

IE-ARM

Access Router Mini



Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 16
32758 Detmold

Tel.: 0 52 31 / 14-0
Fax: 0 52 31 / 14 20 83

Version 3.1.0, March 2006

Copyright

Weidmüller Interface GmbH & Co. KG. All rights reserved.

All rights are reserved, including those of translation, reprinting, and reproduction of this manual, or parts thereof. No part of this manual may be reproduced, processed, copied, or transmitted in any way whatsoever (photocopy, microfilm, or other method) without the express written permission of Weidmüller Interface GmbH & Co. KG, not even for use as training material, or in using electronic systems. All rights reserved in the case of a patent grant or registration of a utility model or design.

Copyright © 2005 by

Weidmüller Interface GmbH & Co. KG

Klingenbergstraße 16

D-32758 Detmold



NOTE

We have checked the contents of this manual for conformity with the hardware and software described. Nevertheless, because deviations cannot be ruled out, we cannot accept any liability for complete conformity. The data in this manual have been checked regularly and any necessary corrections will be included in subsequent editions.

We always welcome suggestions for improvement.

Trademarks

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

All products mentioned herein may be trademarks or registered trademarks of their respective owners.

HEYFRA[®] is a registered trademark of HEYFRA ELECTRONIC GmbH

Weidmüller[®] is a registered trademark of Weidmüller Interface GmbH & Co. KG

5 Year Warranty

Any use other than that as prescribed will render the warranty null and void.

Weidmüller gives a 2 year warranty on all its actively processing Industrial Ethernet products and all actively processing I/O-Interface products in accordance with the warranty terms as described in the general conditions of sale of the Weidmüller company which has sold the products to you.

In addition to the 2 year warranty, Weidmüller warrants to you for a period of 3 additional years that such products the defects of which have already existed at the time when the risk passed will be repaired by Weidmüller free of charge or that Weidmüller will provide a new, functionally equivalent product to replace the defective one.

The warranty referred to above covers Weidmüller products. Safe where expressly described otherwise in writing in this catalogue/product description, Weidmüller gives no warranty or guarantee as to the interoperability in specific systems or as to the fitness for any particular purpose. To the extent permitted by law, any claims for damages and reimbursement of expenses, based on whatever legal reason, including contract or tort, shall be excluded. Where not expressly stated otherwise in this warranty, the general conditions of purchase and the expressive liability commitments therein of the respective Weidmüller company which has sold the products to you shall be applicable.

1	Safety Notes	1-4
1.1	Graduated safety notes	1-4
1.2	Definitions	1-4
1.3	Hazards resulting from use other than as described	1-5
1.4	Hazards resulting from modifications and upgrades	1-5
1.5	Admitted personnel	1-5
1.5.1	Operator	1-6
1.5.2	Start-up engineer	1-6
1.5.3	Service engineer	1-6
1.6	Electrical connections	1-7
1.7	Safety regulations	1-7
1.8	Service and maintenance	1-8
1.9	Waste disposal	1-8
1.10	Liability	1-9
2	Use as Prescribed	2-10
2.1	Range of application	2-10
3	Description of Functions	3-12
3.1	General description of functions	3-12
3.2	Functioning of "Dial on demand"	3-12
3.3	Functioning of "Dial-in server"	3-13
3.4	Call-back functionality	3-14
3.5	Commissioning	3-14
3.6	Connecting	3-14
3.7	Installing the operating system	3-16
3.7.1	Resetting the router to its factory default settings	3-17
3.7.2	Reading the IP address of the router via the console	3-20
4	Configuring the Router	4-21
4.1	Configuring via the Ethernet	4-21
4.1.1	Configuring via the Ethernet interface	4-21
4.1.2	Adapting the IP address of your PC	4-21
4.1.2.1	Windows 2000/Windows XP (classic)	4-22

4.1.2.2	Setting up the network card under Linux	4-24
4.2	Configuration services	4-26
4.2.1	Web browser	4-26
4.2.1.1	Menu option "General"	4-28
4.2.1.2	Menu option "DNS"	4-31
4.2.1.3	Menu option "SSH"	4-31
4.2.1.4	Menu option "HTTP"	4-32
4.2.1.5	Menu option "Date & time"	4-33
4.2.1.6	Menu option "Protocol service"	4-33
4.2.1.7	Configuring the modem	4-35
4.2.1.8	Menu option "Dial-out - modem"	4-37
4.2.1.9	Menu option "Dial-out - DynDNS"	4-38
4.2.1.10	Menu option: "Dial-in"	4-39
4.2.1.11	Menu option "Firewall"	4-40
4.2.1.12	Menu option: "Firewall - Masquerading"	4-41
4.2.1.13	Menu option "Firewall - Routing"	4-41
4.2.1.14	Menu option "Firewall - Trusted Nets"	4-42
4.2.1.15	Menu option "Firewall - Destination NAT" (Port Forwarding)	4-43
4.2.1.16	Menu option "Save all"	4-44
4.2.1.17	Menu option "Restarting the router"	4-44
4.2.1.18	Menu option "Close PPP connections"	4-44
4.2.1.19	Network status statistics	4-45
4.3	Configuring the client computers	4-46
4.3.1	Configuring the PCs integrated into router network	4-46
4.3.2	Configuring a PC not integrated into the router network	4-47
5	Hardware	5-48
5.1	Installation	5-48
5.1.1	Dimensions	5-48
5.1.2	Installing the top-hat rail	5-49
5.2	Installation notes	5-51
5.2.1	Mounting the router on a top-hat rail	5-51
5.2.2	Functional earthing	5-51
5.3	Installation guidelines	5-52
5.4	Storage and storage temperatures	5-52
5.5	Operating temperature, humidity	5-52
5.6	Status display	5-53

5.6.1	Display "Console/modem"	5-54
5.6.2	Display "Ethernet interface active"	5-54
5.6.3	Display "POWER on/off"	5-54
5.7	Connections / interfaces	5-55
5.7.1	Power supply	5-56
5.7.2	Ethernet interface	5-57
5.7.3	RS-232 interface for the "Console" or "Modem" mode	5-57
5.7.4	RS-232 interface for connecting an external modem	5-57
6	Technical Data	6-58
7	Standards and Certifications	7-59
7.1	Harmonised standards	7-59
7.2	Certification to DIN EN ISO 9001	7-59
7.3	Approbations	7-59
7.4	CE marking	7-59
8	Symbols Used	8-60

1 Safety Notes

1.1 Graduated safety notes

In this Instruction Manual, safety notes are marked with a symbol and the keyword DANGER, ATTENTION or NOTE at the page margin. Safety notes are printed in bold letters and are marked with an outside border.

1.2 Definitions



DANGER

The keyword **DANGER** is used to warn you of a possibly hazardous situation.



DANGER

DANGER of electric shock is used to warn of a possibly hazardous situation involving electric current.



ATTENTION

ATTENTION alerts you to hazards and error sources.



NOTE

The keyword **NOTE** is used to draw your attention to an important recommendation to be observed.

1.3 Hazards resulting from use other than as described

**DANGER**

Use other than as prescribed may result in personal injuries to the user or third persons, as well as in material damage to the control system or the product, or in environmental damage. The IE-ARM must only be used according to its intended purpose!

1.4 Hazards resulting from modifications and upgrades

**DANGER**

Unauthorised modifications and amendments are not permitted. Such unauthorised modifications or amendments may impair the proper operation of the device, resulting in personal injuries, material damage or environmental impairments and will render all liability on our part null and void.

1.5 Admitted personnel

**DANGER**

Only sufficiently qualified and instructed personnel are allowed to operate the IE-ARM!

It must only be commissioned by an electrical expert.

Service and maintenance, as well as troubleshooting, must only be carried out by qualified expert personnel.

1.5.1 Operator

The operator:

- is an instructed person
- who is authorised to turn on / turn off the equipment.

1.5.2 Start-up engineer

The start-up engineer:

- is an electrical expert,
- must be an expert in parameterising the device
- who carries out the start-up, observing strict precautions and
- carries out the required test.

1.5.3 Service engineer

The service engineer:

- is a qualified expert
- who services the electrical and mechanical components of the control system,
- carries out maintenance work,
- carries out troubleshooting.

1.6 Electrical connections

The IE-ARM must be connected to an electrical supply system.



DANGER

Power supply connection

The IE-ARM must only be connected to the electrical supply system by an electrical expert.

The power supply of the IE-ARM must be provided exclusively by a power pack which complies with DIN EN 60 742 (VDE 0551).

Make sure that an appropriate fuse is installed in the incoming supply feeder.

For operation of the IE-ARM, please refer to the information provided in Chapter 6 Technical Data.

1.7 Safety regulations

The IE-ARM possesses a housing.



DANGER

Electrical hazards

The operation of the IE-ARM is only allowed with the housing closed.

The housing prevents:

- persons from coming into contact with live parts;
- the penetration of humidity and foreign substances, and
- the impairment of system functions by electromagnetic interference

The housing cover must not be opened.

1.8 Service and maintenance

**DANGER**

Service and maintenance work

Improper service and maintenance may result in loss of life, personal injuries, material damage or environmental impairments.

Service and maintenance work, as well as troubleshooting must only be carried out by qualified expert personnel.

Before performing service or maintenance work, always switch off the power supply of the IE-ARM first!

Reinstall all panelling, protective covering and safety devices immediately at completion of service and maintenance work and check their functioning.

**DANGER**

Spare parts

The use of inappropriate spare parts may result in loss of life, personal injuries, material damage or environmental impairments.

The spare parts must comply with the technical requirements of the manufacturer.

Use exclusively genuine Weidmüller spare parts!

1.9 Waste disposal

**DANGER**

Electrical scrap (components, CRT units, etc.) may harm the environment.

Dispose of electro technical equipment only according to the relevant environmental regulations or entrust an expert company with this job.

1.10 Liability

The contents of the present Instruction Manual are subject to technical modifications, which may result, in particular, from the continuous further development of the products made by Weidmüller. Weidmüller will not assume any liability for printing errors or any other inaccuracies contained in the present Instruction Manual, unless these are serious errors which are evidently known to Weidmüller. In addition, the "General Terms and Conditions for the Supply of Products and Services in the Electrical Industry" shall apply. In any case, the relevant national and international standards and regulations will apply in addition to the notices and instructions contained in this Instruction Manual.

**NOTE****Use other than prescribed - exclusion of liability**

Weidmüller will not be liable for damage resulting from use or application of the products not according to the intended purpose or other than as prescribed.

Use as prescribed or according to the intended purpose also includes the exact knowledge of this Instruction Manual. In particular, the notes and safety notes contained therein must be observed.

If you run the products together with other components, such as safety modules, control systems or sensors, always observe the relevant user information of such devices.

**NOTE**

If the Mini-Router dials in to an Internet provider via the public telephone network, this will incur telephone and dial-in charges. Weidmüller accepts no liability for any charges, including those arising from inadvertent dial-ins.

2 Use as Prescribed

2.1 Range of application

The Mini-Router grants an industrial IP network access to the Internet via an external analog or ISDN modem or via a connected network (IE-ARM-E only).

The Mini-Router provides for the transporting of IP packets between an IP-based industrial network and another network (e.g. Internet). The Internet access is activated automatically as necessary. The Mini-Router is configured either locally via the IP network or externally via the telephone network.

In addition, access from a remote computer to the industrial IP network is also possible. Thus, clients installed in the network can be controlled via IP-based services (SSH, HTTP).

**NOTE**

It is strongly recommended to use a web browser for configuring.

**DANGER**

Any errors in configuration, in the execution of any work or operations, as well as inadvertent false operation may impair the proper functioning of the IE-ARM, resulting in personal injury, or material or environmental damage. Therefore, only sufficiently qualified personnel are allowed to operate the IE-ARM.

Always observe the safety notes!

The IE-ARM is intended exclusively for use in machines complying with the scope of application of DIN EN 60204-1:1998-11 (Electrical Equipment of Machines).

**DANGER**

Do not use the IE-ARM in potentially explosive areas!

When connecting the device, observe, in particular, the information provided in the following sections:

- 1.6 Electrical connections
- 5 Hardware
- 6 Technical Data.

3 Description of Functions

3.1 General description of functions

The Mini-Router permits a local Ethernet based on TCP/IP to communicate with another IP network via a PPP connection (long-distance data transmission).

The PPP connection is established via an external modem by default (analog modem or ISDN modem, see Chapter 6). This grants all clients integrated into the network access to a remote PPP server (Internet provider, in-house monitoring computer) via a single interface.

The connection is only established when necessary using externally addressed IP packets. If the connection is not used for longer period (time can be configured), it is closed down.

Furthermore, dial-in is possible from an authorised remote computer using a modem. By using this connection, the router may also be monitored and configured.

Since the router shows a transparent behaviour with such a direct PPP connection, the clients working in the Ethernet may be addressed directly, and IP-based services, such as FTP, may be used.

With the type "IE-ARM-E", direct access is possible to a connected network (Ethernet 2) via the second TCP/IP even without a modem.

A configurable firewall software is preinstalled, helping protect the Ethernet from unauthorised access from outside.

3.2 Functioning of "Dial on demand"

The Mini-Router establishes a connection to the Internet only when necessary ("on demand"). This situation arises if the router receives an IP packet from the internal Ethernet, which possesses a target address outside the Ethernet. At this time, the router checks whether there is already a modem connection. If this is not the case, the router will use its external modem to dial a number specified by you. Then, a PPP program becomes active which will establish an IP connection using the PPP protocol (point-to-point).

**NOTE**

Depending on the modem type you are using (analog or ISDN) and depending on the quality of the telephone line, this process may take up to 60 seconds. During this time, some applications trigger a time-out and will deem your query to the Internet as failed. It could therefore be necessary to adapt the time-out time to your programs.

When data are being transferred, the LED `con` flashes green.

**ATTENTION**

Check where services can be found in your network which put queries to the Internet automatically at cyclic intervals (e.g. Netscape Mail). Such queries may result in an undesired connection being established or else may prevent disconnection by creating data traffic to the outside. If necessary adapt your firewall settings accordingly (disabling of the port number of the service in "PORTS NOT FORWARDED"; see Section 4.2.1.15).

The automatic closure of the connection with the connection inactive must be adapted individually. With applications that result in periodic data traffic, very short time-out times can hinder the transmission. Therefore, it must be checked whether it is better to maintain the connection or to re-establish the connection for each new transmission. Excessively long time-out times will increase the risk that, for example, a port scanner could create data traffic from outside so that the connection cannot be closed down as configured (see Section 4.2.1.8).

3.3 Functioning of "Dial-in server"

The Mini-Router can be configured as a dial-in server. This means that the modem of the router may accept calls via the telephone network. Thus, a direct PPP (long-distance data transmission) connection may be established to the router.

When the router is called, the modem is requested to pick up. After picking up, a PPP server becomes active on the router and checks the authentication of the caller. Then the IP data set according to Section 4.2.1.10 are transmitted to the remote computer automatically.

With the connection active, you can now communicate transparently with the router services (Webserver, SSH) or the services provided by the clients integrated into the Ethernet.

The connection is only closed if it is quit manually by the remote computer.

**NOTE**

Please note that dialling during an existing modem connection is not possible, since the telephone-line is already busy.

In the case of a IE-ARM-U with two modems connected, concurrent dialling via the second modem is possible if a connection already exists.

3.4 Call-back functionality

The router can be configured such that it will not work as a dial-in server (see Section 4.2.1.10). Instead, in the case of an incoming call, it will hang up immediately after the authentication and will then automatically establish a connection to the Internet provider configured. The router can now be addressed in the Internet.

To address the router using its domain name, it is recommended to configure also an appropriate dynamic DNS provider when selecting this function (see Section 4.2.1.9).

3.5 Commissioning

The commissioning of the Mini-Router includes three steps:

- Connecting - see Section 3.6;
- Booting by switching on the supply voltage;
- Configuring the router - see Section 4.

3.6 Connecting

First connect the router to a switch on the 10/100 Ethernet1 socket using a patch cable. If you only want to connect a single host and not a complete network to the router, use a crossover cable.

Now connect the Sub-D interface marked with Modem or Modem 1 or Modem 2 to a modem using a modem cable, see Section 5.7.3 and 5.7.4.

For diagnostic purposes, the router may also be connected to a computer via the RS232 interface labelled "CONSOLE", see Section 3.7.

Now connect the 24 V power supply to the POWER connection on the front side of the device, see Section 5.7.1 Power supply.

The ON condition could look as follows:

POWER:	green
Console/modem:	yellow/green
Link:	OFF

After switching on the supply voltage, the router will boot.



NOTE

The router does not have its own ON / OFF switch; the operating voltage must be connected in the system into which the router is integrated.



ATTENTION

For information on how to connect the Mini-Router, please refer to the Sections 1.6 Electrical connections, 5.7 Connections / interfaces and 6 Technical Data.

3.7 Installing the operating system

The operating system of the Mini-Router is subject to continuous further development to adapt it to the technical requirements and customer wishes. Devices which are already in use may thus also require a new operating system. The version currently installed on your device is displayed on the welcome page of the web browser (see Section 4.1).



The version number is also output at the end of the boot sequence and can be displayed via the serial interface using a terminal program.

Internet Access Router Version 3.1.1

Heyfra GmbH

The router is now ready to use.
You do not need to login now, this is only for maintenance.

3.7.1 Resetting the router to its factory default settings

If the Mini-Router cannot be reached nor a network connection, neither via a serial connection, as the IP address or the password are not known, you can restore the factory default settings.



ATTENTION

When the router is reset to its factory default settings, all user-specific settings are lost! In this case, the Mini-Router must be configured for its particular application after resetting.

To do so, you will need a PC on which a terminal program is installed, a free RS232 interface, and an RS232 interconnecting cable.

Windows already includes the terminal program HyperTerminal. Other terminal programs (such as "minicom" under Linux, etc.) are also supported.

Connect a free COM interface of your PC to the router's RS 232 interface labelled CONSOLE using the RS232 extension cable.


Make sure that the switch is set to `CON1`.

Now start HyperTerminal and specify a name of your choice for the new connection. Select the COM port you are using from the "New Connection" listbox.

The following settings are required for the serial interface:



The connection data are saved in the file *name.ht*. The connection can be selected and started from the menu "File - Open".

A connection which is already used can be re-established by clicking on the  icon in the toolbar. If no activities are running on the router, the screen remains white when HyperTerminal is running in the windows mode.

The activities display scrolls upwards out of the window. The display can be extended in the full-screen mode depending on the screen resolution (see next illustration).



ATTENTION

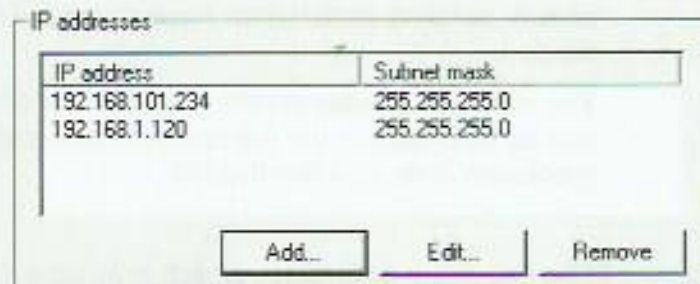
The previous activities, which may also have arisen from other communication activities, are displayed outside the visible window but can be viewed in the full-screen mode.



To load the new image file, proceed as follows:


- Establish a connection between HyperTerminal and the router.
- Boot the router; to do so, disconnect the supply voltage for approx. 5 s.

- During booting, after approx. 10 s, a message prompting you to reload the default settings is displayed for 10 seconds:



IP address	Subnet mask
192.168.101.234	255.255.255.0
192.168.1.120	255.255.255.0

Buttons: Add... Edit... Remove

- Subsequently, press the  key; the boot sequence is continued after loading the default settings.



ATTENTION

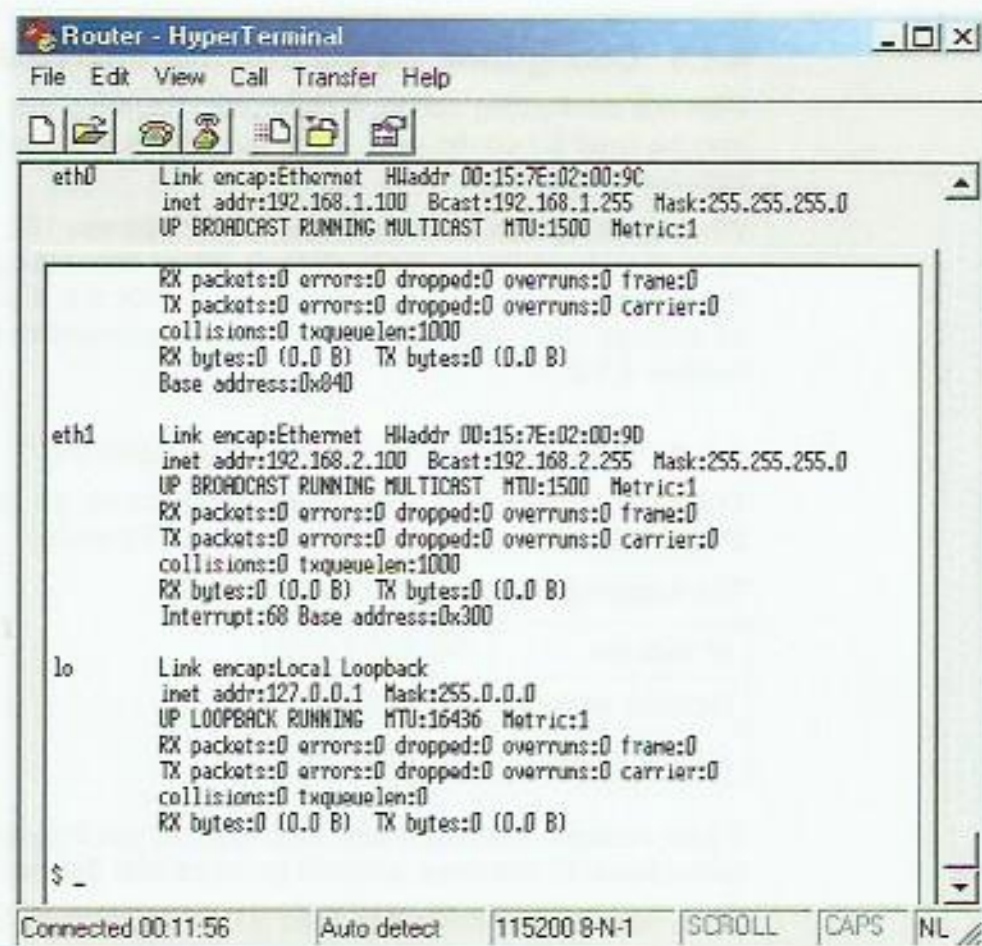
If you have changed passwords or IP addresses, they are also reset to their default settings.

For reconfiguring the router, please refer to the following sections.

3.7.2 Reading the IP address of the router via the console

Use a terminal program to establish a connection to the Mini-Router via a serial interface (see 3.7.1).

After logging in, enter the command `ifconfig`:



```
Router - HyperTerminal
File Edit View Call Transfer Help

eth0  Link encap:Ethernet  HWaddr 00:15:7E:02:00:9C
      inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
      Base address:0x040

eth1  Link encap:Ethernet  HWaddr 00:15:7E:02:00:9D
      inet addr:192.168.2.100  Bcast:192.168.2.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
      Interrupt:68 Base address:0x300

lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

$ _

Connected 00:11:56  Auto detect  115200 8-N-1  SCROLL  CAPS  NL
```

With HyperTerminal, the text lines will scroll out of the display window, but still exist. They become visible again after scrolling back or enlarging the viewing window.

4 Configuring the Router

Before commissioning, the router must be configured. The individual steps for configuring are explained in the present chapter.

4.1 Configuring via the Ethernet

4.1.1 Configuring via the Ethernet interface

With this configuring option, a computer integrated into your Ethernet may be used for configuring. Make sure that a standard web browser is installed on this PC.

When working with a web browser, the IP address 192.168.1.100 is used to address the router by default. When connecting via telephone, the address of the modem interface is 192.168.6.1. If your network uses an address other than 192.168.1.0, please proceed as described in Section 4.1.2.

4.1.2 Adapting the IP address of your PC

The initial configuration of the router must include an adaptation of the IP data of your router to the IP data of your Ethernet.

The following addresses are set by default:

IP address	192.168.1.100
Network address	192.168.1.0
Subnet mask	255.255.255.0

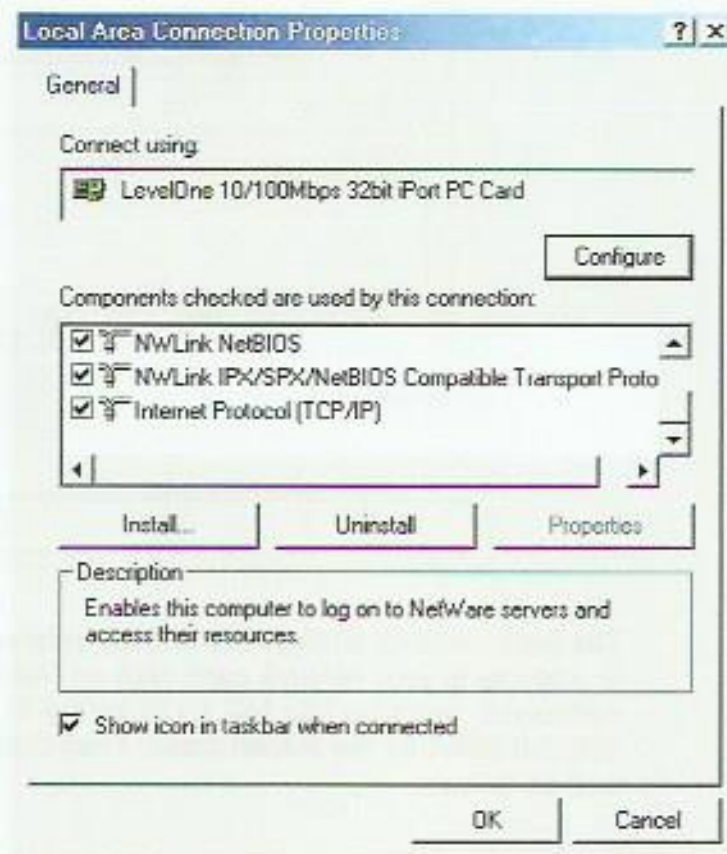
If your network address is also 192.168.1.0, you may skip the following instructions. In this case, you can proceed with Section 4.2.

In the operating systems Windows NT-SP6, Windows 2000, Windows XP or Linux/Unix, you may assign the network card of the appropriate computer more than one IP address (see Section 4.1.2.1 and Section 4.1.2.2). In addition, it is continued to be possible to use the configuring options "via the telephone network" or "via the serial interface" (not recommended).

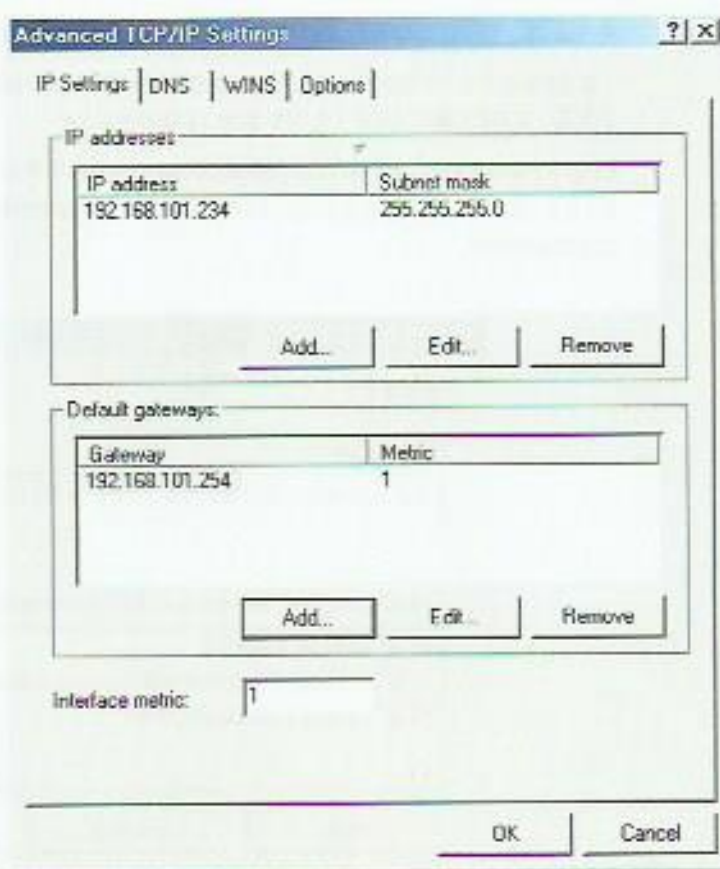
4.1.2.1 Windows 2000/Windows XP (classic)

To assign a network card one or several IP addresses under Windows 2000, administrator rights are required.

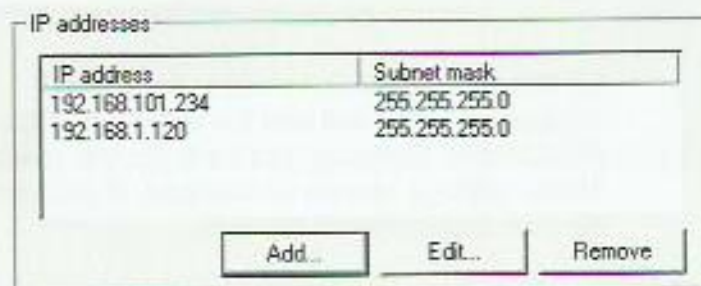
Log in yourself as administrator and open the Control Panel → Dial-Up Networking. Display the properties of your LAN connection:



On this tab, select Internet Protocol (TCP/IP) and click on "Properties". You will see the current configuration of your network card (IP address, Gateway, DNS etc.) in the window which then appears. These settings remain unchanged. If you click on "Advanced", the window shown below appears.



The basic network settings are already entered here. To add a second IP address to your network card, click on "Add" in the upper field "IP addresses" and type 192.168.1.120 for the IP address and 255.255.255.0 for the subnet mask. Then click on OK; the result should look as follows:



The computer you have just configured can be seen both in the network 192.168.101.0 and in the network 192.168.1.0 as of now. It is therefore not necessary any more to restart Windows 2000.

Now call a browser and type the following address: 192.168.1.100

Thereafter, you will be prompted to enter your user name and your password (default: user: admin, password: detmold).



The welcoming text of the embedded web server will appear. To configure the router, please proceed reading in Section 4.2.1.

4.1.2.2 Setting up the network card under Linux

To assign a network card two IP addresses under Linux, you must possess root rights. In addition, the use of a kernel 2.4.x or higher is recommended.

Open a console and assign yourself temporary root rights:

```
> su
Password:
```

Type "ifconfig" to check the status of your network condition:

```
> ifconfig
eth0 ...
lo ...
```

Select the card you want to assign a second IP address (here: eth0) and enter the following:

```
> ifconfig eth0:1 192.168.1.120 netmask
255.255.255.0
```

If you type "ifconfig" anew, the following should be output:

```
> ifconfig
eth0 ...
eth0:1 ...
lo ...
```

Thus, the interface "eth0" only possesses two IP addresses, and you can proceed configuring the router via the web interface. To do so, call a browser and type the following address: 192.168.1.100.

Thereafter, you will be prompted to enter your user name and your password (default: user: admin, pass: detmold).



The welcoming text of the embedded web server will appear. Now you can proceed with Section 4.2.1.

4.2 Configuration services

4.2.1 Web browser

You may use any browser which is able to handle frames as the configuration tool. The configuration can be performed with Internet Explorer 5.x, Mozilla 1.x, Opera 7.x and Conquerer 3.x, as well as with the correspondingly higher versions.

If the factory default settings have not been changed, the integrated web server of the router is started if you enter the IP address 192.168.1.100 (for Ethernet) as the URL. First, you are prompted to enter the user name and the password:

```
User:      admin
Password: detmold
```

The browser will create a dynamic web site from the configuration data of the router:



After selecting the language, the operating window is opened:



The screen is divided into four areas.

The "Navigation" area can be found on the left-hand side. Here you can choose the functionalities. The meaning of the individual elements is explained in the following sections.

To call the start page, click on "Start page" in the top right window.

The dialog language for the menus and help texts can be selected by clicking on the appropriate flag on the home page. At present, German and English are supported.

The central area is the actual working area. The settings are made here and status information is displayed here.

If necessary, help texts are displayed for the individual configuration options. To activate the online help for the individual items, simply click on the appropriate menu option. If a help text exists for the function on which the mouse pointer is positioned, the help text is displayed in a different colour and underlined. Clicking on the selected text activates the online help for the appropriate function.

The size of the help window can be changed by clicking and dragging the separation line.

netmask Ethernet 1:	255.255.255.0	<u>Netmask of the first subnet</u>
IP address Ethernet 2:	192.168.2.100	<u>the router's second IP address</u>
netmask Ethernet 2:	255.255.255.0	<u>Netmask of the second subnet</u>

The hostname is a unique name in the network the router is situated, to clearly identify the router in this network. The full qualified hostname of the router consists of the hostname and a domainname. The full qualified hostname will be compound by "Hostname.Domainname".

4.2.1.1 Menu option "General"

Click on the "General" menu option to call the basic configuration menu of the router. Two general configuration settings can be made there:

- the IP configuration
- the configuration of the administrator access

In addition, with the IE-ARM-E:

- the configuration of the default gateway
- the configuration of a static route.

These configuration options will be explained in the following.

IP configuration

IE-ARM-E:

TCP/IP configuration		
Host:	heyfra	the router's name
Domain:	ctrlink.de	the router's domain
IP address Ethernet 1:	192.168.1.100	the router's first IP address
netmask Ethernet 1:	255.255.255.0	Netmask of the first subnet
IP address Ethernet 2:	192.168.2.100	the router's second IP address
netmask Ethernet 2:	255.255.255.0	Netmask of the second subnet

Enter the host and the domain name, as well as IP address 1 and subnet mask 1 for the routed network here. The router can be reached via the external network using IP address 2 and subnet mask 2.

IE-ARM-U:

TCP/IP configuration		
Host:	heyfra	the router's name
Domain:	ctrlink.de	the router's domain
IP address Ethernet 1:	192.168.1.100	the router's first IP address
netmask Ethernet 1:	255.255.255.0	Netmask of the first subnet

Enter the host and the domain name, as well as IP address and subnet mask for the routed network here.

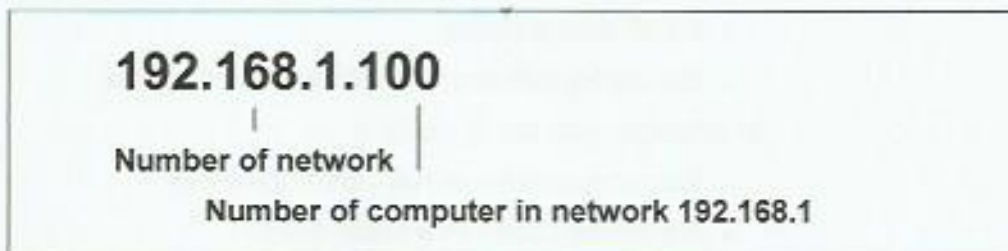


ATTENTION

Each individual interface (Ethernet, modem) must be located in a different network; otherwise, problems will occur in routing. In the worst case, the router can no longer be reached.

Brief information regarding IP addresses:

An IP address consists of the number of the IP network and of the number of a host in this network.



The size of the network portion may be varied via this IP address. It is determined by the network class. The example uses network class C, three numbers for the network, and one for the client.



For the IP addresses, any numbers between 1 and 254 are permissible. If a higher address is set, the router will not be found in the network by the browser. In this case, restore the factory default settings using the serial console (see Section 3.7).

Make sure that the address you are setting is not yet assigned within the network.

The default setting 192.168.1.100 corresponds to client no. 100 in a C class network with no. 192.168.1.0.

IE-ARM-E:

Gateway	
default gateway <input checked="" type="checkbox"/>	establish a default gateway in your LAN (switches off dialout)
Gateway: <input style="width: 100px;" type="text"/>	the gateway's IP address

If you select this option, a default gateway is set up for the router in the network. All packets whose target the router does not know are sent to the default gateway and routed from there further.



If you select this option, dial-out is deactivated.

IE-ARM-E only:

static routes

Net:

Netmask: or significant bits:

Gateway:

current routes

<input type="button" value="Add"/>	<input type="button" value="Delete"/>

A specified static route can be set up for individual networks.

Creating a static route:

- Network address for the static route
Network addresses must always end with ".0", e.g. "xxx.xxx.xxx.0".
- Subnet mask for the network address
Used by the router to determine automatically the number of significant bits.

Alternatively:

- Direct entry of the number of significant bits -
in this case, leave the field "Subnet mask" empty.
- Specify the gateway via which the network above can be reached.
- Add

Static routes created here are also entered automatically for Firewall/routing; there, however, they can be deleted and entered under Masquerading or Trusted Nets.

Clicking on removes a selected static route from the list and also from the Firewall settings Masquerading, Routing or Trusted Nets.

Configuring the administrator access

root access (administrator)

root password: password for root access

re-enter: password for root access (re-entered)

Enter the password for administrator access in these fields. This can be max. 8 characters long and should consist of letters, digits and special characters. If nothing is entered here, the old password is kept.



ATTENTION

It is strongly recommended to replace the default password 'detmold' by your own password with 8 characters. Keeping the default password published in this Manual constitutes a significant safety risk.

4.2.1.2 Menu option "DNS"

DNS configuration	
DNS forwarder: 145.253.2.11	DNS server(s) of your provider (or company)
<input checked="" type="checkbox"/> start "Domain Name Service"	
List of known hosts:	
Host name:	IP address:
heyfra	192.168.1.13
	<input type="button" value="Add"/>
	<input type="button" value="Delete"/>

The domain name service serves to dissolve the names in a network. Dissolving names means that each IP address is assigned a name which is easy to remember. This service is offered by the server. In order not to be compelled to enter all hosts of the entire company or even of the entire Internet here, the DNS forwarder conception has been created. Any addresses which cannot be dissolved by the local name server are forwarded to the host entered here. Therefore, specify either the IP address of the name server of your company or that of your Internet provider here.

In the bottom field, you can enter each host in your network to be dissolved by the router itself and assign the name the appropriate IP address.

4.2.1.3 Menu option "SSH"

Here you can configure the SSH server.

<input checked="" type="checkbox"/> start SSH daemon	
SSH user	
SSH user name: sshuser	user name for SSH access
SSH password:	re-enter:

The SSH server can be reached on port 22.

**ATTENTION**

Please observe that port 22 must not be assigned to another service (DNS, HTTP, etc.).

You may create a user for access to the SSH. If not, no additional user will be created, and only access to the administrator is granted via SSH.

When you select the `Start SSH server` option, a default user `sshuser` is already preconfigured.

**NOTE**

It is recommended to create an additional user here to provide an additional less privileged access to the system.

If you create a user, it is imperative to enter a password; otherwise, you will not be able to create a user. The password will follow the same rules as the password for access to the administrator (max. 8 characters, letter, digits, special characters, etc.).

4.2.1.4 Menu option "HTTP"

Since the HTTP server is required for configuring the router, it cannot be turned off. You may define the port and the user.

start SSH daemon

SSH user

SSH user name: <code>sshuser</code>	user name for SSH access
SSH password: <input type="text"/>	re-enter: <input type="text"/>

Any changes you make here will only come into effect after restarting the router. In other words: You may first finish configuring the router without undue problems before you restart the router.

The default port for an HTTP server is 80; all browsers poll this port by default. If you want to use a different port here, you must add it in the address line of your browser. For example <http://192.168.1.100:8080>, sends an HTTP request to the host to port 8080 instead of port 80, specifying address 192.168.1.100.

**ATTENTION**

Please observe the port entered here must not be occupied by another service (DNS, SSH, VPN, etc.).

Therefore, only use ports whose number is greater than 1,024.

4.2.1.5 Menu option "Date & time"

Time server

Time server

activate time server

Host: 192.53.103.103 the time server's host name or IP address

The Mini-Router does not possess a clock of its own. When the operating voltage is connected, a time counter begins to run whose count is used for the time stamp for the messages. The time counter is not buffered, i.e. when the operating voltage is disconnected, the counter state is lost.

To ensure that the time displayed on the time stamp is correct, you can synchronise the time counter via a time server on the Internet. The default address is only a recommendation; the system operator can select the time server himself. If the time server is activated, it must be ensured that it can be reached by the Mini-Router.

4.2.1.6 Menu option "Protocol service"

start syslog daemon

Syslog service options

60 time intervall between two mark messages in minutes

Logging rules:

Source: auth ▾ Source of messages to be logged

Log level: debug ▾ Level of Messages that shall be logged

Destination: destination host IP address for logged messages

Add

Delete

If the protocolling service is activated, the router issues status messages regarding its current activities. All these status messages are generally output to the serial console. Additionally, it can be configured here which status messages are to be forwarded to a so-called log-host (see below). In addition, the router can forward status messages from computers in a network to a log-host in a different network.

To define which status messages are to be forwarded, appropriate rules can be defined. Each rule specifies the type of service to be protocolled (source), the type of the activities and the IP address of the log-host.

The following services can be configured as the source:

- **auth** - All authentication services are monitored.
- **authpriv** - All services assigning access rights are monitored.
- **cron** - The "cron" service is monitored.
- **daemon** - All active server processes are monitored (SSH, HTTP, DNS etc.).
- **kern** - The operating system kernel is monitored.
- **mark** - "Time marks" (signs-of-life) are sent off at regular intervals.
- **syslog** - The protocolling service itself is monitored.
- **user** - All user processes are monitored.

The type of status messages ranges from very simple information up to critical errors. It is also possible to define that no more messages are received explicitly from certain services. The maximum contents of information is provided by the `debug` level. The `emerg` level contains the least information on the cause of the event. A medium information level is `Info`.

- **debug** - Creates status messages which may signal software errors in the respective service.
- **info** - Creates status messages that only serve for information of the user.
- **notice** - Creates status messages with reference to things that are to be handled in a special manner (no errors!).
- **warning** - Creates status messages that incorporate warnings.
- **err** - Creates status messages indicating errors.
- **crit** - Creates status messages indicating critical things (e.g. hardware error).
- **alert** - Creates status messages with reference to things that should be corrected immediately (for example, errors in configuration files)
- **emerg** - Creates status messages displaying that the appropriate service could either not be started or had to be cancelled.

Target will be the protocol server to which the protocol messages created or forwarded are to be sent.

Add can be used to include any combinations of Program and Log Level with the same or different targets into the message list. The same combinations can also be directed simultaneously to different targets. Thus, very complex signalling rules are possible.

auth.warning	+	192.168.1.10	-	
syslog.info		192.168.1.10		Add
user.notice		192.168.1.20		Delete
user.notice	▼	192.168.1.30	▼	



NOTE

When scrolling in one of the two windows, the display of the other window is only synchronised when a line is clicked. The cursor must be positioned to the same line in both windows.

As a meaningful default setting for logging the system messages, all programs can be set to the `info` level.

4.2.1.7 Configuring the modem

The menu shown below can be used to make settings for configuring a connected external modem.

Modem configuration

IE-ARM-E:

Modem settings

Baud rate: 115200 ▾ baud rate (speed) of Modem

no modem
 analog modem
 GSM modem
 ISDN modem

The configuration depends on the external modem you are using:

Modem settings

Baud rate: 115200 ▾ baud rate (speed) of Modem

no modem analog modem GSM modem ISDN modem

set modem country code

Country code: ▾ country code Modem 2

The menu shown above can be used to configure the speed and the country code of your external modem. The country code is set with placing the tick in the checkbox. If the correct country is already set, the checkbox need not be ticked, since setting of the country code takes some time. Furthermore, setting of the country code is not possible with certain modems.

Modem settings

Baud rate: 115200 ▾ baud rate (speed) of Modem

no modem analog modem GSM modem ISDN modem

PIN on: use PIN for GSM modem

AT command: AT command to send the PIN to your GSM modem

PIN: re-enter:

If a GSM modem is connected to the external interface of your router, specify the AT command with which your PIN is transmitted to your modem, and the PIN itself. This PIN is transmitted to the GSM modem automatically upon completion of configuring and with each start. If an error occurs during these processes, check first the status of your GSM modem. If it is already logged in to your provider, the PIN will be denied with an error message.

Modem settings

Baud rate: 115200 ▾ baud rate (speed) of Modem

no modem analog modem GSM modem ISDN modem

MSN

Use this menu to configure the baud rate and the MSN (Multiple Subscriber Number) of the external modem. The MSN is the dialling number of the modem connected to a multiple device port.

IE-ARM-U:

Two modems can be configured simultaneously. Two menus are offered for configuration, whose functions are similar to those of the IE-ARM-E configuration menu:

- Configuring modem 1
See "Configuring the IE-ARM-E modem"
- Configuring modem 2
See "Configuring the IE-ARM-E modem"

In the menus Dial-out and Dial-in, modem 1 or modem 2 can be selected for the appropriate function.

4.2.1.8 Menu option "Dial-out - modem"

IE-ARM-E:

allow dial-out

Modem options

Dial-out modem commands	ATL0M0X3	additional AT commands to send to the modem
Dial-out timeout	60	connection idle time to hang up the modem

Dial-out targets

Target name: name of the target to add

Dial-out number: number to dialout to

Dial-out user: your username at your internet provider

Dial-out password: your password at your internet provider

List of configured targets:

name	number	user	actually selected target
MSN	0,0192650	msn	<input type="checkbox"/>

MSN

Dial-out (for example, from the intranet to the Internet) is possible via an external modem. This dial-out to the Internet is done once the router receives a request for an IP address which does not belong to "its" network and which it can else not assign to any of its known networks.

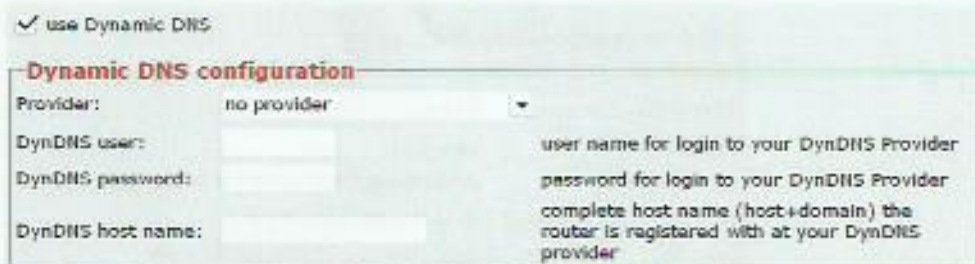
Several targets can be specified. If more than one target is specified, the function "Dial on demand" is deactivated automatically. In this case, a dial-out must be triggered manually by clicking on the button "Select". Manual triggering will naturally also function if only one target is defined and the function "Dial on demand" is activated.

Furthermore, it is possible to deactivate dial-out. Please note that no call-back is possible with dial-out deactivated.

IE-ARM-U:

In addition, you can select whether modem 1 or modem 2 is active for the dial-out.

Activation of dial-out deactivates the default gateway in the menu option "General".

4.2.1.9 Menu option "Dial-out - DynDNS"

use Dynamic DNS

Dynamic DNS configuration

Provider:	no provider	
DynDNS user:	<input type="text"/>	user name for login to your DynDNS Provider
DynDNS password:	<input type="text"/>	password for login to your DynDNS Provider
DynDNS host name:	<input type="text"/>	complete host name (host+domain) the router is registered with at your DynDNS provider

The router offers the possibility of registering with a DynDNS provider in the Internet so that it can be addressed using a fixed host name. This possibility can be configured here.

To be able to use this ability, you must first register with a DynDNS provider. The router in its current version supports the following providers:

- DHS international (<http://www.dhs.org>)
- DynDNS (<http://dyndns.org/>)
- hn.org (<http://hn.org/>)

4.2.1.10 Menu option: "Dial-in"

Dial-in can be performed via the external modem. It is irrespective of the dial-out. In other words: The modem configured for dial-out can also additionally be configured here for dial-in.

IE-ARM-E:

use Modem

Dial-in configuration Modem

Dial-in Callback

User name: extam user name for dial-in/callback

Password: re-enter:

AT command: AT command to initialize the modem

local IP: 192.168.7.1 local IP address for dialin

peer IP: 192.168.7.2 peer (remote) IP-Address for dialin

The difference between dial-in and call-back is that in dial-in the dialling computer establishes a direct telephone connection to the computer. During the call-back, the router determines that it has been dialled, hangs up after authentication immediately and calls back.

With the external connection, it can be configured here that not a modem, but a zero-modem cable was connected so that a connection is possible via zero-modem cable.

IE-ARM-U:

In addition, you can select whether modem 1 or modem 2 is active for the dial-in.

4.2.1.11 Menu option "Firewall"

The firewall offers two data filtering options:

- based on source or target IP addresses
- based on source or target ports.

The router offers three preconfigured packet filters:

- Masked networks
These subnets are masked externally, i.e. these networks appear externally as a host.
- Routed networks
Packets sent into these subnets are forwarded, but not masked.
- Trusted networks
Packets exchanged between these subnets are forwarded unobstructed and not masked. This makes sense, in particular with reference to the port filter and to the black/white lists (see below).

In addition, the router keeps a black or white list of hosts which the access to the routed / masked networks is to be permitted / prohibited explicitly.

When the filtering is performed on the basis of ports, all packets which are directed to a certain port or have been sent by a certain port are discarded. Furthermore, it is possible to forward all packets from a certain port to another computer.



DANGER

Any settings in the "Firewall" area pertain directly to the safety of your network.

Any modifications should therefore only be made if you have the appropriate knowledge.

4.2.1.12 Menu option: "Firewall - Masquerading"

Masquerading

Network:

Netmask: or significant Bits:

192.168.1.0/24

192.168.6.0/24 Add

192.168.7.0/24 Delete

Specify the networks to be masked externally here. If you are using unofficial IP addresses, such as 192.168.x.x, and if the router is nevertheless to be used for access to the Internet, it is imperative to specify them here.

The default addresses are:

- IE-ARM-E: 192.168.1.0/24
- 192.168.2.0/24
- 192.168.6.0/24
- IE-ARM-U: 192.168.1.0/24
- 192.168.6.0/24
- 192.168.7.0/24

Please observe that any network addresses always correspond to the format "xxx.xxx.xxx.0" and always end with zero.

For each network specified, either the appropriate subnet address must additionally be specified, or the number of bits set in the subnet mask (significant bits).

4.2.1.13 Menu option "Firewall - Routing"

Routing

Routing without Masquerading

Network:

Netmask: or significant bits:

Add

Delete

The router forwards packets that belong to connections which were established by hosts of this subnet. Furthermore, packets sent into these networks are not masked.

The same syntactic rules apply as for the masked networks.

Host filter

Host list is white list Host list is black list

Host: IP address of a host to deny/allow access to routed networks

Certain computers may be granted access specifically to other networks (white list) or, similarly, it is possible to prohibit some computers access to other networks (black list). In this case, the packet filter will merely pass packets of the specified computers or will block exactly these.

If no computer is to be prohibited the communication via the router, define an empty black list. This is also the default configuration.

4.2.1.14 Menu option "Firewall - Trusted Nets"

Trusted networks

Network:

Netmask: or significant bits:

192.168.1.0/24

192.168.6.0/24

192.168.7.0/24

By using this configuration menu, the disabling of routing of certain ports (see below) and the black/white list can be disabled for certain networks. Here you can specify subnets which are trusted.

In this conjunction, contrary to the masked or routed networks, all networks must be specified between which packets are to be forwarded. Therefore, at least two networks must be specified to ensure that correct firewall rules can be generated.

4.2.1.15 Menu option "Firewall - Destination NAT" (Port Forwarding)

Destination NAT

Destination NAT

activate DNAT

Address/port: NAT address / port to redirect

Protocol: tcp ▾

real address/port: IP address / port to redirect packets to

	Add
	Delete

For some Internet protocols it is imperative to divert a connection from an external computer to the internal network. If the network is masked externally ("IP masquerading", see 4.2.1.12), i.e. only one official IP address exists for the entire LAN, certain ports or protocols to which access is to be granted from the outside can be diverted to a certain internal computer. Port forwarding or "Destination Network Address Translation", in brief: DNAT, is possible for the protocols tcp, udp and gre.

Port access

Ports to close

Port(s): port(range) of incoming packets

Action: accept ▾ how to treat packets arriving at this port

135:139	reject	
445	reject	Add
		Delete

The routing via certain IP ports can be prevented. For example, it makes sense to prohibit the routing if the NETBIOS ports 137 to 139. Thus, not only the routing of IP packets with specified ports "to the outside" is prevented, but also the routing of these ports between two LANs.

If you run several network cards for several subnets and you want that some clients from a directory of a client, which is shared under Windows, may access from another subnet, the forwarding of the NETBIOS ports should not be prevented here. In this case, trusted networks (see 4.2.1.14) can be specified between which the routing of these ports is nevertheless explicitly permitted.

To handle the data packages, the following functions are provided:

- accept
- accept-tcp
- accept-udp
- drop
- drop-tcp
- drop-udp
- reject
- reject-tcp
- reject-udp

4.2.1.16 Menu option "Save all"

This menu option serves to save all changes made in the configuration permanently. Any changes are only present in the user memory until saving; they are lost when restarting the PC.

Save configuration

Configuration stored successfully.

4.2.1.17 Menu option "Restarting the router"

This menu option can be used to restart the router. This process will take a few minutes.

Router reboot

You have to save changes in configuration if you want to activate them after reboot.

Do you really want to reboot?

Reboot

The button `Restart` must only be clicked to avoid inadvertent restarts.

4.2.1.18 Menu option "Close PPP connections"

Use this menu option to close all modem connections currently active.

Close PPP connections

All PPP connections were cut.



NOTE

Clicking on the menu option will close immediately all PPP connections without any further interrogation.

In this case, no external access to the Mini-Router is possibly any more.

4.2.1.19 Network status statistics

Use this menu option to display all network interfaces currently active and to display various status information.

Example:

Netzwerkstatus

```
eth0  Link encap:Ethernet HWaddr 00:15:7E:02:00:9C
      inet addr:192.168.1.100 Bcast:192.168.1.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:151 errors:0 dropped:0 overruns:0 frame:0
      TX packets:168 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:23925 (23.3 KiB) TX bytes:70507 (76.7 KiB)
      Base address:0xB40

eth1  Link encap:Ethernet HWaddr 00:15:7E:02:00:9D
      inet addr:192.168.2.100 Bcast:192.168.2.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
      Interrupt:69 Base address:0x300

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

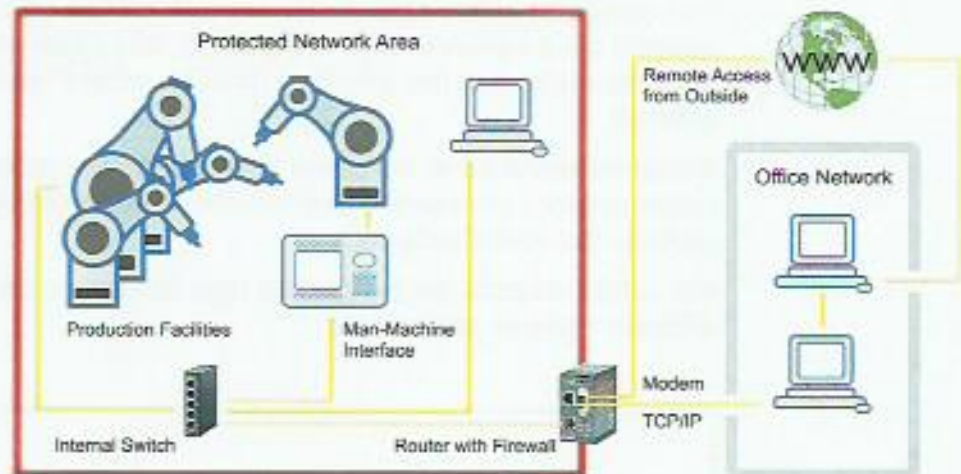

4.3 Configuring the client computers

To run the client computers with the router, no special software needs to be installed, but some configuring notes must be observed.

4.3.1 Configuring the PCs integrated into router network

All IP packets sent from the router Ethernet to the outside must always be routed via the router. Therefore, the IP address of the router (default: 192.168.1.100) must be specified as the standard gateway with all hosts in the Ethernet.

If the internal DNS server of the router is activated, you may address the clients in the Ethernet using names (host name) instead of IP addresses (see Section 4.2.1.2). To this end, the IP address of the router must also be entered for all clients as the DNS.



4.3.2 Configuring a PC not integrated into the router network

The PC not integrated into the router network must be equipped with an analog or an ISDN modem, depending on the router used. Only modems of the same type can communicate with each other.

The steps described here were tested on Windows systems.

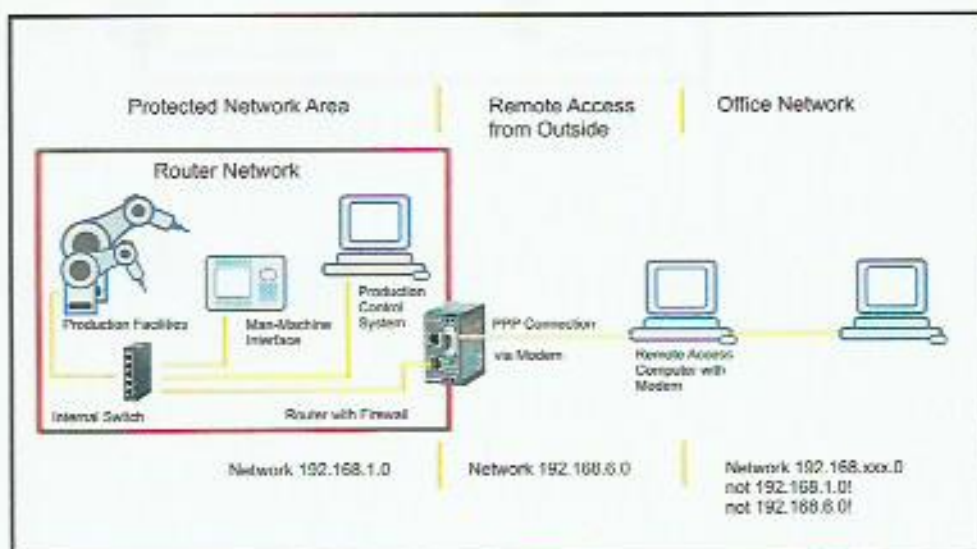
If a PC outside the router network dials in via a direct PPP (long-distance data transmission) connection, the modem interface of the computer is assigned an IP address by this PC. No settings are required here. When the PPP connection is established, the standard gateway of the PC is automatically adapted to the dynamically assigned IP address of the modem interface.

To be able to address the clients in the router network via their (host) names, the address of the DNS server (default: 192.168.1.100) must be specified.

The computer outside the router network can be connected to another network via a network card. It should be taken into account that the network address of this interface must be other than that of the router network.

If both networks have the same IP address, the packets directed to the router network are misdirected into the network of the remote computer (outside the router network).

For safety reasons, all 3 networks (see illustration below) should have different network addresses.



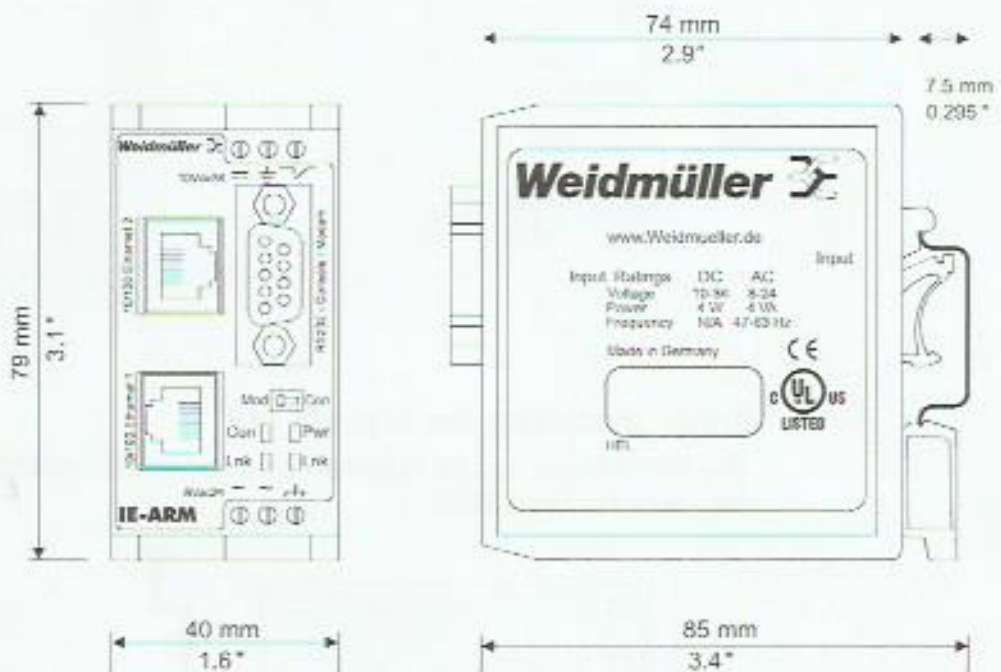
5 Hardware

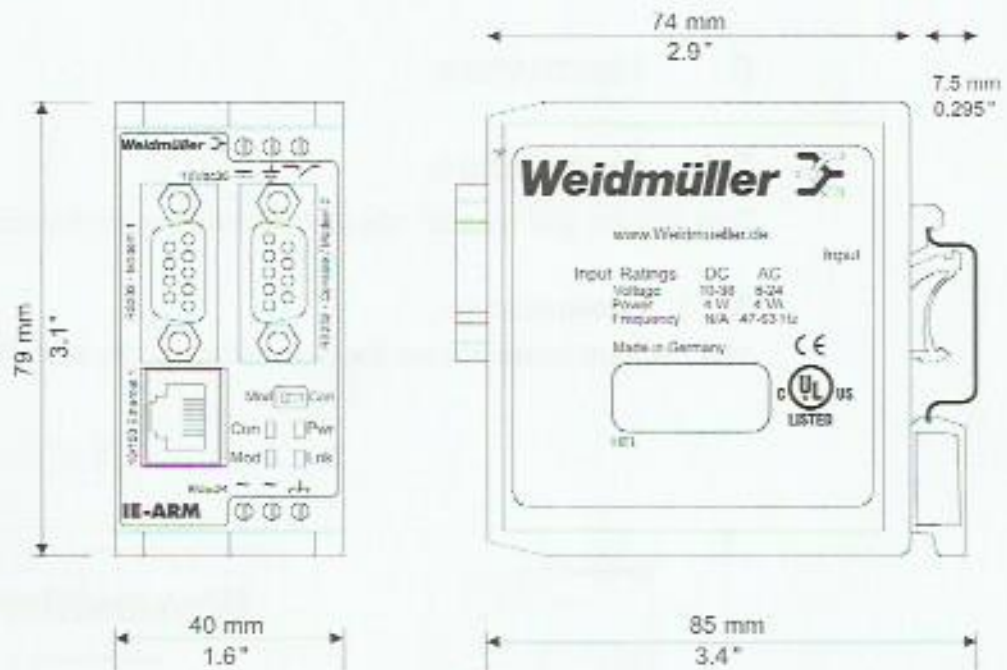
5.1 Installation

This chapter provides all relevant information on the dimensions.

5.1.1 Dimensions

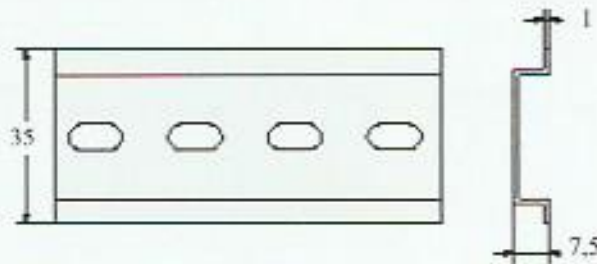
The diagram below shows the dimensions of the Mini-Router:





5.1.2 Installing the top-hat rail

The Mini-Router can be fastened on a top-hat rail which complies with the standard EN 50022:



This top-hat rail must be fastened on the control cubicle wall such that a conductive connection is provided.



NOTE

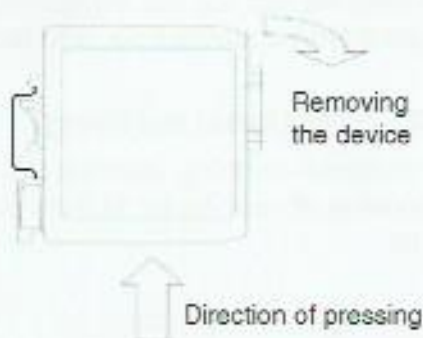
Observe the instructions of the manufacturer with reference to fastening.

Installation

Pull the top-hat rail downwards, at the same time pushing the device back onto the top-hat rail.

Removal

To remove the device, unhook it upwards, at the same time pushing it up, and then remove it from the top-hat rail.



5.2 Installation notes

Make sure that at least 30 mm space are left above the module.

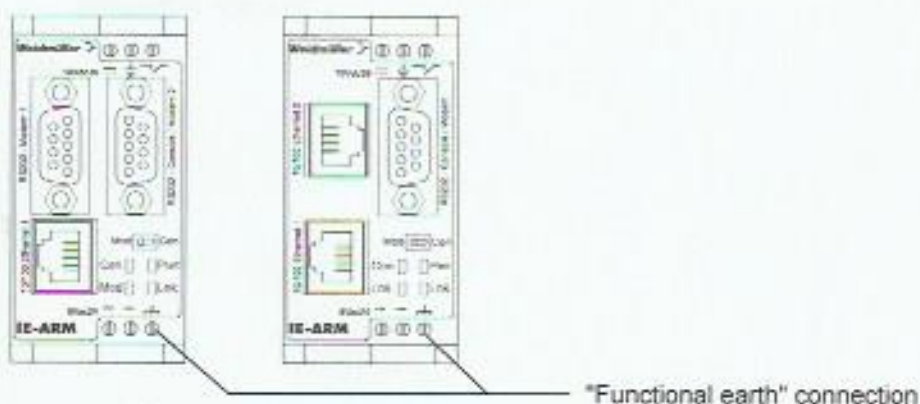
A space of 35 mm must be provided beneath the module for routing of the cables for the interfaces and for the power supply.

5.2.1 Mounting the router on a top-hat rail

The device is intended for mounting on a top-hat rail to DIN EN 50022. Pull the top-hat rail downwards, at the same time pushing the device back onto the top-hat rail. To remove the device, unhook it upwards, at the same time pushing it up, and then remove it from the top-hat rail.

5.2.2 Functional earthing

For functional earthing, connect the "Functional earthing" terminal on the housing of your router to the equipotential bonding of the control cabinet.



The connection "Functional earth" serves for purely operational functions (modem function).

Make sure that the cross-section of the interconnecting line does not exceed 4 mm² / AWG 12.

5.3 Installation guidelines

The specified maximum operating temperature pertains to the air temperature beneath the IE-ARM (air inlet).

Observe a sufficient distance to devices emitting strong electromagnetic radiation (such as frequency converters, transformers, motor controllers, etc.). The clearance between these devices and the IE-ARM should be as large as possible. If necessary install a shielding of partition walls (MU metal).

Do not plug or remove the devices during operation!

Before removing a IE-ARM, also remove the relevant plugs and connectors.

Do not connect or remove the connectors if the supply lines are still live (all-pole disconnection).

5.4 Storage and storage temperatures

The following values will apply for storing:

- Storage temperature: -20 ... +60 °C
- Humidity: 30 ... 95 % (without condensation)

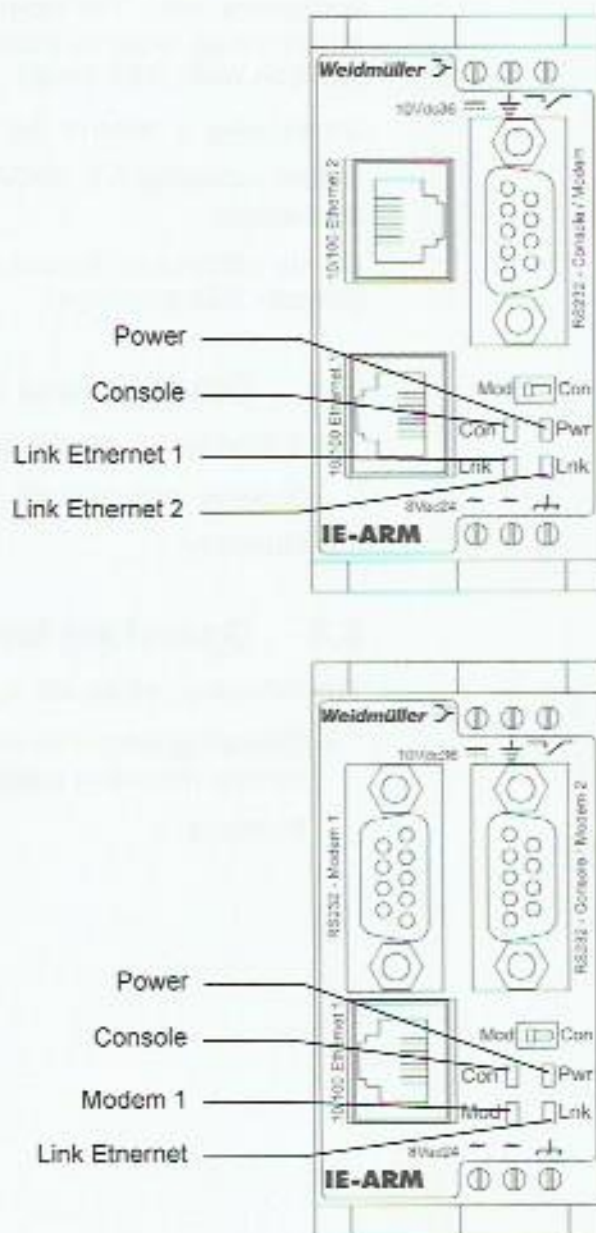
5.5 Operating temperature, humidity

The following values will apply for operation:

- Operating temperature with vertical mounting position: 0 ... +60 °C
- Humidity: 30 ... 95 % (without condensation)

5.6 Status display

Four LEDs are located on the front panel of the IE-ARM to display the operating status.



5.6.1 Display "Console/modem"

LED	Description
Steady orange light	Console mode activated
Flash orange	Data transfer running
Green steady light	Modem mode activated
Green flashing light	Data transfer running

5.6.2 Display "Ethernet interface active"

LED	Description
OFF	Not connected
Steady orange light	Ethernet interface active at 10 Mbit/s
Flash orange	Data transfer running at 10 Mbit/s
Green steady light	Ethernet interface active at 100 Mbit/s
Green flashing light	Data transfer running at 100 Mbit/s



NOTE

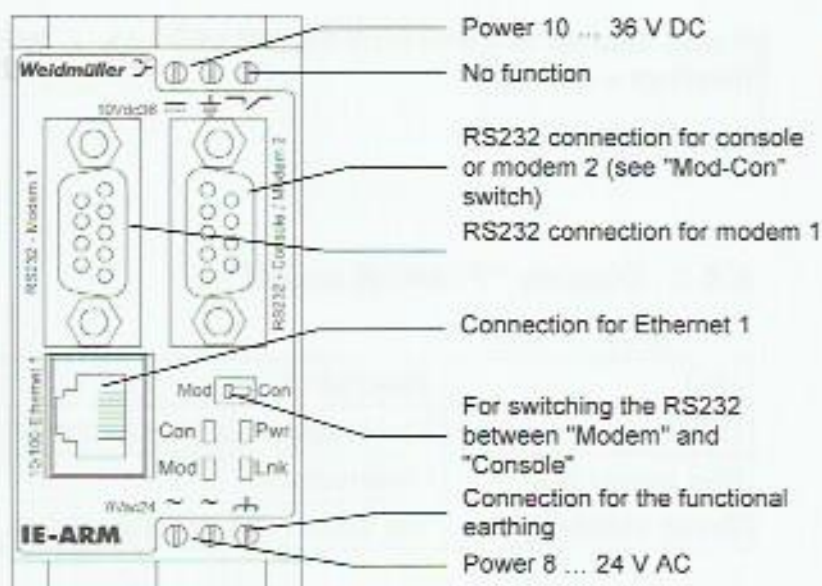
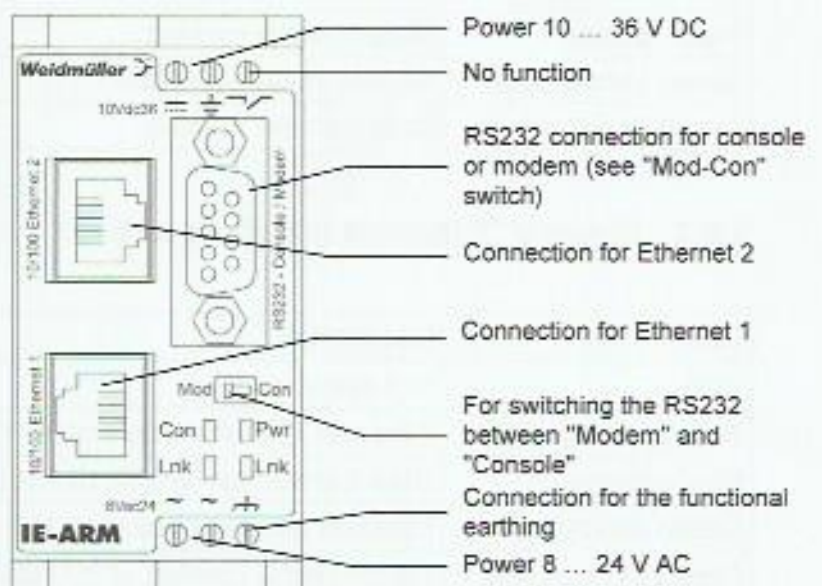
It may take up to 1 min until the left LED Lnk - Ethernet 2 displays a status.

5.6.3 Display "POWER on/off"

LED	Description
OFF	The supply voltage is turned off.
Red steady light	Undervoltage
Green steady light	The supply voltage is turned on.

5.7 Connections / interfaces

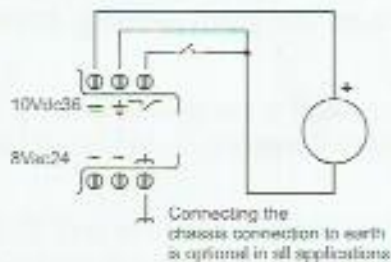
The connection for the power supply, and 3 interfaces are to be found on the front side of your Mini-Router;



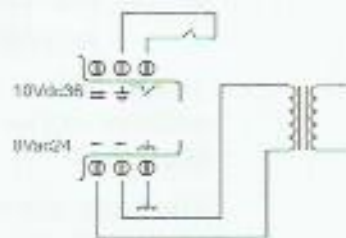
5.7.1 Power supply

The IE-ARM can be supplied either with +10 ... 36 VDC or with 8 ... 24 VAC. The power consumption is approx. 4 W.

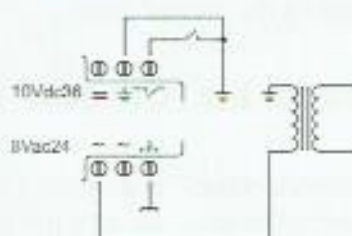
DC POWERED



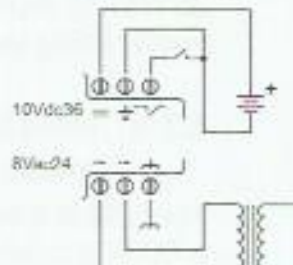
AC POWERED
(ungrounded secondary)



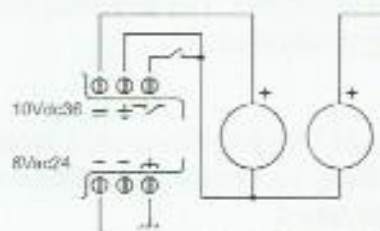
AC POWERED
(grounded secondary)



AC POWERED WITH BATTERY BACKUP



REDUNDANT DC POWERED



DANGER

Power supply connection

The Mini-Router IE-ARM must only be connected to the electrical supply system by an electrical expert.

The power supply of the Mini-Router IE-ARM must be provided exclusively by a power pack which complies with DIN EN 60 742 (VDE 0551).

Make sure that an appropriate fuse is installed in the incoming supply feeder.

5.7.2 Ethernet interface

The IE-ARM-U possesses a 10/100 Mbit Ethernet controller.

The IE-ARM-E possesses two 10/100 Mbit Ethernet controllers.

It is connected to the industrial Ethernet via an RJ45 connector.

5.7.3 RS-232 interface for connecting an external modem

The IE-ARM-U is equipped with a serial interface for connecting to an external modem. The external modem is configured and activated as Modem 1.

The serial interface "RS232 Modem 1" at the unit IE-ARM-U is a "full" serial port and can be used with modems without limitations.

Cables should be as short as possible and not exceed a length of 25 cm / 10 inches. The modem should be powered by the same power supply being used for powering the router itself.

5.7.4 RS-232 interface for the "Console" or "Modem" mode

The RS232 interface "Console/modem" is intended for the connection of a PC or a notebook with which the start-up and parameterisation may be carried out on the spot (see Section 3.7).

The Interface can be used for connecting to a modem by operating the switch Mod/Con. The external modem is being activated as modem 2 during configuration.

**NOTE**

The port "RS232 Console / Modem 2" is only using the RxD and TxD. Only modems capable of working without handshake signals can be used.

The modems "HSM ECO V92" and "HSM ECO TA" of Comtime GmbH were tested.

Cables should be as short as possible and not exceed a length of 25 cm / 10 inches. The modem should be powered by the same power supply being used for powering the router itself.

6 Technical Data

Type Designation	
IE-ARM-U	Ethernet / modem (RS232) router
Art. no.	8845760000
IE-ARM-E	Ethernet / Ethernet router
Art. no.	8845770000

Design	
Material of the housing	Plastic
Colour	deep black matt
Degree of protection - housing	IP40
Degree of protection - terminals	IP20
Protection against hazardous shock currents	Safety extra-low voltage + protective separation

Mechanical Data	
Dimensions (H x W x D)	79 x 40 x 85 mm ³
Fastening on the top-hat rails	to DIN 50 022
Connection technique - Connections of the Power supply - Modem - Ethernet	Plug connector with self-disengaging screw terminals Socket, Sub-D type Socket RJ45 type
Conductor cross-sections of the power supply connections	min. 0.5 mm ² max. 2.5 mm ² flexible, max. 2.5 mm ² solid

Environmental Conditions	
Ambient temperature - operation	0 ... +60 °C
Ambient temperature - storage	-20 ... +60 °C
Relative humidity - operation	min. 30 % / max. 90 % (without condensation)
Relative humidity - storage	min. 30 % / max. 90 % (without condensation)

Electrical Data	
Power supply	The power supply of the IE-ARM must be provided exclusively by a power pack which complies with DIN EN 60742 or VDE 0551.
Rated operating voltage	10 ... 36 VDC / 8 ... 24 VAC
Rated operating capacity	4 W DC, 4 VA AC
Fuse, external	T1A
Rated frequency	50 Hz ... 60 Hz
Redundancy	Redundant power supply

7 Standards and Certifications

7.1 Harmonised standards

EN 50081-1 Noise emission for residential, commercial and light-industrial environment

EN 61000-6-2 Noise immunity for the industrial environment

7.2 Certification to DIN EN ISO 9001

The Weidmüller Interface GmbH & Co. KG is certified to ISO 9001.

7.3 Approbations



Industrial Control Equipment
4EAA
For Use In Class 2 Circuits

7.4 CE marking

EU Low-Voltage Directive

EC Certificate of Conformity on request

8 Symbols Used



Connection for the functional earthing



Mains transformer



d.c. power supply source



Battery (emergency power)

Referenzen

Name: Weidmüller
Firma: Weidmüller Interface GmbH & Co. KG
Strasse: Klingenbergstraße 16
PLZ: 32758
Ort: Detmold
Tel: Tel.: 0 52 31 / 14-0
Fax: Fax: 0 52 31 / 14 20 83
Version: Version 3.1.0, March 2006
Typ: IE-ARM
Typ RS232: IE-ARM-U
Artikel-Nr. U 8845760000
Typ TCP/IP: IE-ARM-E
Artikel-Nr. E 8845770000
Farbe: deep black matt
Untertitel Access Router Mini
Gerät: Mini-Router
User Terminal: root
User Browser: admin
Pass: detmold
IP-Adresse 1 192.168.1.100
IP-Adresse 2 192.168.2.100
Warenzeichen1: HEYFRA[®] is a registered trademark of HEYFRA ELECTRONIC GmbH
Warenzeichen2: Weidmüller[®] is a registered trademark of Weidmüller Interface GmbH & Co. KG