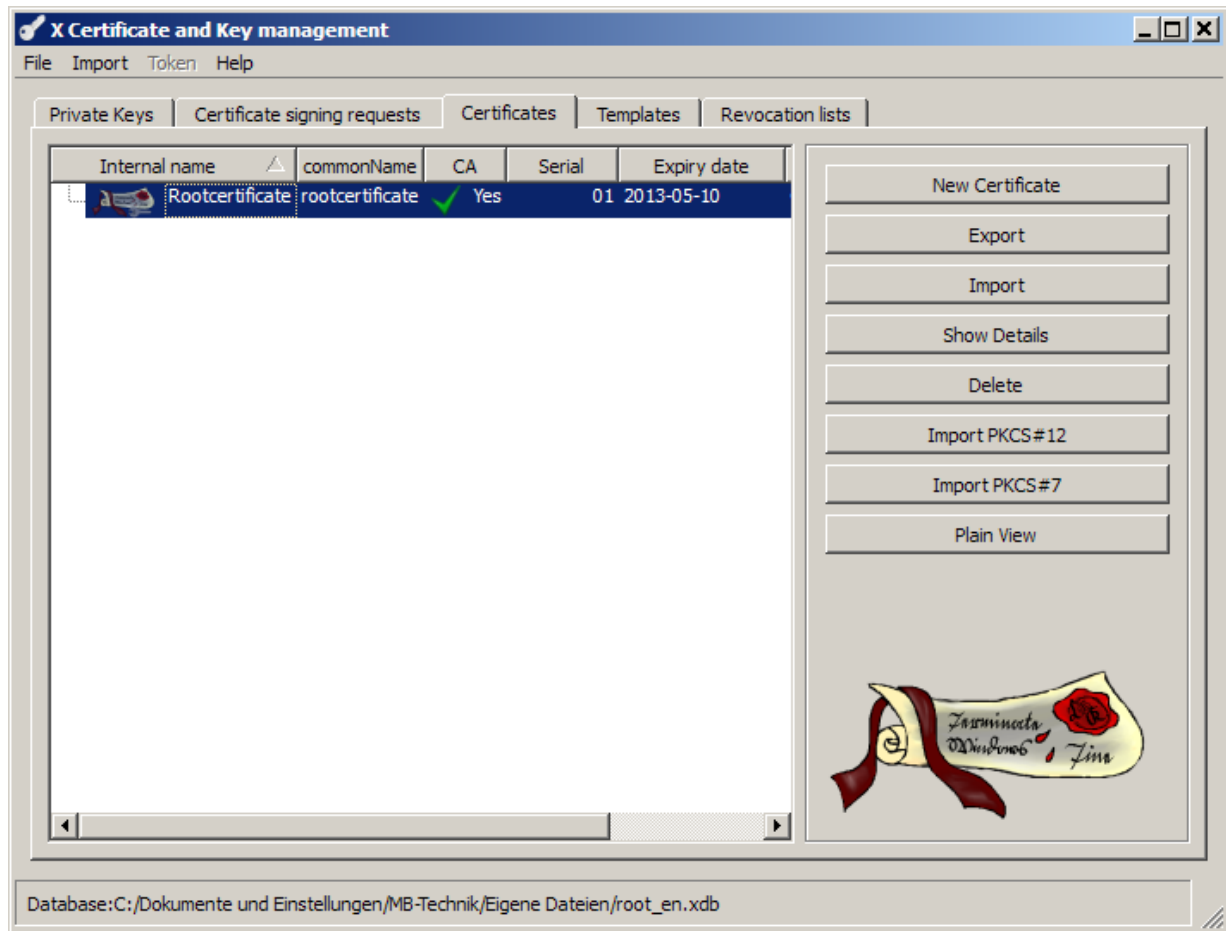


Now click on “OK” to complete root certificate creation.

Your root certificate is now ready and you can now derive and sign your additional certificates.

14.2.2 Creating a client certificate

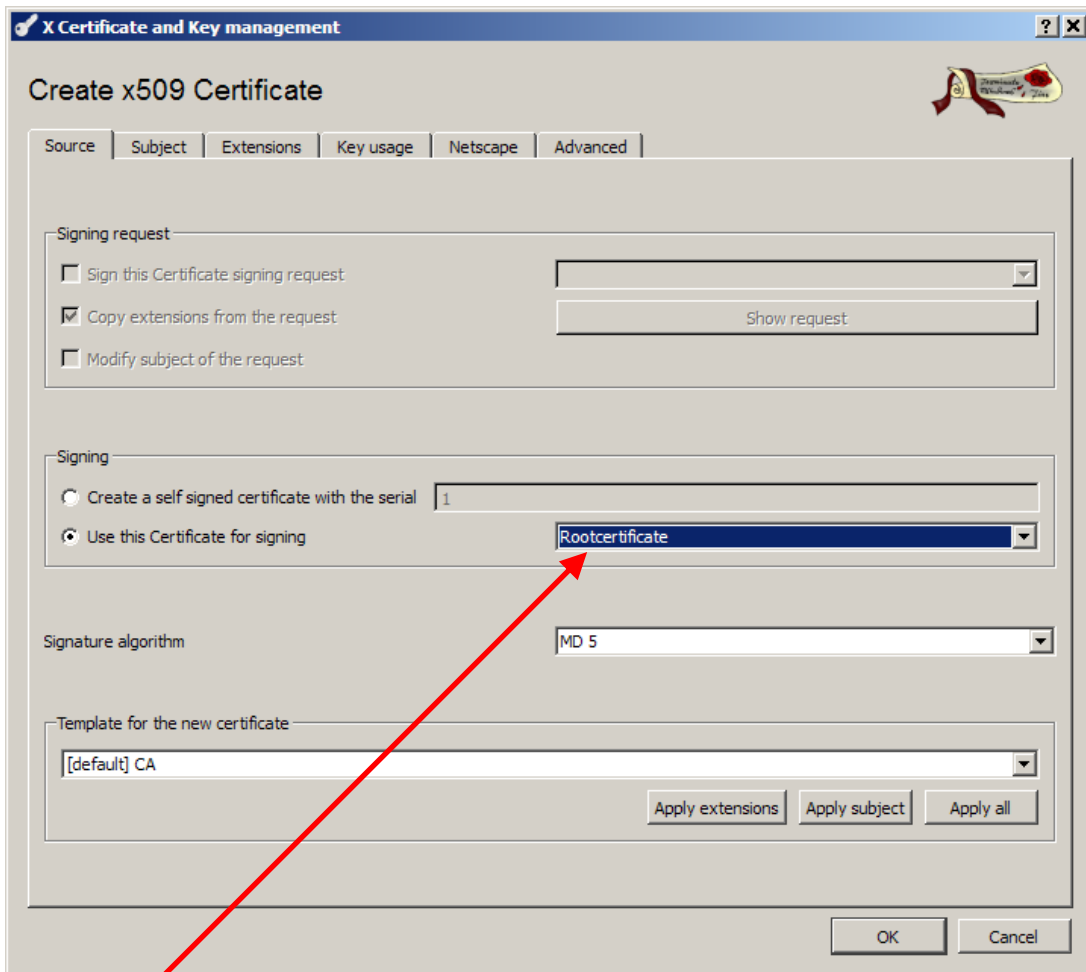
To create a certificate signed by this CA, in the “*Certificates*” tab, highlight the root certificate that you just created, and click again on “*New Certificate*”.



After this, the following dialog appears.

14.2.2.1 Client certificate source

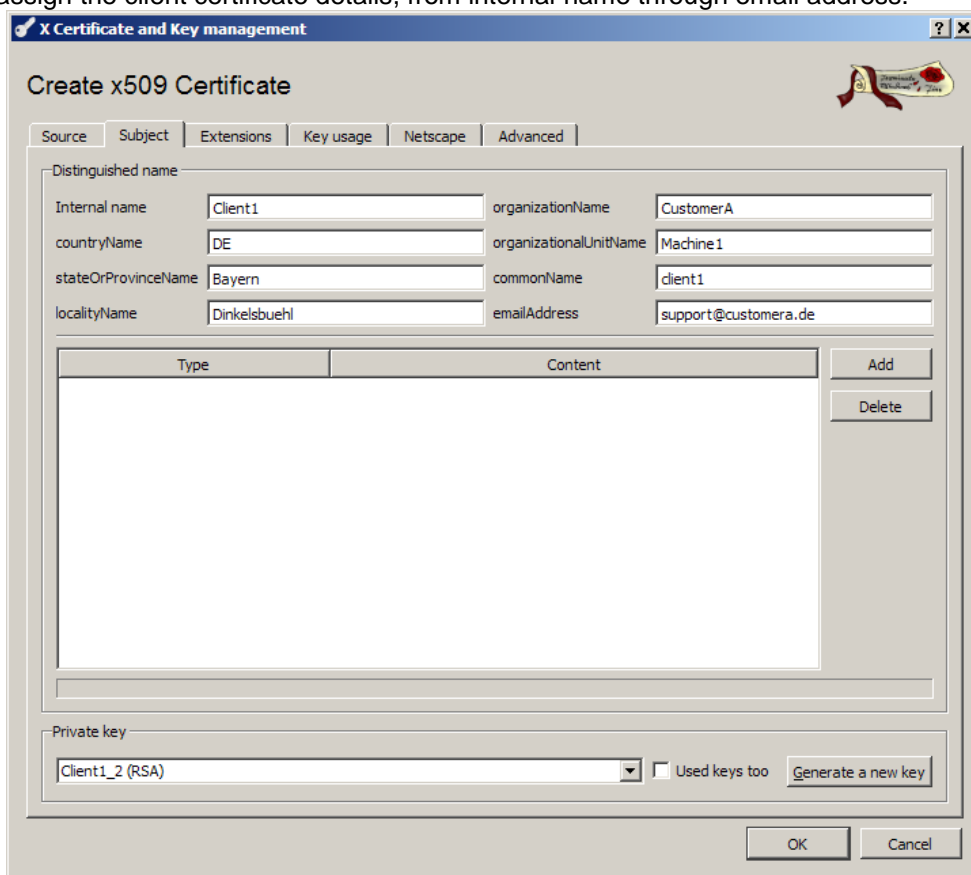
First we need to select our root certificate as the one that will be used as signatory. We also need to set the signature algorithm to MD5 again.



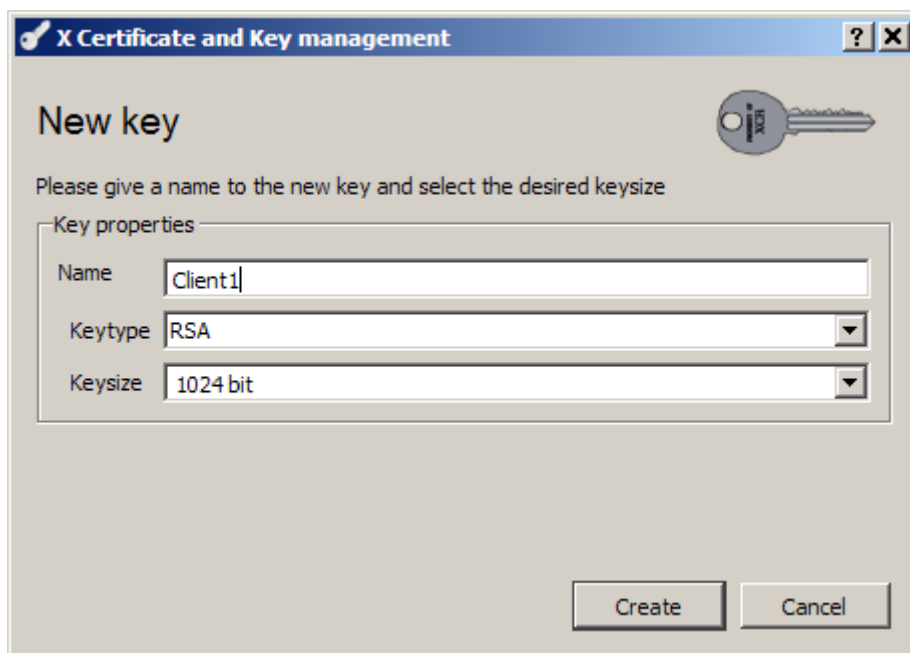
We see here that our root certificate is already set as the one to use as signatory.

14.2.2.2 Client certificate subject

Once again, assign the client certificate details, from internal name through email address.



Then generate a key for the client certificate. It is recommended that the key should be the same size as the one for the root certificate.



14.2.2.3 Client certificate – Extensions

As your client certificate does not need to sign any other certificate, select End Entity as the Certificate Type.

Basic constraints

Type = End Entity

Key identifier

Check the box labeled Subject Key Identifier

Validity

You can enter a specific start and end date in the relevant fields or use the adjacent Time Range field.

Time Range

In the dialog boxes to the right, enter the number of days, months or years. The list below specifies how long individual certificates should be valid for:

- Personal certificates should be valid for 1 year.
- Server (SSL) certificates, 1 year.
- Router certificates should be valid for 1 year (external routers) or 10 years (internal routers).
- CA certificates should have an extended lifespan (e.g. >10 years).

Click "Apply" to confirm the **Time Range** values.

Subject alternative name

The subject alternative name is a list of alternative names for the certificate holder. These can be RFC822 names (email), DNS names, X.400 addresses, EDI names, URIs or IP addresses. In principle, any structured naming system is applicable. If using PKIX, this extension is essential when the certificate subject field is empty.

Issuer alternative name

For issuer alternative names, the same applies as for subject alternative names.

CRL distribution point

To be able to use a public access point for certificate revocation lists, you need to enter the LDAP / or HTTP address of the list. The address should always be prefixed with a **URI** (universal resource indicator) (e.g. URI:http://de.wikipedia.de). For the field separator, use a colon. If you hold local revocation lists, this option is not relevant.

Authority Info Access

This PKIX extension defines how to access additional information and services from the issuer of the certificate. It can then provide more information about the CA (additional guidelines, root certificates ...) or online verification services (e.g. OCSP). Primarily, where certification applications like secure mail (S/MIME) do not return the entire certification path, using this extension in the end certificate is helpful for showing the verifying application where to retrieve the next higher level CA certificate.

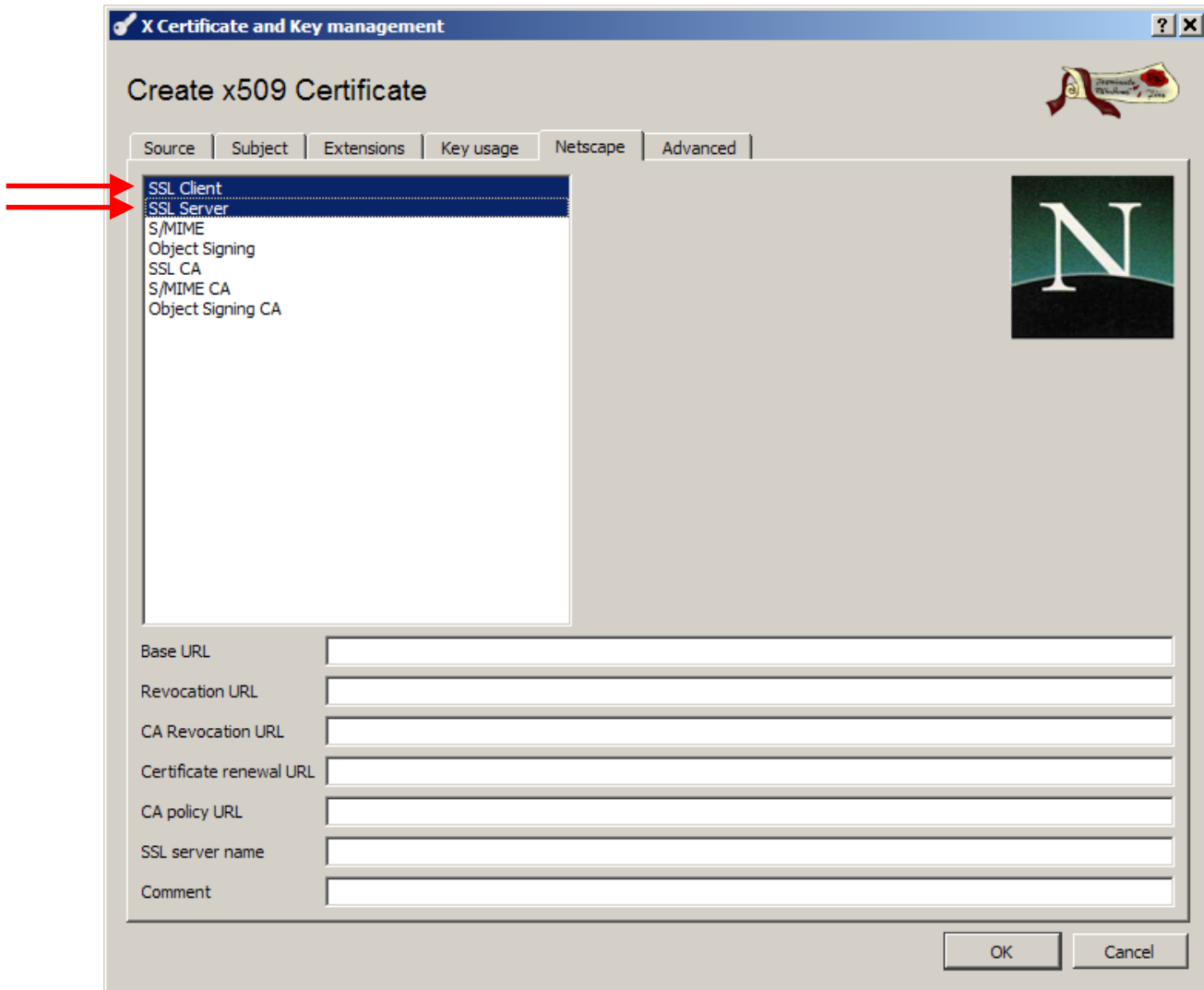
14.2.2.4 Client certificate – Key usage

If you create a client certificate as an end entity, you do not need any of these optional settings. You can proceed straight to the next tab.

14.2.2.5 Client certificate – Netscape

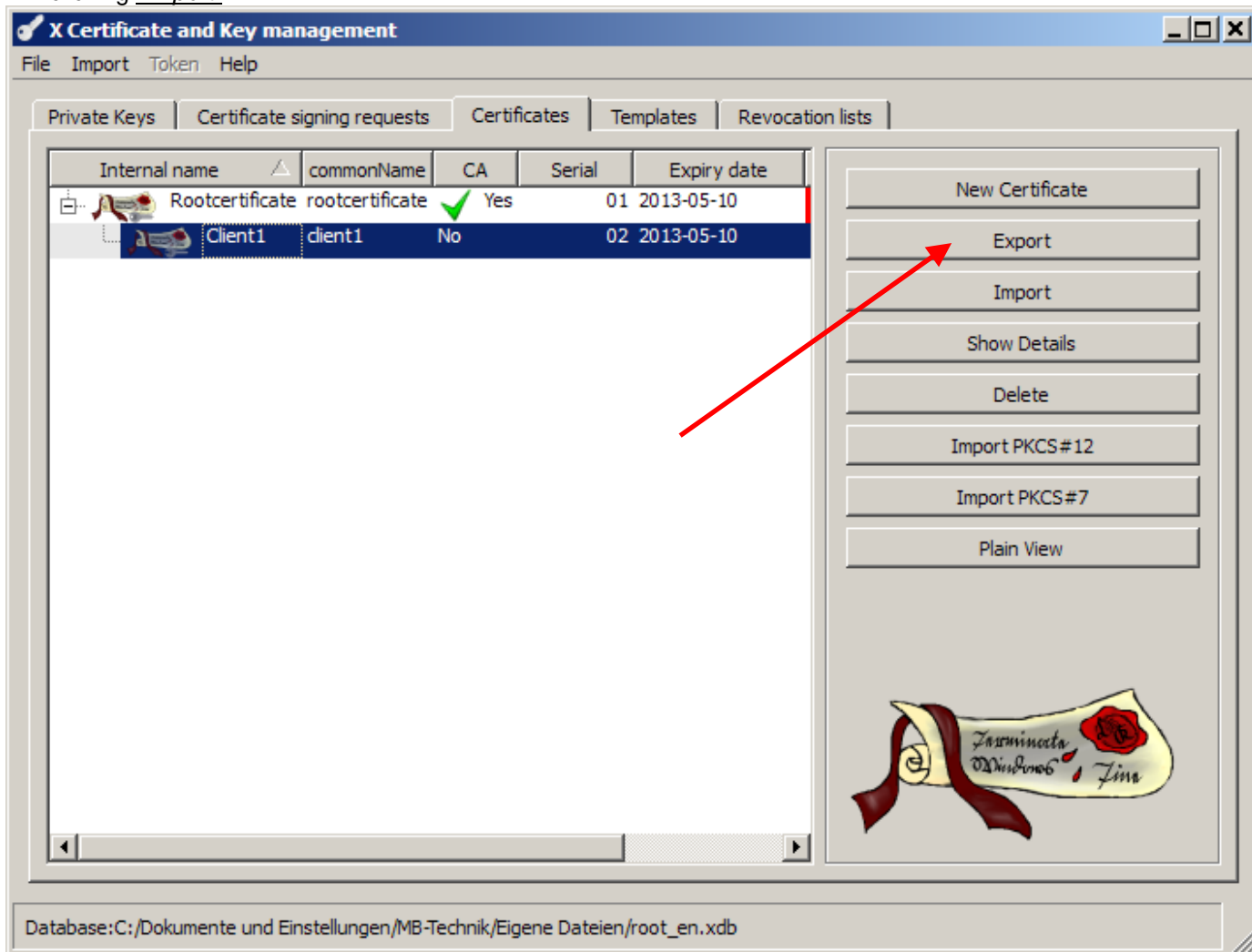
If you would like additional security, you can also select the SSL Server or SSL client option for your VPN subscribers according to their role (client or server).

The advantage of this is that OpenVPN can query whether a VPN server is also equipped with SSL. This option can also be enabled on the **mbNET**. The section on OpenVPN goes into more detail on this, and on the settings options. If you set up your certificate with both elements, it can be used with a VPN client or a VPN server.

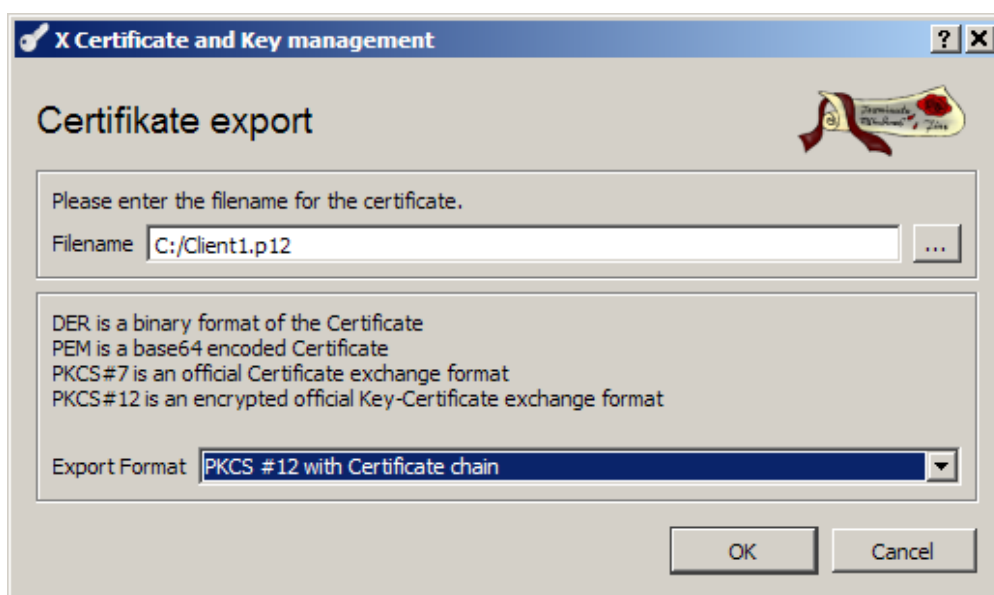


In the *“Netscape”* tab, no IPsec settings are required.
If using OpenVPN with “Peer must be TLS server” enabled, select only the SSL Server option. See also the screenshot above.

Now the certificates need to be published by highlighting the relevant ones in the “Certificates” tab and then clicking “Export”.



In the menu below, you can specify the save location for the certificate on your computer, and also the file format.



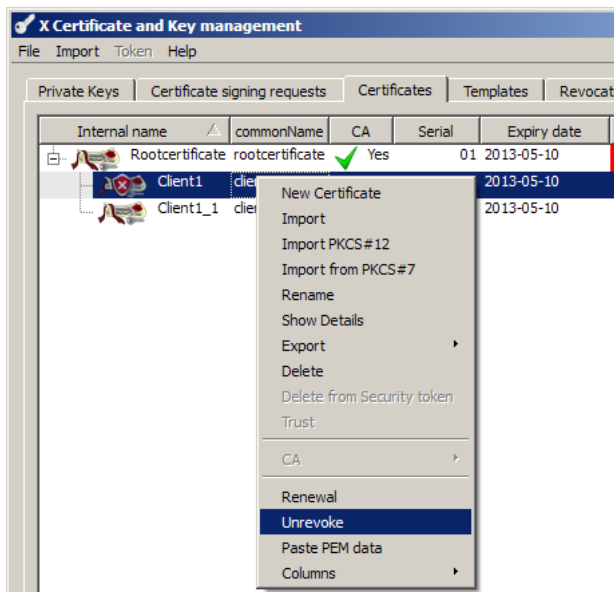
As your client is to be authenticated by the client certificate, it also needs the private key for this certificate. As shown in Figure 112, export the client certificate using export format PKCS #12 with Certificate chain. When you click OK, the client certificate will save to the location that you specified above. The client certificate then has the file extension .p12.

You must use the PEM (file extension .crt) format when exporting the root certificate.

These certificates can then be imported to the *mbNET* router via the web interface (cf. section [System – Certificates](#)).

For an explanation of how to set up these certificates for a Windows client, see [Importing certificates in Windows XP](#).

14.3 Generating CRL-Files (Certificate Revocation Lists)



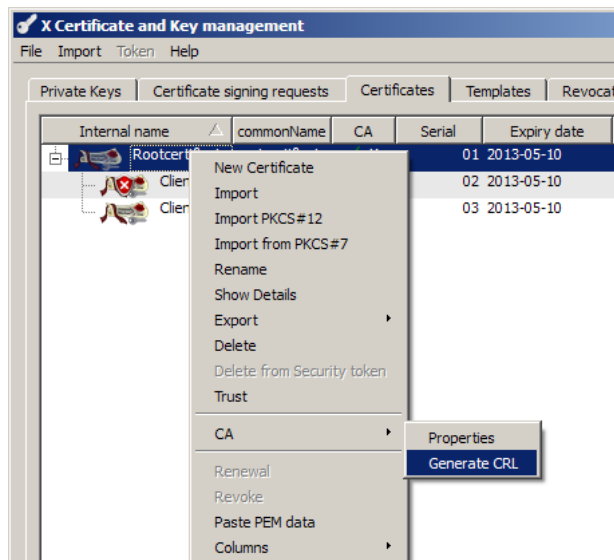
If you wish to withdraw a team member’s rights to use the VPN tunnel, please read this section and create a certificate revocation list.

To do this, re-open XCA. Open the database containing your team member’s certificate. To confirm a certificate as invalid, right-click on it and the dialog box below will appear:

Clicking on “*Revoke*” flags the relevant certificate with a red X, and it is no longer valid. To remove the flag and make the certificate entry valid again, click on “*Unrevoke*” as shown in the screenshot.

Next, right-click on the associated root certificate.

The following dialog box will appear:

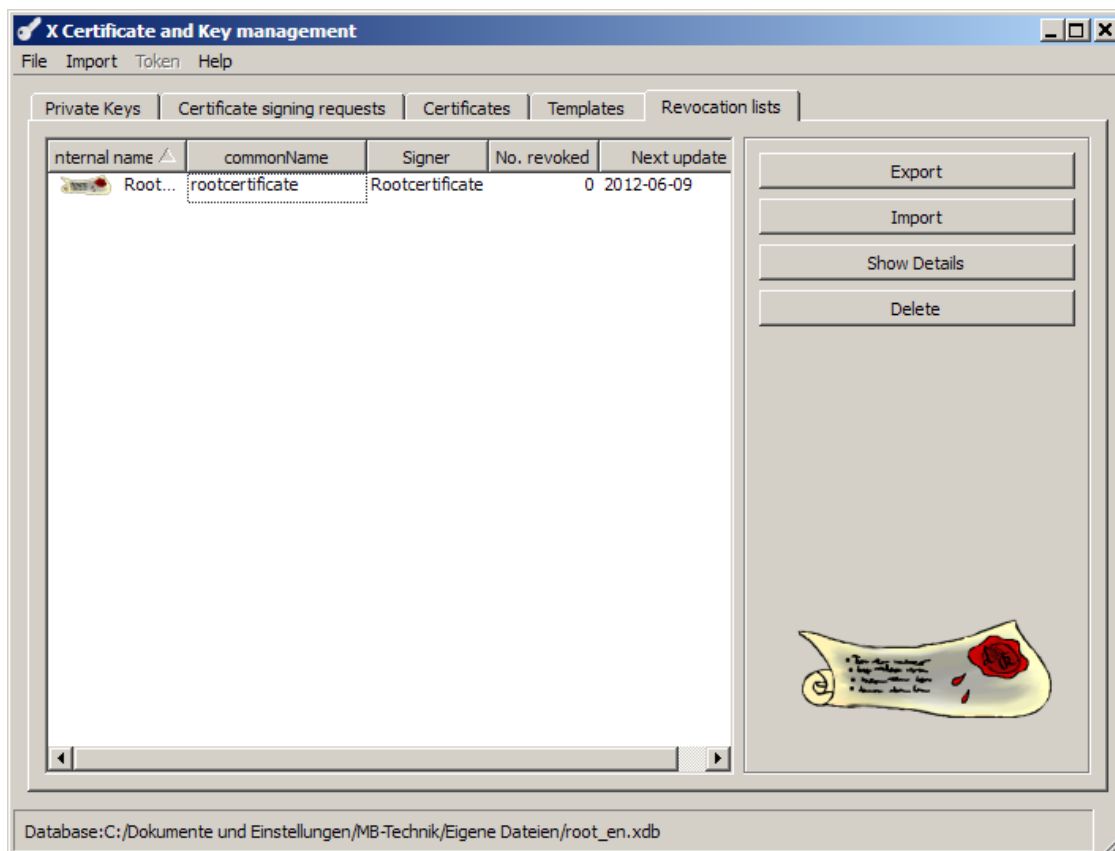


You can create a revocation list here using

“**CA → Generate CRL**”,

as shown in the screenshot above. Please ensure that under “hash algorithm”, you also select **MD5**. There are no check boxes to enable for extensions. The CRL must now be exported, and then imported to the *mbNET*.

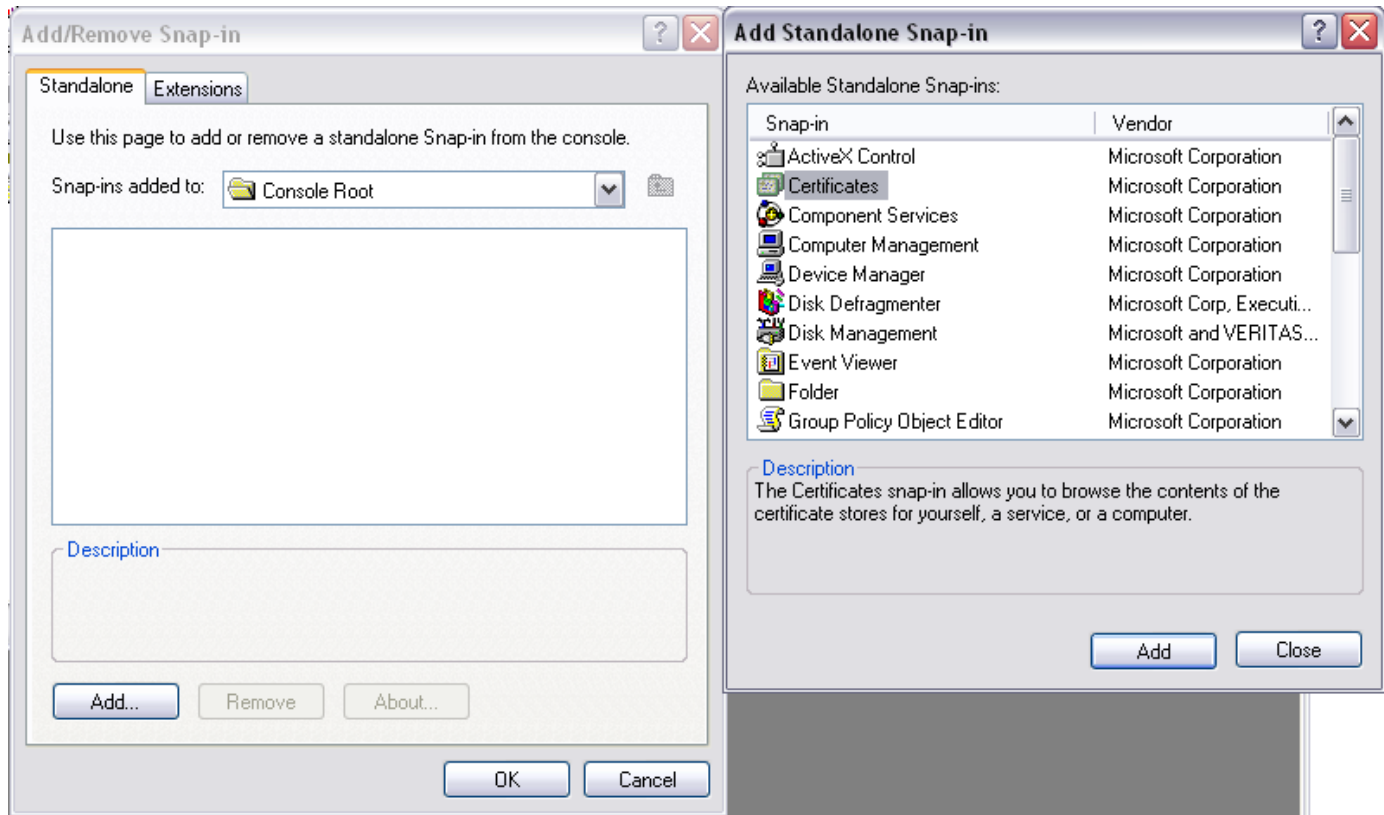
To export, proceed as follows:



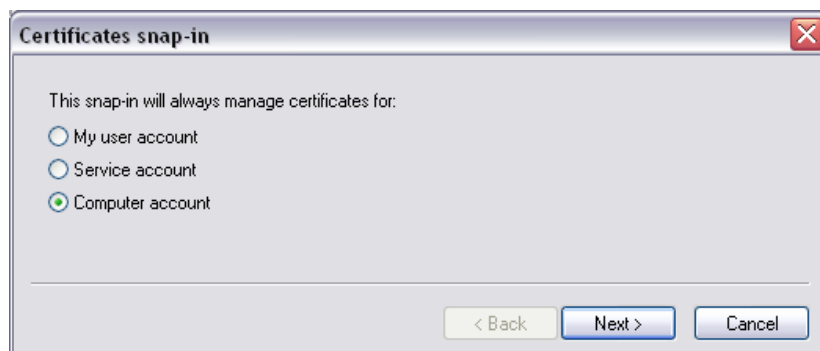
In the *“Revocation lists”* tab you now see the revocation list that you just created. Highlight it, and click *“Export”*. Select **.pem** as the export format. Choose a suitable save location, then confirm with OK. You can now import the list using the **System → Certificates** menu on the **mbNET** web interface (cf. section **CRL**). Restarting the VPN connection or the **mbNET** will enable the CRL and it will no longer be possible to establish a VPN tunnel using the revoked certificate.

15. Importing certificates in Windows XP

To import finished certificates, you need to set up what is known as a Certificate Management Console. To do this, click “Start” -> “Run” and type in “MMC”. Then click on “File – Add/Remove Snap-in” and in the next screen, select “Add”. You can then select **Certificates** from the list of available snap-ins.



In the next window, select “Computer account”



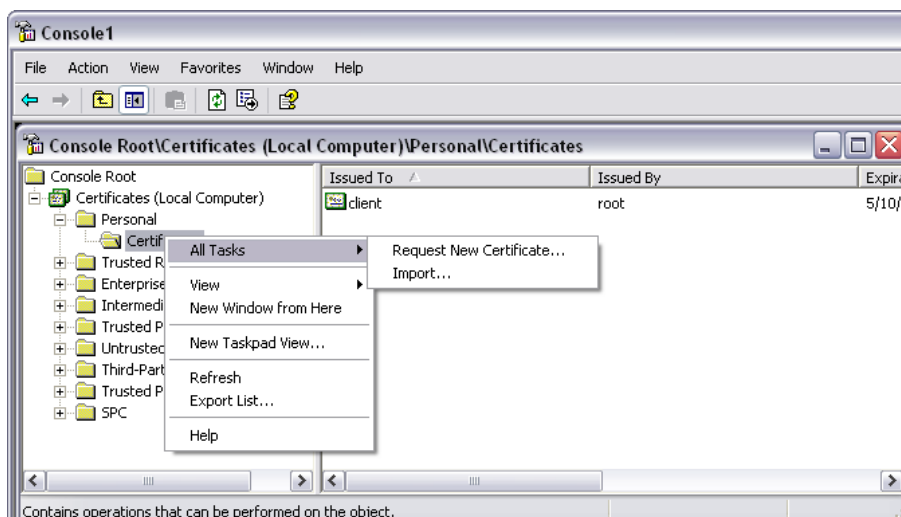
In the next screen, ensure that you select “This Snap-in will always manage” ... “Local computer (computer running this console).

Once you have created the certificate console as described, you can **import a certificate**.

First, open the folder and right-click on “Personal -> Certificates” as shown in the screenshot below, and import the certificate that will be used to identify the client. Be sure to select the “.p12” file for this. Enter the password for the p12 file and then click Next. In the next screen, select “Automatically select the certificate store based on the type of certificate”. When you click “Finish” the relevant certificates will import.



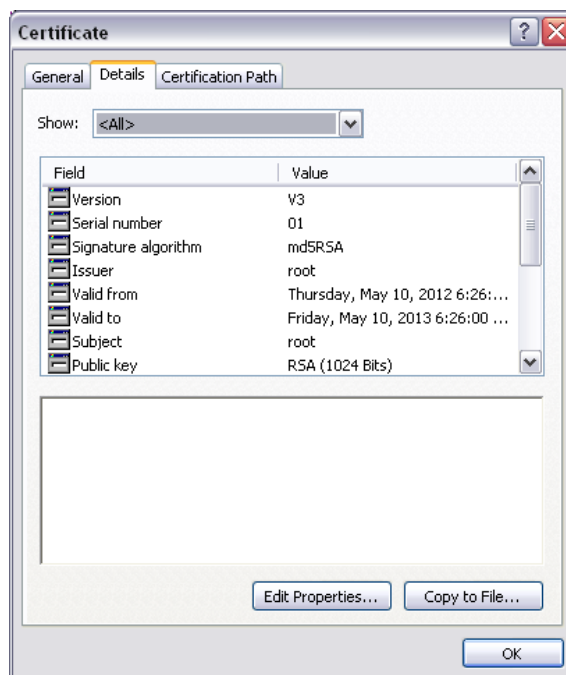
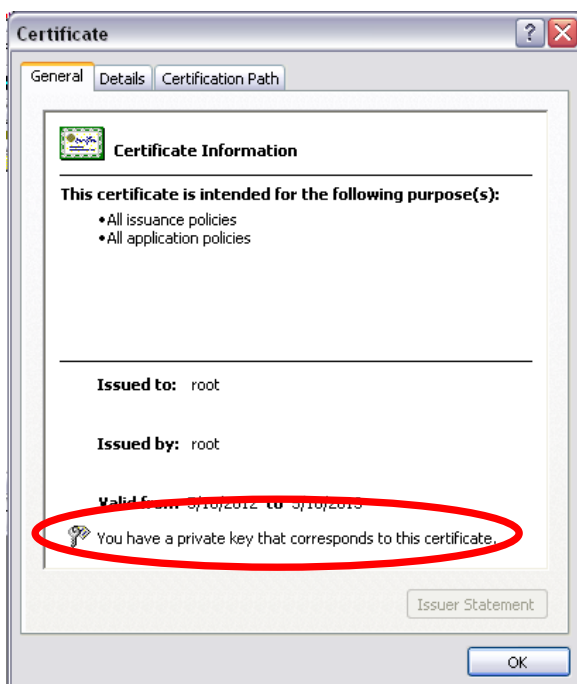
No further certificate imports are required. The CA certificate is automatically imported. Nor is it necessary to save the console



Double-clicking on the relevant certificate displays its properties. In the *“General”* tab you can check, amongst other things, which CA issued the certificate, how long it is valid for and whether you have a private key for it.

This is very important when using certificates for web server publishing.

There is more information about the issued certificate in the "Details" tab.



16. System settings

The most important system settings have already been outlined above in [System Settings](#). A more detailed explanation of additional system settings is given below.

16.1 System – Users

16.1.1 General

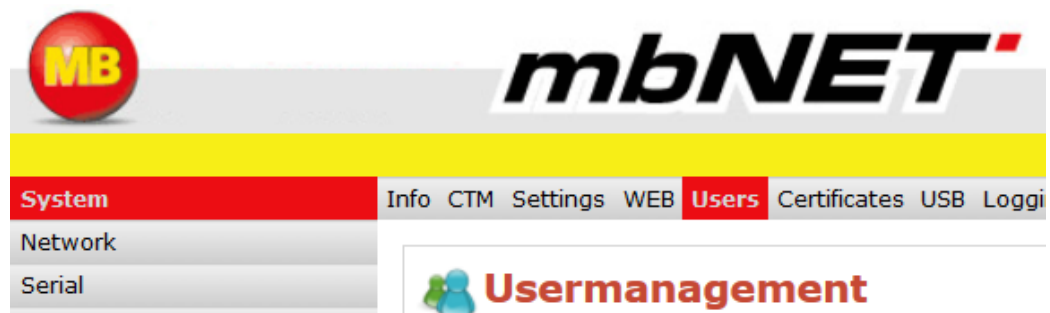
With user management you can:

- Give users access rights to web interface administration, and modem or VPN dial-in.
- Edit or delete existing users, or add new users.

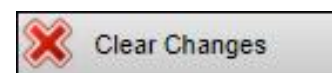
16.1.2 Editing users

To edit a user, proceed as follows:

Select **System** and then **Users**.



- To select a user whose rights you want to change, click on the **edit button**.
The user will be displayed in the first row along with their access settings.
- Amend the relevant field entries and apply the changes.
- Save your changes by clicking the save Button.
- You can undo your changes by clicking on **Clear Changes**.
- Clicking on Apply Changes applies the changes to the router.



16.1.3 Adding users

To add a user, proceed as follows:

In the navigation bar on the left, select **System** and then **Users**.

- In the first row of input fields, enter the **username**, **password** and **full name** of the user.

Usermanagement

Usermanagement

Username	Password	Repeat Password	Fullname
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
admin	*****	*****	Administrator



Please note: All three fields must be completed otherwise you will receive an error message when you save.

- In the three check boxes that follow, specify which rights you want the new user to have. Choose whether the user
 - Can make settings in the web interface (Administration)
 - Can connect to the industrial router's modem (Modem dialin)
 - Can connect to the industrial router via VPN (VPN dialin)

- Click the applicable **option box** to set a hook in it.

Administration	Modem Dialin	VPN Dialin
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
✓	✓	✓



- After you finished your input, press on the **green** plus symbol on the right.
- Click "Save Changes" to do a temporary save.
- To apply the changes to the router, click **Apply Changes**



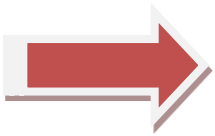
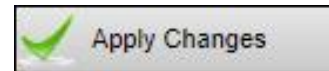
16.1.4 Deleting Users

To delete a user, proceed as follows:

- ❑ In the navigation bar on the left, select **System** and then **Users**
- ❑ Select the row that contains the user name, password and so on, and click the icon to **Delete**



To apply the settings to the router permanently, click **Apply Changes**



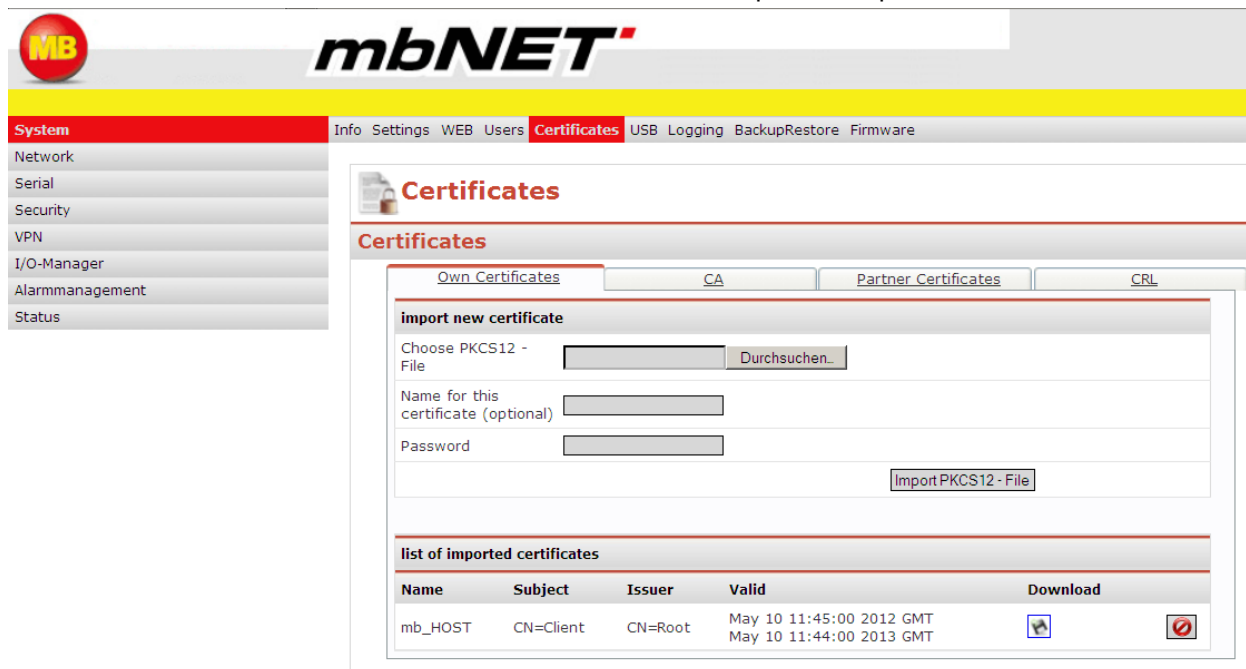
You will now no longer be able to log in or authenticate this user via the web interface, modem or VPN.


16.2 System – Certificates

A key component of VPN connections with IPsec or OpenVPN is the trust relationships between two or more communications peers. Authentication settings are made during configuration, as explained in the **section Authentication**.

For secure communication, authenticity needs to be verified. Certificates help to ensure also that the **right** peers are communicating with each other. A certificate is proof of the holder's identity. The certificate can be issued by a higher authority (called a Certificate Authority, CA for short) or by the actual certificate holder. The certificate holder is called the **Subject**, and whoever issues the certificate is called the **Issuer**.

Below is a screenshot of the relevant certificates tabs and the option to import a new certificate.



Name	Subject	Issuer	Valid	Download
mb_HOST	CN=Client	CN=Root	May 10 11:45:00 2012 GMT May 10 11:44:00 2013 GMT	 

16.2.1 Personal Certificates



Personal certificates are used by the holder, but issued and signed by a higher-level authority (CA/root certificate). For the router to be able to show and use its personal certificate on a remote station, the relevant PKCS12 file (certificate plus private key) first has to be selected and imported to the router.

Single or multiple PKCS files may be imported. Personal certificates also always have a key, which is why a PKCS12 file must be imported.

This is actually made up of a **.crt** file and a **.pem** key file.

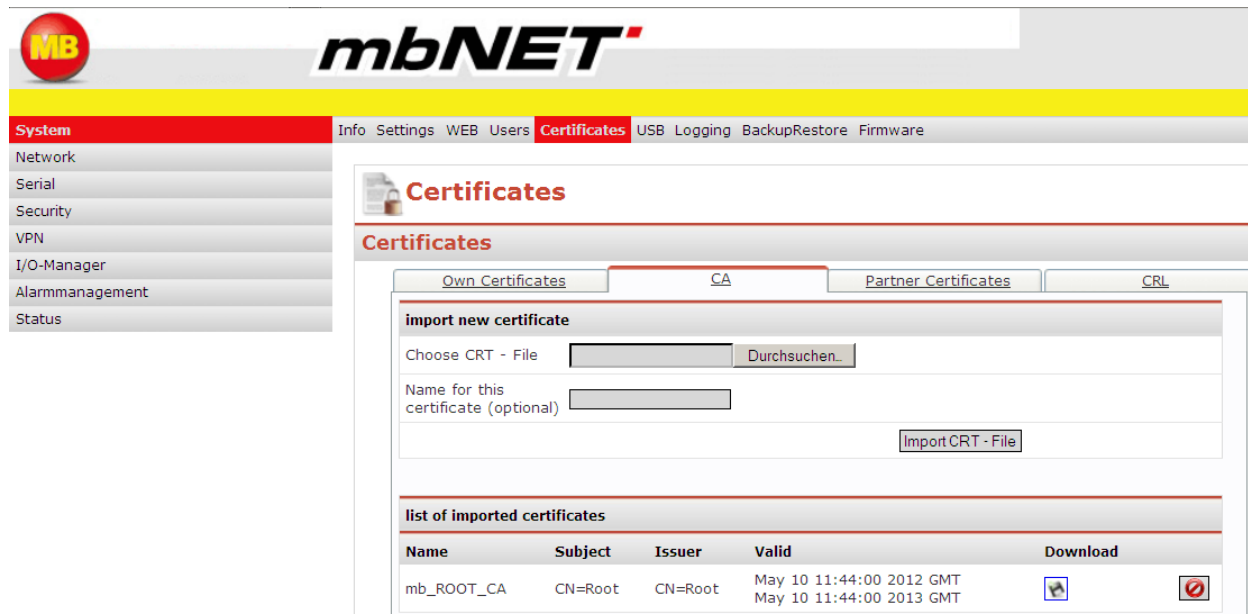


Please note that XCA bundles the key and the certificate to a single file with the extension “.p12”. This is what is meant by a PKCS12 file.

Label	Description			
Import new certificates	<p>Choose PKCS12 file: certificate file selection (PKCS12 file).</p> <p>Browse: provides file path for certificate file.</p> <p>Name for this certificate (optional): optional entry of a name for the certificate file.</p> <p>Password: certificate password entry. The certificate must have been assigned a password when it was created, otherwise it will not import.</p> <p>Import PKCS12 file: As long as the above data have been entered correctly, clicking on this button imports the certificate.</p>			
List of imported certificates	<p>This displays a list of the certificates already imported. More certificates can be included by using Import PKCS12 file.</p>			
Name	<p>Name of the certificate: in this case, mb_HOST</p>			
Subject (certificate holder)	<p>Attributes of certificate holders – in the example, this is:</p>			
	C		C	
	ST		ST	Ws_MASTER
	L		L	
	O		O	
Issuer	<p>For an explanation, see Subject (certificate holder) on previous page.</p>			
Valid	<p>Shows how long the certificate is valid for.</p>			
Download		<p>There is a further step after clicking on this button: to download, right-click on the link and select Save target as</p>		
		<p>Clicking on this button allows you to reset or delete the list of imported certificates.</p>		

16.2.2 Root certificate (CA)

A root certificate verifies whether the remote station certificate is also signed by the root certificate. If the authentication method in the VPN settings is set to “Authentication by certificate from CA”, this root certificate must then be imported. The entry in the root certificate is used to confirm that the person dialing in has a valid certificate. In other words, the CA certificate holds information on the validity of the certificate. The CA certificate is available as a (CRT) file and needs to be imported to the router.

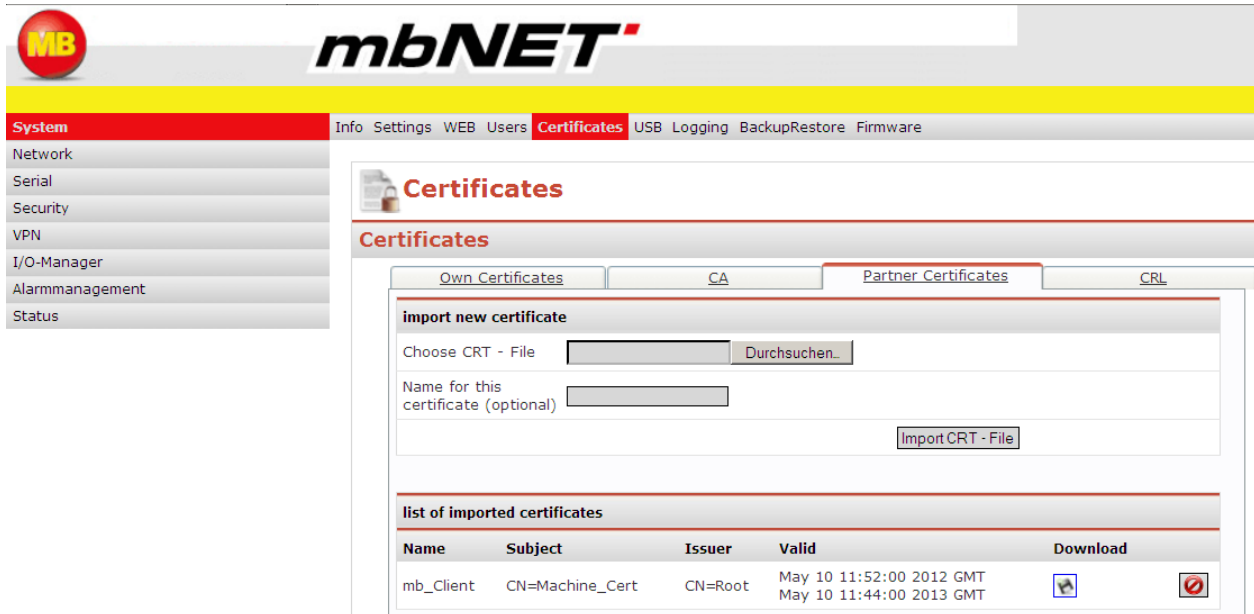


Label	Description
Import new certificates	<p>Choose CRT file: enter the file location or browse the relevant drive for the certificate file. (File extension: .crt)</p> <p>Name for this certificate (optional): optional entry of a name for the certificate file. If you do not enter a name, the common name will be used</p> <p>Import CRT file: As long as the above data have been entered correctly, clicking on this button imports the certificate file.</p>
List of imported certificates	<p>This displays a list of the certificates already imported. More certificates can be collected by clicking Import CRT File.</p> <p>For more info on Name, Subject, Issuer, Valid from/to and Download please see section Personal Certificates</p>

16.2.3 Peer certificates (IPSec)

Peer certificates are remote station certificates. They are only needed if “Authentication by peer certificate” is selected in the VPN settings. In this situation the existence of a local copy of the certificate is confirmation of its validity.

The remote station certificate is selected via the relevant crt file and then imported. You can also import multiple crt files.

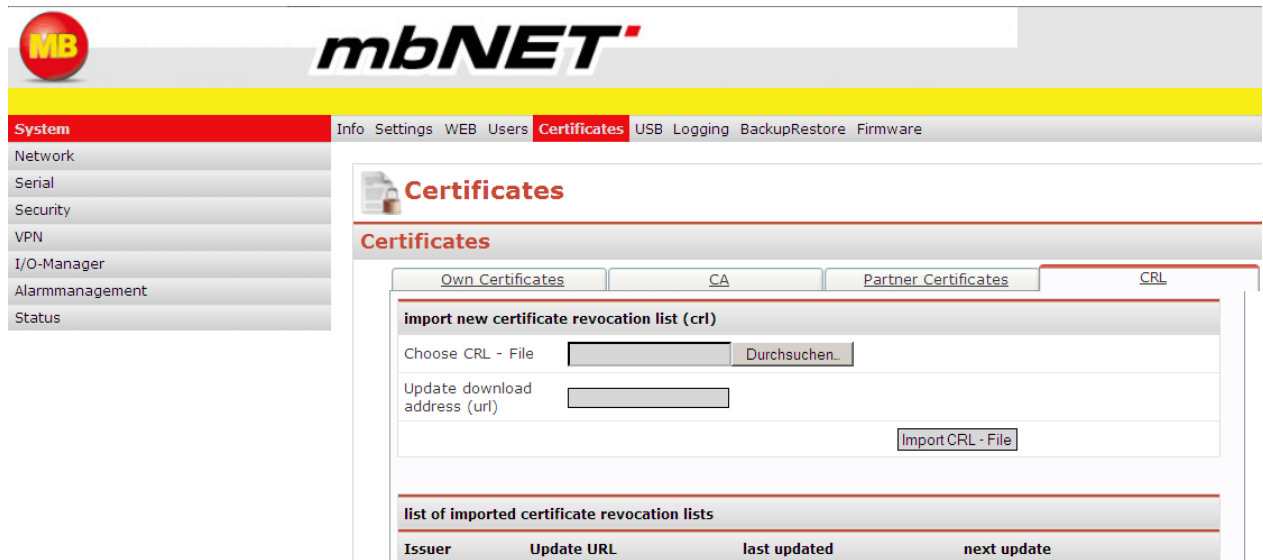


Label	Description
Import new certificates	<p>Choose CRT file: enter the file location or browse the relevant drive for the certificate file. (File extension: .crt)</p> <p>Name for this certificate (optional): optional entry of a name for the certificate file.</p> <p>Import CRT file: as long as the above data have been entered correctly, the certificate file can be imported.</p>
List of imported certificates	<p>This displays a list of the certificates already imported. More certificate files can be collected by using Import CRT file.</p> <p>For more information on Name, Subject, Issuer, valid from/to and Download please see section Personal Certificates</p>

16.2.4 CRL

The Certificate Revocation List (CRL) is used to verify whether or not the computers dialing in hold valid certificates.

The CRL contains the serial numbers of certificates that should be blocked. So if you wish to withdraw someone’s dial-in access rights to the router or the PLC behind it, you just need to create a CRL. XCA makes this easy.



Label	Description
Importing new certificates	<p>Choose CRL File: enter the file location or browse the relevant drive for the blacklist file. (File extension: .pem)</p> <p>Update download address (url): the PEM file can be regularly updated by entering the download address.</p> <p>Import CRL file: as long as the above data have been entered correctly, the blacklist file can be imported.</p>
List of imported certificate revocation lists	<p>This displays a list of the certificates already imported. More certificate files can be collected by using Import CRL file.</p> <p>For more information on Name, Subject, Issuer, valid from/to and Download please see section Personal Certificates</p>
Issuer	See section Personal Certificates
Update URL	Displays the update address for the blacklist file.
Last updated	Displays the date of the most recent update.
Next update	Displays the date of the next scheduled blacklist update.

16.3 System - USB

You can connect a USB device (flash or external drive) to the industrial router's USB port. The USB storage medium can be accessed via SFTP.

To set up the USB port, select **System** on the navigation bar on the left and **USB** on the navigation bar at the top. This will display the screen shown below.

USB Access from Network	
Enable	Check this box if you like the mbNET to mount the USB device.
SFTP User	Displays the SFTP user ("ftp").
SFTP Password	Set an SFTP password (the default is "ftp").
SFTP Password Confirmation	Repeat the password.

To access the USB storage medium via SFTP, specify the IP address of the mbNET as the server, with the sftp:// ... preceded as example: sftp://192.168.0.100

USB devices	
	Gray LED = USB not connected
	Green LED = USB connected
ADVICE: Please note that the connected storage medium must be formatted FAT / FAT32 . With a different file system, such as NTFS can cause problems.	

16.4 System – Logging

System logging for the *mbNET* can be outsourced to another computer by using a log server.

Label	Description
Set debug output to syslog	Output debug info to the syslog.
Log also to USB-Device	The logs are also being saved to an USB-Device.
Enable Remote Logging	To enable a log server, place a check in the box by clicking on it. System logging for the <i>mbNET</i> industrial router can now be outsourced to another computer.
Remote IP address	Remote IP address of log server. In this case: 192.168.0.65
Remote Port	Remote port for log server. In this case: Port 514 We recommend to not change this port, as certain applications may not work properly on a completely different port.

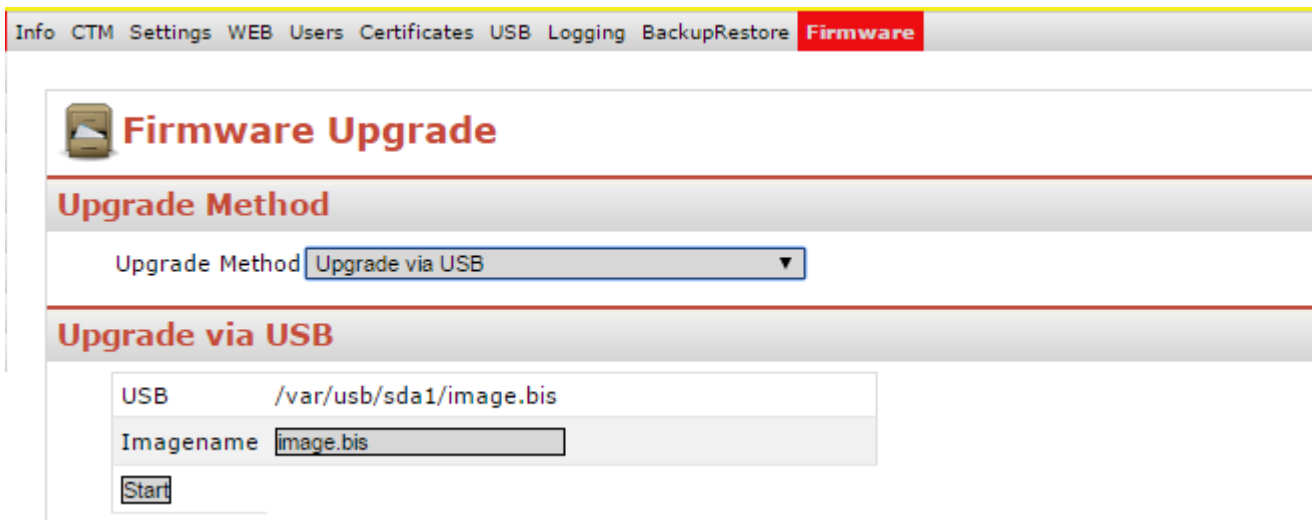
16.5 System – Configuration

Using this menu, you can both backup and restore a system configuration. The configuration can be saved e.g. to a connected USB drive before making major changes, and if necessary, restored onto the industrial router.

Label	Description
Backup Configuration	
Name this configuration	Assign a meaningful name to the configuration. In this case: mbNET
Backup (Button)	Backs up the configuration. After clicking on this button you will be prompted to enter a location, e.g. the USB drive letter.
Include certificates and keys	This configures the system to copy an mbNET . Please note that this configuration file should only be used for one device.
Save on USB device	If a USB storage medium is connected, the configuration can also be stored there.
Overwrite existing file	If this option is not enabled, and a configuration file already exists at the same location, the new configuration will not be stored. Either change the name of one of the files, or choose a different save location for the new configuration.
Encrypt the configuration (.mbns)	set: The config file will be encrypted. not set: The config file will NOT be encrypted.
Encrypt passphrase	Define a passphrase for the config file.
Repeat encrypt passphrase	Retype the passphrase which you just entered
Restore Configuration	
Saved config file (*.mbn, *.mbns):	To restore a configuration, the stored file containing the router configuration must be restored, i.e. transferred back on to the industrial router. To perform a restore, first click Browse , then browse to the file location or directory and select the file. Then click on the Restore button.
Decrypt passphrase	Enter the passphrase which you defined for the config file, to decrypt it.

16.6 System – Firmware

There are two ways to update the industrial router's firmware; both are described on the following page.



The screenshot shows the 'Firmware Upgrade' page in the mbNET web interface. The navigation bar includes 'Info', 'CTM', 'Settings', 'WEB', 'Users', 'Certificates', 'USB', 'Logging', 'BackupRestore', and 'Firmware'. The main heading is 'Firmware Upgrade'. Below it, the 'Upgrade Method' is set to 'Upgrade via USB'. Under the 'Upgrade via USB' section, the 'USB' path is '/var/usb/sda1/image.bis' and the 'Imagename' is 'image.bis'. A 'Start' button is visible at the bottom of the form.

16.6.1 Upgrade via USB

This requires a USB storage device to be connected to the industrial router so that the file can be transferred across. The firmware name (**image.bis**) is listed here. To upgrade the firmware, click **Start**. Then restart the device.



Use the **image.bis** data.

ATTENTION!

Never interrupt the firmware update as the device can not start any more!

The update process can take up to 10 minutes.

16.6.2 Upgrade via Network

In this case you need to enter the IP address of a TFTP server, and the firmware name.

In this case: [image.bin](#)

Before the upgrade can start, the “tftpd32” tool must be launched. You can download this free of charge at <http://tftpd32.jounin.net/>.

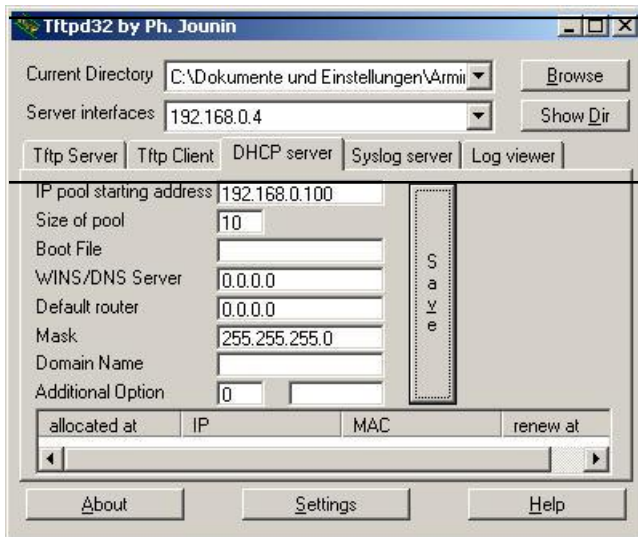
Once you launch the tool, enter the following settings in the “DHCP server” tab:

IP pool starting address: *IP address of the router that you are upgrading.*

Size of pool: *10*

Mask: *Network subnet mask*

Clicking on **Save** will store the settings. In the drop-down field under “Current Directory”, you need to select the folder where the firmware upgrade file is saved. Do not close the tool until the upgrade is complete. Now, in the web interface TFTP Server field, you need to enter the IP of the computer that is currently running Tftpd32. Now click **Start**. Once the process is complete, restart the device



ATTENTION!

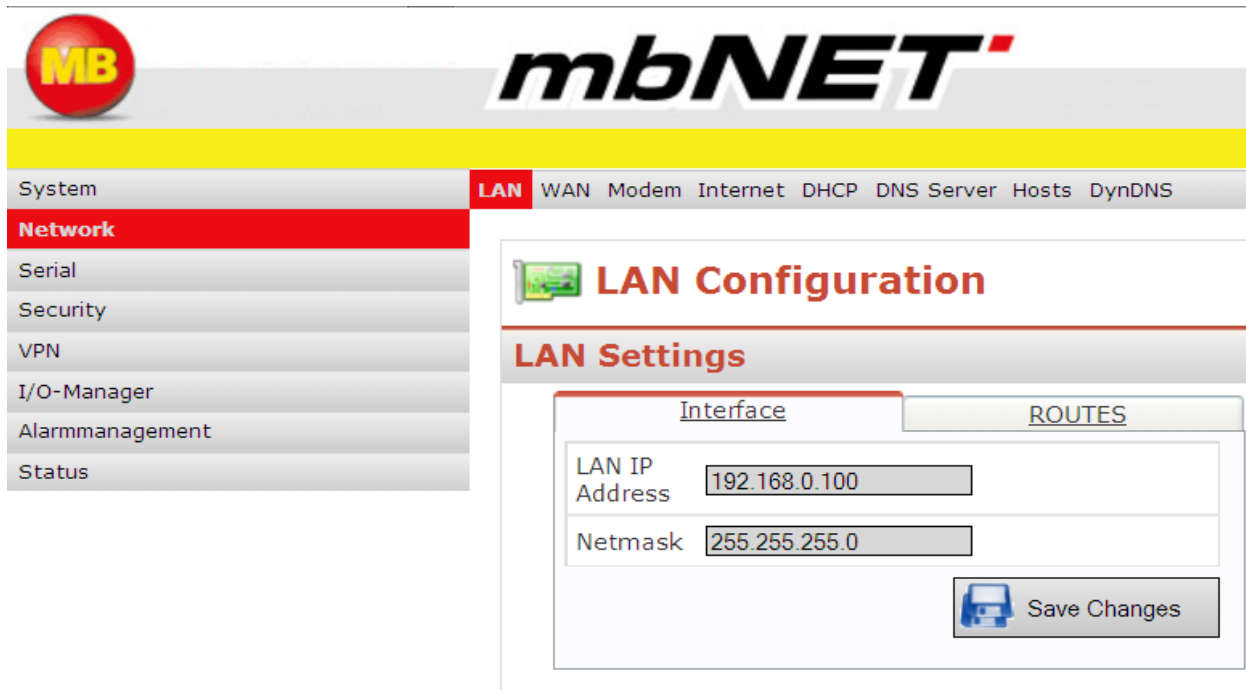
Never interrupt the firmware update as the device can not start any more!


The update process can take up to 10 minutes

17. Network

17.1 Network – LAN

LAN configuration allows you to configure the router IP address (LAN address) and subnet mask. This is the IP address used for accessing the router from the LAN.




Label	Description
Interface	To set up the LAN interface, click on the tab.
LAN IP address	Enter the router IP address.
Netmask	Enter the subnet mask of the network into which the router is to be integrated.
Routes	To set up specific routes, click on the Routes tab. You can enter both network routes in CIDR format (x.x.x.0/24) and host routes here. 

17.2 Network – WAN

The industrial router's WAN interface can connect a local network with a remote network, or with a public network like the Internet. Therefore the WAN interface is configured according to how it will be used.

Label	Description
Interface Type	<p>You can select from the following interface types:</p> <p>DSL: Select this option if your router is directly connected to a DSL modem that connects to the Internet.</p> <p>DHCP: Select this setting if there is a DHCP server on the network which is therefore automatically assigned a new IP address by the industrial router. Please also contact your network administrator to confirm this.</p> <p>Static IP: Select this setting if connection to the Internet is via an existing router which is not acting as a DHCP sever, or if no server is set up to assign addresses. You should also select this setting if you have received a static address from your ISP, e.g. if you have a leased line. Note also that this type of connection requires you to enter a DNS server (see Network – DNS Server).</p> <p>WAN IP address: IP address of the router connected to the WAN port.</p> <p>Netmask: enter the subnet mask.</p> <p>Default gateway: enter details of the gateway that connects you to the Internet, i.e. the IP address of the existing router.</p>

Label	Description
<p>Connection mode</p>	<p>When selecting interface type, choosing DSL also requires you to select one of the following options:</p> <p>PPPoE: Select this option if your ISP requires a PPPoE (Point to Point Protocol over Ethernet) connection. A lot of modems are set to this option. The external IP address that a remote station uses to access the router is specified by the ISP. Please refer to your ISP documentation for the necessary details. PPP User Login: enter your Internet access user name as provided by your ISP. PPP User Pass: Enter your Internet access password as provided by your ISP.</p> <p>PPTP: Select this option if your ISP requires a PPTP connection (Point to Point Tunneling Protocol) connection. For example, in Austria, PPTP is used with DSL connections. PPP User Login: see the access user name provided by your ISP. PPP User Pass: see the access password provided by your ISP. WAN IP address: here, enter the IP address of the mbNET router connected to the WAN port. This is the address that devices use to access the router if they are connected to the WAN. If your ISP's IP address is not automatically assigned here, you should manually enter the IP that the PPTP server uses to access the router. Please refer to your ISP documentation for the necessary details. Subnet mask: enter the subnet mask of the network connected to the LAN port. PPTP Server IP address: enter your ISP server IP address.</p>
<p>Routes</p>	<p>This enables you to specify routes to other networks. If the local network has additional subnetworks, you can specify routes for these here. You can enter network routes in CIDR format (x.x.x.0/24) or routes to individual subscribers here.</p>  <p>The screenshot shows a configuration window with two tabs: 'Interface' and 'ROUTES'. The 'ROUTES' tab is active. Below the tabs, there are two columns: 'Network' and 'Gateway'. Each column has a text input field. To the right of the 'Gateway' field is a green plus icon in a square box.</p>

17.3 Network – Modem

Notice: Not valid for *mbNET* variants with WiFi

17.3.1 Network – Modem –Incomming

The industrial router's integrated modem is for dial-in or Internet connection (analog, ISDN, GSM) where there is no available DSL or network connection.



NOTE:
If the modem is used for an outgoing Internet connection, it cannot be used for an incoming connection.

LAN WAN **Modem** Internet DHCP DNS Server Hosts DynDNS

Modem Configuration

Modem Settings

Modem Type

Modem Init

Modem Init

Outgoing SIM1 Outgoing SIM2 Settings SIM **Incoming** Call Back SMS

Dialin enable

PPP Server IP-Address (here)

PPP Client IP-Address

Dialin Authentication

Authentication via PAP

Authentication via CHAP

User

Password

close connection after inactivity of [s]

Save Changes

Label	Description
Modem Init	<p>ANALOG: If using an analog device, enter the command +GCI=country code (for country codes, see Country codes for analog devices) here, and in the second row, the command X3 (do not wait for dial tone).</p> <p>ISDN: If using an ISDN device, you need to enter your MSN number with the command AT#Z=n (n= MSN number) If you enter "n" as "*", every call will be accepted.</p> <p>GSM: if using a GSM device, you must use the preset X3 command. The +GCI=country code may not be used.</p>

Label	Description
Incoming	
You need to enable this option for the router to handle incoming dial-in or ISDN connections.	
Dial-in enable	You need to enable this function by checking the box so that a client computer can access the router.
PPP Server IP address (here)	You need to enter the router IP address here. You can use the same network area as the local network. But please ensure that you do not re-use assigned addresses as this may lead to address conflicts.
PPP Client IP address	<input type="checkbox"/> Here, enter the IP address that the router sends to the client (the remote station dialing in) as soon as a PPP connection is established. On connection, the router and the remote station establish a separate network.
Dial-in Authentication	Specify whether a user name and password (i.e. authentication) will be required to dial in to the router. The options are: <ul style="list-style-type: none"> <input type="checkbox"/> Only following user: only the user entered in subsequent input fields in this dialog window has rights to dial in to the router. <input type="checkbox"/> every user with dial-in rights: any user who has been assigned “modem” rights under user management can dial in.
Authentication via PAP / CHAP	Use the default setting. PAP/CHAP are types of authentication. Ensure that this setting matches that of the subscribers dialing in. Disabling PAP/CHAP means that this authentication will not be accepted and that your sent data can be read by others.
User name & password	Enter the user name and associated password for PPP dial-in. These fields will only be available if you selected “only following user”.
close connection after inactivity of [s]	This is used to set the time for the existing connection to be disconnected as soon as data packets are no longer sent by the router. No input turns off this function.

17.3.2 Network – Modem – Outgoing

Following settings are relating to the outgoing connections of the modem.

Label	Description
Input select	<p>If you would like to call multiple terminals, set this option to “yes”. You will then see three more fields where you can enter numbers that will be selected on receipt of a signal at digital inputs 2 to 4. Enter the numbers and user credentials for PPP dial-in in these additional fields. Switch on the first, and one or two of the other three inputs to start dialing. Note that you need to switch on the one/two other inputs before switching on the first. Also note that the industrial router is acting only as a PPP client here, and that there must be another industrial router, or a computer, acting as the PPP server to handle the request.</p> <p>Under Network – Internet, set the Internet connection to “On demand” and set the subsequent option to “Connect on Sign 1 at Input”.</p> <ul style="list-style-type: none"> To call the first number: switch on input 1 To call the second number: switch on input 2 and then input 1 To call the third number: switch on input 3 and then input 1 To call the fourth number: switch on input 2&3 and then input 1
Telephone number	Here, enter the telephone number of the relevant mobile broadband provider. For GSM modems this number always uses the format *99***1#
User	Enter the user name required to dial in via the relevant provider. You can obtain further details on this direct from your provider. For GSM modems there is more information for example at http://www.mbconnectline.de/gsm/grps/mobilfunk.html
Password	Enter the password required to dial in via the relevant provider. You can obtain further details on this direct from your provider. For GSM modems there is more information for example at http://www.mbconnectline.de/gsm/grps/mobilfunk.html

Authentication via PAP	Use the default setting for the authentication protocol. In principle this is preset when a dial-up connection is set up.
Authentication via CHAP	Use the default setting for the authentication protocol. In principle this is preset when a dial-up connection is set up. As a rule, CHAP is the process used by ISPs for Internet access log in via a modem or ISDN adapter.
Timeout Dialout in [s]	After the length of time entered here, dialing attempts will stop, and restart anew.

For MDH8xx mobile broadband devices there are two “Outgoing” menus. These are simply SIM1 and SIM2. There is also a second menu, “SMS” settings.

- Various provider specifications for every SIM card possible.
- Switching between SIM1 and SIM2 at network disturbances or roaming.
- SMS remote control

Label	Description
SIM-PIN	Enter the SIM card personal identification number (PIN) to ensure access. If you would like to switch PIN security on or off, you will need a cellphone
Provider	You can select your mobile broadband provider here. If it does not appear, select "Other". If your provider was not shown, you can also manually enter the APN (Access Point Name) here. You can obtain details of the APN from your mobile broadband provider.

17.3.3 Menu Settings SIM

Modem Configuration

Modem Settings

Modem Type	GSM
Modem Init	<input type="text"/>
Modem Init	<input type="text"/>

<u>Outgoing SIM1</u>	<u>Outgoing SIM2</u>	<u>Settings SIM</u>
Select primary SIM card	<input type="text" value="SIM card 1"/>	
Switch to secondary SIM card when roaming is detected	<input checked="" type="checkbox"/>	
Switch to secondary SIM card when there is a failure with the primary SIM card	<input checked="" type="checkbox"/>	

First, we need to specify a primary SIM card, which will always be verified or used first. The secondary SIM card is always the non-primary one.

Switching is based on two (selectable) criteria:

- The SIM card fails to initialize, or to register on the cellphone network
- Roaming is detected on the SIM

Label	Description
<u>Outgoing SIM 1 / 2</u>	
SIM Pin (only GSM)	You can enter the PIN for the SIM card here if necessary. Note: The device is also working, if the SIM card is not protected by a PIN.
Provider (only GSM)	You can select your mobile broadband provider here. If it does not appear, select "Other"
Providename (only GSM)	If your provider was not shown, you can also manually enter the APN (Access Point Name) here. You can obtain details of the APN from your mobile broadband provider or from our website at http://www.mbconnectline.de/gsm/grps/mobilfunk.html
Authentication via PAP	Authentication protocol that transfers your login credentials (Password A uthentication P rotocol). However, we recommend using the more secure CHAP variant alongside this, as PAP sends your credentials unencrypted.
Authentication via CHAP	Authentication protocol that transfers your login credentials securely (C hallenge H andshake P rotocol)
Timeout Dialout in [s]	Enter a time in seconds (for example 300 (=5 minutes)), after dialing should be discontinued.
<u>Settings SIM</u>	
Select primary SIM card	Choose the primary SIM Card (SIM 1 or SIM 2)

Switch to secondary SIM card if roaming is detected	On / Off
Switch to secondary SIM card when there is a failure with the primary SIM card	On / Off
SMS	
<i>Remotely control services via SMS</i>	
Enable Service Control via SMS	On / Off
Check the Phone Number of the Sender	On / Off
Senders Phone Number	Enter the phone number of the sender.
<i>Send a SMS when ...</i>	
Internet connection established	Sends SMS if the internet connection was established successfully.
Receivers phone number	<i>Sends SMS if the telephone number of the receiver equals the number which is entered here.</i>

17.3.4 Network – Modem – Callback

The settings below apply to the call back function. This function triggers Internet dial-in remotely via a telephone or dial-up connection. It must be set up so that the Internet connection will be established via WAN or modem.

Note that call back does NOT work with UMTS-enabled devices.

Label	Description
Call back enable	Checking this option enables the call back function.
How to call back	<p>Activate Call Back via Phone: With this setting, the mbNET will connect to the Internet if called from a phone. To establish a connection, the mbNET must be alerted by four rings. After this happens, the mbNET hangs up and then starts Internet dial-in. This can take 30-40 seconds.</p> <p>Log in and press a button: With this setting, the mbNET will connect to the Internet if you have set up a dial-up connection with the mbNET and you click on the Call Back button in the System – Info menu of the user interface. After 30 seconds, the mbNET will establish an Internet connection unless you close the dial-up connection.</p>

17.3.5 Network – Modem – SMS

System LAN WAN **Modem** Internet DHCP DNS Server Hosts DynDNS

Network Serial Security VPN I/O-Manager Alarmmanagement Status

Modem Configuration

Modem Settings

Modem Type GSM
 Modem Init
 Modem Init X3

Outgoing SIM1 Outgoing SIM2 Settings SIM Incoming Call Back **SMS**

Remote Service Control via SMS

Enable Service Control via SMS
 Check the Phone Number of the Sender
 Senders Phone Number

Send a SMS when...

Internetconnection established
 Receivers Phone Number

Save Changes

Label	Description
Enable Service Control via SMS	This function enables the use of service control via SMS
Check the Phone Number of the Sender	This ensures that the mbNET only accepts SMS commands from a specific number. Then enter the sender's cell number in "Senders Phone Number" in the next field. Commands sent from any other number will now be rejected.
Send an SMS when Internet Connection Established	The mbNET can send you an SMS as soon as it has connected to the Internet. In the next field, you also need to enter the telephone number to which this SMS should be sent.



Please note that your cell numbers cannot begin with 0. You must use the international format e.g. +49 for Germany.

17.3.6 Remote service control commands using SMS

- **INET START** or **INET STOP**
This controls the industrial router's Internet connection. Note that you can only control an Internet connection that is active and has been established by the industrial router.
- IPSEC START [connection name] or IPSEC STOP [connection name]
PPTP START [connection name] or PPTP STOP [connection name]
OPENVPN START [connection name] or OPENVPN STOP [connection name]
Whichever type of VPN you select, this must always be followed by the name of the connection (e.g. OPEN-VPN START Wizard). In addition, be aware that connection name is case sensitive.
- **REBOOT**
This will restart your industrial router. Please note that it cannot receive any commands while restarting.
- **OUT ON** or **OUT OFF**
Using **OUT ON[outputnumber]** or **OUT OFF[outputnumber]** you can also switch your router's inputs on or off (e.g. OUT ON 1 switches on output 1; OUT OFF 1 switches off output 1)
- **IN STATUS**
The **IN STATUS** command returns input status
- **GSM CMD**
Using the **GSM CMD [at-command]** you can send any AT command to the modem. The modem response will be returned to the sender's number by SMS (e.g. "GSM CMD AT+cops?" returns network and provider details). Please note that only the first 160 characters of the modem response will be transmitted.

17.4 Network – Internet

Router Internet dial-in is dependent on connection type and on the appropriate configuration of specific settings.

17.4.1 Network – Internet – Internet Connections

Label	Description
Internetconnection	<p>Following options are available at the drop down menu:</p> <ul style="list-style-type: none"> <input type="checkbox"/> internet via WAN (external Router, fixed line) Select this Setting if the mbNET does not create the internet connection automatically. For example if there is already another router in your network, which is responsible for the internet connection, or if there is only an incoming dial-up connection over the public telephone network. <input type="checkbox"/> Internet via Modem Note: Not possible for the mbNET variant with WLAN. With this setting selected, the connection will be established via modem. Enter the login information under Network – Modem. <input type="checkbox"/> Internet via WAN If the internet connection should be established via DSL-Modem, then select this option. You also have to enter the internet login data under Network – WAN Restart your mbNET router after this, to save the configuration. <input type="checkbox"/> Internet via WLAN If the internet connection should be established via WLAN, then select this option. You also have to enter the internet login data under Network – WLAN Restart your mbNET router after this, to save the configuration.
Failover	The failover function enables you to switch between different internet connections. If this function is active, you can set the desired priorities of the network interfaces, depending on the device type.
Internet connection check internet connection	
PING IP	Ping different IP addresses to check the availability of the internet connection. You can enter up to three different IP addresses with different intervals.

Internet Settings

Internet Configuration

Internet Settings

Internet Connections

Internet Settings

Connection Mode on demand ▼

lock connection by don't lock ▼

broadcast IP-Adress via email

email

Default Routing Modem ▼

Connection Mode	<input type="checkbox"/> keep connection Select this setting if the router should try to connect to the Internet immediately after restarting or after pressing the RESET button on the front of the router. Important: with this setting, the connection will stay on
	<input type="checkbox"/> on demand Select this setting if you want the router to connect to the Internet when one or more of the options listed below are selected: <ul style="list-style-type: none"> <input type="radio"/> Connect while pushing Dial Out button <input type="radio"/> Connect when a signal is received at inputs I1,I2,I3 or I4 <input type="radio"/> Connect on traffic
lock connection by	<input type="checkbox"/> don't lock: select this option if you want to prevent the Internet connection from being closed by a signal to a digital input.
	<input type="checkbox"/> Input1, Input2, Input3, Input4: select this option if you want to be able to interrupt the Internet connection using a signal to one of the selected digital inputs.
Send IP address via email	Here, you can set whether to have an email containing the current public IP address sent to a pre-specified email address.
Email	If you select "send IP address via email", your need to enter your email address here. However you can also enter it manually in this field.
Default Routing	This checkbox is only available if you have selected " Internet via Modem " under Internet Connections. If the default route is selected via Modem , the standard gateway is always the Internet connection via the modem. The standard route via WAN Ethernet always uses the WAN socket as the standard gateway. In this case, explicitly specific routes for Internet traffic must be specified.

Internet settings
Settings

The **Settings** tab is only displayed if Internet connection via WAN or modem has been selected along with **on demand** for the connection mode.
The following settings options will be displayed:

Settings	
Connect on traffic	<input checked="" type="checkbox"/>
Ignore traffic on LAN	<input type="checkbox"/>
Ignore traffic from internal services	<input type="checkbox"/>
Connect on "Dial-Out"	<input checked="" type="checkbox"/>
Connect on Sign 1 at Input	don't connect ▼
close connection after inactivity of [s]	100

Connect on traffic	To connect to the Internet when a data packet is sent, check this box. In other words, an Internet connection will be established if the LAN is trying to contact a subscriber outside of the LAN.
Ignore traffic on LAN	If this check box is activated, no connection that differs from the setting under "Connection Mode" can be established. For example, a component connected to the LAN uses the device (router) as a gateway.
Ignore traffic from internal services	If this check box is activated, no connection that differs from the setting under "Connection Mode" can be established. For example, if an e-mail is to be sent by the device (router) or an automatic time synchronization is to be executed.
Connect when pushing Dial Out button	If you wish an Internet connection to be triggered by pressing the Dial out button on the front of the router, check this box. ADVICE: Press and hold the Dial Out button until the Con LED starts to flash.
Connect on Sign 1 at Input	<ul style="list-style-type: none"> • Don't connect: Select this option if you want to prevent the Internet connection from being triggered by a signal to one of the digital inputs. • Input1, Input2, Input3, Input4: Select this option if you want to establish a connection using a signal to the selected digital input.
close connection after inactivity of [s]	Here, enter the length of time before the connection should be closed if the router has sent no further data packets in the interim. Leaving this blank switches off the function.

17.4.3 Internet failover connection

Firmware versions 3.x.x. and higher have an optional failover function for the Internet connection.

Internet Connections
Internet Settings

Failover ▼

Failover of Internet interfaces

Retry interface before switch to next interface

Priority	Enable	Internet Interface			
	<input type="checkbox"/>	system restart	▼		
1	<input checked="" type="checkbox"/>	Internet via WAN	▼		
2	<input checked="" type="checkbox"/>	Internet via Modem	▲		

Connection monitoring

PING IP ▼

PING IP or host address 1

PING interval 1 [s]

PING IP or host address 2

PING interval 2 [s]

PING IP or host address 3

PING interval 3 [s]

PING retry before switch to next interface

Save Changes

First you need to switch on this function.

The screenshot shows the 'Internet Settings' tab. A dropdown menu labeled 'Failover' is set to 'yes'.

In the table below, you can select a priority order for the Internet interfaces. The order and number of interfaces are freely definable.

Priority	Enable	Internet Interface			
	<input type="checkbox"/>	system restart			
1	<input checked="" type="checkbox"/>	Internet via WAN			
2	<input checked="" type="checkbox"/>	Internet via Modem			

The "Retry interface before switch to next interface" parameter specifies how many times an Internet connection should be allowed to fail before switching to the next interface.

The screenshot shows the 'Failover of Internet interfaces' section. A text input field labeled 'Retry interface before switch to next interface' contains the value '1'.


There are additional settings for monitoring e.g. an Internet connection via WAN

The screenshot shows the 'Connection monitoring' section. It includes a dropdown for 'PING IP' set to 'yes', and three rows for monitoring settings:

- PING IP or host address 1: [empty text box]
- PING interval 1 [s]: [5]
- PING IP or host address 2: [empty text box]
- PING interval 2 [s]: [5]
- PING IP or host address 3: [empty text box]
- PING interval 3 [s]: [5]
- PING retry before switch to next interface: [2]

You can enter up to three different IP addresses which will then be run through in the following order. If the first IP fails, the second will be used. If this one also fails, the third will be used and once all three have been run through, a test will be carried out. If the set test retry limit is reached, the interface will switch. If the system gets to the last interface, it will start again with the first.

In addition, routers with a GSM/UMTS module and double SIM slot can switch between SIM1 and SIM2.



Modem Configuration

Modem Settings

Modem Type	GSM
Modem Init	<input style="width: 100%;" type="text"/>
Modem Init	<input style="width: 100%;" type="text"/>

<u>Outgoing SIM1</u>	<u>Outgoing SIM2</u>	<u>Settings SIM</u>
Select primary SIM card	<input style="width: 100%;" type="text" value="SIM card 1"/>	
Switch to secondary SIM card when roaming is detected	<input checked="" type="checkbox"/>	
Switch to secondary SIM card when there is a failure with the primary SIM card	<input checked="" type="checkbox"/>	

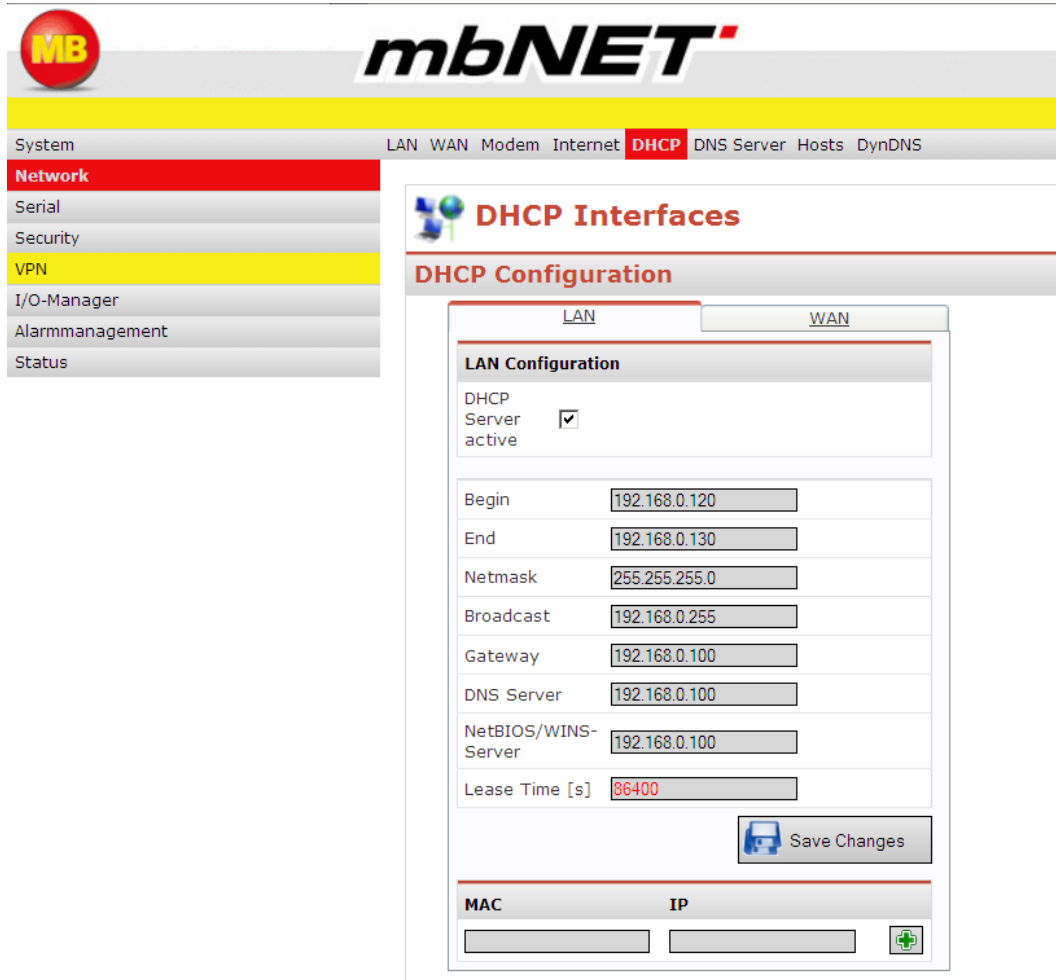
First, we need to specify a primary SIM card, which will always be verified or used by default. The secondary SIM card is always the non-primary one.

Switching is based on two (selectable) criteria:

- The SIM card fails to initialize, or to register on the mobile broadband network
- Roaming is detected on the SIM

17.5 Network – DHCP

You can configure the industrial router as a LAN or WAN DHCP server. DHCP enables you to integrate a new computer into an existing network without the need for any additional configuration. The only requirement is for the computer to be set up to acquire the IP address automatically.



Label	Description
LAN – WAN	Selects to configure LAN or WAN interface.
DHCP Server active	Checking the box for this function allows the router to be enabled as a DHCP server for the relevant interface.
Begin	Enter the start address for the address range managed by the DHCP server here.
End	End address of the range managed by the DHCP server.
Netmask	Subnet mask of the range managed by the DHCP server.
Broadcast	Broadcast address of the range managed by the DHCP server.
Gateway	Optional entry. Here, you can enter the address of a router that connects network clients to the Internet or to another network. Enter the router's LAN IP address here.
DNS Server	Optional entry of an existing network DNS server. Enter the router's LAN IP address here.
NetBIOS/WINS-Server	Optional entry of an existing network NetBIOS/WINS server.
Lease Time [s]	Length of time for which a client is allocated a specific IP address by a DHCP server.
MAC/IP table	Here, enter the fixed assignment between IP address and MAC address. In other words, you can specify that a device with a certain MAC address always receives the same IP.

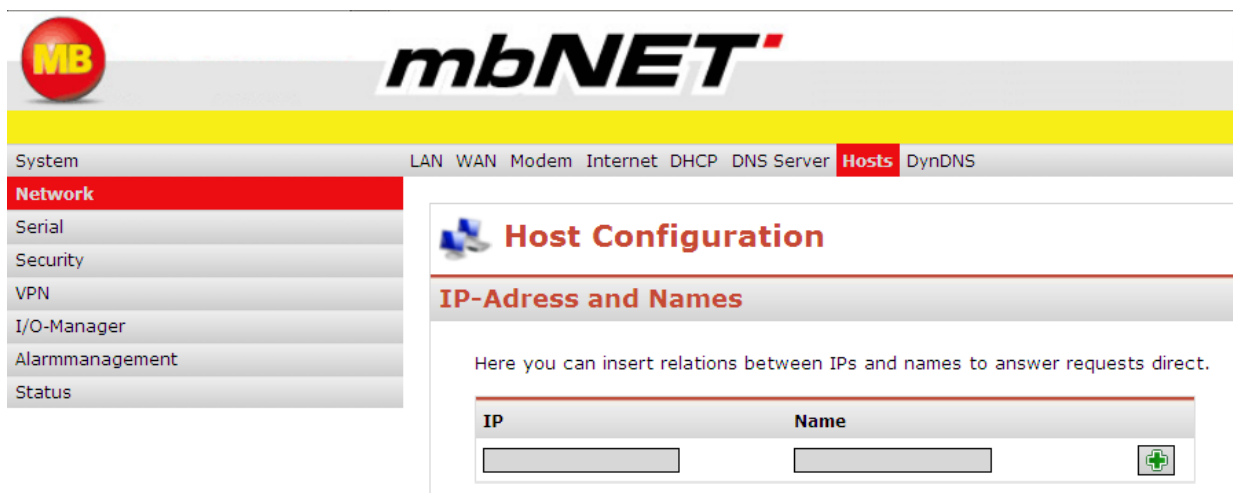
17.6 Network – DNS server

DNS is used to resolve IP addresses to names. The factory settings on the industrial router are configured so that the DNS server is assigned by the ISP. If you have a permanent industrial router connection, you can add a private DNS server here. This, rather than the ISP-assigned server, will then be the preferred server.

Label	Description
Servers	After clicking on this tab, you can enter up to five DNS server.
Settings	This tab allows you to activate or enter the DNS server settings listed below.
No Hosts	Computer names entered under the Network – Host menu are ignored.
Strict Order	The exact order set under “Servers” will be adhered to.
Filter WIN2K	Filters continuous and unnecessary requests from older Windows clients. This setting is useful when using a “on demand” connection as it avoids every request resulting in a connection to the Internet.
Domain	You can enter what is known as a domain suffix here.
Cache Size	Input the number of cached names here, in other words, the number of names that are stored with IP addresses.

17.7 Network – Hosts

This setting allows you to allocate one particular IP address to a specific name, enabling a direct response to DNS requests. You can input and store, or delete, IP addresses and their associated names in these fields. This means that the **mbNET** must answer the request directly rather than forwarding the request to another DNS server.



The screenshot shows the mbNET web interface. At the top, there is a navigation menu with options: System, LAN, WAN, Modem, Internet, DHCP, DNS Server, **Hosts**, and DynDNS. On the left, there is a sidebar menu with options: **Network**, Serial, Security, VPN, I/O-Manager, Alarmmanagement, and Status. The main content area is titled 'Host Configuration' and 'IP-Adress and Names'. Below the title, there is a text box that says 'Here you can insert relations between IPs and names to answer requests direct.' Below this text box, there is a table with two columns: 'IP' and 'Name'. There are two empty input fields under these columns, and a green plus icon in a square button to the right of the 'Name' field.

17.8 Network – DynDNS

17.8.1 General

As the industrial router is assigned a unique IP address whenever it dials in to the Internet, a client PC can locate it via this IP. However, as soon as it closes this connection and dials in again, it receives a new IP address. The DynDNS service makes the industrial router contactable using the same address every time. It resolves addresses to names and vice versa.

17.8.2 How to set up DynDNS configuration

ADVICE: A built-in DynDNS service is included with firmware versions 1.4.0 and higher. This DynDNS service is operated by MB Connect Line. *No log in or registration is required.*

To use a public version of the DynDNS service you first need to register. Registration is usually free, and should not be particularly complicated. If you are registered for a DynDNS service that is supported by the industrial router, you can input or select the options in the screenshot below.



The screenshot shows a box titled 'More Services' with the following text:

- ez-ip: www.EZ-IP.Net
- dyndns: www.dyndns.org
- ods: www.ods.org
- tzo: www.tzo.com
- easydns: www.easydns.com
- www.justlinux.com
- dyns: www.dyns.cx
- heipv6tb: www.he.net
- dyndns-static: www.dyndns.org
- dyndns-custom: www.dyndns.org
- dhs: www.dhs.org

System	LAN WAN Modem Internet DHCP DNS Server Hosts DynDNS
Network	
Serial	
Security	
VPN	
I/O-Manager	
Alarmmanagement	
Status	

DynDNS Configuration

System Dynamic DNS

Get access to the unit via: **06128342533.mbNET.mymbnet.biz**

The DNS name is made up of the serialnumber.hostname.mymbnet.biz.
Change the hostname to get your own name. The serialnumber could not be changed.

Enable System Dynamic DNS

Save Changes

public DynDNS Service

Enable

Provider dyndns

User

Password

Host Name

Interval [s]

Save Changes

MB connect line DynDNS Service	
Label	Description
Enable system dynamic DNS	This option enables MB Connect Line's automatic DynDNS service. The name structure is fixed in this case, and can only be freely defined on one host: Name: Serialnumber.Hostname.mymbnet.biz The serial number is fixed and the host name can be anything you choose. <u>Example:</u> Device name: mbNET834 Serial number: 123456789 = Name on Internet: "123456789.mbNET834.mymbnet.biz" The name will be globally available approx. 1-2 minutes after Internet dial-in.

Public DynDNS Service	
Label	Description
Enable	If you are registered with a DynDNS provider that you wish the industrial router to use, check this box by clicking on it. The next time the industrial router dials into the Internet and receives a current IP address from the ISP, it will announce this address to the DynDNS service.
Provider	Using the drop-down field, select the name of the provider with whom you are registered, e.g. DynDNS.
User	Enter the user name that you used to register for the DynDNS service.
Password	Enter the password that you used to register for the DynDNS service.
Host Name	Enter the name that you assigned to the industrial router for the DynDNS service.
Interval[s]	This field is for whenever the industrial router name changes, e.g. after a new Internet dial-in. Enter the time interval after which the industrial router will inform the DynDNS provider of the new IP address.

18. Serial interfaces

18.1 General

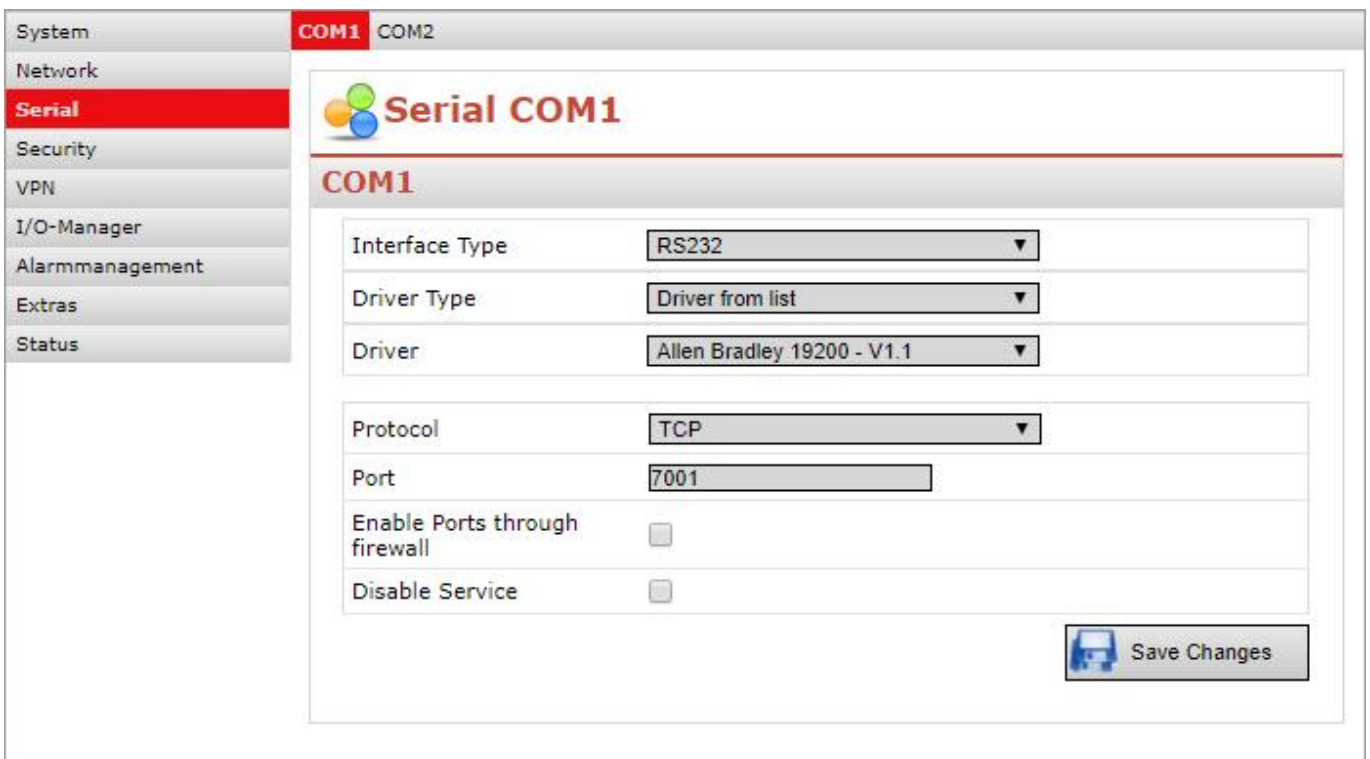
Both serial interfaces can be accessed via a dial-up or Internet connection using a known IP address.

Serial interface **COM1** can be directly configured to **RS232**, **RS485** and **RS422** using the web interface, and any associated control commands can be forwarded to the connected controller or device.

Depending on device model, **COM2** is an MPI/PROFIBUS interface on one model, and on other models it is the same as **COM1**. The MPI/PROFIBUS interface allows remote access to control systems e.g. S7-300/400, and supports baud rates of up to 12Mbit/s.

Clicking on the **Serial** button will display the following screen:

18.1.1 RS232/485 serial interfaces




System		COM1	COM2
System			
Network			
Serial			
Security			
VPN			
I/O-Manager			
Alarmmanagement			
Extras			
Status			

Serial COM1

COM1

Interface Type	RS232 ▼
Driver Type	Driver from list ▼
Driver	Allen Bradley 19200 - V1.1 ▼
Protocol	TCP ▼
Port	7001
Enable Ports through firewall	<input type="checkbox"/>
Disable Service	<input type="checkbox"/>



Label	Description
COM 1	Configuration options for COM1 interface The settings that follow it apply only to this interface.
Interface Type	Use this drop-down field to set the interface type for COM1. The options are as follows: RS232, RS485 2-wire, RS485 4-wire, RS422
Drivers	<p><u>Driver from list:</u> Select a product/brand-specific driver to control your serial device.</p> <p><u>User settings:</u> If no suitable driver is available or you need to enter your own configuration parameters. These can be entered manually.</p> <p style="padding-left: 40px;"><u>Baud rate:</u> Enter the baud rate for communication here.</p> <p style="padding-left: 40px;"><u>Data format:</u> Select one of the settings for data bits, parity or stop bits</p> <p style="padding-left: 40px;"><u>Handshake:</u> Select a handshake (flow control) option.</p> <p style="padding-left: 40px;"><u>Receive loops:</u> This is a start counter for serial signals, i.e. how many cycles the system goes through until it sends the data packet.</p>
Driver	<p>Select the driver that you want to load. Device drivers can be selected for the following brands:</p> <p>AllanBradley, AMK, ASB, AtlasCopco, AVAT, Baumüller, Berger, Bosch, B&R, DanfossVLT, Elau, F-Tron, GE_Fanuc, Hitachi, I-for-T, Indramat, IQ2000, KEB, Kuhnke, Lauer, Lenze, Locon, Micro Innovation, Mitsubishi, Möller, Motoman, Npos, Omron, Parker Hauser CompaxC3, Phoenix, Pilz, PLC Direct, Primo, Proface, Promicon, Quin, SCS Automata, Seidel Kollmorgen, SEW, Siemens, Stoeber, Stromag, Sütron, Tsx37, Tsx47, Tsx57, Vectron, Vega Sensor, Voelkel Grenzlastregler, Winloc</p>
Protocol	The protocol for communicating with the connected device: TCP
Port	Enter the port that will be used for communication.
Enable ports through firewall	Checking this box means that you can access the serial devices via the public address through the port assigned above, without being blocked by the firewall.
Disable Service	<p>Checkbox for activating / deactivating the function.</p> <p>If this function is activated, the serial driver for communication between mbDIALUP / VCOM-LAN and the serial interface is not started.</p>

18.1.2 MPI/PROFIBUS Interface

Communication with S7 via

- VCOMLAN2 (PC adapter in SIMATIC Manager)
- RFC1006
- mbNETS7 driver (direct installation in SIMATIC Manager)

The screenshot shows the 'Serial COM2' configuration window in SIMATIC Manager. The left sidebar contains navigation options: System, Network, Serial (selected), Security, VPN, I/O-Manager, Alarmmanagement, Extras, and Status. The main area is titled 'Serial COM2' and contains the following settings:

- Interface Type: MPI/PROFIBUS
- Protocol: MPI/PROFIBUS Network Driver
- Enable RFC1006:
- Own station address: 0
- Enable RFC1006 Routing:
- Station address of the routing gateway: 2
- Protocol: TCP
- Port: 7002
- Enable Ports through firewall:
- Disable Service:

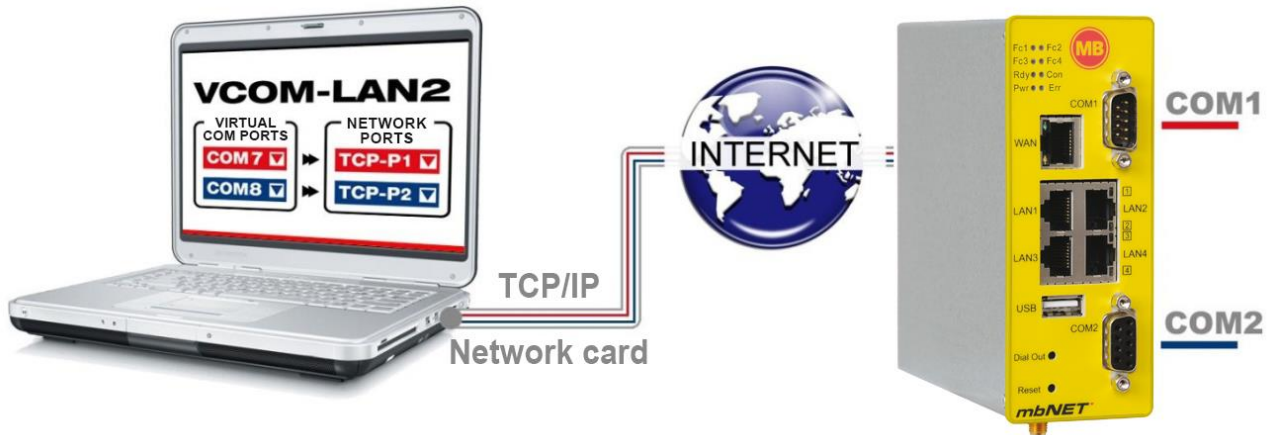
A 'Save Changes' button is located at the bottom right of the configuration area.

Label	Description
Protocol	<p><u>VCOM-LAN2/PC adapter</u> <u>MPI/PROFIBUS Baud rate</u> If you select “VCOM-LAN2/PC adapter”, the PG/PC interfaces must be installed on a PC adapter (MPI/PROFIBUS). For bus speeds higher than 1.5 Mbit/s this must be manually assigned.</p> <p><u>MPI/PROFIBUS network driver</u></p> <p>ADVICE: Enabling this option launches the installation of network drivers on the client PC. Dispensing with separate driver installation and using the “TCP/IP (Auto)” option with a PG/PC interface is only possible if the RFC1006 option is enabled. Instructions on this are available on our website support pages under the heading “RFC1006”. RFC1006 uses TCP Port 102.</p> <p><u>Enable RFC1006</u> You can select to enable the RFC1006 protocol here.</p> <p><u>Own station address</u> If RFC1006 is enabled, assign a unique MPI/DP station address for the router.</p> <p>ADVICE: The connected router will use this station address to log into the MPI/DP network. This is necessary if you are using RFC1006 communication exclusively. In a mixed operation of connections using network drivers and RFC1006, the router always logs in using the address assigned to the first connection used.</p>

	<p>Enable RFC1006 routing This option enables routing via RFC1006.</p> <p>Station address of the routing gateway If RFC1006 routing is enabled, you must enter the address of the routing gateway (14 – see example below)</p> <p>ADVICE: To access a slave subscriber station in a subnetwork that is not directly connected, the master gateway must be assigned as the PLC routing gateway station address on the router.</p> <p><i>Example:</i> The PLC (master) is connected to the router (e.g. address 13) via MPI Bus (e.g. address 14) and a subscriber station (e.g. address 5) is connected to the master PROFIBUS (e.g. address 4). To now be able to access the subscriber with address 5 on the PROFIBUS via the router (13) using MPI, routing needs to be enabled.</p> <p>More information on installation is available via our Support Portal at www.connect-line.com</p>
MPI/PROFIBUS baud rate	Select from the following options: PG/PC Interface Settings, 3Mbit/s, 6Mbit/s and 12Mbit/s
Protocol	The protocol for communicating with the connected device: TCP
Port	Enter the port that will be used for communication.
Enable ports through firewall	Checking this box means that you can access the Internet through the port assigned above, without being blocked by the firewall.
Disable Service	<p>Checkbox for activating / deactivating the function.</p> <p>If this function is activated, the serial driver for communication between mbDIALUP / VCOM-LAN / mbNET-S7 and the serial interface is not started.</p>

18.2 Redirecting serial interfaces to your PC (VCOM LAN2)

To make serial interfaces (including MCI/PROFIBUS) available on your PC, you need the VCOM LAN2 software utility. VCOM LAN2 can be downloaded free of charge from www.mbconnectline.com. VCOM LAN2 installs two virtual COM interfaces on your client PC. Data is then exchanged over these virtual COMs



With firmware version 2.0 and higher, the Fc1 LED lights up when a MPI or PROFIBUS connection is established, and the Fc2 LED flashes when data is being transferred over either of these connections.

COM 7 <> COM 1
COM 8 <> COM 2

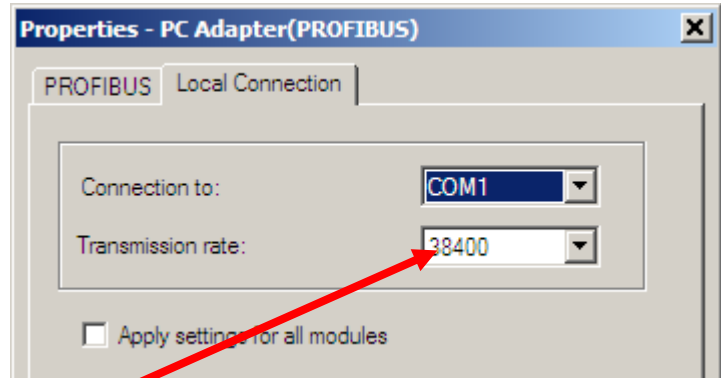
Run the VCOM LAN2 set up file and follow the installation instructions. When installing a system you should be aware that the ports (**TCP/UDP 254000 and 25401, depending on settings**) are enabled on both client side and router side. Note also that if you select the connection setting “connect when the virtual COM-Port was opened from an application program”, a small amount of data may be lost while the virtual COM port is being opened, as some programs send data to the port immediately, before the virtual COM port has established a connection. More information is available under VCOM LAN2 program Help

18.2.1 Settings for Simatic Manager

If you wish to set up a connection to a Siemens control system, you first need to verify the settings in Simatic Manager by selecting

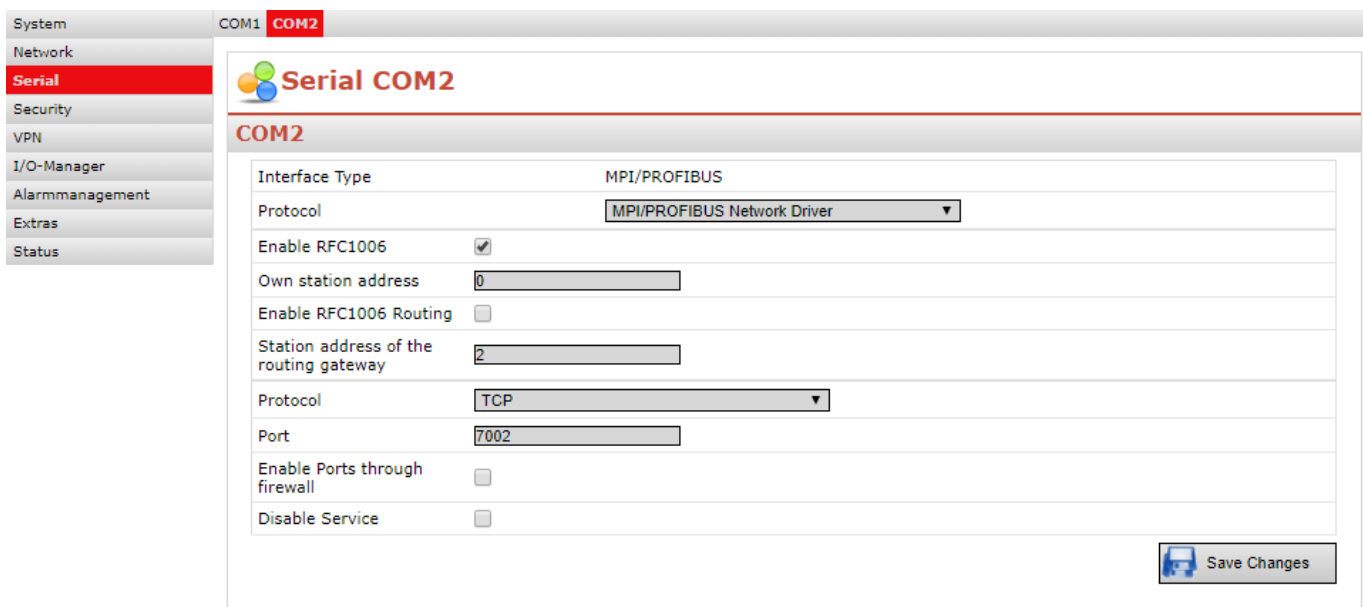
Extras → *Set up PG/PC interface* → *PC adapter (PROFIBUS)* or *PC adapter (MPI)*

and then clicking on Properties. This will open a menu screen with a "Local Connection" tab. The transmission rate here **MUST** be set to 38400.



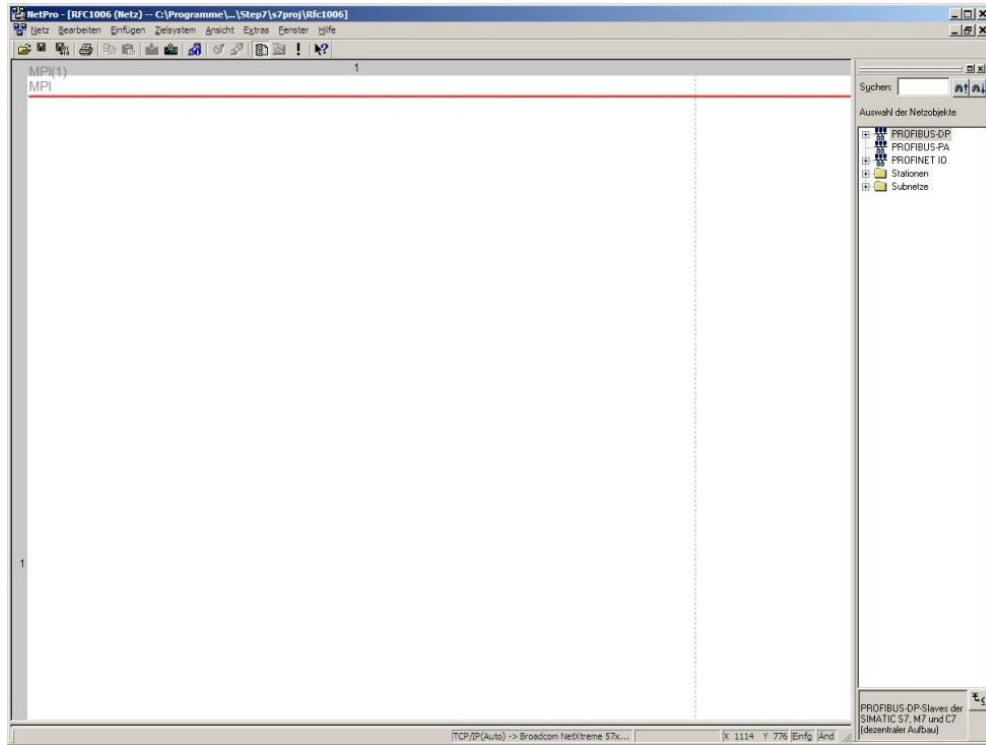
18.3 Enabling RFC1006 on the mbNET

Enable the RFC1006 option under the "Serial Interfaces", "COM2" menu. Specify the own station address for the **mbNET**.



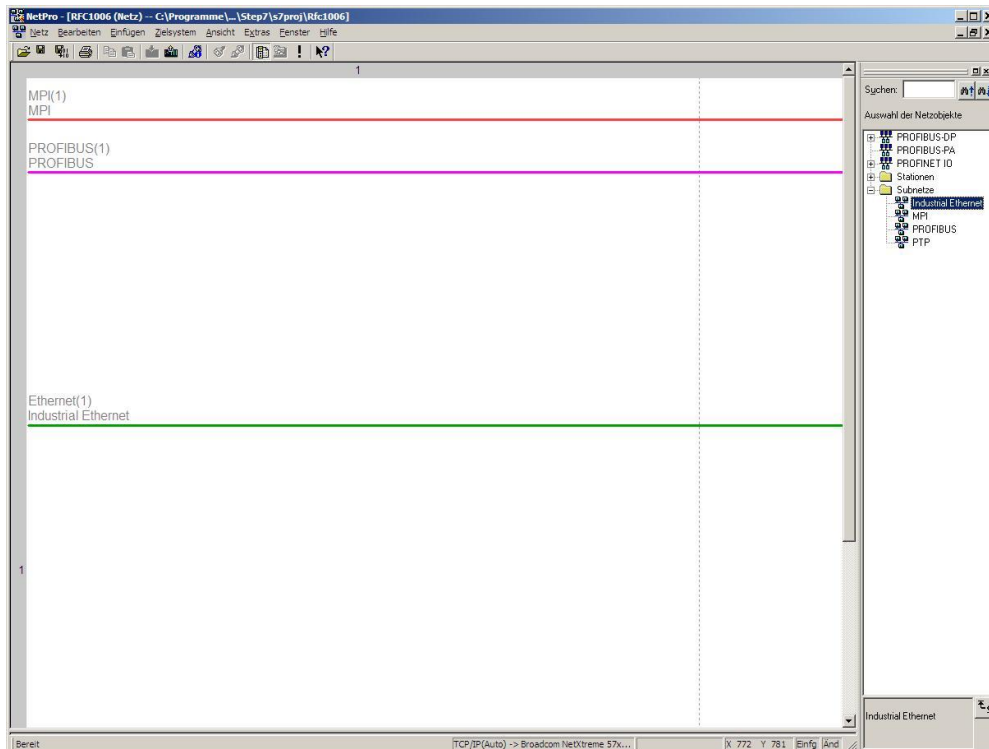
18.3.1 Settings for NETPro Step 7

Launch the NETPro application in Simatic Manager.



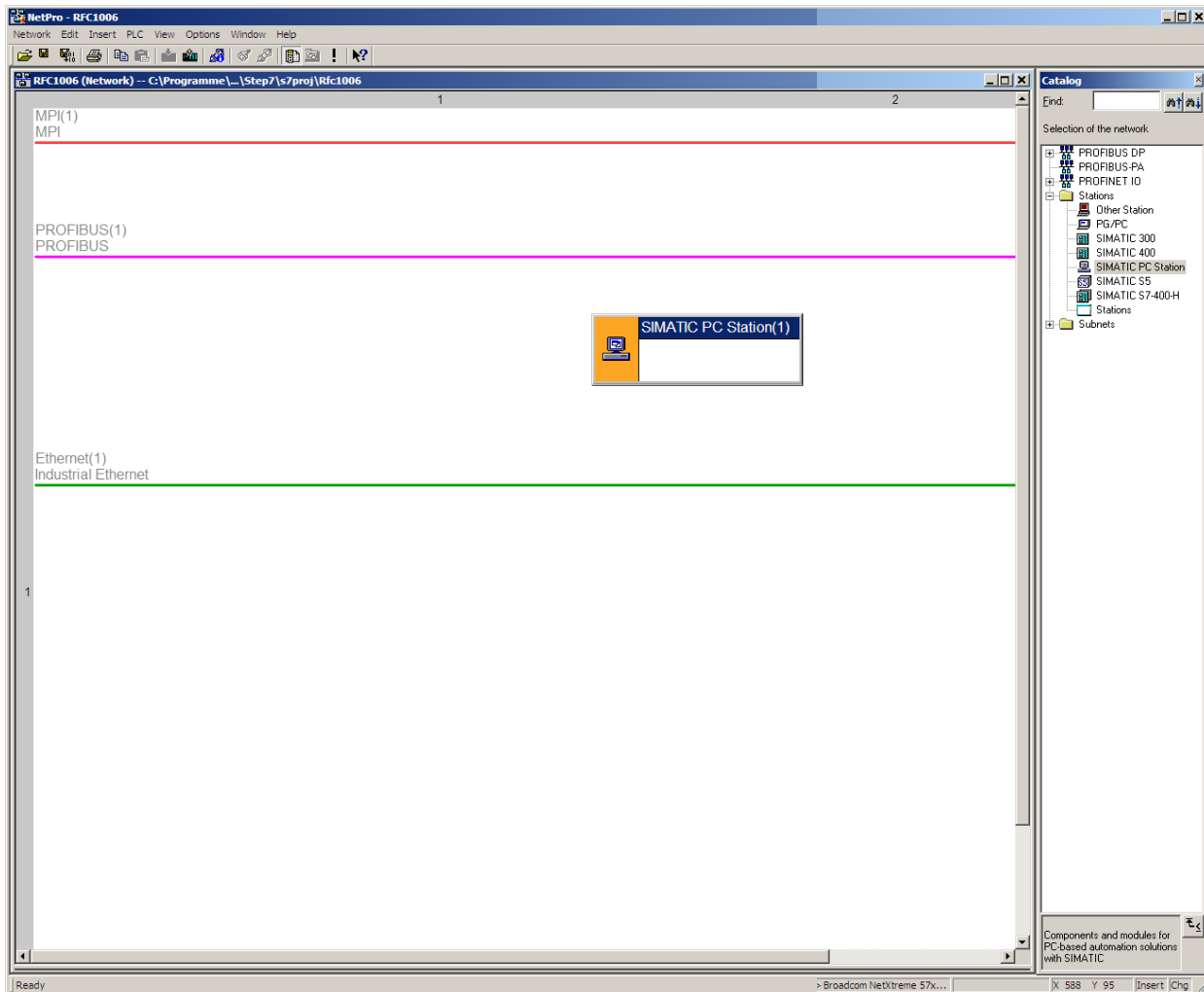
18.3.2 Create subnets

Create a "PROFIBUS" and an "Industrial Ethernet" subnet.



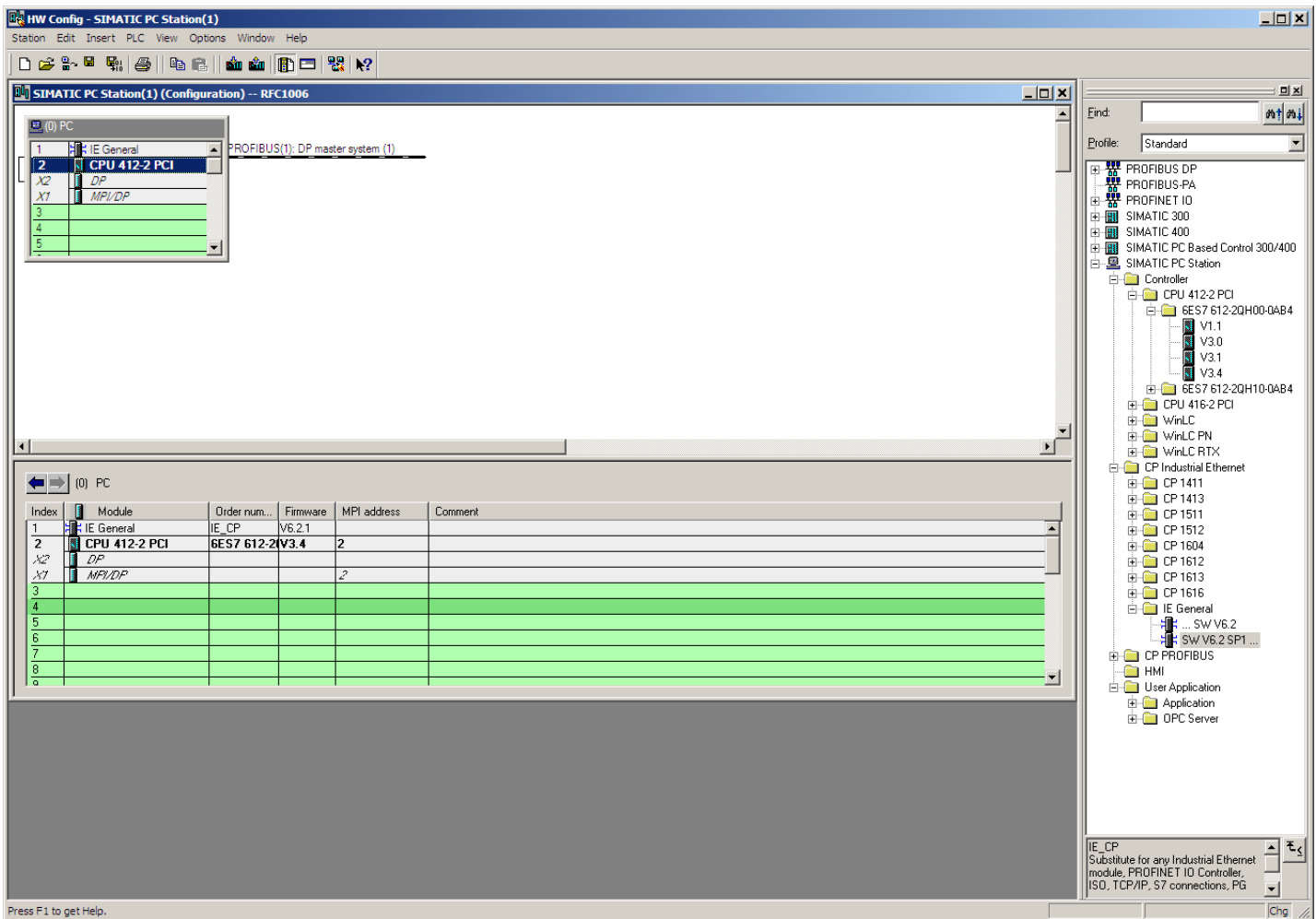
18.3.3 Add PC station

Following step 2.1 you need to add a PC station. You can skip steps 2.2 to 2.3 if you are using the “NETPro” Import function. A pre-configured **mbNET** station is available as an annex to these instructions. You can download this as a Zip file from our homepage www.mbconnectline.com under Support/Manuals.



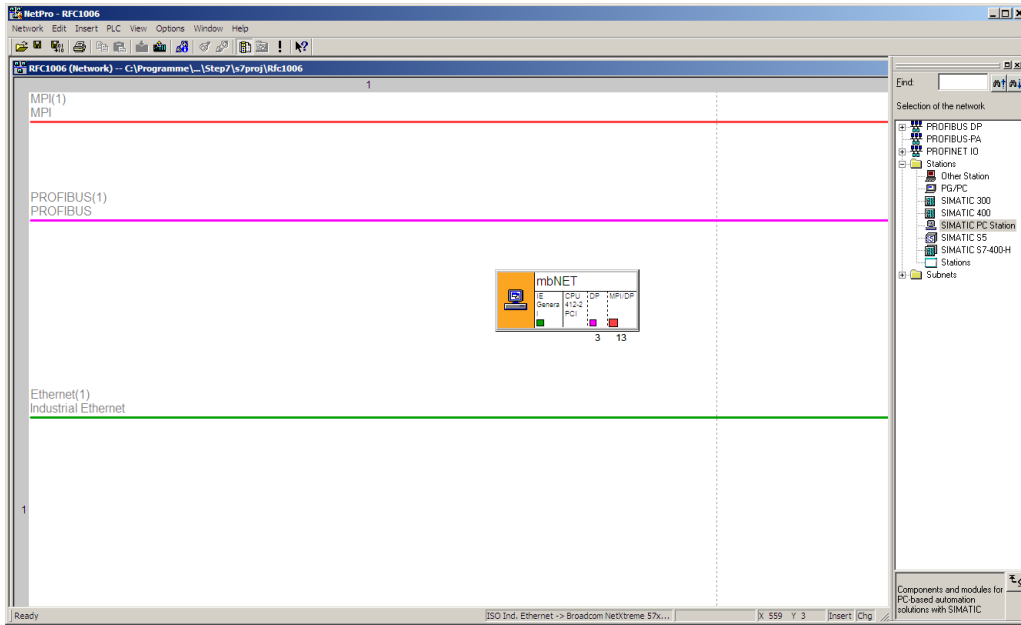
18.3.4 Configure PC station

This “PC Station” requires the integration of a “CPU 412-2 PCI (6ES7 612-2QH00-0AB4 V3.4)”, found by selecting “Simatic PC Station -> Controller -> CPU412-2 PCI” and a “IE_CP V6.2.1 (IE General)” found by selecting “Simatic PC Station -> CP-Industrial Ethernet -> IE General-> IE_CP SW V6.2 SP1”.

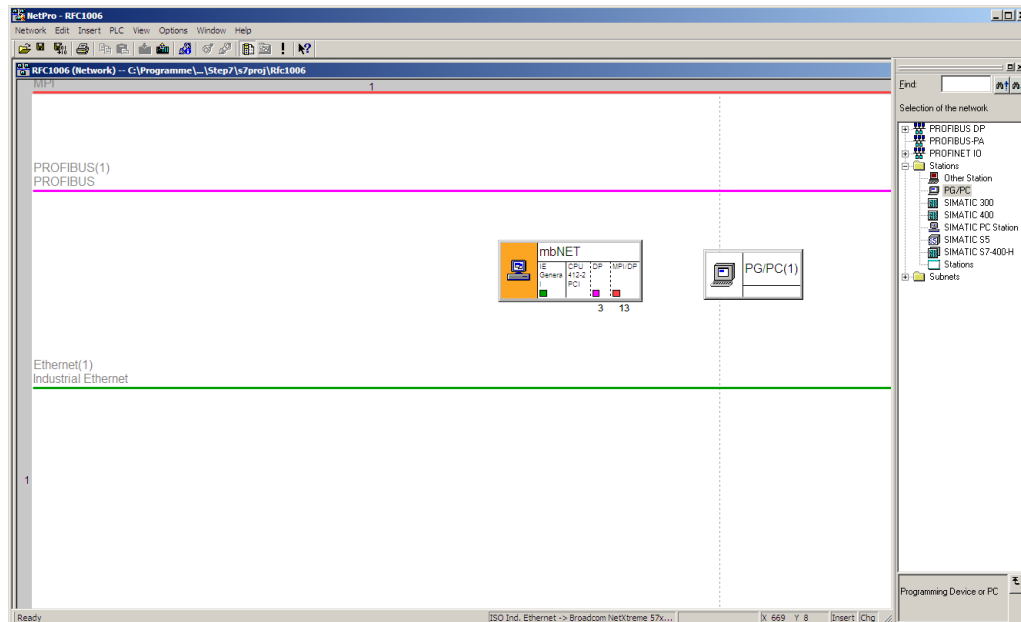


The finished station must now be saved, and appears in “NETPro”.
 The MPI/DP address must match the settings entered in “own station address” on the **mbNET**.

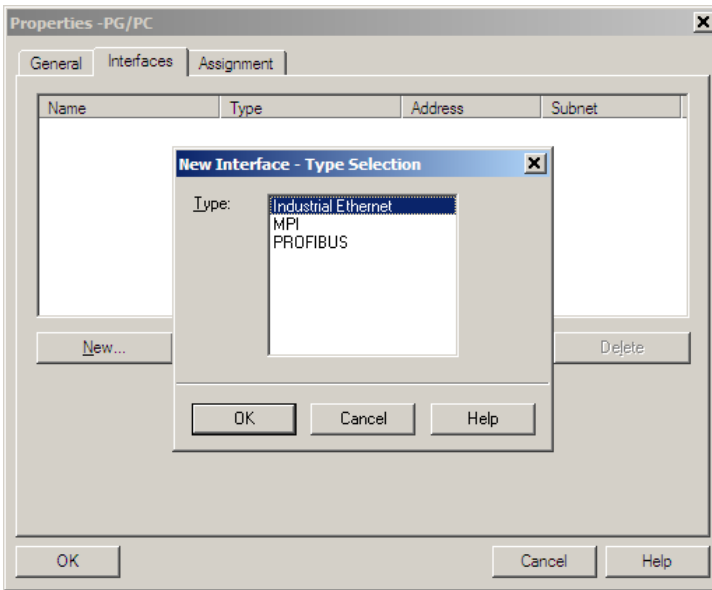
18.3.5 Add PC/PG station



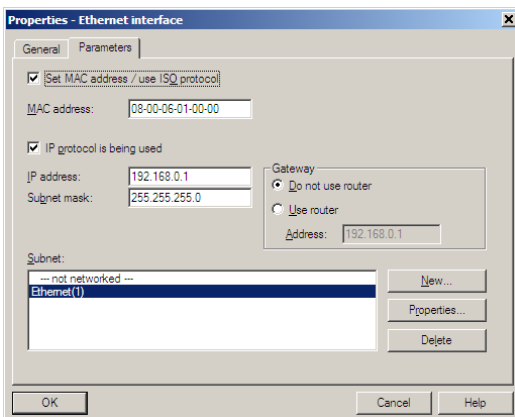
Now you need to add a PC/PG station.



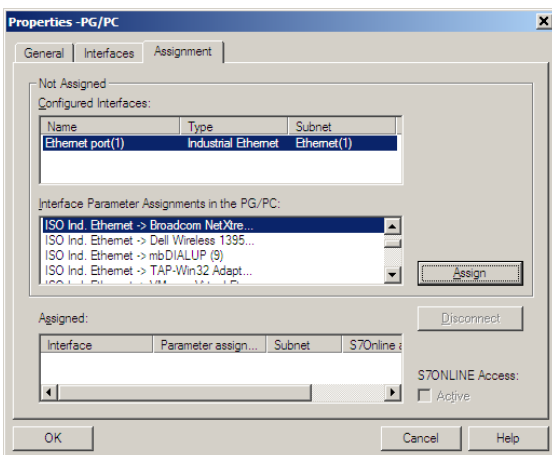
Double clicking on “PG/PC Station” opens the Properties window for this. Here, you need to add this interface by selecting “Interfaces -> New ...-> Industrial Ethernet”.



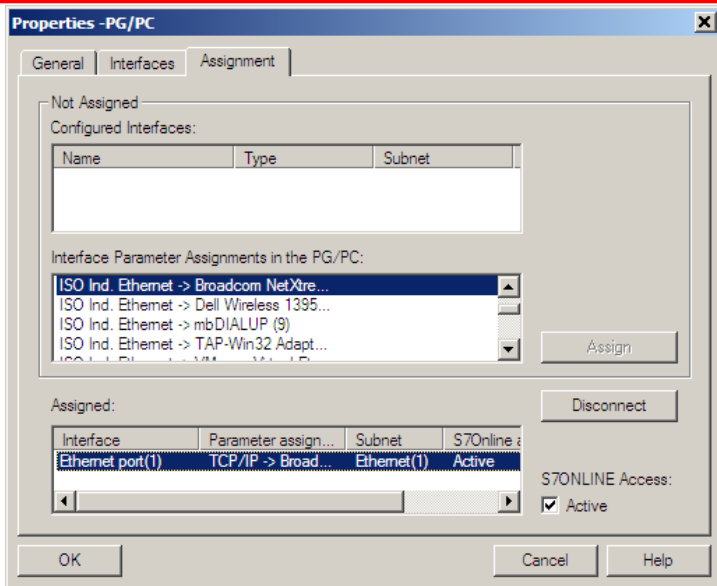
This opens a window where you need to make the “Industrial Ethernet” settings for the PC. Specify the PG/PC subnet mask and IP address here. The PG/PC IP address can be from anywhere in the network range but may not overlap with other addresses on the network and must not be the real IP address of the PG/PC.



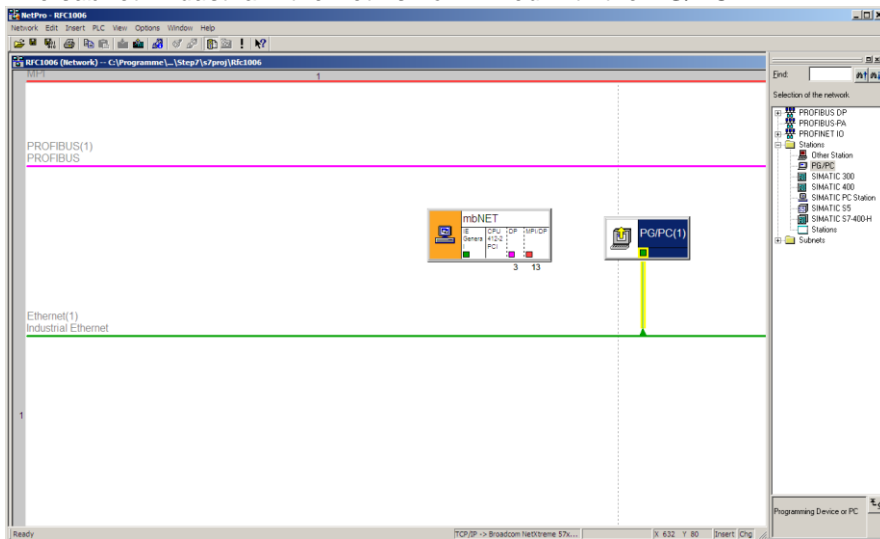
Next, in the “Assignment” tab, find the interface that you intend to use as the “Ethernet Interface” and link this to “TCP/IP (Auto) -> xxx” (the LAN card in use) by clicking on the “Assign” button.



After assigning your chosen interface, the window should look like this. STONLINE access must be set to „Active“.

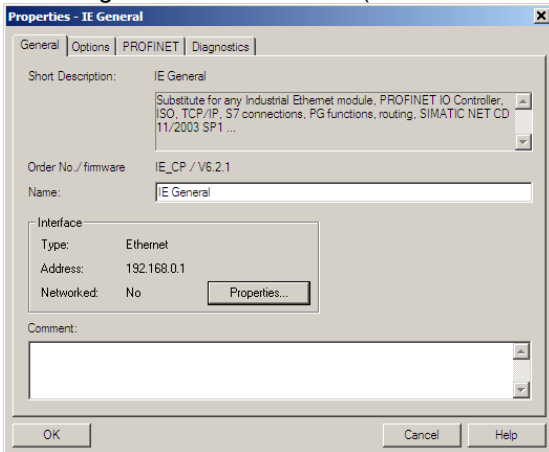


The subnet "Industrial Ethernet" is now linked with the PG/PC.

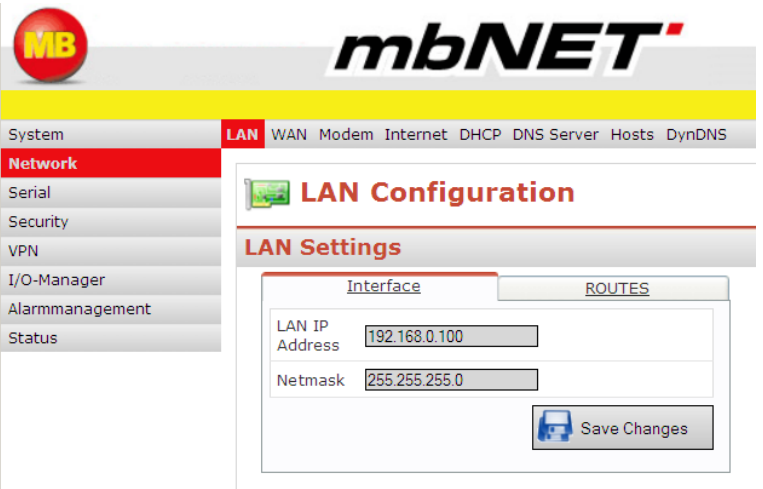
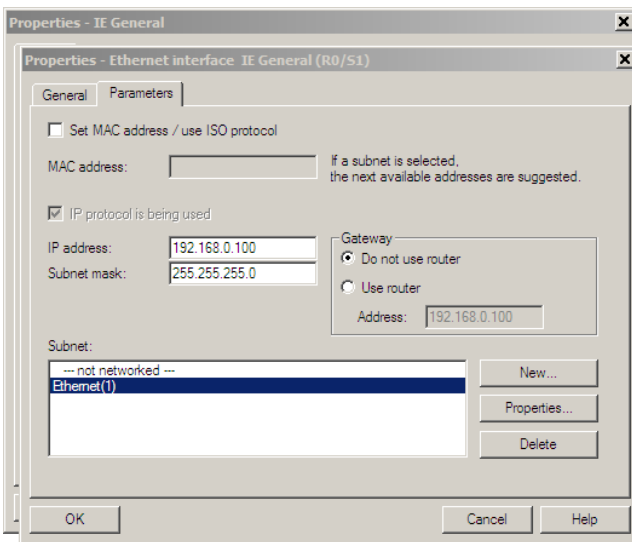


18.3.6 Configure mbNET PC station

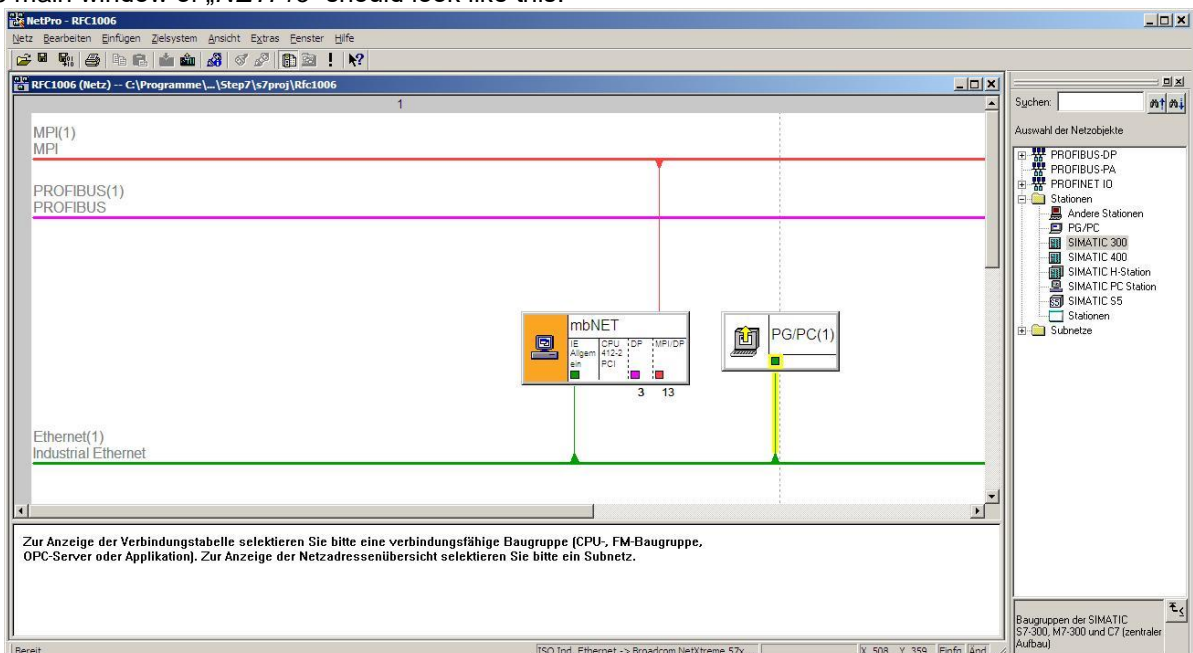
To configure this “PC Station” (in this case: **mbNET**), double-click on “IE General”.



Click on “Properties” to set the interface parameters. Enter the IP address and subnet mask here. The IP address and subnet mask must be the same as those entered in the **mbNET** LAN settings.

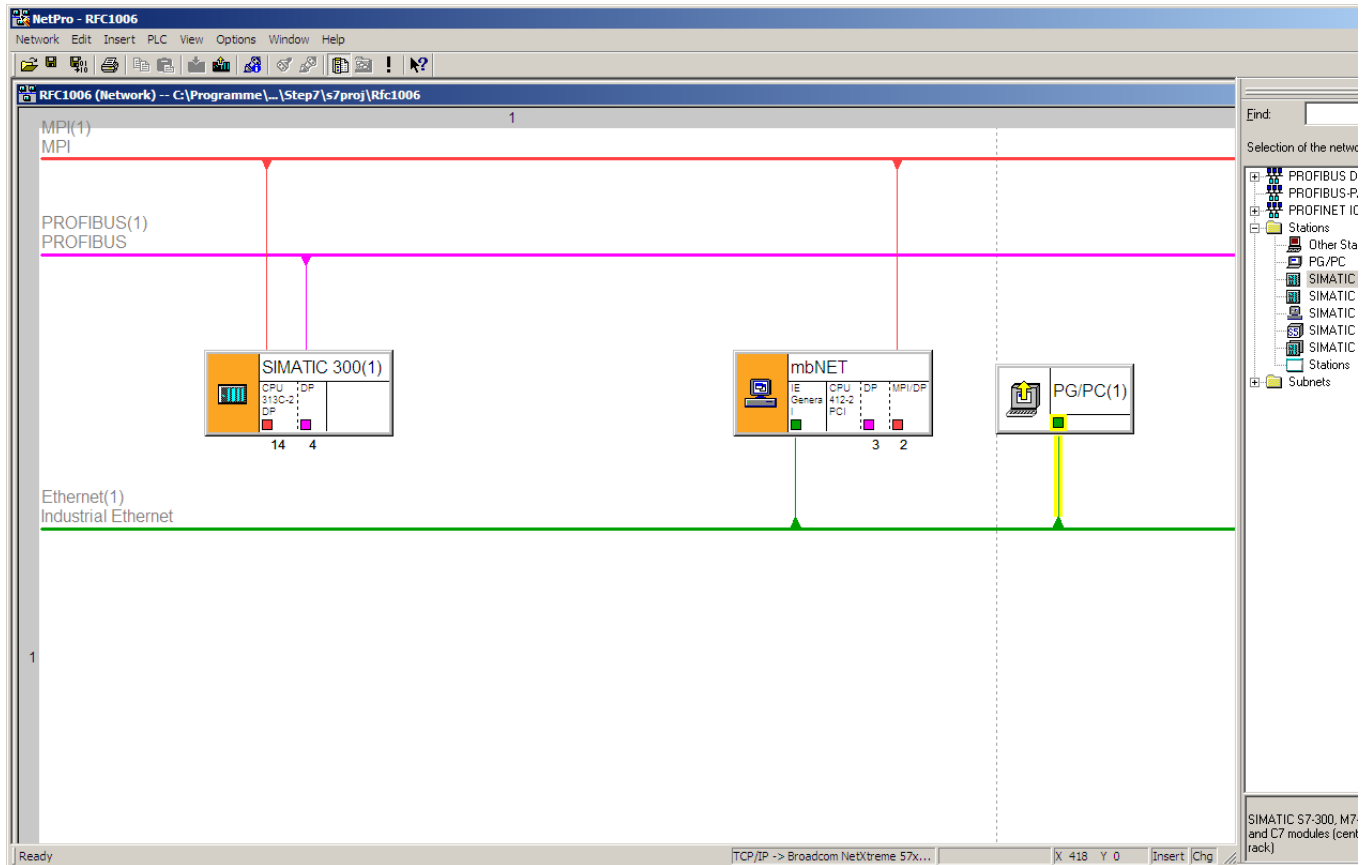


Now the main window of „NETPro“ should look like this.



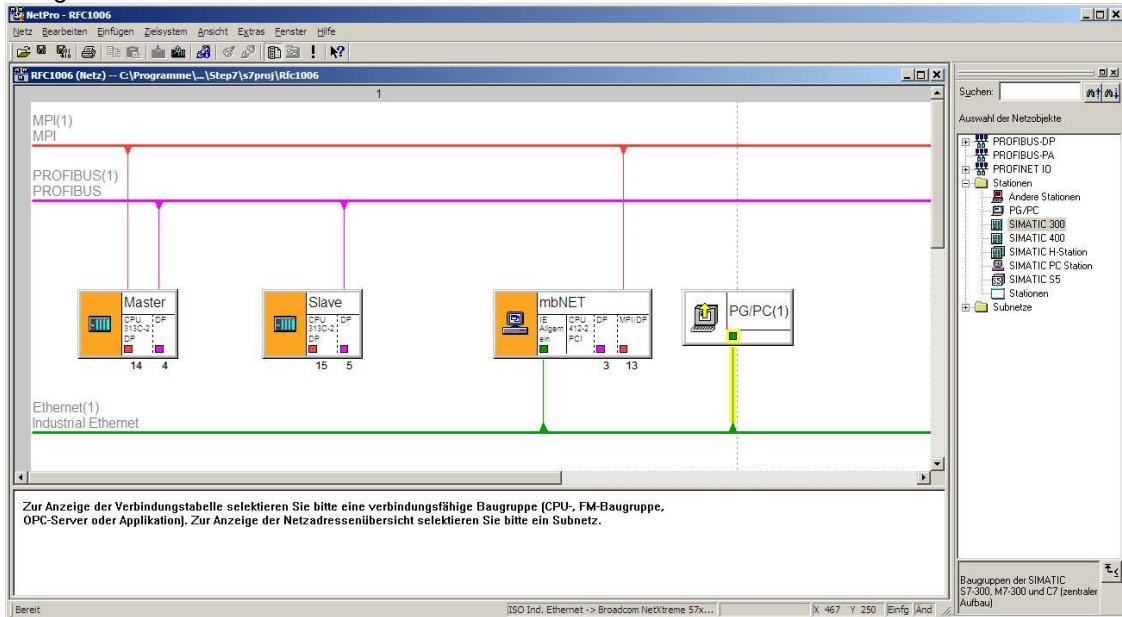
If everything has worked as it should, then “TCP/IP (Auto) -> xxx” (network card) will appear in the bottom border of the screen as “PG/PC interface”. It is recommended at this stage to assign a bus address (in this case, MPI) to the PC station and link this with the subnet.

Finally, a CPU of your choice can be added to the relevant subnet.
The example here uses a “CPU 313-C2DP”



18.3.7 Routing

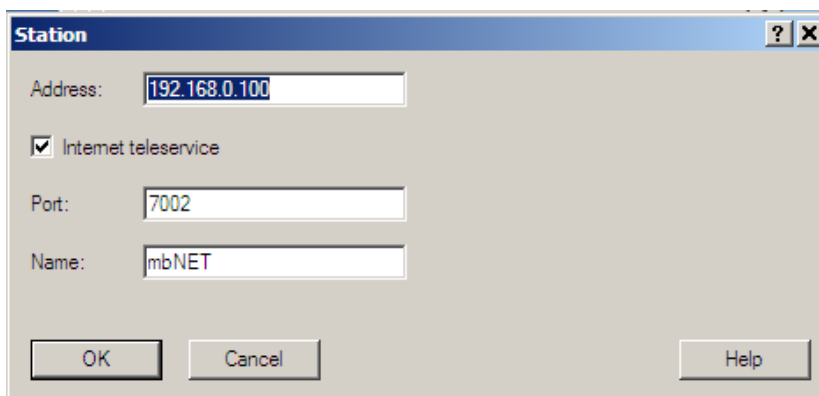
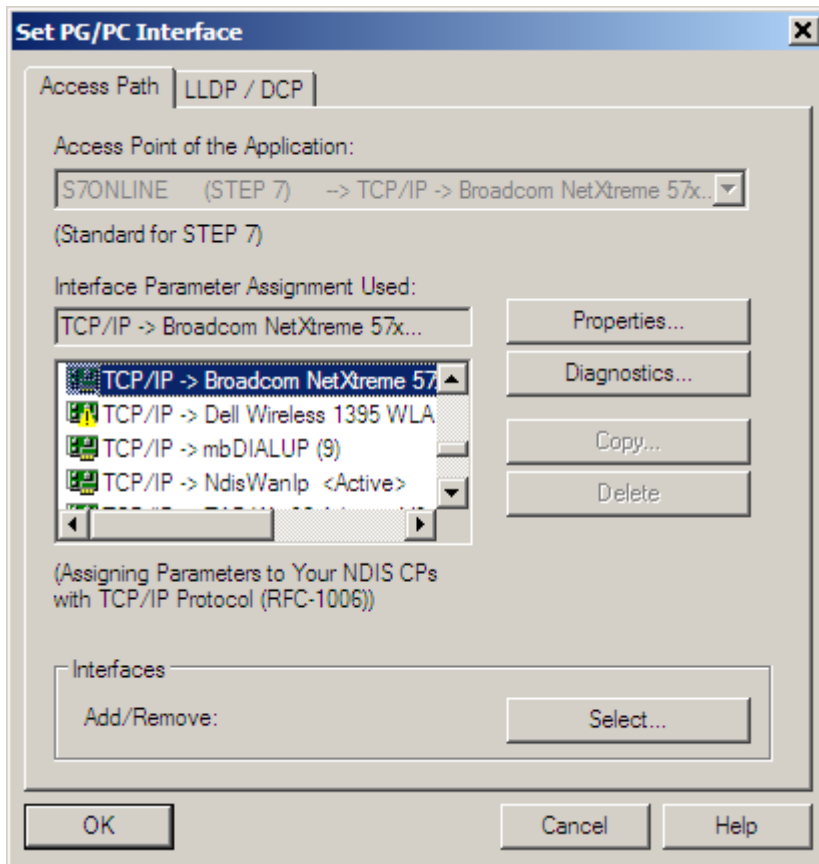
For the station to be able to contact a subscriber from another (slave) network (see picture), you need to make the following settings.



In the **mbNET** settings, enable RFC1006 routing and enter the station address of the (master) routing gateway.

18.4 Connecting to S7 using the *mbNET* S7 driver

Alternatively, the licensed *mbNET* S7 driver can be used. Once installed, this is directly available as an adapter in Simatic Manager.



The router settings for this must be as shown below.

System	COM1 COM2
Network	
Serial	
Security	
VPN	
I/O-Manager	
Alarmmanagement	
Status	

Serial COM2

COM2

Interface Type	MPI/PROFIBUS
Protocol	MPI/PROFIBUS Network Driver
Enable RFC1006	<input type="checkbox"/>
Own station address	0
Enable RFC1006 Routing	<input type="checkbox"/>
Station address of the routing gateway	2
Protocol	TCP
Port	7002
Enable Ports through firewall	<input type="checkbox"/>

Save Changes

RFC1006 can be operated in parallel with this.

19. Security

19.1 Firewall General

The industrial router has an integrated firewall to protect against third-party and unauthorized access and connection attempts. Incoming and outgoing data traffic is checked, logged and allowed or denied via this firewall.

The firewall can generally be configured with one of the following four settings:

maximum Security

All incoming Packages (Data from Internet) are **rejected**
 All outgoing Packages (Data from LAN) are **rejected**
 except: DNS, FTP, IMAP, HTTP, HTTPS, POP3, SMTP, Telnet, NTP

With this setting, rules for allowing data traffic must be configured accordingly. Both incoming and outgoing data traffic is denied.

For accessing the web interface (from outside the network), the **TCP protocol** and the **destination port 80** must be entered and enabled in the **WAN > LAN** rules. If, however, you start a VPN connection, access is accordingly allowed for the data packets from the VPN tunnel.

normal Security

All incoming Packages (Data from Internet) are rejected
 All outgoing Packages (Data from LAN) are accepted.

With this setting, incoming data traffic (data from the Internet) is denied while outgoing data traffic is allowed.

minimum Security

All incoming Packages (Data from Internet) are accepted.
All outgoing Packages (Data from LAN) are accepted.

With this setting, all incoming and outgoing data traffic is allowed.

Firewall off

All incoming Packages (Data from Internet and WAN Ethernet*) are accepted.
All outgoing Packages (Data from LAN) are accepted.

Routing between all interfaces is **on**

With this setting, all incoming and outgoing data traffic is allowed.
Furthermore, all entered firewall rules are deactivated and routing between WAN <> LAN is active.


* For devices without a WAN Ethernet interface, this is only "Data from Internet".

ADVICE: The variants "**minimum Security**" and "**Firewall off**" should be selected only briefly and for test purposes or during initial configuration, if you want to ensure that a configured rule is not to be accessed.




All data traffic from inside to outside and external access is possible!
The integrity of your **mbNET** and the devices connected to it is threatened when selecting one of these two variants!

SNAT

	Replace the senders IP-address of all outgoing (LAN) packages with the LAN-IP address of this router (SNAT)
Activate	<input checked="" type="checkbox"/>

This function transparently passes on the incoming data traffic from Internet or VPN connections to the LAN. In other words, all data packets going to the LAN are assigned the IP address of the router as the sender address. This means that none of the LAN subscribers need the router as a "gateway". This is a considerable advantage when integrating remote maintenance into existing network structures as it means that these structures do not need to be changed.

	Replace the senders IP-address of all outgoing (WAN) packages with the WAN-IP address of this router (SNAT)
Activate	<input type="checkbox"/>

If this checkbox is activated, incoming traffic from LAN participants is transparently forwarded to the WAN network. That that all data packets sent to the WAN receive the sender address as the WAN IP address of the router.

19.2 WAN > LAN

This setting governs the **incoming** data traffic, i.e. the following settings only apply to data traffic arriving from outside the network.

Depending on the router type, the selection field for the WAN interface may vary.

“WAN” is always the currently active interface with the Internet as far as the **mbNET** firewall is concerned. The following rule is determined by the setting under “**Network > Internet**”:

Internet Connection:

Internet via WAN (external router, fixed line)

Here the WAN Ethernet is the interface to the Internet. The firewall therefore checks the data traffic from WAN Ethernet to LAN Ethernet.






Internet via Modem

The modem is the interface with the Internet here. The firewall therefore checks the data traffic from the modem to the LAN Ethernet. All data traffic on the WAN Ethernet interface is denied with this setting.

Internet via WAN

The “DSL data traffic” via the WAN Ethernet is the interface with the Internet here. The firewall therefore checks the data traffic from the DSL modem to the LAN Ethernet. All other data traffic on the WAN Ethernet interface is denied with this setting.

Label	Description
Enable	Check the box by clicking it to enable the subsequent settings after they are saved.
Action	<p>The following options are available for selection:</p> <ul style="list-style-type: none"> • Drop If this option is selected, it means that no data packets can pass and the packets are also deleted immediately. The sender is not notified about the whereabouts of the data packets. • Reject If this option is selected, the data packets are rejected. The sender is notified that the data packets have been rejected. • Accept If this option is selected, the data packets can pass.
WAN interface	<p>This setting defines the WAN interface to which the rule is to be applied.</p> <ul style="list-style-type: none"> • Internet • WAN Ethernet • OpenVPN • IPSecVPN • PPTPVPN • all

Source IP	Here, enter the IP addresses for whose incoming data packets one of the set actions is to be executed. If you leave the field blank, the set action applies to all IP addresses (only on the selected interface).
Source Port	Enter the ports via which the data packets arrive here.
Protocol	The following options are available for selection: <ul style="list-style-type: none"> • All - the set rule applies to all protocols. • tcp - the set rule only applies to the TCP protocol. • udp - the set rule only applies to the UDP protocol. • icmp - the set rule only applies to the ICMP protocol.
LAN Interface	Use this selection field to specify the LAN interface to which the rule is to be applied. You can choose from: <ul style="list-style-type: none"> • local Services • LAN Ethernet • all
Destination IP	Enter the IP addresses to which the data packets are to be forwarded here.
Destination Port	Enter the ports via which the data packets are forwarded here.
	Accepts a new rule.
	Deletes entries in the current line.
	Edits the settings in the current line.
	Temporarily saves the created rule.
	Changes the order of the created rules.

ADVICE

You can enter address **ranges** in the input fields for the **IP** address.
Example of address ranges: 192.168.0.100-192.168.0.110 or 192.168.0.20/30

Address listings are **not** possible!

In the input fields for the **ports**, you can enter **ranges or enumerations**.

Example of a port range: 502-504

Example of port enumeration: 502,677,555

Both, range and enumeration **can not** be used simultaneously in the same field.

Ranges must be separated by a **hyphen (-)** and **enumerated** by **comma (,)**.







No spaces between the elements to be separated!

The input of IP and port is not mandatory. If neither an IP nor a port is specified, a rule applies only to the selected interfaces.

19.3 LAN > WAN

This setting governs the **outgoing** data traffic, i.e. the following settings only apply to outgoing data traffic.

Label	Description
Enable	Check the box by clicking it to enable the subsequent settings after they are saved.
Action	<p>The following options are available for selection:</p> <ul style="list-style-type: none"> • Drop If this option is selected, it means that no data packets can pass. The sender is not notified about the whereabouts of the data packets. • Reject If this option is selected, the data packets are rejected. The sender is notified that the data packets have been rejected. • Accept If this option is selected, the data packets can pass.
LAN Interface	<p>Use this selection field to specify the LAN interface to which the rule is to be applied. You can choose from:</p> <ul style="list-style-type: none"> • local Services • LAN Ethernet • all
Source IP	Enter the IP addresses of the computers from which data packets are sent to the Internet (gateway). If you leave the field blank, the set action applies to all IP addresses.
Source Port	Enter the ports via which the data packets go to the Internet here.
Protocol	<p>The following options are available for selection:</p> <ul style="list-style-type: none"> • All - the set rule applies to all protocols. • tcp - the set rule only applies to the TCP protocol. • udp - the set rule only applies to the UDP protocol. • icmp - the set rule only applies to the ICMP protocol (ping).
WAN Interface	<p>This setting defines the WAN interface to which the rule is to be applied.</p> <ul style="list-style-type: none"> • Internet • WAN Ethernet • OpenVPN • IPSecVPN • PPTPVPN • all
Destination IP	Enter the destination addresses of the data packets on the Internet here.

Destination Port	Enter the ports via which the data packets are sent to the destination IP here.
	Accepts the new rule and temporarily stores it.
	Deletes entries in the current line.
	Edits the settings in the current line.
	Temporarily saves the created rule.
 	Changes the order of the created rules.

ADVICE

You can enter address **ranges** in the input fields for the **IP** address.
Example of address ranges: 192.168.0.100-192.168.0.110 or 192.168.0.20/30

Address listings are **not** possible!

In the input fields for the **ports**, you can enter **ranges or enumerations**.

Example of a port range: 502-504

Example of port enumeration: 502,677,555

Both, range and enumeration **can not** be used simultaneously in the same field.

Ranges must be separated by a **hyphen (-)** and **enumerated** by **comma (,)**.



No spaces between the elements to be separated!

The input of IP and port is not mandatory. If neither an IP nor a port is specified, a rule applies only to the selected interfaces.

19.4 Forwarding

This setting is forwarding requests from specific IP addresses and ports to defined IP addresses and ports.

Label	Description
Enable	Check the box by clicking it to enable the subsequent settings after they are saved.
Source IP	You can enter the IP addresses from which data packets are received here. If an entry is made here, only packets from these addresses are forwarded.
Source Port	You can specify the ports via which the data packets arrive here. If an entry is made here, only packets specifically sent via this port are forwarded.
Protocol	The following protocols are available for selection: <ul style="list-style-type: none"> • All - the set rule applies to all protocols. • tcp - the set rule only applies to the TCP protocol. • udp - the set rule only applies to the UDP protocol.
Destination IP	Enter the IP addresses to which the data packets were originally to be sent here.
Destination Port	Specify the ports via which the data packets are sent to the destination IP here.
Interface	This setting defines the WAN interface to which the rule is to be applied. You can choose from: <ul style="list-style-type: none"> • Internet • WAN Ethernet • OpenVPN • IPSecVPN • PPTPVPN • LAN Ethernet • all
Forward IP	Enter the IP to which the data packets are actually to be sent here.
Forward Port	Specify the port via which the data packets are actually forwarded here.
	Accepts the new settings and temporarily stores them.
	Deletes entries in the current line.
	Edits the settings in the current line.

	Temporarily saves the created rule.
	Changes the order of the created rules.

ADVICE

You can enter address **ranges** in the input fields for the **IP** address.
Example of address ranges: 192.168.0.100-192.168.0.110 or 192.168.0.20/30

Address listings are **not** possible!

In the input fields for the **ports**, you can enter **ranges or enumerations**.

Example of a port range: 502-504

Example of port enumeration: 502,677,555

Both, range and enumeration **can not** be used simultaneously in the same field.

Ranges must be separated by a **hyphen (-)** and **enumerated** by **comma (,)**.





No spaces between the elements to be separated!

The input of IP and port is not mandatory. If neither an IP nor a port is specified, a rule applies only to the selected interfaces.

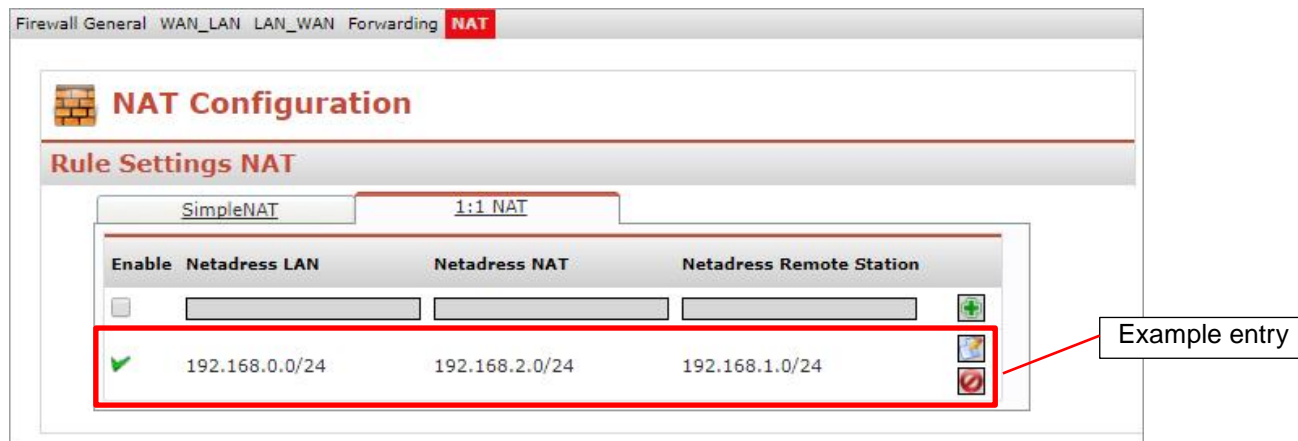
19.5 NAT

19.5.1 SimpleNAT

SimpleNAT is about making an IP from the LAN network 1:1 accessible in the WAN Ethernet network. For this purpose, a free WAN ethernet address from the WAN network is entered as WAN IP. This IP address is then added in addition to the WAN interface and is mapped directly to the registered LAN IP "1:1". I. e. the IP from the WAN reaches directly the IP of the LAN. This has the advantage that you do not have to forward ports etc.

Label	Description
Enable	Checkbox for activating / deactivating this function.
WAN IP	Enter here a free WAN ethernet address from the WAN network (e.g., 192.168.1.101).
LAN IP	Enter the LAN IP address that you want to reach (e.g., 192.168.0.1).
Comment	Here you can enter a comment about this rule.
	Accepts the new settings and temporarily stores them.
	Edits the settings in the current line.
	Deletes entries in the current line.
	Changes the order of the created rules.

19.5.2 1:1 NAT



This setting enables two networks in the same address range to be connected. If, for example, a network with the address 192.168.0.0/24 is to be connected to a network with the same address, this is only possible if one of the two networks is assigned another address. NAT technology is an easy way of achieving this since only the real network address (LAN address) and the substitute address (NAT network address) are required. The NAT algorithm makes sure that the addresses in the data packets are only substituted in communications between these two networks. This means that you do not have to adapt your entire network addressing scheme.

Label	Description
Enable	Check the box by clicking it to enable the subsequent settings after they are saved.
Netaddress LAN	Enter the real address of the network here (e.g.192.168.0.0/24). Please note that the IP address must be entered in CIDR notation.
Netaddress NAT	Enter the translated address of your network here (e.g. 192.168.1.0/24). Please note that the IP address must be entered in CIDR notation.
Netaddress Remote Station	Enter the address of the network to which the translated packets are to be routed here. If the remote station also uses address translation, the NAT address of the remote station must be entered here.
	Accepts the new settings and temporarily stores them.
	Edits the settings in the current line.
	Deletes entries in the current line.
	Changes the order of the created rules.

20. VPN

20.1 VPN-IPSec

20.1.1 Configuring a VPN-IPSec connection with two routers

- The settings for a VPN connection via the IPSec protocol are described below.
- From the start page, click **VPN** in the navigation bar on the left and **IPSec** in the navigation bar at the top.
- Click the button on the right to create an IPSec connection.
- The following screen appears:

The screenshot displays the mbNET web interface for configuring a VPN-IPSec connection. The left sidebar contains a navigation menu with 'VPN' highlighted. The main content area is titled 'VPN-IPSec Configuration' and 'IPSec Configuration - Edit Connection'. Below the title are four tabs: 'Connection Settings', 'Network Settings', 'Authentication', and 'Protocol options'. The 'Connection Settings' tab is selected, showing the following configuration options:

- Active:** A checkbox that is currently unchecked.
- Connection name:** An empty text input field.
- Connection type:** A dropdown menu set to 'Router <-> Router Connection'.
- Link connection:** A dropdown menu set to 'Connect immediately'. Below this dropdown is a warning message: 'One of this routers has to be set to wait mode!'.
- Peer address (IP, DNS):** An empty text input field.

At the bottom of the configuration area, there are two buttons: 'Apply Changes' (with a green checkmark icon) and 'Clear Changes' (with a red X icon). A diagram in the center of the configuration area shows two yellow routers connected by a VPN tunnel to a central 'INTERNET' cloud.

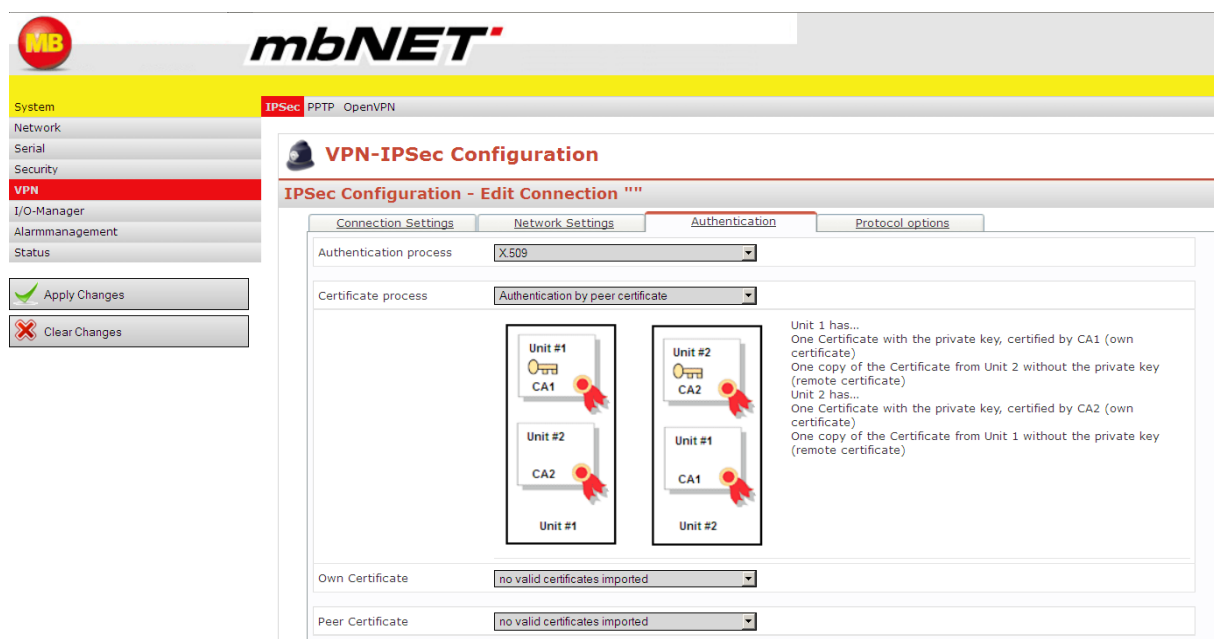
20.1.1.1 Connection settings

Tab	Label	Description
Connection Settings	Active	Check this box to activate the VPN connection.
	Connection name	Enter a name for the connection in the input field.
	Connection type	Select the connection type Router <> Router Connection or Client <> Router Connection via the drop-down field.
	Link connection (only with a router-router connection)	<p>Please note that to communicate with another router, this router must be configured for accessing the Internet and for requests from clients.</p> <p>With a router-router connection, one of the following options for establishing a connection must be selected:</p> <p>Connect immediately: A connection is established following a restart or boot routine.</p> <p>Connect on traffic The connection with the router or remote network is established in response to requests from the local network.</p> <p>Wait for incoming Connection The router on standby is the so-called VPN server. It waits for incoming connections.</p>
	Peer address (IP, DNS) (only with a router-router connection)	The appropriate peer address must be specified on the router responsible for the outgoing connections. This can be an IP address or even the DNS name under which the remote router can be reached.

20.1.1.2 Network Settings

Tab	Label	Description
Network Settings	Local network	Enter the address range of the local network in CIDR notation here. E.g. 192.168.0.0/24
	Peer network (only with a router-router connection)	Enter the address range of the local network in CIDR notation here. E.g. 192.168.10.0/24
	NAT-Traversal (only with a router-router connection)	This setting is necessary if the VPN connection is established via the Internet and natted between the LAN and WAN (NAT: Network address Translation). This setting is generally enabled.
	Permitted network for the client (only with a client-router connection)	Set the network accessed by the client here. It must be entered in CIDR notation.
	Client has a fixed IP address or name (only with a client-router connection)	If the client has a fixed static address, this address must be entered in this input field.
	Win2000 / XP Client (L2TP) (only with a client-router connection)	Set whether the client is a PC running the Windows 2000 or XP operating system here.

20.1.1.3 Authentication



Authentication

Select the **Authentication process** via the drop-down field.

Authentication by peer certificate:

The certificates can be signed by different CAs. A personal certificate+key (.p12 file) must be imported into each router. Each router must also have a copy of the respective peer certificate, naturally WITHOUT the key (.crt file).

Own Certificate: Select the router's personal certificate via the drop-down field.

Local ID: This ID is normally assigned by the certificate. This field can be left blank.

Peer Certificate: Select the peer certificate here.

Peer ID:

This ID can only be assigned by the certificate if **Authentication by peer certificate** was selected. The field can be left blank in this case. If, however, **Authentication by certificate from CA** was selected, you must specify the peer ID (**in case you want to establish the connection**).

This ID is selected when the certificate is created (see the section [Creating certificates and revocation lists using XCA](#) under the tab Subject). It is the certificate subject and must be entered as follows:

/C=country/ST=state/L=city/O=organization/OU=department/CN=certificate_name/E=email_address

If some fields on the **Subject** tab were left blank when the certificate was created, the corresponding entries must be omitted (cf. the section [Creating certificates and revocation lists using XCA](#)).

Peer Certificate:

Only if **Authentication by peer certificate** was selected. Select the corresponding certificate via the drop-down field.

Authentication by certificate from CA:

The root certificate (certificate authority, CA for short) and a personal certificate including key (.p12 file) must be imported into the router for this. (See the section System – Certificates). The remote station must have the same root certificate and a certificate signed by the CA including key.

PSK: Both keys must be known before data can be exchanged between the client and router. The longer the keys, the more secure the connection.

Only one key can be specified. Even if there are several PSK connections entered, the key for the **FIRST** connection is universally valid.

Local ID: Assign a name for your router here. This name must be communicated to the peer.

Peer ID: Enter the name of the peer here.

X.509: You can choose between two authentication processes via the drop-down field:

20.1.1.4 Protocol settings

VPN-IPSec Configuration
IPSec Configuration - Edit Connection ""

System **IPSec** PPTP OpenVPN

Network

Serial

Security

VPN

I/O-Manager

Alarmmanagement

Status

Apply Changes
 Clear Changes

Connection Settings
Network Settings
Authentication
Protocol options

Phase 1 (IKE ISAKMP)

Coding algorithm

Hash total algorithm

Lifetime of ISAKMP SA [seconds]

Aggressive Mode

Phase 2 (ESP IPSec SA)

Coding algorithm

Hash total algorithm

PFS (Perfect Forward Secrecy) active

Lifetime of IPSec SA [seconds]

Do initiate Renegotiation keys before end (rekey) active

Number of tries for connection startup [0= no limit]

Rekeymargin [seconds]

Rekeyfuzz [%]

DPD (Dead Peer Detection)

Delay [seconds]

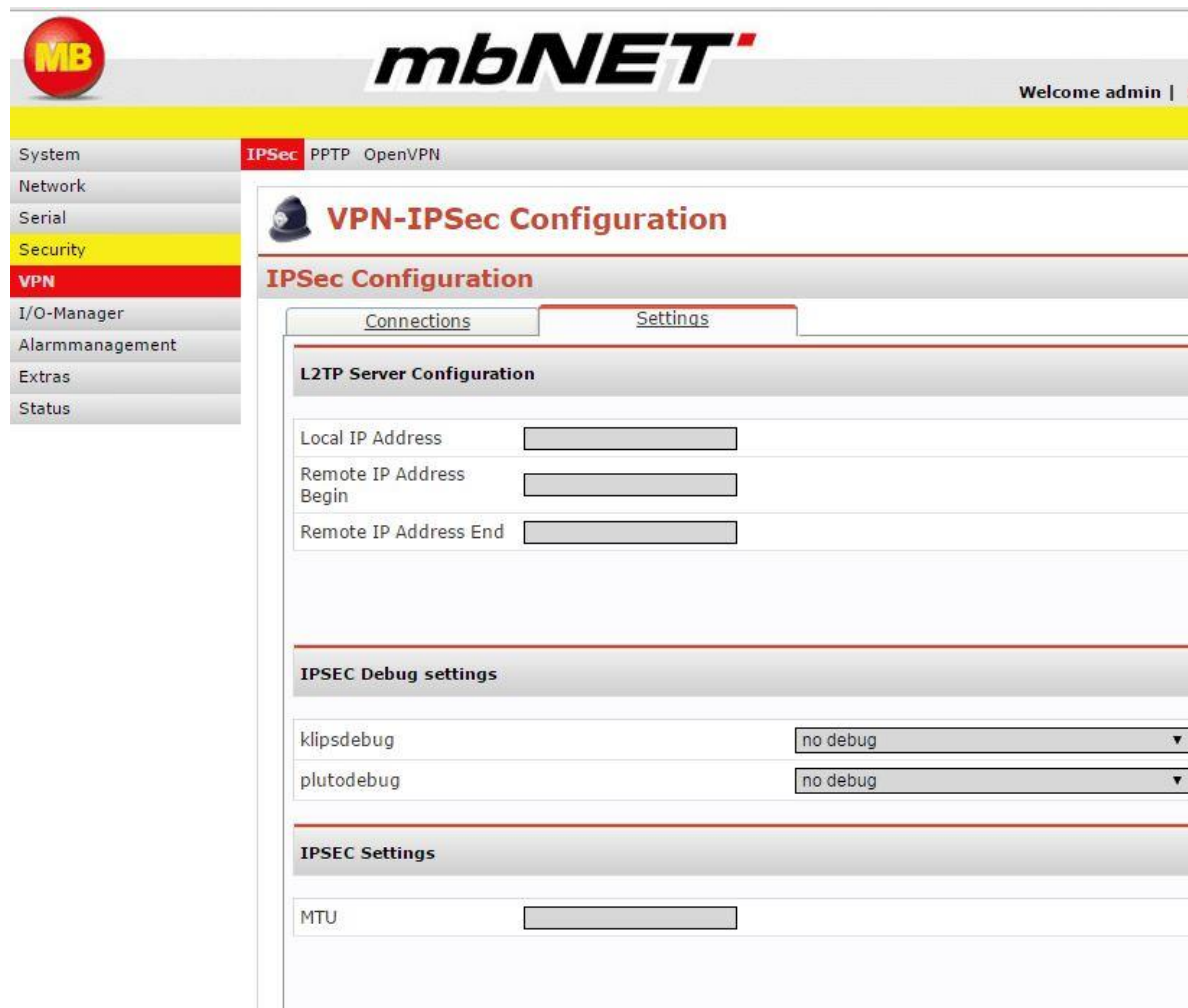
Timeout [seconds]

Action after dead peer detected

Label	Description
Protocol options	You select the coding algorithms, hash total algorithms, etc. used during the various phases on this tab.
	PFS: This setting is only supported for the router-router connection. PFS must be disabled if you want to set up a client-router connection.

20.1.1.5 L2TP Server Configuration

The L2TP server can be used for VPN-IPSec communication between the industrial router and a Windows client. The only setting required here is a freely selectable local IP address. The addresses for the clients should be from the same network (the start and end of the range are set under the IP address field). The L2TP server then works in a similar way to a DHCP server and can automatically assign the addresses from the set range to the clients dialing in.



Label	Description
Local IP address	The name or IP address to be assigned to the server during communication with the Window client must be entered here. In the example this is 192.168.0.100
Remote IP address Begin	Assignment of client IP addresses. The address range from which remote clients are assigned their IP address can be set here. In the example this is 192.168.0.130 to 192.168.0.140
Remote IP address End	

20.2 VPN - PPTP
20.2.1 Server settings

The screenshot shows the 'VPN-PPTP Configuration' interface. It has two tabs: 'Server' and 'Clients'. The 'Server' tab is active, showing the 'Server Configuration' panel. This panel includes an 'Enable' checkbox (unchecked), an 'Autoconfig' dropdown menu (set to 'no'), and several text input fields: 'Local IP Address or Range' (192.168.0.100), 'Remote IP Address or Range' (192.168.0.101-110), 'Give DNS Address to the Client' (192.168.0.100), and 'Give WINS Address to the Client' (empty). To the right is the 'Encryption Configuration' panel, which has an 'Encryption' dropdown menu (set to 'MPPE V2 All') and an 'Authentication Configuration' section with four checkboxes: 'Authentication via PAP' (checked), 'Authentication via CHAP' (unchecked), 'Authentication via MS-CHAP' (checked), and 'Authentication via MS-CHAP V2' (unchecked). A 'Save Changes' button is at the bottom right.

Label	Description
Server Configuration	
Enable	Check this box by clicking it if the industrial router is to be enabled as a VPN server.
Autoconfig	The local address of the <i>mbNET</i> will be used if you select “yes” here.
Encryption Configuration	
Encryption	Select the encryption method here via the drop-down field: None: No encryption MPPE V2 40: 40-bit encryption MPPE V2 128: 128-bit encryption MPPE V2 All: All encryption methods
Authentication Configuration	
Authentication via PAP	Select the authentication method here. The client keeps sending the username/password combination to the host until it accepts or rejects authentication of the client.
Authentication via CHAP	Select the authentication method here. This authentication method is controlled by the host. When a client dials in, it is prompted by the host to authenticate itself. The client sends username/password using MD5 encryption. The authentication is accepted if the user data sent matches the data on the host. If not, it is rejected. If the authentication is accepted, the user data is periodically checked during the connection.
Authentication via MS-CHAP	Proprietary authentication protocol developed by Microsoft.
Authentication via MS-CHAP V2	Proprietary authentication protocol developed by Microsoft.

20.2.2 Client settings

IPSec **PPTP** OpenVPN

VPN-PPTP Configuration

PPTP Configuration

Server | Clients

Client Configuration

Enable	Name	Host Name or IP	Local IP	Remote IP	
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

Label	Description
Enable	Check this box by clicking it if the industrial router is to be enabled as a VPN client.
Name	Enter a name for the client here.
Host Name or IP	Enter the name or IP address under which the client accesses the server here. Example 123456789@mbNET.mymbnet.biz or 80.187.33.55
Local IP	This entry is optional. If the server is not configured to assign an IP address to the client, the client can request the IP address entered here. The settings are generally made on the VPN server. This setting is for compatibility with other routers.
Remote IP	Enter the network address of the server in CIDR notation here (e.g. 192.168.0.0/24) in order to have a route into the server network.

20.3 VPN – OpenVPN

20.3.1 Basics about OpenVPN

-OpenVPN basically works with two tunnel IP addresses, i.e. each connection has two IP addresses via which the data traffic is processed.

- Depending on the authentication method, OpenVPN either works in point-to-point mode (with static key or no authentication) or in server/client mode (with X.509 certificates).

- OpenVPN can use three different authentication methods:

- **None:** No certificate or key is needed. Used primarily for testing the connection. The tunnel data is also **NOT** encrypted.
- **Static key:** A 1024-bit key as required by each peer is generated for the connection. Similar to the password.
- **Certificates, X.509:** The following certificate variants are distinguished:
 - Each subscriber needs the same root CA and a personal certificate signed by the root CA.
 - Like 1, but with additional username/password verification.
 - Like 2, but without a personal certificate. In other words, subscribers only need a root CA and username/password.

- OpenVPN can use an http proxy server as the outgoing connection. This is important for integration into existing corporate networks with an Internet connection.

- The transmission protocol setting (UDP or TCP) can be freely selected with OpenVPN. The same applies to the port numbers to be used for the transmission protocol.

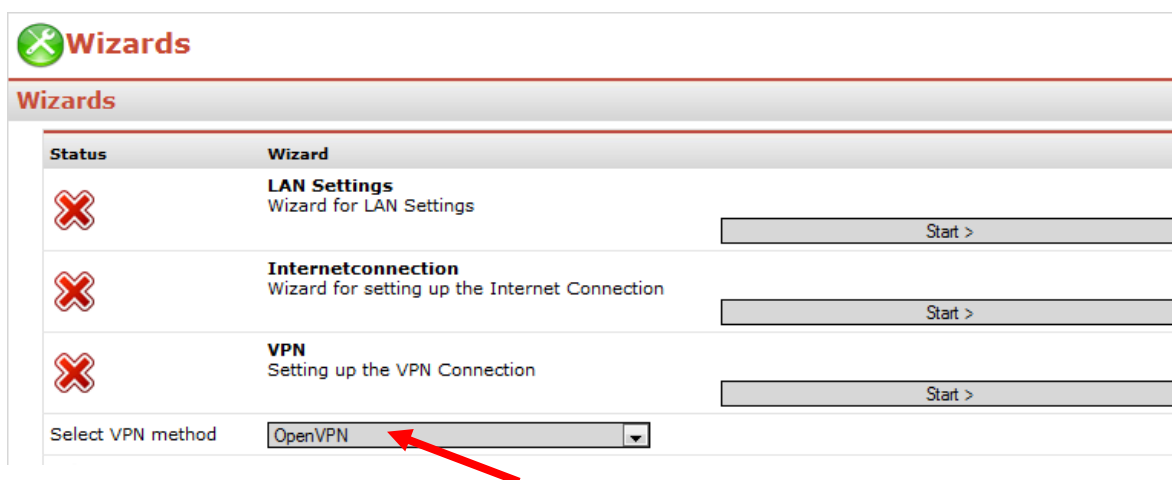
- The settings for various OpenVPN connection scenarios are described below.
- From the start page, click **VPN** in the navigation bar on the left and **OpenVPN** in the navigation bar at the top.
- Click the button on the right to create an OpenVPN connection.



20.3.2 Connection scenarios

20.3.2.1 Client – router

- ❑ **The connection wizard** helps you to configure your connections quickly and easily. To access the wizard, click the “Wizards” link in the top right of the web interface. If you have disabled the auto launch function for the wizard, click the Start button for the wizard for VPN connections.
- ❑ Please note that you must first select “OpenVPN” in the menu under the Start button for the VPN wizard. You must then click “Save Changes” and “Apply Changes” so that you can configure a connection with OpenVPN.



- ❑ Select the option “Connection between Network client and **mbNET**”.
- ❑ Next select the static key. If you have not yet created a static key, you can use the key created by **mbNET**. Click „Next”.
- ❑ Clicking “Next” completes the configuration of the connection. Click “Finish” to apply your settings. You must have OpenVPN installed on your computer to establish a connection. You can find out more about this in section 18.2.1.3 “Configuring an OpenVPN Windows client”.
- ❑ Select the option “Connection between Network client and **mbNET**”.
- ❑ Next select the static key. If you have not yet created a static key, you can use the key created by **mbNET**. Click „Next”.
- ❑ Clicking “Next” completes the configuration of the connection. Click “Finish” to apply your settings. You must have OpenVPN installed on your computer to establish a connection. You can find out more about this in section 18.2.1.3 “Configuring an OpenVPN Windows client”.



20.3.2.1.1 Connection Settings

Connection Settings
Network Settings
Authentication
Protocol options

Active

Connection name

Connection type

VPN

<u>Connection Settings</u>	
Label	Description
Active	Check this box to activate the OpenVPN connection.
Connection name	Enter a name for the connection in the input field.
Connection type	Select the connection type Client <> Router Connection via the drop-down field.



Only one “client to network” connection can be created. Depending on the authentication method, the client receives an IP address from a defined range or each subscriber specifies its requested address.

Example:

```
Client PC          mbNET
[10.1.0.6] VPN - TUNNEL [10.1.0.5] <> ROUTING <> LAN [192.168.0.100]
```

20.3.2.1.2 Network Settings (no authentication or static key)

Connection Settings	Network Settings	Authentication	Protocol options
Local network	<input type="text" value="10.1.0.5"/>		
Peer network	<input type="text" value="10.1.0.6"/>		
NAT-Traversal	<input type="checkbox"/>		

Network Settings	
Label	Description
Local IP address	Enter the IP address of the local VPN tunnel end point here, e.g. 10.1.0.5
Peer IP address	Enter the IP address of the peer VPN tunnel end point here, e.g. 10.1.0.6
NAT-Traversal	All packets coming into the LAN receive the sender IP address of the mbNET. Although this means that it is then no longer possible to distinguish between senders in the LAN, the LAN subscribers do NOT have to have the mbNET entered as a gateway.

With authentication without certificates, only one IP channel (local IP address and peer IP address) can be specified per connection entry.



With manual configuration of the VPN client, the setting “Local IP address” and “Peer IP address” must be reversed accordingly on the client.

20.3.2.1.3 Authentication with certificates

Connection Settings	Network Settings	Authentication	Protocol options
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Client IP address pool <input type="text" value="10.1.0.0/24"/></p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Client NAT behind the local network (The client will send the IP of the gateway for traffic through the local network) <input type="checkbox"/></p> </div>			

Tag	Label	Description
Network Settings	Client IP address pool	With authentication with certificates, multiple clients can dial into the server simultaneously and are automatically assigned an IP address from the "Client IP address pool". Enter the address range in CIDR notation. E.g. 10.1.0.0/24 (corresponds to the subnet mask: 255.255.255.0).
	Client NAT behind the local network (The client will send the IP of the gateway for traffic through the local network)	The option "Client NAT behind the local network (The client will send the IP of the gateway for traffic through the local network)" assigns all packets coming into the LAN the sender IP address of the mbNET. Although this means that it is then no longer possible to distinguish between senders in the LAN, the LAN subscribers do NOT have to have the mbNET entered as a gateway. NOTE - this can become confusing with multiple clients.



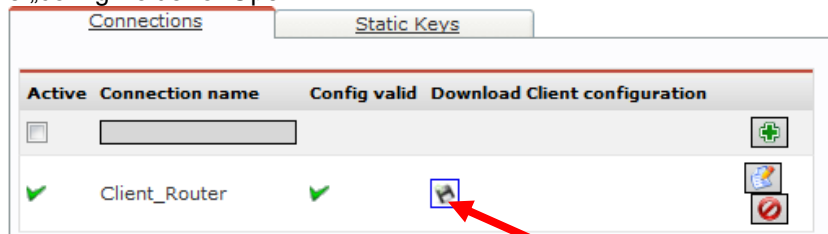
No network settings need to be made on the client side. The server automatically passes all the information to the client in this mode.

20.3.2.2 Configuring an OpenVPN Windows client

To be able to use the OpenVPN Windows client, it must first be installed on the computer. The installation routine can be downloaded from

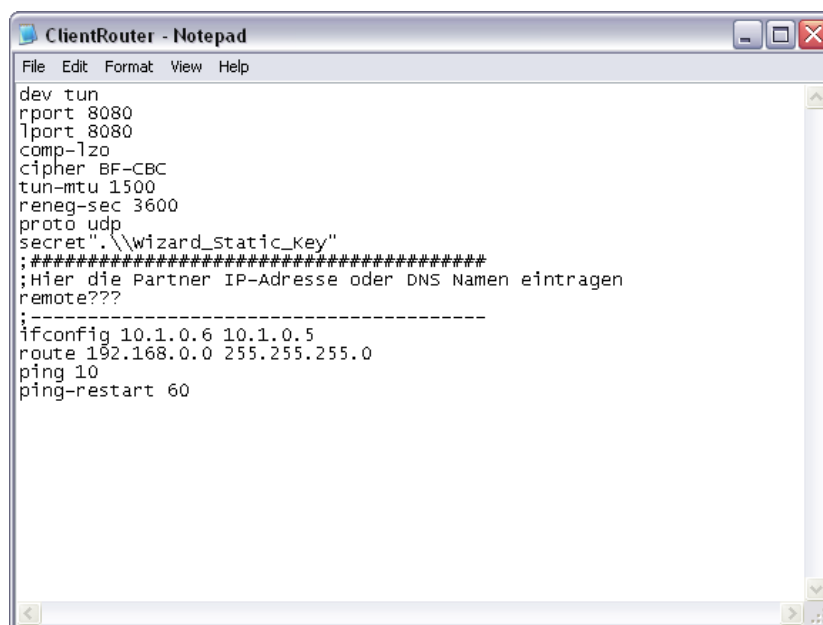
<http://openvpn.net/index.php/open-source/downloads.html> .

The corresponding client setting can be downloaded from the mbNET via the “Download” link (see arrow). Save this file in the „config“ folder of OpenVPN.



With manual configuration of the VPN client, the setting “Local IP address” and “Peer IP address” must be reversed accordingly on the client.

The downloaded file corresponds to the settings for OpenVPN for Windows. Open the settings file using a text editor to make the additional settings:



```

ClientRouter - Notepad
File Edit Format View Help
dev tun
rport 8080
lport 8080
comp-lzo
cipher BF-CBC
tun-mtu 1500
reneg-sec 3600
proto udp
secret "\\wizard_static_key"
;#####
;Hier die Partner IP-Adresse oder DNS Namen eintragen
remote???
:-----
ifconfig 10.1.0.6 10.1.0.5
route 192.168.0.0 255.255.255.0
ping 10
ping-restart 60

```

20.3.2.2.1 No authentication

```

dev tun
rport 8080
lport 8080
comp-lzo
cipher BF-CBC
tun-mtu 1500
reneg-sec 3600
proto udp
secret ".\\wizard_static_key"
;#####
;Hier die Partner IP-Adresse oder DNS Namen eintragen
remote 80.23.45.123
;-----
ifconfig 10.1.0.6 10.1.0.5
route 192.168.0.0 255.255.255.0
ping 10
ping-restart 60
  
```

To be able to establish an OpenVPN connection with your **mbNET** without encryption, you just need to delete the `????` after "remote". Next enter the public IP address of the **mbNET** (the address accessible via the Internet) or use MB Connect Line's DynDNS service. You must then enter the name specified under **Network DynDNS**. (E.g. remote 0123456789.mbNET.mymbnet.biz)

20.3.2.2.2 Authenticating a Windows client with static key

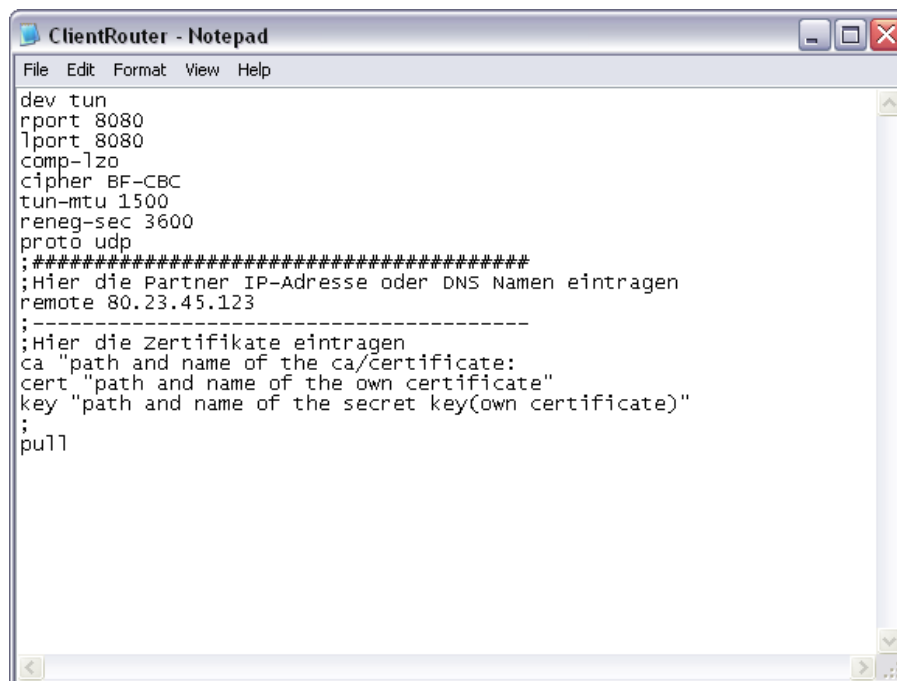
```

dev tun
rport 8080
lport 8080
comp-lzo
cipher BF-CBC
tun-mtu 1500
reneg-sec 3600
proto udp
secret C:\\Programme\\openVPN\\config\\clientkey.txt
;#####
;Hier die Partner IP-Adresse oder DNS Namen eintragen
remote 80.23.45.123
;-----
ifconfig 10.1.0.6 10.1.0.5
route 192.168.0.0 255.255.255.0
ping 10
ping-restart 60
  
```



If you have decided on the method with the static key, you must make a private (secret) entry in addition to entering the IP address (see arrow). **Note** that you must always use two backslashes in the path name.

20.3.2.2.3 Authenticating a Windows client with certificates



```
ClientRouter - Notepad
File Edit Format View Help
dev tun
rport 8080
lport 8080
comp-lzo
cipher BF-CBC
tun-mtu 1500
reneg-sec 3600
proto udp
;*****
;Hier die Partner IP-Adresse oder DNS Namen eintragen
remote 80.23.45.123
;-----
;Hier die Zertifikate eintragen
ca "path and name of the ca/certificate:"
cert "path and name of the own certificate"
key "path and name of the secret key(own certificate)"
;
pull
```

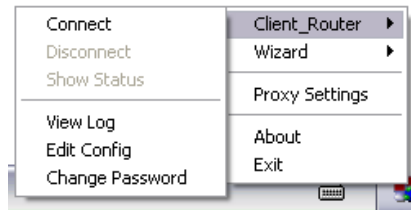
Change the indicated options as appropriate to your circumstances. Note that you must always use **two backslashes** in the path name and that you need the key of your personal certificate for the directive "key".

20.3.2.2.4 Starting the OpenVPN connection

After completing the configuration, you can right-click the .ovpn file or start the connection via the graphical interface in the toolbar as shown below.

20.3.3 Router-Router

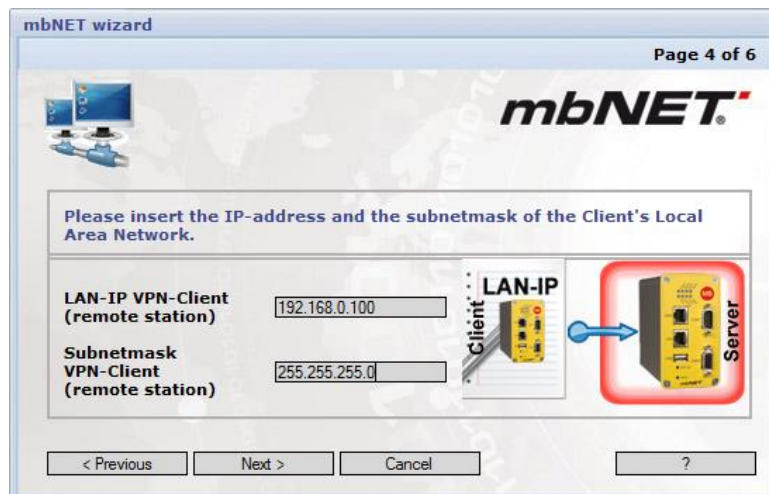
20.3.3.1 Using the connection wizard



- ❑ **Using the connection wizard:** Click the “Wizards” link in the top right of the web interface. Then click the Start button for the wizard for VPN connections, followed by “Next”.
- ❑ Select “**Connection between 2 Networks**”.



- ❑ Select the VPN server in the following window and click “Next”.
- ❑ You must then specify the local network address and subnet mask of the VPN client.



- ❑ Enter the key of your choice in the following window or use the key generated by mbNET.
- ❑ Click “Finish” to complete the configuration and accept your settings. Repeat this configuration with the VPN client. This time, however, you must select the VPN client instead of the VPN server.

Connection Settings
Network Settings
Authentication
Protocol options

Active

Connection name

Connection type

Link connection

One of this routers has to be set to wait mode!

Tab	Label	Description
Connection Settings	Active	Check this box to activate the OpenVPN connection.
	Connection name	Enter a name for the connection in the input field.
	Connection type	Select the connection type via the drop-down field.

A “network to network” connection can be created here. Depending on the authentication method, the client receives an IP address from a defined range or each subscriber specifies its requested address.

Example:

```
LAN                               mbNET Client                               mbNET Server LAN
[192.168.99.100]<>ROUTING<>[10.1.0.2] VPN - TUNNEL [10.1.0.1]<>ROUTING<>[192.168.0.100]
```

Link connection

Connect immediately

Start with an active internet connection

Wait for incoming Connection

Connect when input 1 has High-signal

Connect when input 2 has High-signal

Connect when input 3 has High-signal

Connect when input 4 has High-signal

Connect when input 1 has High-signal, disconnect at Low-Signal

Connect when input 2 has High-signal, disconnect at Low-Signal

Connect when input 3 has High-signal, disconnect at Low-Signal

Connect when input 4 has High-signal, disconnect at Low-Signal

Connect while pushing dialout button

If „Wait for incoming Connection“ was selected, then this mbNET is in Server Mode and is called “**Server**” in the further documentation, otherwise if “Connect immediately” was selected, then the mbNET is in Client Mode and is called “**Client**”.

20.3.3.2 Server – no authentication or static key

Connection Settings	Network Settings	Authentication	Protocol options
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Local IP address <input type="text" value="10.1.0.1"/></p> <p>Peer IP address <input type="text" value="10.1.0.2"/></p> <p>Local network <input type="text" value="192.168.0.0/24"/></p> <p>Peer network <input type="text" value="192.168.99.0/24"/></p> </div>			

Tab	Label	Description
Network Settings	Local IP address	Enter the IP address of the local VPN tunnel end point here, e.g. 10.1.0.1
	Peer IP address	Enter the IP address of the peer VPN tunnel end point here, e.g. 10.1.0.1
	Local network	Enter your network address in CIDR notation here (192.168.0.0/24).
	Peer network	Enter the network address of your peer in CIDR notation here (192.168.99.0/24).

With authentication without certificates, only one IP channel (local IP address and peer IP address) can be specified per connection entry.



With manual configuration of the VPN client, the setting “Local IP address” and “Peer IP address” must be reversed accordingly on the client.

20.3.3.3 Server – authentication with certificates

With authentication with certificates, multiple clients can dial into the server simultaneously and are automatically assigned an IP address from the “Client IP address pool”. There are two different operating modes in server mode with certificates.

20.3.3.3.1 Single client: Only one client can dial in

Connection Settings	Network Settings	Authentication	Protocol options
Client IP address pool: 10.1.0.0/24			
Local network: 192.168.0.0/24			
Multi peer mode: no			
Peer network: 192.168.99.0/24			

Tab	Label	Description
Network Settings	Client IP address pool	With authentication with certificates, multiple different clients can dial into the server (not simultaneously) and are automatically assigned an IP address from the “Client IP address pool”. Enter the address range in CIDR notation. E.g. 10.1.0.0/24
	Local network	Enter the address range of the local network in CIDR notation here. E.g. 10.1.0.2/24
	Multiple peers with different network addresses can establish a VPN connection.	“no” selected Each client is assigned the peer network address range, which means that simultaneous client logins make no sense here.
	Peer network	Enter the network address of your peer in CIDR notation here (192.168.99.0/24).

No network setting is needed on the client because it is sent to the client by the server.



The local network and the peer network must be specified. OpenVPN then creates the necessary routing entries using these entries.

20.3.3.3.2 Multi-client: Multiple clients can dial in

Connection Settings
Network Settings
Authentication
Protocol options

Client IP address pool

Local network

Multi peer mode

Peer Name	Peer network	
<input style="width: 80%;" type="text"/>	<input style="width: 80%;" type="text"/>	
ovpn	192.168.99.0/24	
Client1	192.168.98.0/24	
Client2	192.168.97.0/24	

Tab	Label	Description
Network Settings	Client IP address pool	With authentication with certificates, multiple different clients can dial into the server simultaneously and are automatically assigned an IP address from the "Client IP address pool". Enter the address range in CIDR notation. E.g. 10.1.0.0/24
	Local network	Enter the address range of the local network in CIDR notation here. E.g. 10.1.0.2/24
	Multiple peers with different network addresses can establish a VPN Connection.	"yes" selected With authentication with certificates and this operating mode, multiple clients can dial into the server simultaneously and are automatically assigned an IP address from the "Client IP address pool".
	Peer Name	The local network (top) and the peer network must be specified. Each client is assigned a network in the list below these. Depending on the authentication setting (with certificate name or username), the CN (common name in the certificate) or username will be used. OpenVPN creates an appropriate routing entry for the client currently dialing in.



No network setting is needed on the client because it is sent to the client by the server.

20.3.3.4 Client authentication: No or static key

Connection Settings	Network Settings	Authentication	Protocol options
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Local IP address <input type="text" value="10.1.0.2"/></p> <p>Peer IP adress <input type="text" value="10.1.0.1"/></p> </div>			
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Local network <input type="text" value="192.168.0.0/24"/></p> </div>			
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Peer network <input type="text" value="192.168.99.0/24"/></p> </div>			
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Do NAT for all outgoing traffic <input type="checkbox"/></p> </div>			

Tab	Label	Description
Network Settings	Local IP address	Enter the IP address of the local VPN tunnel end point here, e.g. 10.1.0.2
	Peer IP address	Enter the IP address of the peer VPN tunnel end point here, e.g. 10.1.0.1
	Local network	Enter your network address in CIDR notation here (192.168.0.0/24).
	Peer network	Enter the network address of your peer in CIDR notation here (192.168.99.0/24).
	Do NAT for all outgoing traffic	This option was introduced for compatibility with mdex. It replaces the sender IP address with the current Internet IP address.



With authentication without certificates, only one IP channel can be specified per connection entry (local IP address and peer IP address).

The setting “**Local IP address**” and “**Peer IP address**” from the server must be reversed accordingly on the client.

20.3.3.5 Client authentication: With certificates

Connection Settings	Network Settings	Authentication	Protocol options
<div style="border: 1px solid gray; padding: 10px;"> <p>Do NAT for all outgoing traffic <input type="checkbox"/></p> </div>			

Tab	Label	Description
Network Settings	Do NAT for all outgoing traffic	This option was introduced for compatibility with mdex. It replaces the sender IP address with the current Internet IP address.



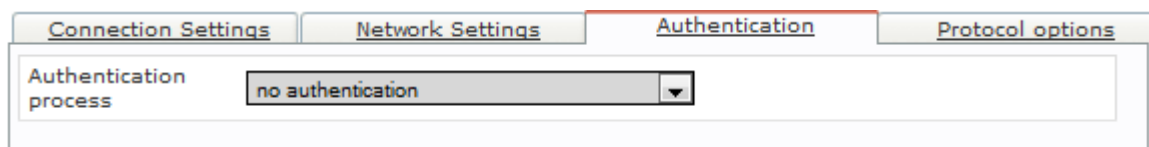
No network setting is needed on the client because it is sent to the client by the server.

20.3.4 Authentication

OpenVPN offers three fundamentally different authentication methods.

- None: no certificate or key is needed. Used primarily for testing the connection. The tunnel data is also NOT encrypted.
- Static key: a key as required by each peer is generated for the connection. Similar to the password.
- Certificates, X.509: the following three certificate variants are distinguished:
 - Each subscriber needs the same root CA and a personal certificate signed by the root CA.
 - Like 1, but with additional username/password verification.
 - Like 2, but without a personal certificate. In other words, subscribers only need a root CA and username/password.

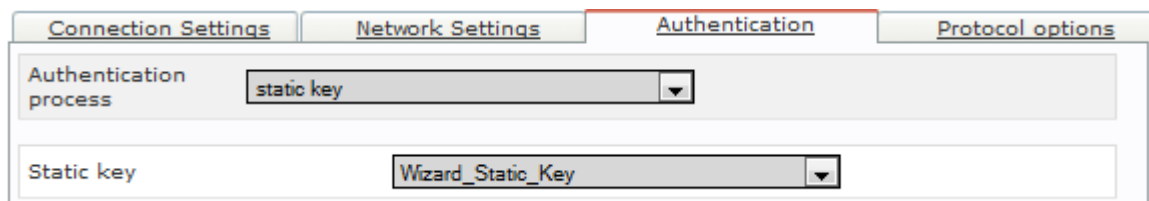
20.3.4.1 No authentication



The screenshot shows the 'Authentication' tab of the configuration wizard. The 'Authentication process' dropdown menu is set to 'no authentication'.

This setting should primarily be used for test purposes. It provides a quick and easy way of testing the connection with a peer (e.g. whether the correct ports are enabled). The data is sent UNENCRYPTED in this mode.

20.3.4.2 Authentication with static key



The screenshot shows the 'Authentication' tab of the configuration wizard. The 'Authentication process' dropdown menu is set to 'static key', and the 'Static key' dropdown menu is set to 'Wizard_Static_Key'.

With symmetric encryption, authentication and encryption/decryption of the data is performed using one and the same key (static key). The advantage of symmetric encryption is its speed: encryption and decryption take much less time than with asymmetric encryption since the symmetric key is secure from a size of 90 bits.

The asymmetric key, on the other hand, must be at least 1024 bits. The disadvantage of symmetric encryption is that stations need to exchange keys. Each subscriber must obtain the key in a secure manner. A previously imported or generated key can be selected in the screen shown above.

20.3.4.2.1 Key management

You can import a key or generate it yourself. All imported keys can be downloaded as a copy under “Download”.

Connections
Static Keys

generate new static key

Name for this static key

import new static key

Choose static key file

list of imported static keys

Name	Download
Wizard_Static_Key	<input type="button" value="Download"/> <input style="float: right;" type="button" value="Delete"/>
Static_key_Client1	<input type="button" value="Download"/> <input style="float: right;" type="button" value="Delete"/>
Static_key_Router	<input type="button" value="Download"/> <input style="float: right;" type="button" value="Delete"/>

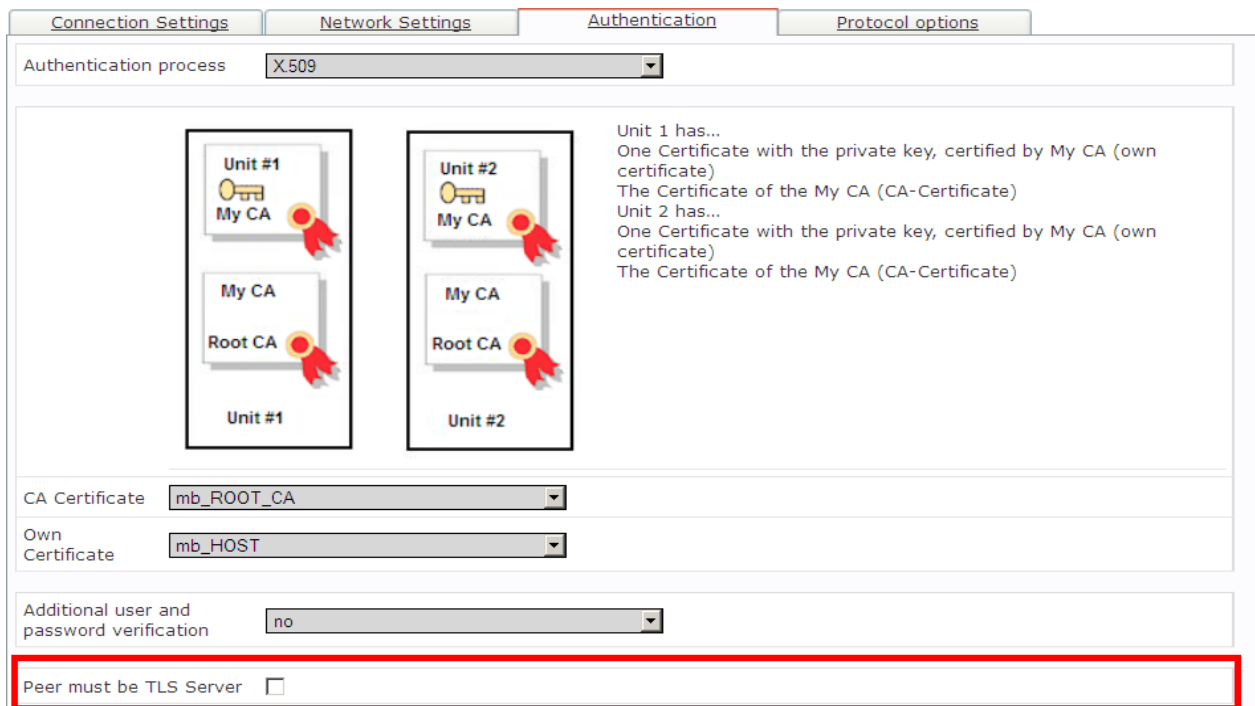
Tab	Label	Description
Static Keys	Name for this static key	Enter the name of the key to be generated here.
	Choose static key file	A key previously generated on another system can be imported here.

20.3.4.3 Authentication with certificates

There are three different types of authentication with certificates:

1. Each subscriber needs the same root CA and a personal certificate signed by the root CA.
2. Like 1, but with additional username/password verification.
3. Like 2, but without a personal certificate. In other words, the stations only need a root CA and username/password.

20.3.4.3.1 Authentication with CA certificate and own certificate



Tab	Label	Description
X.509 authentication	CA Certificate	This is the root certificate (root CA). All other certificates must come from this certificate.
	Own Certificate	You use this certificate to authenticate yourself to your VPN peer.
	Additional user and password verification	Additional user data may be required from a client dialing in. Please note that this user data must be entered in the VPN server under <i>System User</i> .
	User	Enter the user data of the VPN server (from the System User menu) here.
	Use only CA and User/password for client verification	With this option, you authenticate yourself using the CA certificate and the user data of the VPN server (from the System User menu) only.
	Peer must be TLS Server	This is an additional security option. The "server certificate" must include the extension <code>nsCert-Type=server</code> (see section Creating certificates).



20.3.4.3.2 Authentication with CA certificate and own certificate and user/password

This setting varies depending on the mode.

20.3.4.3.3 Server

Connection Settings
Network Settings
Authentication
Protocol options

Authentication process: X.509

Unit 1 has...

- One Certificate with the private key, certified by My CA (own certificate)
- The Certificate of the My CA (CA-Certificate)

Unit 2 has...

- One Certificate with the private key, certified by My CA (own certificate)
- The Certificate of the My CA (CA-Certificate)

CA Certificate: mb_ROOT_CA

Own Certificate: mb_HOST

Additional user and password verification: yes

Use only CA and User/password for client verification:

Tab	Label	Description
X.509 authentication (server)	CA Certificate	This is the root certificate (root CA). All other certificates must come from this certificate.
	Own Certificate	You use this certificate to authenticate yourself to your VPN peer.
	Additional user and password verification	Additional user data may be required from a client dialing in. Please note that this user data must be entered in the VPN server under <i>System User</i> .
	Use only CA and User/password for client verification	With this option, you authenticate yourself using the CA certificate and the user data of the VPN server (from the System User menu) only.

20.3.4.3.4 Client

Connection Settings
Network Settings
Authentication
Protocol options

Authentication process: X.509

Unit 1 has...

- One Certificate with the private key, certified by My CA (own certificate)
- The Certificate of the My CA (CA-Certificate)

Unit 2 has...

- One Certificate with the private key, certified by My CA (own certificate)
- The Certificate of the My CA (CA-Certificate)

CA Certificate: mb_ROOT_CA

Own Certificate: mb_HOST

Additional user and password verification: yes

User:

Password:

Do not use my own certificate for verification. Use only CA and User/password verification:

Peer must be TLS Server:

Tab	Label	Description
X.509 authentication (client)	CA Certificate	This is the root certificate (root CA). All other certificates must come from this certificate.
	Own Certificate	You use this certificate to authenticate yourself to your VPN peer.
	Additional user and password verification	Additional user data may be required from a client dialing in. Please note that this user data must be entered in the VPN server under <i>System User</i> .
	User	Enter the user data of the VPN server (from the System User menu) here.
	Do not use my own certificate for verification. Use only CA and User/password for verification	With this option, you authenticate yourself using the CA certificate and the user data of the VPN server (from the System User menu) only.
	Peer must be TLS Server	This is an additional security option. The “server certificate” must include the extension <code>nsCertType=server</code> (see section Creating certificates).

20.3.5 Inactivity settings

Connection Settings	Network Settings	Authentication	Protocol options
Active <input checked="" type="checkbox"/>			
Connection name <input type="text" value="Test_serverroom"/>			
Connection type <input type="text" value="Router <> Router Connection"/>			
Link connection <input type="text" value="Connect while pushing dialout button"/>			
One of this routers has to be set to wait mode!			
Peer address (IP, DNS) <input type="text" value="321.mbNET.mymbnet.biz"/>			
Close connection after ... seconds inactivity <input type="text" value="3600"/>			

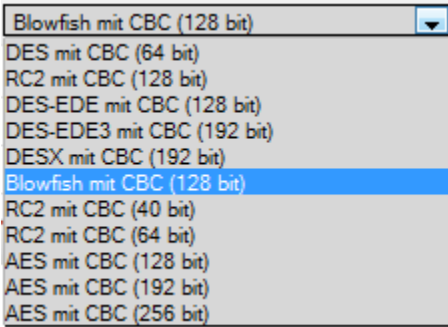
If the OpenVPN connection is to be started via a digital input or the dial-out button, the connection is automatically dropped after a defined time without any data traffic.

20.3.6 Protocol options

If the OpenVPN connection is to be started via a digital input or the dial-out button, the connection is automatically dropped after a defined time without any data traffic.

OpenVPN offers a range of additional settings. An overview described is shown on the next page.

Connection Settings	Network Settings	Authentication	Protocol options
Networkadapter			
Adaptertype		tun	
Protocol			
Encryption Method		Blowfish mit CBC (128 bit)	
Protocol		udp	
local port		1194	
peer port		1194	
Misc			
Bind the local IP-address and port		<input checked="" type="checkbox"/>	
Allow the peer to change the IP-address dynamically		<input type="checkbox"/>	
LZO compress active		<input checked="" type="checkbox"/>	
Ping interval [seconds]		10	
Ping restart [seconds]		60	
MTU [bytes]		1500	
Fragment the UDP packets in... [bytes]			
Regenerate a new key after... [seconds]		3600	
Send more Information to the System Protocol		<input checked="" type="checkbox"/>	
HTTP Proxy			
Enable connection through a HTTP proxy		<input type="checkbox"/>	
HTTP proxy name			
HTTP proxy port		8080	
HTTP proxy username			
HTTP proxy password			

Tab	Label	Description
Protocol options	Encryption Method	 <p>This setting must be the same on the peers.</p>
	Protocol	UDP or TCP can be selected. The default setting is UDP. If the http proxy is selected, TCP is automatically valid.
	local/peer port	OpenVPN communication is conducted via the set ports. These ports generally have the same settings. The default port is 1194.
	Bind the local IP address and port.	OpenVPN cannot change the ports dynamically while the connection is active.
	Allow the peer to change the IP address dynamically	This option allows the VPN peer to change its IP address while the connection is active.
	LZO compress active	Compression method of OpenVPN.
	Ping interval [seconds]	A ping is sent to the VPN peer if the OpenVPN tunnel has not been used for n seconds.
	Ping restart [seconds]	The tunnel is restarted if the VPN peer does not respond to the ping within n seconds or no data packet is received.
	MTU [bytes]	The default MTU size is 1500 bytes.
	Fragment the UDP packets in ... [bytes]	Packets bigger than n bytes will be fragmented.
	Regenerate a new key after ... [seconds]	A new key will be generated after n seconds. This is set to 3600 seconds by default.
	Send more Information to the System Protocol	This corresponds to the “verb 3” setting of OpenVPN. The default is „off“.
	Enable connection through a HTTP proxy	You must check this box if you want to establish your connection with the Internet via an http proxy server.
	HTTP proxy name	Enter the IP address or DNS name of the proxy server here.
	HTTP proxy port	Enter the port via which your proxy server accepts requests here (e.g. 8080 or 3128).
	HTTP proxy username	If your proxy server requests authentication, enter a valid username and the associated password.

21. I/O Manager

The I/O Manager integrated in the router performs the following functions:

- Displays PLC variables
- Reads variables from the PLC and saves them to the USB stick at a set interval (logging).
- Places the logged archives (GZIP) on an external FTP server at a fixed interval.

Variables of the type flags, times, counters, inputs, outputs, data blocks and peripherals can currently be read from an S7 controller via RFC1006. The PLC can communicate directly with the router via its Ethernet interface or via the MPI/PROFIBUS interface of the router.

Limits:

- Max. 4 connections to the controllers
- Max. 256 tags (variables) per connection
- The maximum size of a tag is one DWORD (32 bits)

21.1 Configuring the connection

If using the MPI/PROFIBUS interface of the router, the RFC1006 protocol must first be activated for this interface.

The screenshot shows the mbNET web interface. On the left is a navigation menu with items: System, Network, Serial (highlighted in red), Security, VPN (highlighted in yellow), I/O-Manager, Alarmmanagement, and Status. The main content area is titled 'Serial COM2' and shows configuration for 'COM2'. The 'Interface Type' is 'MPI/PROFIBUS'. The 'Protocol' is set to 'MPI/PROFIBUS Network Driver'. The 'Enable RFC1006' checkbox is checked. The 'Own station address' is '0'. The 'Enable RFC1006 Routing' checkbox is unchecked. The 'Station address of the routing gateway' is '2'. The 'Protocol' for the lower section is 'TCP' and the 'Port' is '7002'. The 'Enable Ports through firewall' checkbox is unchecked. A 'Save Changes' button is at the bottom right.

Interface Type	MPI/PROFIBUS
Protocol	MPI/PROFIBUS Network Driver
Enable RFC1006	<input checked="" type="checkbox"/>
Own station address	0
Enable RFC1006 Routing	<input type="checkbox"/>
Station address of the routing gateway	2
Protocol	TCP
Port	7002
Enable Ports through firewall	<input type="checkbox"/>

Save Changes

21.1.1 Creating the PLC connection

Servers		Logging	
Enable	Driver	Name	Description
<input type="checkbox"/>	S7_ISOTCP	SPS1	TestSPS

The "Name" field must not contain any control characters or spaces. Click the „+“ button after entering the data.

Server Configuration

Server Configuration - Edit Server "S7_ISOTCP SPS1"

Enable	<input checked="" type="checkbox"/>
Driver	<input type="text" value="S7_ISOTCP"/>
Name	<input type="text" value="SPS1"/>
Description	<input type="text" value="TestSPS"/>
PLC IP-Address	<input type="text" value="192.168.0.100"/>
PLC Slot-Address	<input type="text" value="2"/>










If using the MPI/PROFIBUS interface, the IP of the router's LAN interface must be entered in the PLC IP address field. Otherwise the IP address of the PLC. The slot address is the bus address with MPI/PROFIBUS communication and, in the case of direct Ethernet communication, the slot space of the PLC on the rack (generally two).

21.1.1.1 Creating the tags

Tags can be added if there is at least one PLC connection created.
The following address syntax must be used for this driver:

Tag Configuration

I/O Manager Tags

Enable	Server	Address	Display Value	Description	Interval [x 100ms]	Logging	
<input type="checkbox"/>	SPS1		BIN			<input type="checkbox"/>	
<input checked="" type="checkbox"/>	SPS1	Z1	DEZ	Counter1	5	<input checked="" type="checkbox"/>	 
<input checked="" type="checkbox"/>	SPS1	T1	DEZ	Time1	6	<input checked="" type="checkbox"/>	 
<input checked="" type="checkbox"/>	SPS1	DB1.DBD4	FLOAT	Temperature	10	<input checked="" type="checkbox"/>	 
<input checked="" type="checkbox"/>	SPS1	MB0	BIN	Clock pulse1	5	<input checked="" type="checkbox"/>	 

- DBx.DBXy.z = data block x, data bit y.z, BOOL
- DBx.DBBy = data block x, data byte y, BYTE
- DBx.DBWy = data block x, data word y, WORD
- DBx.DBDy = data block x, data double word y, DWORD
- Fy.z = flag bit y.z, BOOL
- FBy = flag byte y, BYTE
- FWy = flag word y, WORD
- FDy = flag double word y, DWORD
- Iy.z = input bit y.z, BOOL
- IBy = input byte y, BYTE
- IWy = input word y, WORD
- IDy = input double word y, DWORD
- Oy.z = output bit y.z, BOOL
- OBy = output byte y, BYTE
- OWy = output word y, WORD
- ODy = output double word y, DWORD
- Ply.z = peripheral input bit y.z, BOOL
- PIBy = peripheral input byte y, BYTE
- PIWy = peripheral input word y, WORD
- PIDy = peripheral input double word y, DWORD
- Ty = Timer y, TIMER
- Cy = Counter y, COUNTER

Display Value This format is used for the status display and in the logging data.

Description Free label field.

Interval [x 100ms] this tag is read from the PLC during this interval.

Logging This tag is enabled for logging if this option is checked. The tag is only displayed on the status display if this option is not checked.

21.2 Configuring the logging function

The logging function can be configured on the second tab under Server Configuration. The logging function applies to all PLC connections.

A storage medium must be inserted into the USB socket for the logging function. This can be e.g. a USB stick.

The screenshot shows the 'Server Configuration' web interface. It has two tabs: 'Servers' and 'Logging'. The 'Logging' tab is active. Under 'Logging Configuration', there are two input fields: 'Interval [s]' with the value '60' and 'Max archive period time [h]' with the value '0'. Below this is the 'FTP Upload Configuration' section with four input fields: 'Interval [min]' with '30', 'Server address' with 'ftp://mysite.com', 'Server Username' with 'ftpupload', and 'Server password' with masked characters. A 'Save Changes' button is at the bottom right.

Interval [s]

The tags are written to the storage medium at the specified interval.

Max archive period time [h]

The log file is archived and a new log file is started at the latest after the time in seconds set here.

FTP Upload Configuration

The logged tags can also be archived on an FTP server. The following settings are required for this.

The "Maximum" firewall security setting does not permit the agreement of a dynamic communication port as required during FTP communication between the client and server. The router firewall must therefore be set to "Normal" in this case.

Interval [min]

The log file is compressed and loaded onto the FTP server at the specified interval. A copy of the log file also remains on the storage medium (compressed).

Server address Enter the address of the FTP server here.

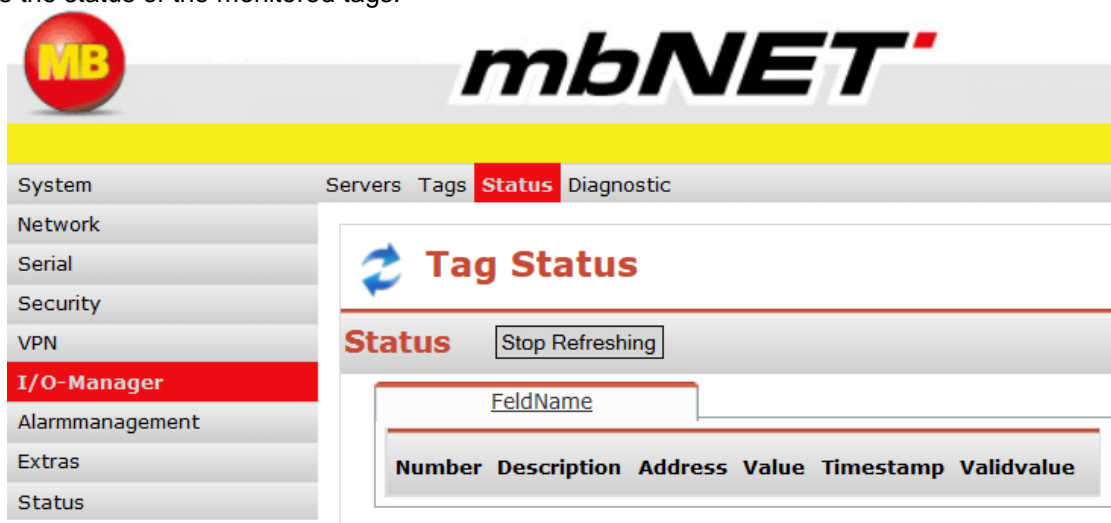
Server Username Enter the username for authentication on the FTP server here

Server password Enter the password for authentication on the FTP server here.

Log files are in CSV format. The current file is always called logfile.log and is stored in the subdirectory \log-files\ on the USB stick. Archived files use the following naming convention: log-file.log.[Date(yyyymmdd)]_[Time(hhmmssms3)].gzip

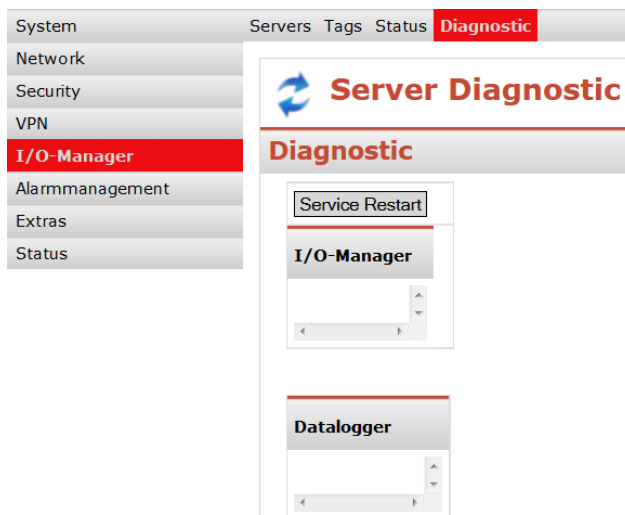
21.3 Tag status

Shows the status of the monitored tags.



Label	Description
Number	Number of the tag.
Description	Description of the tag
Address	Address of the tag
Value	Value of the tag, in the data format which was set at the tag.
Timestamp	Shows the exact time when the tag was readed.
Valid value	Shows if the tag is valid / reachable or not.

21.4 Diagnostic



You can restart the I/O-Manager here. You can also analyze the logging and the data logger of the I/O-Manager here.

22. Alarm management

22.1 General

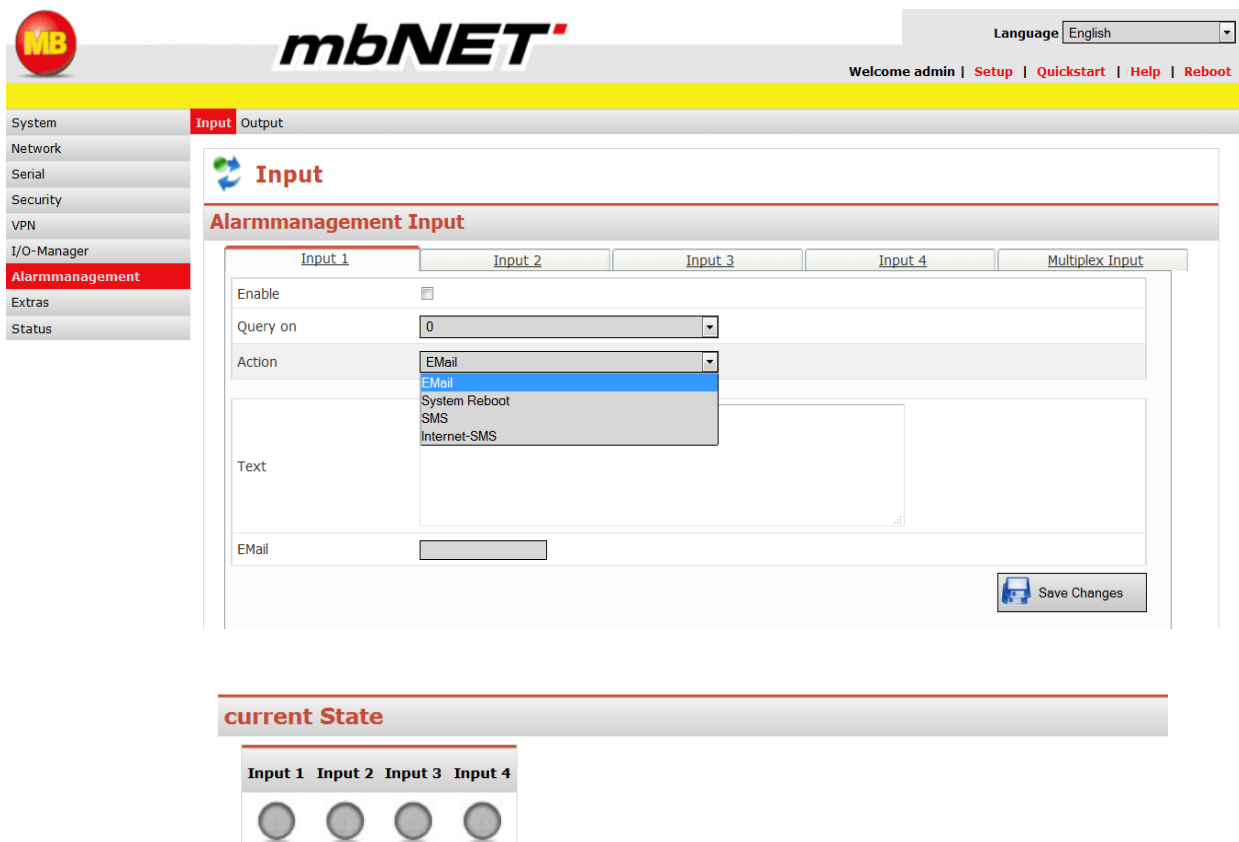
- The alarm management function can be used to query the states at the four digital inputs and, depending on the result, send an appropriate text to an email address you have specified.

switch two digital outputs independent of each other in the event of a fault, when there is an active Internet connection or manually.

22.2 Digital inputs

Click **Alarmmanagement** in the navigation bar, followed by **Input**.

The following screen for configuring the four available digital inputs is then displayed. The inputs can be individually configured using the four different tabs.



Label	Description
-------	-------------

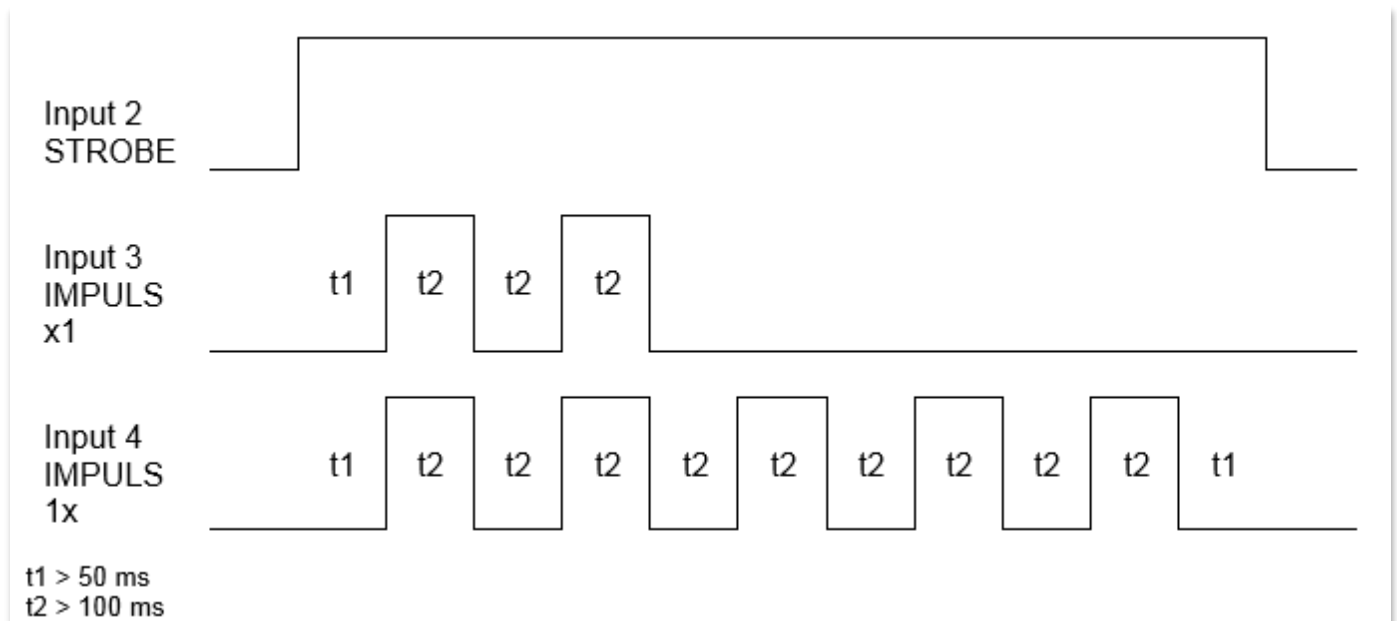
Input 1 ... 4 tabs	Each input can be separately configured. Select the input to be configured by clicking the corresponding tab.
Enable	The input is enabled by checking the box. This is how you determine whether the input in question is to be enabled ("activated").
Query on	Set the input level for the industrial router in this drop-down field. The available signal levels are 1 and 0.
Action	There are three possible actions: <ul style="list-style-type: none"> <input type="checkbox"/> Email <input type="checkbox"/> SMS (only available at mbNET variants with modem!) <input type="checkbox"/> System Reboot <input type="checkbox"/> Internet-SMS
Text	Enter the text to be sent to the specified email address in this input field. The following special characters are permitted in the text: Ä Ü Ö , ; . : - _ # + * ~ ^ ° ! () = ? § \$ % & / < >
Email/Mobile Phone	Enter the email address or phone number* to which the industrial router should send the text when the input is activated and the relevant signal level has resulted in the action being initiated. * Up to three mobile phone numbers are possible - separated by semicolon or comma.
current State	You can read off the current state at the inputs via the LED icons at the bottom of the screen. Gray indicates state 0, green indicates state 1.

22.2.1 Multiplex inputs

Brief description

There are four digital inputs on the mbNET. An action assignment (number) can be communicated serially via three of these inputs (2-4), i.e. one input is STROBE, one is IMPULS_x1 and one is IMPULS_1x. The pulse at IMPULS_x1 (one digit) and IMPULS_1x (tens digit) can be counted with a rising edge at STROBE. The action is executed in accordance with the entered action with a falling edge at STROBE.

Graph



The action **52** is initiated in the sample graph.

Action table

System

Network

Serial

Security

VPN

I/O-Manager

Alarmmanagement

Extras

Status

Apply Changes

Clear Changes

Input
Output

Input

Alarmmanagement Input

Input 1
Input 2
Input 3
Input 4
Multiplex Input

Enable

Uses the Input 2 for STROBE, Input 3 for IMPULS digit x1 and Input 4 for IMPULS digit 1x

Save Changes

Number	Aktion	Text	Number/Email
3	email		
1	email	This is an e-mail	support@mbconnectline.de
2	Internet-SMS	This is an Internet SMS	01609999999

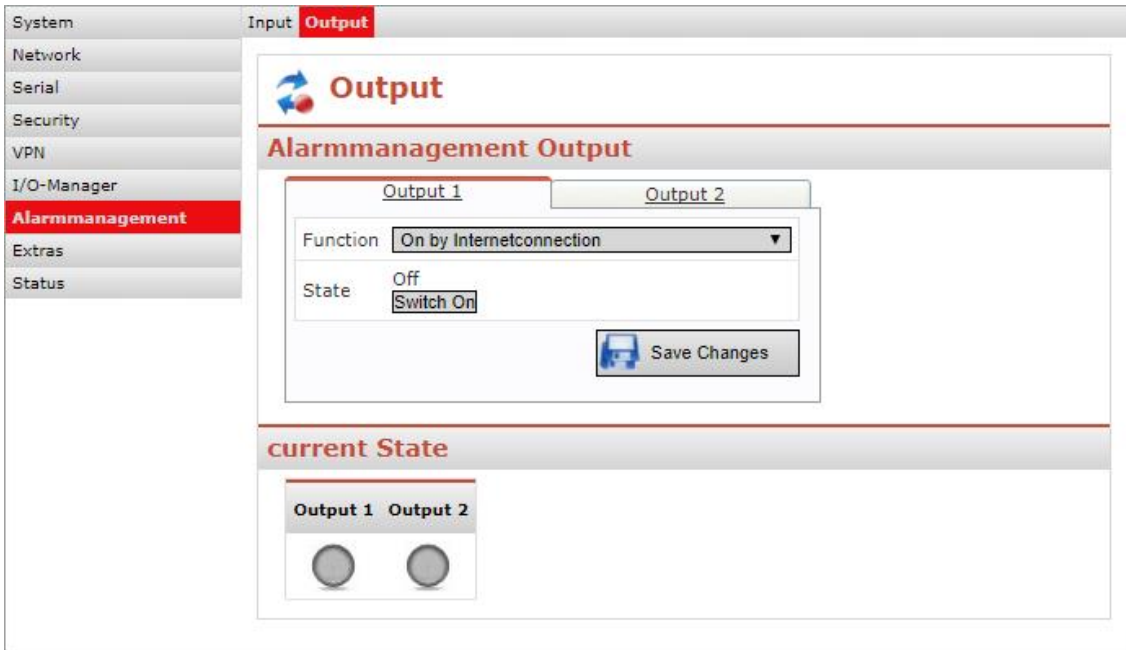
current State

Input 1
Input 2
Input 3
Input 4

The action number is defined in the Number drop-down field. There are different actions available depending on device model. The “E-Mail” function is available with all devices, the “SMS” option is available with devices with a mobile broadband modem.

22.3 Digital outputs

Click **Alarmmanagement** in the navigation bar, followed by **Output**.



Label	Description
Output 1 Output 2	Each output can be separately configured. To configure an output, select the corresponding tab.
Function	<p>You can chose between the following settings using the drop-down field:</p> <p>Off Select this setting if you do not want to evaluate the outputs for possible switching operations.</p> <p>On by Malfunction Select this setting if the corresponding output of the industrial router is to be set to signal level 1 in the event of a malfunction.</p> <p>On by Internetconnection Select this setting if the corresponding output of the industrial router is to be set to 1 in the event of an active Internet connection. For example, an active Internet connection can then be indicated by an LED connected at the corresponding output.</p> <p>On by any VPN-connection Select this setting if the corresponding output is to be set to 1 as soon as a user has connected to the mbNET via an active VPN connection. If no active connection is available, the output is switched off again. For example, a VPN connection can then be indicated by an LED connected at the corresponding output.</p> <p>On by any User-Cloudserver-connection Select this setting if the corresponding output of the industrial router is to be set to 1 as soon as at least one mbCONNECT24 user has connected to the mbNET via an active connection. If no active connection is available, the output is switched off again. For example, a VPN connection can then be indicated by an LED connected at the corresponding output.</p>

State	<p>Switch On or Switch Off</p> <p>This button can be used to switch the currently selected output on and off. The text Off or On above the button shows the current output state in the same way as the LED icons under “current State”.</p> <p>Green LED icon: Signal level 1 at output Gray LED icon: Signal level 0 at output</p>
--------------	---

23. Status messages

23.1 General

The industrial router must be analyzed using certain status information when errors occur. For example, a flashing ERROR LED indicates that a system error has occurred on the router. The cause of the error can be determined e.g. via **Status** – **System** using the list.

The various status displays are described below:

23.2 Status – Interfaces

The screenshot shows the mbNET web interface. On the left is a navigation menu with items: System, Network, Security, VPN, I/O-Manager, Alarmmanagement, Extras, and Status (highlighted in red). The main content area is titled 'Interfaces' and contains three sections:

- WAN (eth1)**: Shows MAC Address 70:B3:D5:2C:F1:CB, IP Address (empty), Received 0 pkts (), and Transmitted 0 pkts ().
- WLAN (ra0)**: Shows MAC Address 7C:DD:90:6A:ED:04, IP Address (empty), Received 0 pkts (), and Transmitted 0 pkts ().
- LAN (eth0)**: Shows MAC Address 70:B3:D5:2C:F1:CA, IP Address 192.168.0.240, Received 102.5k pkts (), and Transmitted 2.1k pkts ().

Label	Description
WAN	Shows the settings at the router’s WAN connection (external connection). The IP address is displayed as soon as the router has a physical connection to the network or is assigned a static IP address. The number of data packets received and transmitted is displayed.
WLAN	Note: Only at mbNET variants with WiFi. Shows the settings at the router’s LAN connection (local connection). The IP address is displayed when the router has a physical connection. The number of data packets received and transmitted is displayed.
LAN	Shows the settings at the router’s LAN connection (local connection). The IP address is displayed when the router has a physical connection. The number of data packets received and transmitted is displayed.

23.3 Status - Network

Interfaces **Network** Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System

Networkstatus

Networkstatus

General Firewall

Physical Connections : Ethernet Connections

IP address	HW type	Flags	HW address	Mask	Device
192.168.0.70	0x1	0x2	dc:0e:a1:54:31:b5	*	eth0

Routing Table

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
255.255.255.255	0.0.0.0	255.255.255.255	UH	0	0	0	eth0
10.112.112.112	0.0.0.0	255.255.255.255	UH	0	0	0	ppp0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
0.0.0.0	0.0.0.0	0.0.0.0	U	0	0	0	ppp0

Router Listening Ports

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	192.168.0.100:102	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:139	0.0.0.0:*	LISTEN
tcp	0	0	192.168.0.100:7001	0.0.0.0:*	LISTEN
tcp	0	0	192.168.0.100:7002	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:445	0.0.0.0:*	LISTEN
tcp	0	0	:::80	:::*	LISTEN
udp	0	0	127.0.0.1:514	0.0.0.0:*	
udp	0	0	0.0.0.0:58242	0.0.0.0:*	

Router Connections : Connections to the Router

Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	402	::ffff:192.168.0.100:80	::ffff:192.168.0.:53283	ESTABLISHED

Label	Description
Physical Connections	Shows the physical connections via which the router is connected to other computers.
Routing Table	Shows all routes used.
Router Listening Ports	Shows all monitored ports.
Router Connections: Connections to the Router	Shows all IP addresses with ports, e.g. of computers that are connected to the router.

23.3.1 Firewall

23.3.1.1 IN / OUT / FORWARD

System

Network

Serial

Security

VPN

I/O-Manager

Alarmmanagement

Extras

Status

Interfaces: **Network** Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System

Networkstatus

General
Firewall

IN/OUT/FORWARD

Chain INPUT (policy DROP 0 packets, 0 bytes)

num pkts	bytes	target	prot	optin	out	source	destination	options
1	0	0 DROP	all	-- *	*	0.0.0.0/0.0.0.0/0		state INVALID
2	1641	180K ACCEPT	all	-- *	*	0.0.0.0/0.0.0.0/0		state RELATED,ESTABLISHED
3	0	0 DROP	tcp	-- *	*	0.0.0.0/0.0.0.0/0		tcp option=12 flags:0x02,0x02
4882939351K		input_rule	all	-- *	*	0.0.0.0/0.0.0.0/0		
5440614662K		input_wan_eth	all	-- eth1 *	*	0.0.0.0/0.0.0.0/0		
6440614662K		input_wan	all	-- eth1 *	*	0.0.0.0/0.0.0.0/0		
7882939351K		LAN_ACCEPT	all	-- *	*	0.0.0.0/0.0.0.0/0		
8	2	96 ACCEPT	icmp	-- *	*	0.0.0.0/0.0.0.0/0		
9	0	0 ACCEPT	47	-- *	*	0.0.0.0/0.0.0.0/0		
10	241	12212 REJECT	tcp	-- *	*	0.0.0.0/0.0.0.0/0		reject-with tcp-reset
11438184650K		REJECT	all	-- *	*	0.0.0.0/0.0.0.0/0		reject-with icmp-port-unreachable

Chain FORWARD (policy DROP 0 packets, 0 bytes)

num pkts	bytes	target	prot	optin	out	source	destination	options
1	0	0 DROP	all	-- *	*	0.0.0.0/0.0.0.0/0		state INVALID
2	0	0 TCPMSS	tcp	-- *	*	0.0.0.0/0.0.0.0/0		tcp flags:0x06,0x02 TCPMSS clamp to PMTU
3	0	0 ACCEPT	all	-- *	*	0.0.0.0/0.0.0.0/0		state RELATED,ESTABLISHED
4	0	0 forwarding_rule	all	-- *	*	0.0.0.0/0.0.0.0/0		
5	0	0 forwarding_lan_wan_eth	all	-- eth0 eth1		0.0.0.0/0.0.0.0/0		
6	0	0 forwarding_lan_wan	all	-- eth0 eth1		0.0.0.0/0.0.0.0/0		
7	0	0 forwarding_wan	all	-- eth1 *	*	0.0.0.0/0.0.0.0/0		
8	0	0 ACCEPT	all	-- eth0 eth0		0.0.0.0/0.0.0.0/0		
9	0	0 ACCEPT	all	-- eth0 eth1		0.0.0.0/0.0.0.0/0		
10	0	0 forwarding_l2tp	all	-- *	*	0.0.0.0/0.0.0.0/0		

Chain OUTPUT (policy DROP 0 packets, 0 bytes)

num pkts	bytes	target	prot	optin	out	source	destination	options
1	0	0 DROP	all	-- *	*	0.0.0.0/0.0.0.0/0		state INVALID
2	2229	1137K ACCEPT	all	-- *	*	0.0.0.0/0.0.0.0/0		state RELATED,ESTABLISHED
3	25432019	output_rule	all	-- *	*	0.0.0.0/0.0.0.0/0		
4	65	6912 output_wan_eth	all	-- *	*	eth1 0.0.0.0/0.0.0.0/0		
5	65	6912 output_wan	all	-- *	*	eth1 0.0.0.0/0.0.0.0/0		
6	18925107	ACCEPT	all	-- *	*	0.0.0.0/0.0.0.0/0		
7	0	0 REJECT	tcp	-- *	*	0.0.0.0/0.0.0.0/0		reject-with tcp-reset
8	0	0 REJECT	all	-- *	*	0.0.0.0/0.0.0.0/0		reject-with icmp-port-unreachable

Chain LAN_ACCEPT (1 references)

num pkts	bytes	target	prot	optin	out	source	destination	options
1440614662K		RETURN	all	-- eth1 *	*	0.0.0.0/0.0.0.0/0		
2442324688K		ACCEPT	all	-- *	*	0.0.0.0/0.0.0.0/0		

Chain forwarding_l2tp (1 references)

num pkts	bytes	target	prot	optin	out	source	destination	options

Chain forwarding_lan_wan (1 references)

num pkts	bytes	target	prot	optin	out	source	destination	options

Chain forwarding_lan_wan_eth (1 references)

num pkts	bytes	target	prot	optin	out	source	destination	options

Chain forwarding_rule (1 references)

num pkts	bytes	target	prot	optin	out	source	destination	options

Chain forwarding_wan (1 references)

num pkts	bytes	target	prot	optin	out	source	destination	options

Chain forwarding_wan_eth (0 references)

num pkts	bytes	target	prot	optin	out	source	destination	options

Chain input_rule (1 references)

num pkts	bytes	target	prot	optin	out	source	destination	options

Chain input_wan (1 references)

num pkts	bytes	target	prot	optin	out	source	destination	options

Chain input_wan_eth (1 references)

num pkts	bytes	target	prot	optin	out	source	destination	options

Chain output_rule (1 references)

num pkts	bytes	target	prot	optin	out	source	destination	options

Chain output_wan (1 references)

num pkts	bytes	target	prot	optin	out	source	destination	options
1	0	0 ACCEPT	tcp	-- *	*	0.0.0.0/0.0.0.0/0		multiport dports 53,21,143,80,443,110,25,23,123,1723
2	0	0 ACCEPT	udp	-- *	*	0.0.0.0/0.0.0.0/0		multiport dports 53,21,143,80,443,110,25,23,123,500,4500
3	0	0 REJECT	tcp	-- *	*	0.0.0.0/0.0.0.0/0		reject-with tcp-reset
4	0	0 RETURN	icmp	-- *	*	0.0.0.0/0.0.0.0/0		
5	65	6912 REJECT	all	-- *	*	0.0.0.0/0.0.0.0/0		reject-with icmp-port-unreachable

23.3.1.2 NAT
NAT
Chain PREROUTING (policy ACCEPT 31413 packets, 3015K bytes)

numpkts	bytes	target	prot	optin	out	source	destination	options
131373	3010K	NEW	all	-- *	*	0.0.0.0/0	0.0.0.0/0	state NEW
231373	3010K	prerouting_rule	all	-- *	*	0.0.0.0/0	0.0.0.0/0	
3	0	prerouting_wan_eth	all	--	eth1 *	0.0.0.0/0	0.0.0.0/0	
4	0	prerouting_wan	all	--	eth1 *	0.0.0.0/0	0.0.0.0/0	

Chain POSTROUTING (policy ACCEPT 7 packets, 625 bytes)

numpkts	bytes	target	prot	optin	out	source	destination	options
1	6	535postrouting_rule	all	-- *	*	0.0.0.0/0	0.0.0.0/0	
2	0	postrouting_wan_eth	all	-- *	eth1	0.0.0.0/0	0.0.0.0/0	
3	0	postrouting_wan	all	-- *	eth1	0.0.0.0/0	0.0.0.0/0	
4	0	MASQUERADE	all	-- *	eth1	0.0.0.0/0	0.0.0.0/0	

Chain OUTPUT (policy ACCEPT 7 packets, 625 bytes)

numpkts	bytes	target	prot	optin	out	source	destination	options

Chain NEW (1 references)

numpkts	bytes	target	prot	optin	out	source	destination	options
131371	3010K	RETURN	all	-- *	*	0.0.0.0/0	0.0.0.0/0	limit: avg 50/sec burst 100
2	0	ODROP	all	-- *	*	0.0.0.0/0	0.0.0.0/0	

Chain postrouting_rule (1 references)

numpkts	bytes	target	prot	optin	out	source	destination	options

Chain postrouting_wan (1 references)

numpkts	bytes	target	prot	optin	out	source	destination	options
1	0	ORETURN	tcp	-- *	*	0.0.0.0/0	0.0.0.0/0	multiport dports 53,21,143,80,443,110,25,23,123,1723
2	0	ORETURN	udp	-- *	*	0.0.0.0/0	0.0.0.0/0	multiport dports 53,21,143,80,443,110,25,23,123,500,4500
3	0	ORETURN	esp	-- *	*	0.0.0.0/0	0.0.0.0/0	
4	0	ORETURN	icmp	-- *	*	0.0.0.0/0	0.0.0.0/0	
5	0	ODROP	all	-- *	*	0.0.0.0/0	0.0.0.0/0	

Chain postrouting_wan_eth (1 references)

numpkts	bytes	target	prot	optin	out	source	destination	options

Chain prerouting_rule (1 references)

numpkts	bytes	target	prot	optin	out	source	destination	options

Chain prerouting_wan (1 references)

numpkts	bytes	target	prot	optin	out	source	destination	options

Chain prerouting_wan_eth (1 references)

numpkts	bytes	target	prot	optin	out	source	destination	options

23.4 Status – Modem

Note: Not available at mbNET variants with WiFi.

Interfaces Network **Modem** Internet DHCP DNS Server DynDNS NTP VPN-IPSec

Modem

Modem

Modem-Connection	Active	IP local	IP remote
User:	<input type="radio"/>		



Information from the last connection

Connected: 0 sec.

Bytes sent: 0

Bytes received: 0

Modem Commands

Modem Command

(without AT):

Systemloggings

Modemloggings

GSM information

Manual Control of the GSM modem

Signal Quality

Possible: -51 dBm Total: -105 dBm

Quality: -105 dBm (12 %)

GSM service

HSDPA and HSUPA available in currently used cell

Provider

Telekom Deutschland GmbH

SIM card SIM1

OK

GSM Modemloggings

```
<12>Mar 23 09:57:05 GSM-Modem: The GSM Modem is not registered. It is searching for a network.
<14>Mar 23 09:57:05 GSM-Modem: The GSM Modem does not require a SIM Pin
<14>Mar 23 09:56:59 GSM-Modem: Switch to SIM socket sim1
<14>Mar 23 09:56:51 GSM-Modem: The GSM Modem is switching on.
<14>Mar 23 09:56:50 GSM-Modem: The GSM Modem is shutting down.
```



Label	Description
Modem-Connection	Shows the user who dialed into the router via modem. The IP address of the PPP server and PPP client (remote station) is displayed when a dial-up connection is successfully established. The connections are always incoming connections. An active connection is indicated by a green dot.
Information from the last connection	Shows the connection time and the number of bytes sent and received during the most recent connection as long as the router was not restarted or switched off in the interim.
Modem Commands	This input field can be used to issue a command directly to the internal modem. This function should only be used as directed by MB Connect Line support personnel.
Systemloggings	Shows the type of connection and the assigned IP and DNS addresses.
Modemloggings	Shows the commands sent to the modem to initialize it and the status of the connection process. The error messages that occur when establishing the connection are also displayed here.
Manual Control of the GSM modem	You can use this button to restart the internal modem. This function should only be used as instructed by MB Connect Line support personnel.
Signal Quality	Specifies the current network availability in percent and dBm. If you have an mbNET with mobile broadband and UMTS, the device will automatically change networks when UMTS becomes available again or UMTS is no longer available.
GSM service	Shows the respective transmission method. The following are possible: <ul style="list-style-type: none"> <input type="checkbox"/> GSM/GPRS <input type="checkbox"/> EDGE <input type="checkbox"/> UMTS
Provider	Shows the current mobile broadband provider (T Mobile Germany as shown in Figure 211).
SIM card SIM1	Shows the status of your SIM card in mbNET.
GSM Modemloggings	Shows all events and errors related to the GSM modem.

23.5 Status – Internet

Interfaces Network Modem **Internet** DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement System

Internet

Manual Control of the Internet Service

Internet Service Restart

Internet Service Stop Internet Service Start

Internet-Connection	Active	IP local	IP remote
Internet (Modem)	<input type="radio"/>		

Information from the last connection

Connected: - sec.

Bytes sended:

Bytes received:

DNS Servers	IP

Systemloggings

1: <14>Mar 23 09:58:24 Internet: Start with prio. level = 1

Modemloggings

Label	Description
Internet 	<p>Shows outgoing connections to the Internet. These can be both outgoing connections via the modem and connections via WAN. The IP addresses of the local and remote stations are displayed. An active connection is indicated by a green dot. You can manually connect or disconnect the Internet connection here also.</p> <p><u>However it is not recommended to use these buttons unless requested to do so by a member of the support team.</u></p>
Information from the last connection	Shows the connection time and the number of bytes sent and received during the most recent connection as long as the router was not restarted or switched off in the interim.
DNS Servers	Shows the IP address of the DNS server.
Systemloggings	Shows the type of connection and the assigned IP and DNS addresses.
Modemloggings	Shows the commands sent to the modem to initialize it and the status of the connection process. The error messages that occur when establishing the connection are also displayed here.

23.6 Status – DHCP

Label	Description
DHCP Server	The IP addresses that the DHCP server assigns to connected clients are listed here.
System loggings	Shows the IP addresses that the DHCP assigns and which IP addresses are not allowed.
Client Information	Information about connected clients on the WAN port.
System loggings	All events and errors relating to the DHCP server and client are logged.

23.7 Status – DNS Server


Label	Description
Name	Shows the name of the DNS server if not assigned by the Internet service provider.
IP address	Shows the IP address of the DNS server if not assigned by the Internet service provider.
Systemloggings	Shows the individual operations executed by the DNS server.

23.8 Status – DynDNS

Label	Description
Updated IP address	Shows the current IP address assigned to the router via the Internet.
Systemloggings	Shows all events and faults related to the DynDNS service.

23.9 Status – NTP

Interfaces Network Modem Internet DHCP DNS Server DynDNS **NTP**



NTP

Date and Time

Date Time (UTC)	Fri Mar 23 09:00:50 UTC 2012
Locale Date Time	Fri Mar 23 10:00:50 CET 2012
<input type="button" value="Start NTP update"/>	

Systemloggings

▲
▼

◀
▶

Label	Description
Date Time (UTC)	Shows the current system time in Universal Time Coordinates (UTC).
Local Date Time	Shows the time using the time zone setting.
Systemloggings	Shows all notifications and error messages related to the service.

23.10 Status – VPN-IPSEC

System Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP **VPN-IPSec** VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement

System Network Serial Security VPN I/O-Manager Alarmmanagement Extras **Status**

IPSec

Connections inbound/outbound

Name	Active	Connectiondata lokal	Connectiondata peer	Status	Logging	Stop Connection	Start Connection

Systemloggings: Connection

Systemloggings: IPSec

Delete Logscreen

Show all Logscreen

Label	Description
<p>Connections inbound / outbound</p>	<p>Shows both the incoming and outgoing VPN connections of the router. An active connection is indicated by a green dot. The connection duration and active user are displayed. After the connection is disconnected, the active connection time is displayed. You can manually connect or disconnect the connection here also.</p> <p><u>However it is not recommended to use these buttons unless requested to do so by a member of the support team.</u></p>

23.11 Status – VPN-PPTP

Label	Description
Server	<p>The incoming VPN connections of the router are listed here. An active connection is indicated by a green dot.</p> <p>The connection duration, active user, local and remote IP address are displayed. After the connection is disconnected, you can read off the active connection time.</p>
Clients	<p>Shows the outgoing VPN connections of the router. An active connection is indicated by a green dot.</p> <p>The connection duration, active user, local and remote IP address are displayed.</p> <p>The connections are logged.</p> <p>After the connection is disconnected, you can read off the active connection time.</p>
Systemloggings: Connection	<p>Shows all notifications and error messages related to the PPTP service.</p>

23.12 Status – VPN OpenVPN

System Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP **VPN-OpenVPN** Diagnostics USB Alarmmanagement

Network Serial Security VPN I/O-Manager Alarmmanagement Extras **Status**

OpenVPN

Connections inbound/outbound

Name	Active	Common Name	Connectiondata local	Connectiondata peer	Logging	Stop Connection	Start Connection
Systemloggings: Connection							

Label	Description
<p>Connections in-bound/outbound</p>	<p>Shows both the incoming and outgoing VPN connections of the router. An active connection is indicated by a green dot. The name, local address and peer address are displayed here. You can manually connect or disconnect the connection here also. <u>However it is not recommended to use these buttons unless requested to do so by a member of the support team.</u></p>

23.13 Status – Diagnostics

System Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN **Diagnostics** USB Alarmmanagement

System

Diagnostics

Network Utilities

Ping:	<input type="text" value="google.com"/>	<input type="button" value="Ping"/>
TraceRoute:	<input type="text" value="google.com"/>	<input type="button" value="TraceRoute"/>
NS Lookup:	<input type="text" value="google.com"/>	<input type="button" value="NS Lookup"/>
TCPDUMP Options:	<input type="text" value="-i eth0 not port 80"/>	<input type="button" value="TCPDUMP"/>

Label	Description
Ping	After an Internet address or IP address is entered, the ping command can determine whether the address in question can be reached. This is e.g. an easy way of determining whether there is an Internet connection active.
TraceRoute	This command provides more information about the network connection between the router and a remote or other computer. It traces and displays the route.
NS Lookup	This function can be used to check whether name resolution (https://www.google.com = 216.58.209.206) takes place. If this function ends in an error message, check whether there is a DNS server address under <i>Network DNS</i> in your mbNET or whether your network's DNS server is available.
TCPDUMP Options	<p>You can use the command TCPDUMP to track the network traffic. Exempels of using TCPDUMP:</p> <p>-i eth0 not port 80</p> <p>Show all TCP/IP Connections on the interface (-i) LAN (eth0), but don't (not) show connections who are using port 80. (<i>http</i>)</p> <p>-i eth1 port 23</p> <p>Show all TCP/IP Connections on interface (-i) WAN (eth1), with port 23. (<i>port 23</i>)</p> <p>-vvv -i eth1</p> <p>Show all data traffic in verbose mode level 3 (-vvv) on interface (-i) WAN (-eth1)</p> <p>For more detailed information about TCPDUMP, visit: www.tcpdump.org</p>

23.14 Status – USB

USB Devices

All connected devices (excluding system hubs)

Vendor	Model	Type	Version
USB	Flash DISK	Direct-Access ANSI SCSI	02

Mounted USB / SCSI devices

```
/dev/sda1 on /var/usb/sda1 type vfat (rw,mask=0000,dmask=0000,allow_utime=0022,codepage=cp437,ioccharset=iso8859-1)
/dev/sda1 on /var/sshd/usb type vfat (rw,mask=0000,dmask=0000,allow_utime=0022,codepage=cp437,ioccharset=iso8859-1)
```

Label	Description
All connected devices (excluding system hubs).	The manufacturer, model, type and version are displayed for connected USB storage media.
Mounted USB / SCSI devices	Shows how the USB storage medium is integrated in the routers file system and the file system created on the USB storage medium.

23.15 Status – Alarmmanagement

Input/Output

Input

Input 1 Input 2 Input 3 Input 4

Output

Output 1 Output 2

Messages

Systemloggings

Label	Description
Input	Shows the states at the four inputs. The states are queried and updated approx. every three seconds.
Output	Shows the states at the two outputs. The states are queried and updated approx. every three seconds.
Systemloggings	All events and error messages related to alarm management are saved here (e.g. SMS, activity of inputs).

23.16 Status – System

System

Network

Serial

Security

VPN

I/O-Manager

Alarmmanagement

Extras

Status

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostics USB Alarmmanagement **System**

Device Status

RAM Usage

Total: 125212 KB 29%
 Used: 35824 KB (29%)

Memory Usage

Configuration Flash 41%
 Used: 840 KB (41%)

Temp Memory 4%
 Used: 274 KB (4%)

Tracked Connections

Maximum: 8192 1%
 Used: 59 (1%)

System informations

[Generate support file and download it](#)

Systemloggings: Kernel

```

                    <6>Sep 18 06:35:20 kernel: usb 2-1: SerialNumber: 351579050670585
                    <6>Sep 18 06:35:20 kernel: usb 2-1: Manufacturer: Telit wireless solutions
                    <6>Sep 18 06:35:20 kernel: usb 2-1: Product: Telit Wireless Module
                    <6>Sep 18 06:35:20 kernel: usb 2-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
                    <6>Sep 18 06:35:20 kernel: usb 2-1: New USB device found, idVendor=1bc7, idProduct=0021
                    <6>Sep 18 06:35:20 kernel: cdc_acm 2-1:1.12: ttyACM6: USB ACM device
                    <6>Sep 18 06:35:20 kernel: cdc_acm 2-1:1.10: ttyACM5: USB ACM device
                    <6>Sep 18 06:35:20 kernel: cdc_acm 2-1:1.8: ttyACM4: USB ACM device
                    <6>Sep 18 06:35:20 kernel: cdc_acm 2-1:1.6: ttyACM3: USB ACM device
                    <6>Sep 18 06:35:20 kernel: cdc_acm 2-1:1.4: ttyACM2: USB ACM device
                    <6>Sep 18 06:35:20 kernel: cdc_acm 2-1:1.2: ttyACM1: USB ACM device
                    <6>Sep 18 06:35:20 kernel: cdc_acm 2-1:1.0: ttyACM0: USB ACM device
                    <6>Sep 18 06:35:20 kernel: usb 2-1: configuration #1 chosen from 1 choice
                    <6>Sep 18 06:35:19 kernel: usb 2-1: new high speed USB device using ixp4xx-ehci and address 22
                
```

Error loggings

[Sep 18 06:32:56] > (none) GSM-Modem: There is no SIM Card inserted. Please insert a SIM Card

[clear all error messages](#)

Label	Description
RAM Usage	Shows the amount of RAM memory currently being used by the router.
Memory Usage	Shows the amount of configuration memory and temporary memory currently being used.
Tracked Connections	Shows the usage of the packet filter.
System information	The system information can be used to establish the cause of errors on the router. If, for example, the ERROR LED on the front is flashing, it may be possible to determine the cause of the error using the log.
Error loggings	Firmware versions 2.1.0 and higher feature a direct error logging function in the web interface. This function logs all of the errors until the “ clear all error messages ” button is clicked. The most recent error is also displayed on the system information page and the <i>wizard’s page</i> . Simply click the last error message to go from one of these two pages directly to the error memory.

Page 223 of 237
Version: 5.1.6 – June 4th, 2018

24. Extras

24.1 LUA

You can activate LUA to write and execute LUA scripts.

LUA

LUA programming language

LUA control

LUA active

LUA stopped

LUA script

```
-- -----  
-- function CONN_plc() --  
-- -----  
function CONN_plc(...)  
  local arg = {...};  
  local _ip = arg[1];  
  local _slot = arg[2];  
  local PLC_HANDLE = nil;  
  
  PLC_HANDLE = plc_connect("ISOTCP", _ip, _slot);  
  return PLC_HANDLE;  
end;
```

Import script (*.lua)

LUA output

LUA logging

24.2 Toolbox

- System
- Network
- Serial
- Security
- VPN
- I/O-Manager
- Alarmmanagement
- Extras
- Status

⚙️

Toolbox

Toolbox control

Toolbox active

Toolbox stopped Start

Toolbox load from ... USB ▼

USB Configuration

no toolbox file found. Please copy the toolbox file to the USB memory stick.

Webserver Configuration

Listen on port

Toolbox data storage

Toolbox store data on ... USB ▼

store on USB folder ...

Save Changes

Label	Description
Toolbox active	If this checkbox is active, then the toolbox is going to be executed after every router re-start.
Status Symbol	The Status Symbol shows if the toolbox is executed or not. By using the button start / stop you can control the toolbox manually.
Toolbox load from...	You can only load the toolbox from an USB-Storage at the moment.
USB Configuration	The newest toolbox version is displayed here.
Webserver Configuration	<p>The toolbox is executed on a separate webserver on the router. The default port for the webserver is 80. But this port is already occupied by the web interface of the router. The default value for the toolbox webserver is port 81. You can access the webserver via http://router-LAN-ip:81</p> <p>You can adjust the default webserver port of the router via System > Web > HTTP-Port (e.g. 8080). Now you can set the port of the toolbox webserver to port 80, then you can access the toolbox via: http://router-LAN-IP</p> <p>Note: It is not necessary to write the port number behind the URL if you use Port 80! (This is only true for port 80!)</p>
Store on USB folder...	The toolbox must also store your configuration on the USB memory. To do this, enter the folder for this. All data is stored in this folder and can be easily duplicated to other devices.

25. Firmware update directly via USB

You can update the **mbNET** directly via the USB interface. The device automatically detects the firmware stored on a connected USB stick. The firmware update starts after pressing the Dial Out button.

Preparation:

- Go to **www.mbconnectline.com** and download the latest firmware version (e.g. "mbNET_FW_V500.zip").
- After unpacking, you will find the actual firmware file "**image.bis**" next to the file "Changelog.txt".
- Save the "**image.bis**" to a USB memory stick.

ADVICE: The "**image.bis**" firmware file may not be renamed and must be saved in the top-level directory (root) of the USB drive. The USB drive must have the file format FAT / FAT32.

ATTENTION: DO NOT disconnect the power supply to the device during the firmware update!

Execution:

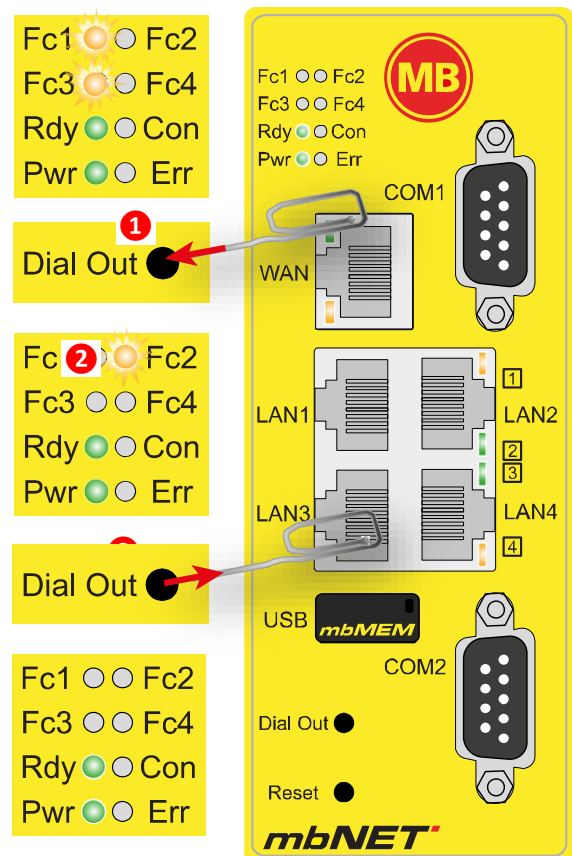
When the **mbNET** is ready for operation (LED **Pwr** + **Rdy** light up), plug the USB stick into the device's USB port.

- As soon as the device has recognized the configuration file, LEDs **Fc1** + **Fc3** start to **flash** synchronously.
- Now push and hold down the **Dial Out** button **1** until LED **Fc2** flashes **2**.
- Now release the **Dial Out** button **3**.

The **mbNET** now reboots.

When both LEDs **Pwr** and **Rdy** light up, the firmware update is completed **4**.

The **mbNET** is now ready again for operation and can be used as usual.



ADVICE: If the firmware and an **mbCONNECT24** portal configuration are located on the USB stick, the firmware is always recognized by the **mbNET** (**Fc1** + **Fc3** flashing) first.

If you do not press the **Dial Out** button within 10 seconds, the **mbNET** will change to the portal configuration (**Fc1** + **Fc2** flashing). If you do not react within 10 seconds, the device returns to normal mode.

26. Importing the portal configuration into an mbNET via USB

If you have created the **mbNET** device configuration in the **mbCONNECT24** service portal, you can import this portal configuration directly into the **mbNET** via the USB interface. The device automatically detects the portal configuration stored on a connected USB stick. Press the **Dial Out** button to start the reading.

Requirement:

You have configured the **mbNET** in the **mbCONNECT24** portal and saved the configuration file (mbconnect24.mbn / mbconnect24.mbnx) to a USB flash drive using the "Download to PC" mode.

ADVICE: The downloaded "mbconnect24.mbn/-mbnx" configuration file may not be renamed and must be saved in the top-level directory (root) of the USB drive. The USB drive must have the file format FAT / FAT32.

Informationen about **mbCONNECT24** can be found at

- our Internet pages at <https://www.mbconnectline.com>
- or in the **mbCONNECT24** online help

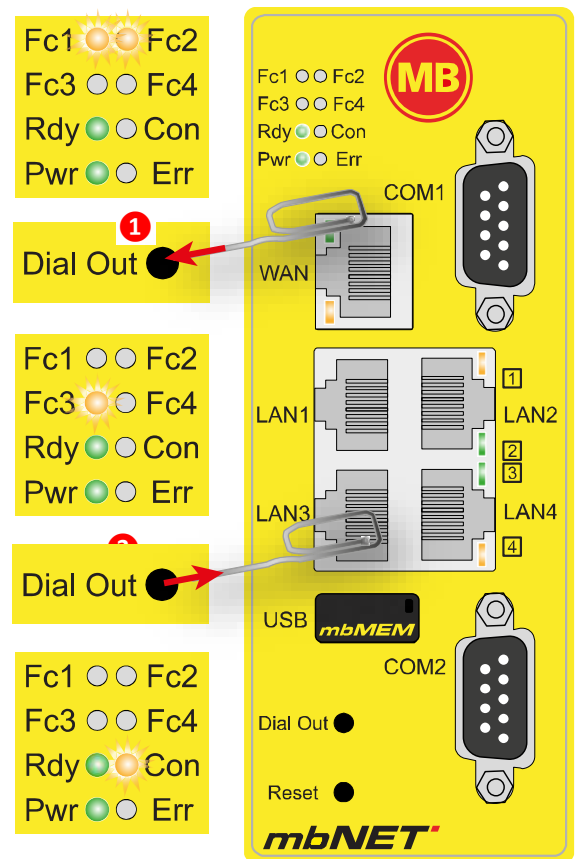
Execution:

When the **mbNET** is ready for operation (LED **Pwr** + **Rdy** light up), plug the USB stick into the device's USB port.

- As soon as the device has recognized the configuration file, LEDs **Fc1** + **Fc2** start to **flash** synchronously.
- Now push and hold down the **Dial Out** button **1** until LED **Fc3** flashes **2**.
- Now release the **Dial Out** button **3**.

The settings from **mbCONNECT24** are now automatically copied to the mbNET and the device reboots.

If the **mbNET** is able to connect to the Internet (e.g. network, telephone cable, SIM card, antennae installed), the device will subsequently log in to your account. This is indicated by the **flashing** LED **Con**. **4**.



ADVICE: If the firmware and an **mbCONNECT24** portal configuration are located on the USB stick, the firmware is always recognized by the mbNET (**Fc1** + **Fc3 flashing**) first. If you do not press the **Dial Out** button within 10 seconds, the **mbNET** will change to the portal configuration (**Fc1** + **Fc2 flashing**). If you do not react within 10 seconds, the device returns to normal mode.

27. Factory settings on delivery

27.1 Username and password

The router is shipped with the following username and password:

Username: admin

Password: No password required


27.2 IP address of the router

The router is set to the following IP address in the factory:

IP address: 192.168.0.100


28. Loading the factory settings

Follow the steps outlined below to reset the industrial router to the factory settings:

 **IMPORTANT:** You should first **back up** your configuration. Once you have carried out these steps, your previous settings will no longer be available.

1. Switch on the device
2. Wait until the **Rdy** LED **blinks**
3. Press and hold the dial-out button until the **Fc4** / TxD2 LED lights up
4. Press the dial-out button again (**Fc3** / Rx D2 lights up)
5. Press the dial-out button again (**Fc2** / Tx D1 lights up)
6. Finally press the dial-out button one last time

The custom configuration is then deleted. The industrial router is reset to the factory settings and can be reconfigured.

 **IMPORTANT:** The IP address of the industrial router is reset to 192.168.0.100. The computer's network settings must be changed accordingly.

29. Restart the mbNET router

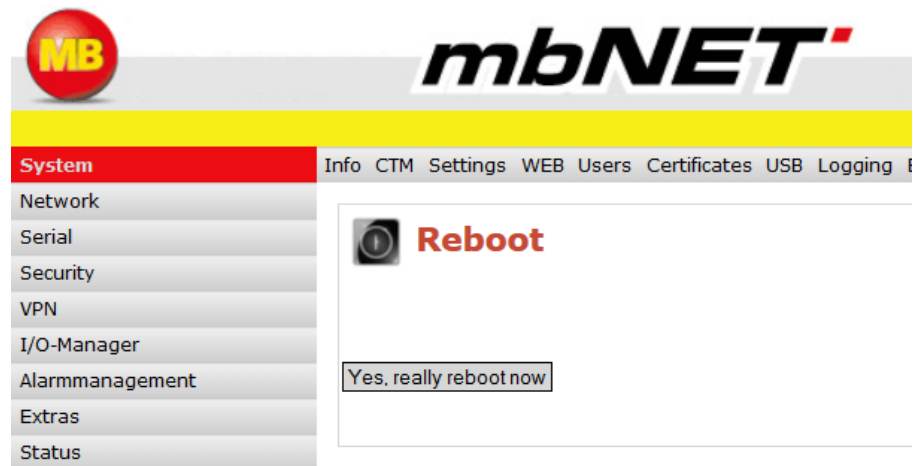
29.1 Via webinterface

Click on „Restart“ on top right of the page screen.



Now click on auf den Button „Yes, really reboot now“.

The restart process takes about 2 minutes.



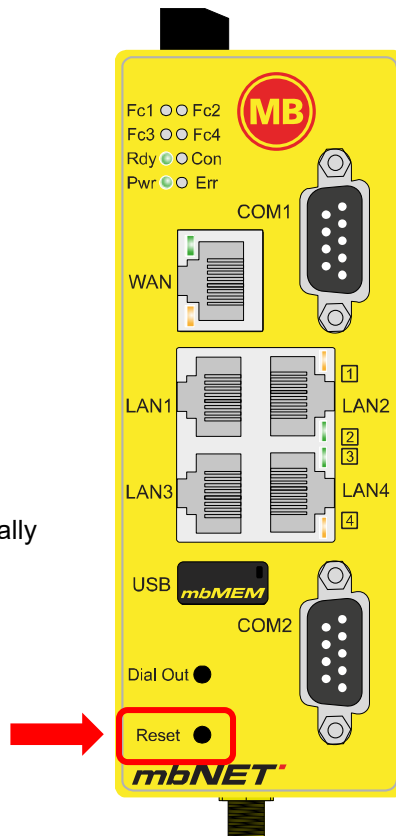
29.2 Via reset button

Press the „Reset“ button on the **mbNET**.

This initiates the booting process. The restart is complete, when both LED „Rdy“ and „Pwr“ illuminate.

Note:

The „Reset“ Button does not actually Reset the router. It just reboots it.



30. Initializing the modem

General information on the AT commands

The commands can be entered in the input interface (modem settings) in the two fields “Modem Initialization”.

The **prefix** always consists of the letters “AT”.
This does not have to be entered in the field.

The **command** consists of individual characters that are written as described below. It is made up of a code and, if applicable, any associated values.

Letters can be in uppercase and lowercase. Multiple commands can be combined into a command line.

Example: L1M1\N5

30.1 Analog modem commands

B **Selects the communication standard**

ATB0 CCITT modulation
 ATB1 Bell modulation

\B **Treatment of the break signal**

AT\Bn Send break signal to remote station
 n= 0-9 in 100 ms units (AT\B3 standard)
 Only possible with a non-error corrected connection

%C **Data compression setting**

AT%C0 Data compression inactive
 AT%C1 Data compression active

+GCI **Country-specific setting**

This command configures the analog modem to the country-specific setting
 Example +GCI=B5

Initializing the modem (continued)

L Loudspeaker volume

ATL0,1 Low volume
 ATL2 Medium volume
 ATL3 High volume

M Loudspeaker mode

ATM0 Loudspeaker always on
 ATM1 Loudspeaker on until data carrier signal is detected
 ATM2 Loudspeaker on when the modem is ready to dial
 ATM3 Loudspeaker off while the number is being dialed and then, after dialing, until a data carrier signal is detected

+MS Selects the modulation type

This command sets the modulation type and the bit rates negotiated between the local and remote modems.

Syntax: +MS=[<carrier>[,<auto-mode>[,<min_tx_rate>[,<max_tx_rate>[,<min_rx_rate>[,<max_rx_rate>]]]]]

Example: AT+MS= V34,1,9600,33600,9600,33600

Modulation	<carrier>	Possible baud rates
Bell 103	B103	300
Bell 212	B212	1200 Rx 75 Tx or 75 Rx/1200 Tx
V.21	V21	300
V.22	V22	1200
V.22 through	V22B	1200, 2400
V.23	V23C	1200
V.32	V32	4800, 9600
V.32 through	V32B	4800, 7200, 9600, 12000, 14400
V.34	V34	2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, 31200, 33600

Automode 0=disabled
 1=enabled (default)

AT+MS? Shows the current setting

W Selects the error correction settings

AT\N0 Error correction switched off
 AT\N1 Transparent transmission of any data widths via the serial interface, without data buffering and error correction.
 AT\N2 V.42LAP-M or MNP 4 error correction. The modem hangs up if a failsafe connection cannot be established.
 AT\N3 V.42LAP-M or MNP 4 error correction. A non-failsafe connection will be attempted if a failsafe connection cannot be established.
 AT\N4 V.42LAP-M error correction; the modem hangs up if this is not possible.
 AT\N5 MNP error correction; the modem hangs up if this is not possible.

Initializing the modem (continued)**X Message output, dial tone detection**

This command controls how the modem reacts to the dial tone and busy signal and how it displays the CONNECT messages.

- ATX0 No busy and dial tone detection
i.e. NO CARRIER is displayed in response to a failed dialing attempt. Messages: OK, CONNECT, RING, NO CARRIER, ERROR and NO ANSWER are displayed
- ATX1 Like ATX0 but CONNECTxxx messages with speed specification
- ATX2 Busy tone detection disabled, dial tone detection enabled
Messages: OK, CONNECT, RING, NO CARRIER, ERROR, NO ANSWER and NO DIAL TONE are displayed
- ATX3 Busy tone enabled, dial tone detection disabled
Messages: OK, CONNECT xxx, RING, NO CARRIER, ERROR, NO ANSWER
- ATX4 Busy tone and dial tone detection enabled
Messages: OK, CONNECTxxx, RING, NO CARRIER, ERROR, NO ANSWER and NO DIAL TONE

30.2 ISDN terminal adapter (TA) commands**B Defines the transmission protocol in the B channel**

- ATB0: V.110 asynchronous
ATB3: PPP asynchronous to synchronous conversion (PPP asynchronous single link)
ATB4: HDLC transparent
ATB5: Byte transparent (B channel data)
ATB10: X.75 transparent
ATB13: V.120
ATB20: X.31 B channel (X.25 B channel)
ATB21: X.31 D channel

N Defines the transmission rate in V.110 mode

- ATN0 Automatic connection speed
ATN1 Connection speed 1,200 bps
ATN2 Connection speed 2,400 bps
ATN3 Connection speed 4,800 bps
ATN4 Connection speed 9,600 bps
ATN5 Connection speed 19,200 bps

#Z Defines the MSN (multiple subscriber number)

All calls are accepted if the number is set to "*" (asterisk) (default setting).
An MSN generally has to be entered as this is required by most PBX systems. The MSN must also be enabled for the data service.

AT#Z=n Sets MSN to n

31. Appendix

31.1 Country codes for analog devices

Nr.	Country	Modem operation setting
1	Afghanistan	B5
2	Albania(AL)	B5
3	Algeria(DZ)	B5
4	American Samoa(AS)	B5
5	Andorra(AD)	B5
6	Angola(AO)	B5
7	Anguilla(AI)	B5
8	Antarctica(AQ)	B5
9	Antigua and Barbuda(AG)	B5
10	Argentina(AR)	07
11	Armenia(AM)	B5
12	Aruba(AW)	B5
13	Australia(AU)	09
14	Austria(AT)	FD
15	Azerbaijan(AZ)	B5
16	Bahamas(BS)	B5
17	Bahrain(BH)	B5
18	Bangladesh(BD)	B5
19	Barbados(BB)	B5
20	Belarus(BY)	B5
21	Belgium(BE)	FD
22	Belize(BZ)	B5
23	Benin(BJ)	B5
24	Bermuda(BM)	B5
25	Bhutan(BT)	B5
26	Bolivia(BO)	B5
27	Bosnia and Herzegovina(BA)	B5
28	Botswana(BW)	B5
29	Bouvet Island(BV)	B5
30	Brazil(BR)	16
31	British Indian Ocean Territory(IO)	B5
32	Brunei Darussalam(BN)	B5
33	Bulgaria(BG)	FD
34	Burkina Faso(BF)	B5
35	Burundi(BI)	B5
36	Cambodia(KH)	B5
37	Cameroon(CM)	B5
38	Canada(CA)	B5
39	Cape Verde(CV)	B5
40	Cayman Islands(KY)	B5
41	Central African Republic(CF)	B5
42	Chad(TD)	B5
43	Chile(CL)	B5
44	China(CN)	B5
45	Christmas Island(CX)	B5

Nr.	Country	Modem operation setting
46	Cocos (Keeling) Islands(CC)	B5
47	Colombia(CO)	B5
48	Comoros(KM)	B5
49	Congo(CG)	B5
50	Cook Islands(CK)	B5
51	Costa Rica(CR)	B5
52	Cote D'Ivoire(CI)	B5
53	Croatia(HR)	B5
54	Cuba(CU)	B5
55	Cyprus(CY),	FD
56	Czech Republic(CZ)	FD
57	Denmark(DK)	FD
58	Djibouti(DJ),	B5
59	Dominica(DM)	B5
60	Dominican Republic(DO)	B5
61	East Timor(TP)	B5
62	Ecuador(EC)	B5
63	Egypt(EG)	B5
64	El Salvador(SV)	B5
65	Equatorial Guinea(GQ)	B5
66	Eritrea(ER)	B5
67	Estonia(EE)	FD
68	Ethiopia(ET)	B5
69	Falkland Islands (Malvinas)(FK)	B5
70	Faroe Islands(FO)	B5
71	Fiji(FJ)	B5
72	Finland(FI)	FD
73	France(FR)	FD
74	France-Metropolitan(FX)	FD
75	French Guiana(GF)	B5
76	French Polynesia	B5
77	French Southern Territories(TF)	B5
78	Gabon(GA)	B5
79	Gambia(GM)	B5
80	Georgia(GE)	B5
81	Germany(DE)	FD
82	Ghana(GH)	B5
83	Gibraltar(GI)	B5
84	Greece(GR)	FD
85	Greenland(GL)	B5
86	Grenada(GD)	B5
87	Guadeloupe(GP)	B5
88	Guam(GU)	B5
89	Guatemala(GT)	B5
90	Guinea(GN)	B5
91	Guinea-Bissau(GW),	B5
92	Guyana(GY)	B5
93	Haiti(HT)	B5
94	Heard and Mc Donald Islands(HM)	B5

Nr.	Country	Modem operation setting
95	Honduras(HN)	B5
96	Hong Kong(HK)	99
97	Hungary(HU)	FD
98	Iceland(IS)	FD
99	India(IN)	B5
100	Indonesia(ID)	99
101	Iran(Islamic Republic of)(IR)	B5
102	Iraq(IQ)	B5
103	Ireland(IE)	FD
104	Israel(IL)	B5
105	Italy(IT)	FD
106	Jamaica(JM)	B5
107	Japan(JP)	00
108	Jordan(JO)	B5
109	Kazakhstan(KZ)	B5
110	Kenya(KE)	B5
111	Kiribati(KI)	B5
112	Korea-Democratic People's Republic(KP)	B5
113	Korea-Republic of(KR)	B5
114	Kuwait(KW)	B5
115	Kyrgyzstan(KG)	B5
116	Lao People's Democratic Republic(LA)	B5
117	Latvia(LV)	FD
118	Lebanon(LB)	B5
119	Lesotho(LS)	B5
120	Liberia(LR)	B5
121	Libyan Arab Jamahiriya(LY)	B5
122	Liechtenstein(LI)	FD
123	Lithuania(LT)	FD
124	Luxembourg(LU)	FD
125	Macau(MO)	B5
126	Macedonia(MK)	B5
127	Madagascar(MG)	B5
128	Malawi(MW)	B5
129	Malaysia(MY)	6C
130	Maldives(MV)	B5
131	Mali(ML)	B5
132	Malta(MT)	FD
133	Marshall Islands(MH)	B5
134	Martinique(MQ)	B5
135	Mauritania(MR)	B5
136	Mauritius(MU)	B5
137	Mayotte(YT)	B5
138	Mexico(MX)	B5
139	Micronesia(Federated States of)(FM)	B5
140	Moldova-Republic of(MD)	B5
141	Monaco(MC)	B5
142	Mongolia(MN)	B5
143	Montserrat(MS)	B5

Nr.	Country	Modem operation setting
144	Morocco(MA)	B5
145	Mozambique(MZ)	B5
146	Myanmar(MM)	B5
147	Namibia(NA)	B5
148	Nauru(NR)	B5
149	Nepal(NP)	B5
150	Netherlands(NL)	FD
151	Netherlands Antilles(AN)	FD
152	New Caledonia(NC)	B5
153	New Zealand(NZ)	7°
154	Nicaragua(NI)	B5
155	Niger(NE)	B5
156	Nigeria(NG)	B5
157	Niue(NU)	B5
158	Norfolk Island(NF)	B5
159	Northern Mariana Islands(MP)	B5
160	Norway(NO)	FD
161	Oman(OM)	B5
162	Pakistan(PK)	B5
163	Palau(PW)	B5
164	Panama(PA)	B5
165	Papua New Guinea(PG)	B5
166	Paraguay(PY)	B5
167	Peru(PE)	B5
168	Philippines(PH)	B5
169	Pitcairn(PN)	B5
170	Poland(PL)	FD
171	Portugal(PT)	FD
172	Puerto Rico(PR)	B5
173	Qatar(QA)	B5
174	Reunion(RE)	B5
175	Romania(RO)	FD
176	Russian Federation(RU)	B5
177	Rwanda(RW)	B5
178	St. Helena(SH)	B5
179	Saint Kitts and Nevis(KN)	B5
180	Saint Lucia(LC)	B5
181	St. Pierre and Miquelon(PM)	B5
182	Saint Vincent and the Grenadines(VC)	B5
183	Samoa(WS)	B5
184	San Marino(SM)	B5
185	Sao Tome and Principe(ST)	B5
186	Saudi Arabia(SA)	B5
187	Senegal(SN)	B5
188	Seychelles(SC)	B5
189	Sierra Leone(SL)	B5
190	Singapore(SG)	9C
191	Slovakia(SK)	FD
192	Slovenia(SI)	FD

Nr.	Country	Modem operation setting
193	Solomon Islands(SB)	B5
194	Somalia(SO)	B5
195	South Africa(ZA)	9F
196	South Georgia, South Sandwich Islands(GS)	B5
197	Spain(ES)	FD
198	Sri Lanka(LK)	B5
199	Sudan(SD)	B5
200	Suriname(SR)	B5
201	Svalbard and Jan Mayen Islands(SJ)	B5
202	Swaziland(SZ)	B5
203	Sweden(SE)	FD
204	Switzerland(CH)	FD
205	Syrian Arab Republic(SY)	B5
206	Taiwan-Province of China(TW)	FE
207	Tajikistan(TJ)	B5
208	Tanzania-United Republic of(TZ)	B5
209	Thailand(TH)	B5
210	Togo(TG)	B5
211	Tokelau(TK)	B5
212	Tonga(TO)	B5
213	Trinidad and Tobago(TT)	B5
214	Tunisia(TN)	B5
215	Turkey(TR)	FD
216	Turkmenistan™	B5
217	Turks and Caicos Islands(TC)	B5
218	Tuvalu(TV)	B5
219	Uganda(UG)	B5
220	Ukraine(UA)	B5
221	United Arab Emirates(AE)	B5
222	United Kingdom(UK)	FD
223	United States(US)	B5
224	United States Minor Outlying Islands(UM)	B5
225	Uruguay(UY)	B5
226	Uzbekistan(UZ)	B5
227	Vanuatu(VU)	B5
228	Vatican City State (Holy See)(VA)	B5
229	Venezuela(VE)	B5
230	Vietnam(VN)	99
231	Virgin Islands (British)(VG)	B5
232	Virgin Islands (U.S.)(VI)	B5
233	Wallis and Futuna Islands(WF)	B5
234	Western Sahara(EH)	B5
235	Yemen(YE)	B5
236	Yugoslavia(YU)	B5
237	Zaire(ZR)	B5
238	Zambia(ZW)	B5
239	Zimbabwe(ZW)	B5