CTRLink-Router EIAR-10T

Internet Access Router

Contemporary Controls GmbH
Fuggerstraße 1 B
04158 Leipzig
Tel.: 341-520359-0
Fax: 341-520359-16

Version 2.4.1, Oktober 2005

Copyright

Contemporary Controls GmbH. 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 Contemporary Controls GmbH, not even for use as training material, or using electronic systems. All rights reserved in the case of a patent grant or registration of a utility model or design.

Copyright © 2004 by

Contemporary Controls GmbH

Fuggerstraße 1 B
04158 Leipzig

NOTE

We have checked the content 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.

CTRLink ™® are trademarks registrated by Contemporary Controls GmbH and Contemporary Control Systems Inc.

HEYFRA® registrated trademark by HEYFRA ELECTRONIC GmbH

Handbuch:	Manual CTRLink Router EIAR-10T
Datei:	manualrouter en 11-1-05.doc 26.10.2005
Revision	c 11-1/05

1 Safety Notes

1.1 Graduated safety notes

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

1.2 Definitions

CAUTION

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

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

CAUTION

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 Internet Access Router must only be used according to its intended purpose!

1.4 Hazards resulting from modifications and upgrades

The Internet Access Router is an in-house development designed exclusively by our company.

⚠ CAUTION

Unauthorised modifications and amendments are not permissible.

Such unauthorised modifications or amendments may impair the proper operation of the remote diagnosis unit, resulting in personal injuries, material damage or environmental impairments and will render all liability on our part null and void.

1.5 Admitted personnel

⚠ CAUTION

Only sufficiently qualified and instructed personnel are allowed to operate the Internet Access Router!

It must only be started up 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
- 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 Internet Access Router must be connected to an electrical supply system.

⚠ CAUTION

Power supply connection

The Internet Access Router must only be connected to the electrical supply system by an electrical expert.

The power supply of the Internet Access Router 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 Internet Access Router, please refer to the information provided in Chapter 6. "Technical Data".

1.7 Safety regulations

The Internet Access Router possesses a housing cover.

⚠ CAUTION

Electrical hazards

The operation of the Internet Access Router is only allowed with the housing closed.

The housing cover 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 only be opened by electrical experts.

1.8 Service and maintenance

⚠ CAUTION

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 Internet Access Router first!

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

⚠ CAUTION

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 only original spare parts from Contemporary Controls.

1.9 Waste disposal

⚠ CAUTION

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

Dispose of all electrical devices and materials 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 Contemporary Controls. Contemporary Controls 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 Contemporary Controls. In addition, the "General Terms and Conditions for the Supply of Products and Services in the Electrical Industry" shall apply. Irrespective thereof, 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

Contemporary Controls 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

The Internet access routers dialling to an Internet provider via the public telephone network, results in telephone and dial-in changes. Contemporary Controls does not assume any liability for any charges, including changes in case of an inadvertent dial-in.

2 Use as Prescribed

2.1 Range of application

The Internet Access Router grants an industrial IP network access to the Internet via its integrated analog or ISDN modem.

It provides the transport of IP packets between IP-based industrial network and another network (e.g. Internet). The Internet access is activated automatically as necessary. The Internet Access Router is configured at its site of installation via the IP network, an RS 232 interface 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 (Telnet, SSH).

⚠ CAUTION

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

Always observe the safety notes!

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

⚠ CAUTION

Do not use the Internet Access Router in potentially explosive areas!

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

- 1.6 Electrical connections
- 3.6 Connecting
- 6 Technical Data

3 Description of Functions

3.1 General Description of Functions

The Internet Access Router provides a local Ethernet based on TCP/IP the transition to another IP network via a PPP connection (long-distance data transmission).

This transition is normally provided via the internal modem integrated into the router (56k 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.

In this case, the connection is only established when necessary (IP packets addressed externally) and is cleared if not used for a longer period.

Additionally, an authorised computer may establish a direct PPP connection to the router via its integrated modem. By using this connection, the router can be monitored and configured.

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

In addition, it is possible to establish a VPN connection via the Internet.

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

3.2 Functioning of "Dial on Demand"

As already mentioned, the Internet Access Router only establishes a connection to the Internet if required ("on demand").
This situation arises if the router receives an IP packet from your 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 dial a number specified by you using the internal or external modem. Then, a PPP program becomes active to 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 timeout and will treat your query to the Internet as failed.
It may therefore be necessary to adapt the timeout times of your programs.

The MODEM status LED is lit in green once the connection is established. After the PPP connection has been established, your query will be processed. The modem connection will remain active for a certain period which can be specified. Each computer in the Ethernet may use this connection. The period you are connected extends automatically with each query put to the Internet. If during this period no data traffic takes place, the connection is cleared automatically.

The status LED "MODEM" is lit in red once the connection is established or cancelled or interrupted.

The status LED "MODEM" is off if there is no PPP connection via the internal modem.

CAUTION

Check whether there are services 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 or prevent a connection being cleared by creating external data traffic.

If necessary adapt your firewall settings accordingly (disabling of the port number of the service in "PORTS NOT FORWARDED"; Section 4.3.1.12)!

3.3 Functioning of "Dial–In Server"

The Internet Access Router is configured as a dial-in server by default. 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 4.3.1.15 is transmitted to the remote computer automatically.

If the connection is active, the MODEM status LED is lit in green.

Now you may communicate transparently with the router services (Web server, SSH) or the services provided by the clients integrated into the Ethernets.

The connection is only cleared if this is specified 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.

3.4 Call-back functionality

The router can be configured such that it will not work as a dial-in server (see Section 4.3.1.15). Instead, in the case of an incoming call, it will hang up immediately and 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 4.3.1.14).

To provide a secure connection via the Internet, it is additionally recommended to set up a Virtual Private Network (VPN).

3.5 Start-up

The start-up of the Internet Access Router is carried out in 3 steps:

- Connecting
- Executing the boot process
- Configuring the router

3.6 Connecting

First connect the router to the hub (switch) at the 10-Base-T socket using a patch cable. If you want to connect only a single host to the router and not a complete network, use a cross-over cable.

Now connect the RJ-11 interface labelled with MODEM to a TAE socket using a telephone cable

NOTE

With this device, it is also possible to use an external modem (analog, ISDN, GSM), alternatively to the internal modem integrated into the router.

To do so, connect the modem to the RS232 interface of the router labelled EXTERNAL using an RS232 connection cable.

For configuration, the router may also be connected to a computer via the RS232 interface labelled "CONSOLE". This possibility, however, is not recommended, since errors could easily result in the configuration file when using this method. Therefore, you should use the console only in an extreme emergency.

Now connect the 24 V power supply to the POWER connection on the front side of the device.

NOTE

Directly after connecting the power, the status display of the LEDs may vary; only the "Power" LED must be lit in green. The LED will only indicate the status correctly when starting the boot process, see 3.7.

The ON condition could look as follows:

ACTIVE MODEM:	off
ACTIVE ETHERNET:	red
ERROR:	orange
POWER:	green

The "orange" display is no error condition!

After switching on[1] the power supply, the router will start booting.

When connecting the Internet Access Router, observe the notes provided in the Sections 1.6 Electrical connections1.6, 5.7 Connections / Interfaces and in Chapter 6 Technical Data.

[1] The router does not have its own ON / OFF switch; connecting the operating voltage is a function of the system/installation into which the remote diagnosis unit will be integrated.

3.7 The boot process

During the boot process, all services and programs required are started automatically.

This process will take approx. 2 minutes.

Starting the boot process:

States of the LEDs:

ACTIVE MODEM:	off
ACTIVE ETHERNET:	off
ERROR:	off
POWER:	green

The settings are loaded.

States of the LEDs:

ACTIVE MODEM:	off
ACTIVE ETHERNET:	off
ERROR:	red
POWER:	green

A check is carried out to see whether the ETHERNET connection can be addressed.

States of the LEDs:

ACTIVE MODEM:	off
ACTIVE ETHERNET:	red
ERROR:	red
POWER:	green

All relevant services, such as firewall and routing, are initialised. The configuration of the ETHERNET connection is finished.

States of the LEDs:

ACTIVE MODEM:	off
ACTIVE ETHERNET:	green
ERROR:	red
POWER:	green

The boot phase is now completed; the router is ready for operation.

States of the LEDs:

ACTIVE MODEM:	off
ACTIVE ETHERNET:	green
ERROR:	green
POWER:	green

4 Configuration

Before the router can be started up, it must be configured. The individual steps for starting up will be explained in the present chapter.

4.1 Configuring options

4.1.1 Configuring via the Ethernet interface

With this configuring option, a computer integrated into your Ethernet may be used for configuring. Either an SSH client or a standard web browser (recommended) must be installed on this PC.

When working with a web browser, the IP (Ethernet) address 192.168.1.100 is used by default to address the router. 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 4.1.1.1 and 4.2.1.

4.1.1.1 Setting the IP address in accordance with the local network

It is not always possible to set the local network to 192.168.1.x, or else the address 192.168.1.100 may already exist. The router can be set to any address via a serial connection using a terminal program to allow access via a browser. Any further configurations can subsequently be made in the browser.

You will need a PC on which a terminal program is installed, a free RS232 interface and an RS232 interconnecting cable.

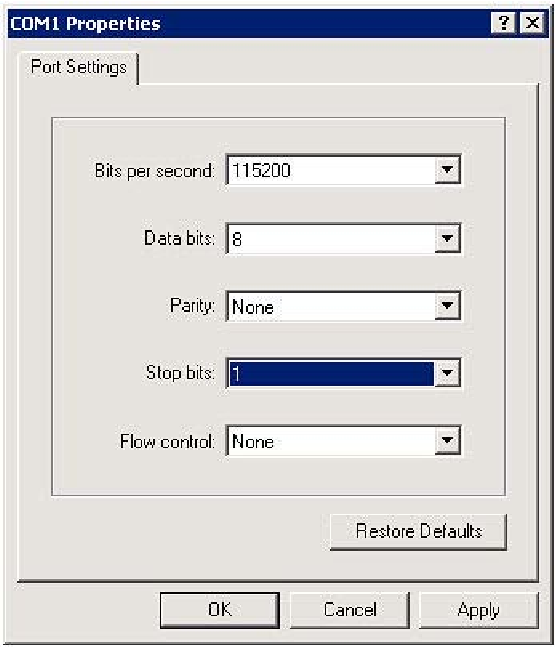
The connection between computer and router is established using the RS232 interconnecting cable. To this end, connect a serial interface of the PC to the "Console" interface of your router. You can use the Windows program "HyperTerminal".

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

The description provided below refers to HyperTerminal.

First, establish a connection using "File - New Connection". Enter a name for the new connection and select a symbol. Do not enter a dialling number under "Connect To"! Only the serial interface to be used is important.

The following settings are required for the serial interface:



Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Then click on the ☎ icon in the toolbar to start the connection. The connection is established.

A log-in window will appear on the router. If not, press ENTER.

Enter the password (default: `ctr`)

To set the IP address, type the command "setip" followed by the address and the subnet mask of the local network using the following format. Please note the spaces!

Example: `setip 192.168.1.150 255.255.255.0`

The change is written to the configuration file of your router and stored permanently using the command "save"; see the following illustration.

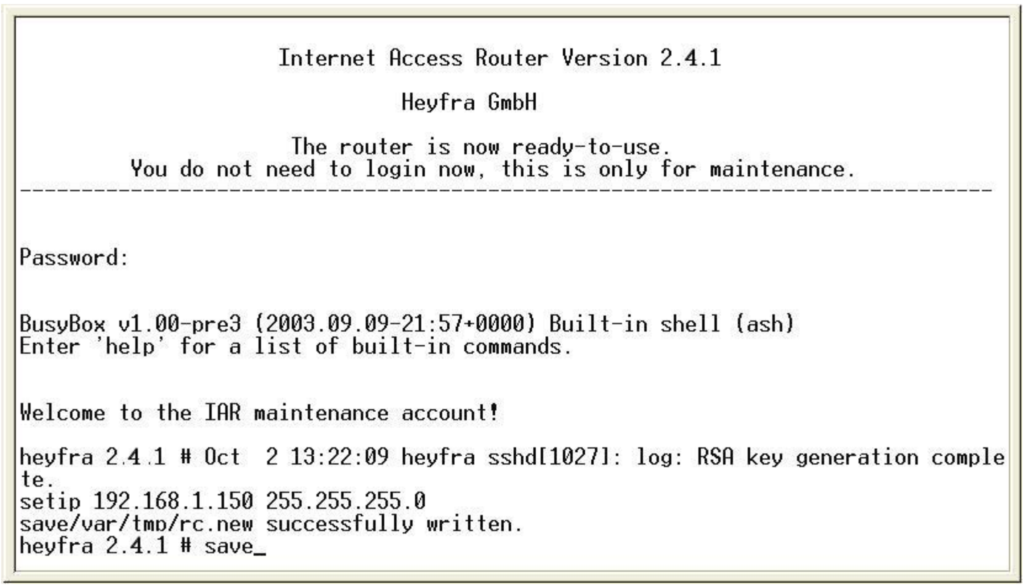
For subnetting (a smaller network), it is additionally necessary to specify the number of the significant bits.

Example: `setip 192.168.1.150 255.255.255.80 25`

The default value for a Class C network is 24.

CAUTION

The change in the IP address is only stored permanently in the flash of your router with the command "save". Without "save", all your changes are lost when the router is restarted.



```
                    Internet Access Router Version 2.4.1

                               Heyfra GmbH

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


Password:


BusyBox v1.00-pre3 (2003.09.09-21:57+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.


Welcome to the IAR maintenance account!

heyfra 2.4.1 # Oct  2 13:22:09 heyfra sshd[1027]: log: RSA key generation comple
te.
setip 192.168.1.150 255.255.255.0
save/var/tmp/rc.new successfully written.
heyfra 2.4.1 # save_
```

The current IP address of the router can be interrogated in the terminal using the command "ifconfig". If you use the parameter "ifconfig eth0", only the IP address is displayed.

NOTE

The commands "setip", "save" and "ifconfig" are additional scripts and are therefore not shown in the list of "build-in commands".

4.1.2 Configuring via a null-modem cable

With this configuring option, the connection between computer and router is established using a null-modem cable. The relevant procedure is described in Section 4.2.2. Either a standard web browser (recommended) or an SSH client (not recommended) can be used for configuring the router.

4.1.3 Configuring via the telephone network

The user dials into the router via the telephone network. In this case, either the internal modem is used or else an external modem connected to the RS 232 interface "External". This connection constitutes a direct PPP (long-distance data transmission) connection. The router acts as a PPP server (see section 4.2.3).
Either a standard web browser (recommended) or an SSH client (not recommended) can be used for configuring the router.

4.1.4 Configuring via the RS 232 interface

The router is connected to a PC via the RS 232 interface "Console" using a null-modem cable. The RS232 protocol is used directly so that no IP communication is possible. The difference to configuration using a zero-modem cable connected to the external modem connection is that no full PPP connection is created; the router cannot be addressed from the SSH or using a web browser.

The use of the RS 232 interface provides expanded diagnosis options through direct output of all screen contents to the serial CONSOLE output of the router, which is especially advantageous for the configuring and maintenance of the router itself. Access to the underlying network, however, is not possible.

It is also possible, however, to reload the original default settings if the router is configured not correctly if you press the ENTER key when prompted to do so during booting.

4.1.4.1 Available configuration services for different connections

	Web Browser	**RS232**	**SSH**
Ethernet	possible	not possible	possible
Telephone network	possible	not possible	possible
RS 232	not possible	possible	not possible

NOTE

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

4.2 Configuring via the Ethernet

4.2.1 Adaptation of the IP address

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

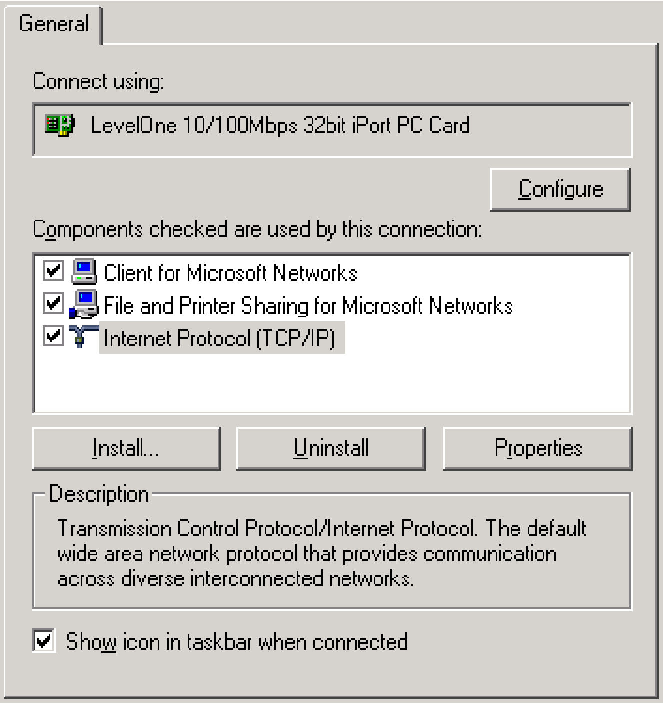
If your Ethernet network address is also 192.168.1.0, you may skip the following instructions. In this case, you can proceed with Section 4.1 Configuring options.

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 4.2.1.1 and Section 4.2.1.2). In addition, it is still possible to use the configuring options "via the telephone network" or "via the serial interface" (not recommended).

4.2.1.1 Windows 2000

To assign a network card one or several IP addresses under Windows2000, administrator rights are required.

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



General

Connect using:

LevelOne 10/100Mbps 32bit iPort PC Card

Components checked are used by this connection:

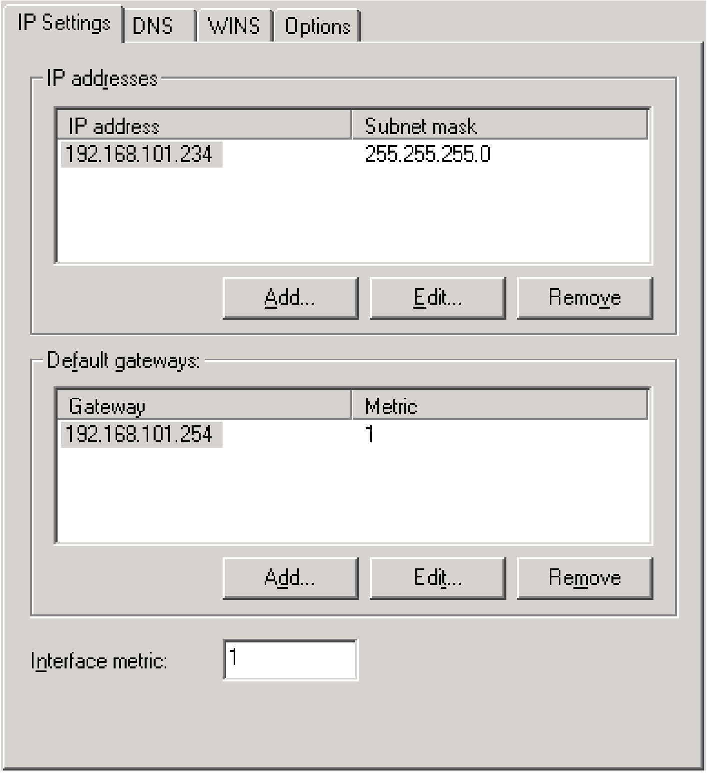
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

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.



IP addresses

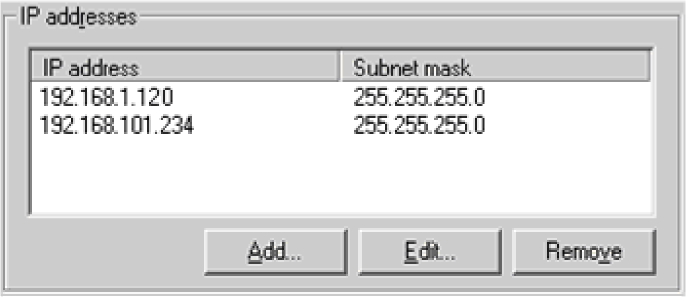
IP address	Subnet mask
192.168.101.234	255.255.255.0

Default gateways:

Gateway	Metric
192.168.101.254	1

Interface metric: 1

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:



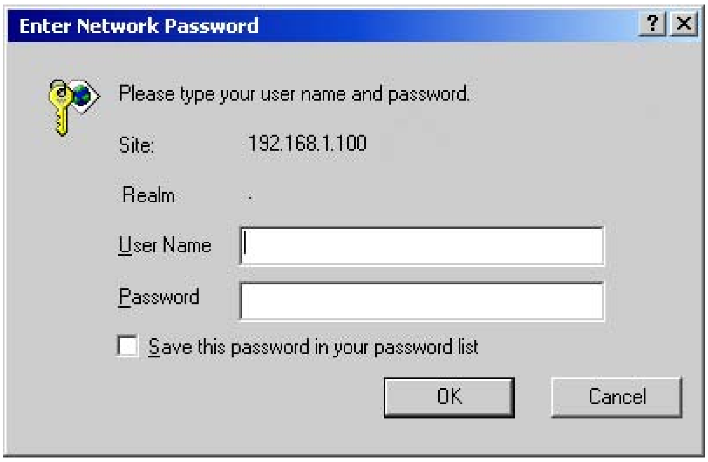
IP addresses

IP address	Subnet mask
192.168.1.120	255.255.255.0
192.168.101.234	255.255.255.0

The computer you have just configured can now be seen both in the network 192.168.101.0 and in the network 192.168.1.0. It is therefore not necessary 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, pass: ctr).



Enter Network Password

Please type your user name and password.

Site: 192.168.1.100

Realm .

User Name

Password

☐ Save this password in your password list

The welcoming text of the embedded web server will appear.

To configure the router, proceed as described in Section 4.3.1.

4.2.1.2 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 your self 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:

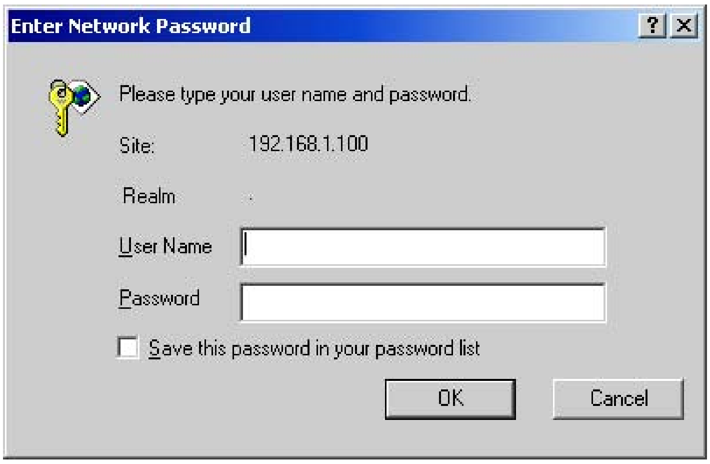
```
➢  ifconfig eth0:1 192.168.1.120 netmask 255.255.255.0
```

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: ctr).



Enter Network Password

Please type your user name and password.

Site: 192.168.1.100

Realm

User Name

Password

☐ Save this password in your password list

The welcoming text of the embedded web server will appear. Now you can proceed with Section 4.3.1.

4.2.2 Configuring via a null-modem cable

Prerequisites:

A PC with web browser and a free 9-pin serial interface, as well as a zero-modem cable are required. Connect the zero-modem cable to the free serial connection on the PC side, and to the RS 232 jack labelled "External" on the router side.

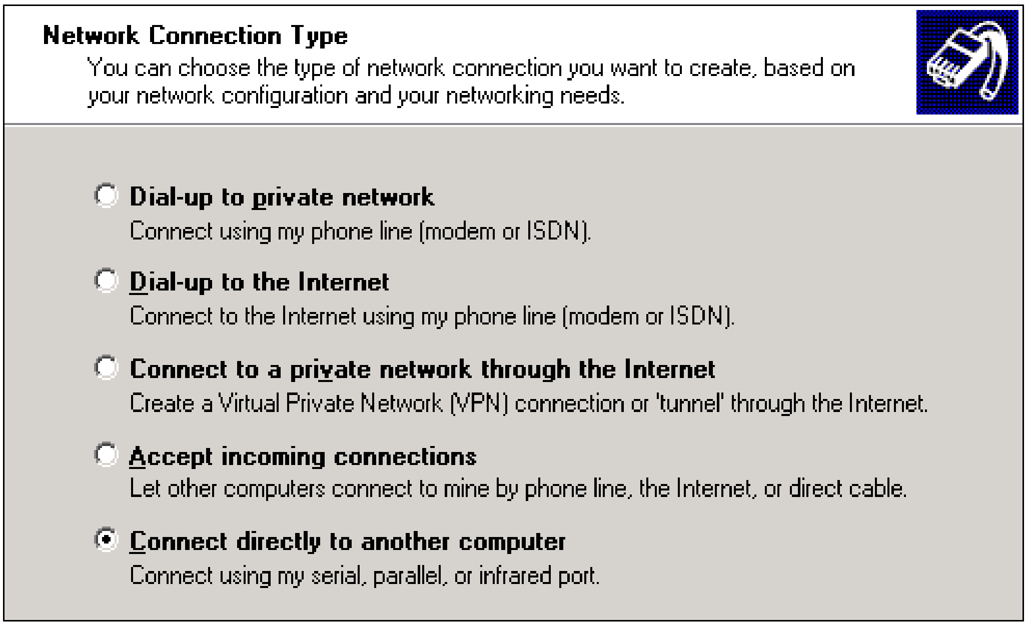
It is not relevant whether MS Windows or Linux is installed on your PC, because both operating systems include the required tools.

NOTE

The method described here pertains to Windows 2000.

Now go to `Control Panel`→`Network Connections` and start the "New Connection Wizard".

Choose "Connect directly to another computer" for the type of connection:



Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

○ **Dial-up to private network**
Connect using my phone line (modem or ISDN).

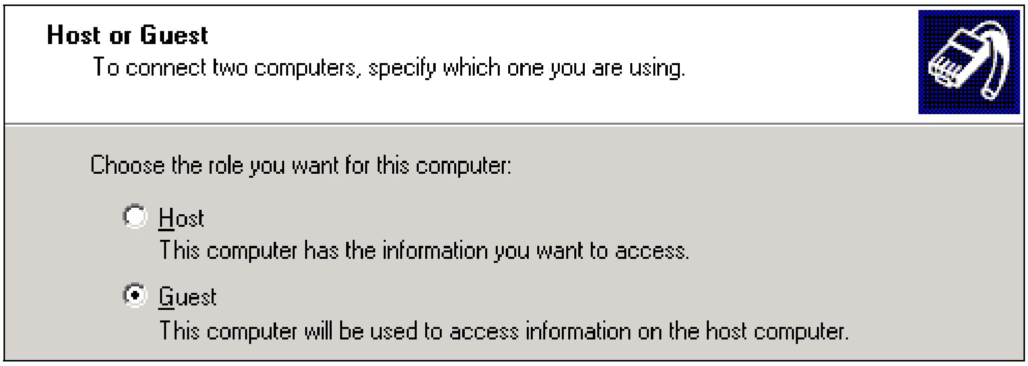
○ **Dial-up to the Internet**
Connect to the Internet using my phone line (modem or ISDN).

○ **Connect to a private network through the Internet**
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

○ **Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.

● **Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

Set the role you want to choose for this computer in the next tab to "Host":



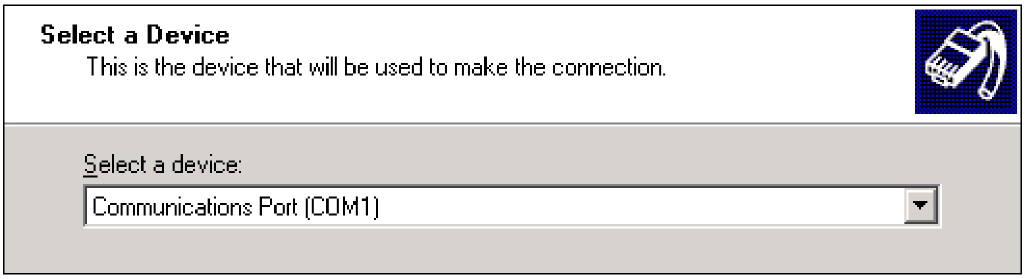
Host or Guest
To connect two computers, specify which one you are using.

Choose the role you want for this computer:

○ Host
This computer has the information you want to access.

● Guest
This computer will be used to access information on the host computer.

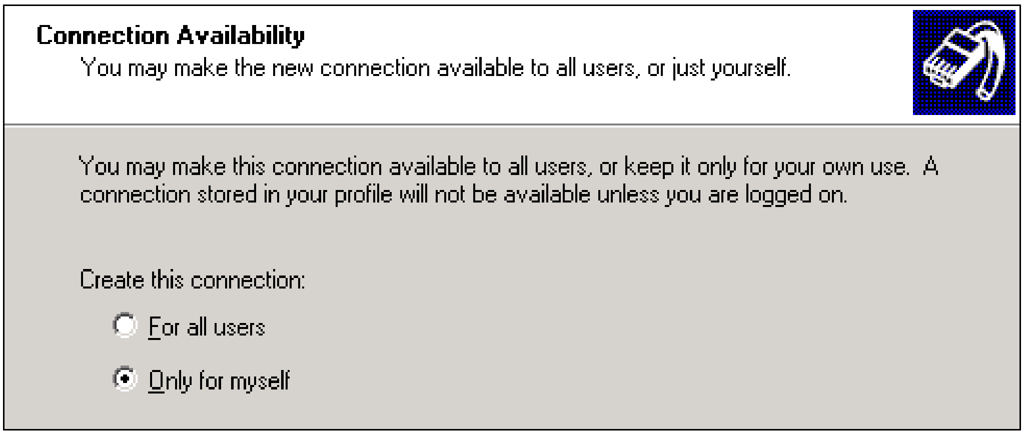
Now select the connection to which your zero-modem cable is connected:



Select a Device
This is the device that will be used to make the connection.

Select a device:
Communications Port (COM1)

Answer the next question with "Use connection exclusively":



Connection Availability

You may make the new connection available to all users, or just yourself.

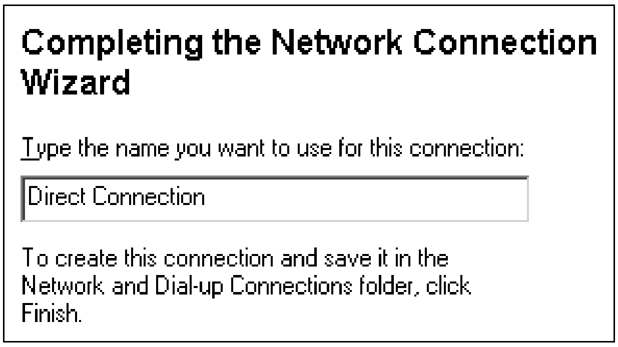
You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.

Create this connection:

○ For all users

● Only for myself

Enter a name for your connection (e.g.: "Zero modem"):



Completing the Network Connection Wizard

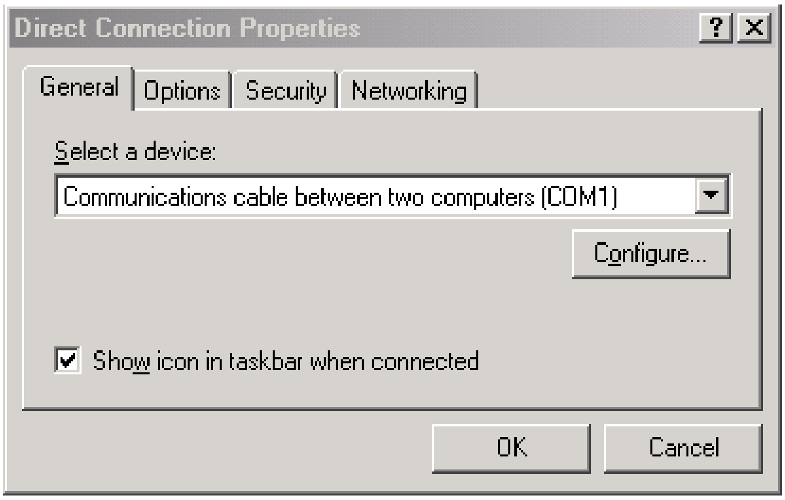
Type the name you want to use for this connection:

Direct Connection

To create this connection and save it in the Network and Dial-up Connections folder, click Finish.

Click on "Finish". If your PC attempts to establish a new connection immediately, this should first be cancelled.

To process the connection just established, choose "Properties" from the context menu:



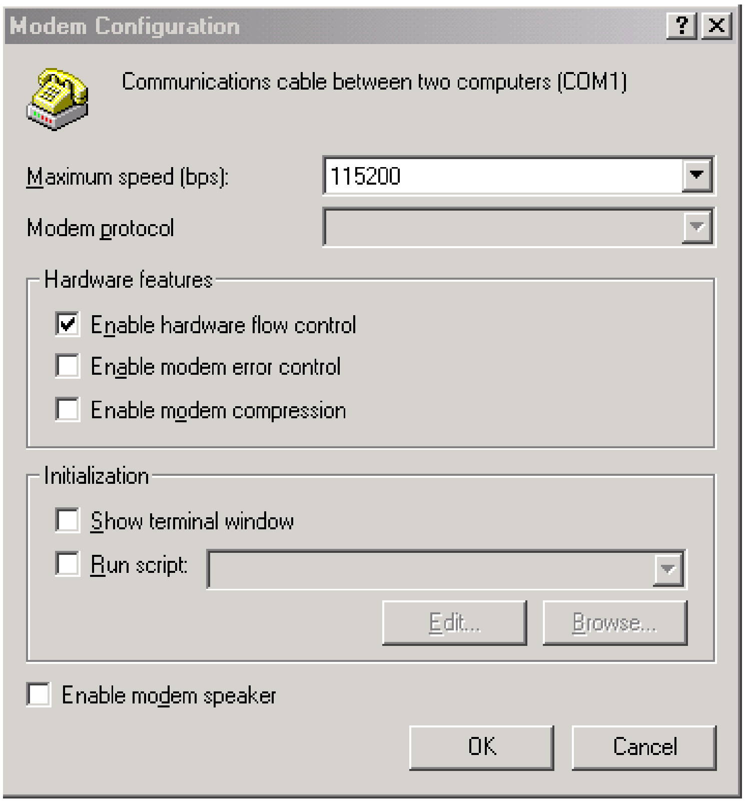
Direct Connection Properties

Select a device:

Communications cable between two computers (COM1)

☑ Show icon in taskbar when connected

On the "General" tab, click on the "Configure" button. In the dialog box that now appears, set the maximum transfer rate to 115,200 bits/s:



Modem Configuration

Communications cable between two computers (COM1)

Maximum speed (bps): 115200

Modem protocol

Hardware features

☑ Enable hardware flow control

□ Enable modem error control

□ Enable modem compression

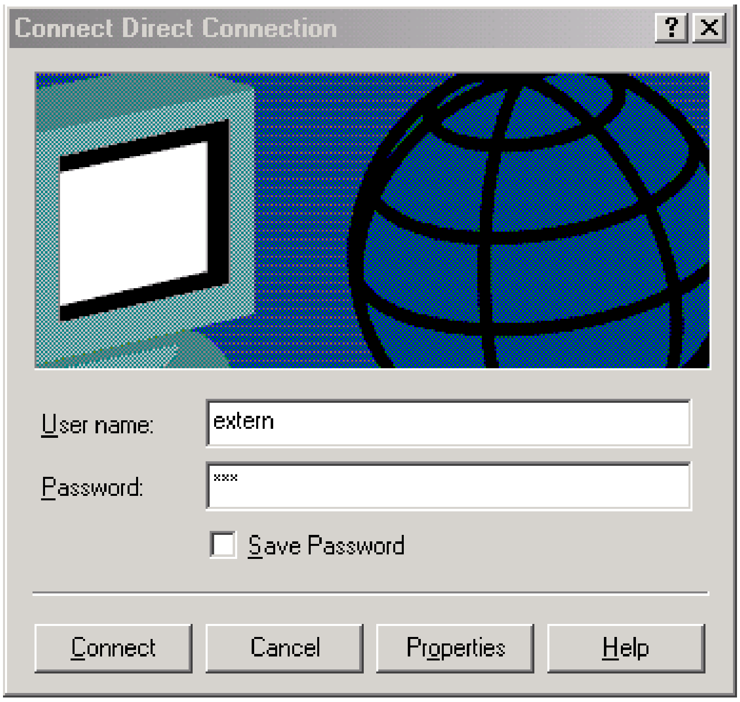
Initialization

□ Show terminal window

□ Run script:

□ Enable modem speaker

Now you can establish a connection. If you double-click on the zero-modem connection, the following screen should appear:



Connect Direct Connection

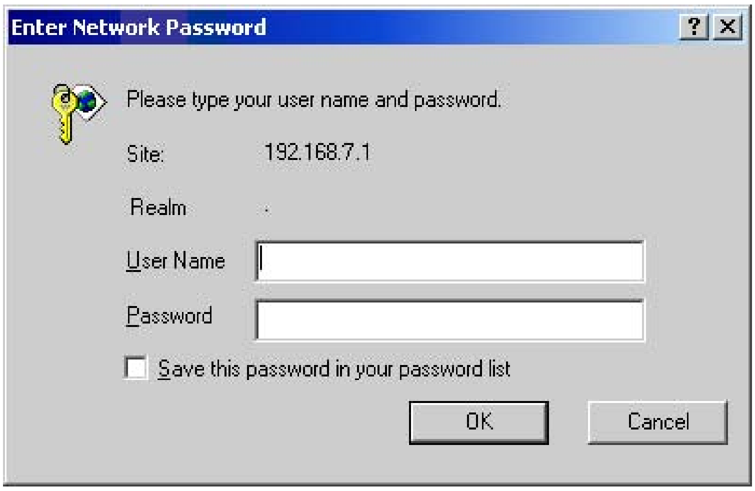
User name: extern

Password: ***

□ Save Password

Enter ’extern’ as the user name for yourself, too, and ’ctr’ for the password (default values). Call a browser and type the address 192.168.7.1

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


Enter Network Password

Please type your user name and password.

Site: 192.168.7.1

Realm .

User Name

Password

□ Save this password in your password list

The welcoming text of the embedded web server will appear. Now you can proceed with Section 4.3.1 .

4.2.3 Configuring via the telephone network

Prerequisites:

You will need a PC on which a Web browser is installed and a modem. The PC must be connected to a different telephone connection with a separate number to that of the router. A long-distance data transmission will be established.

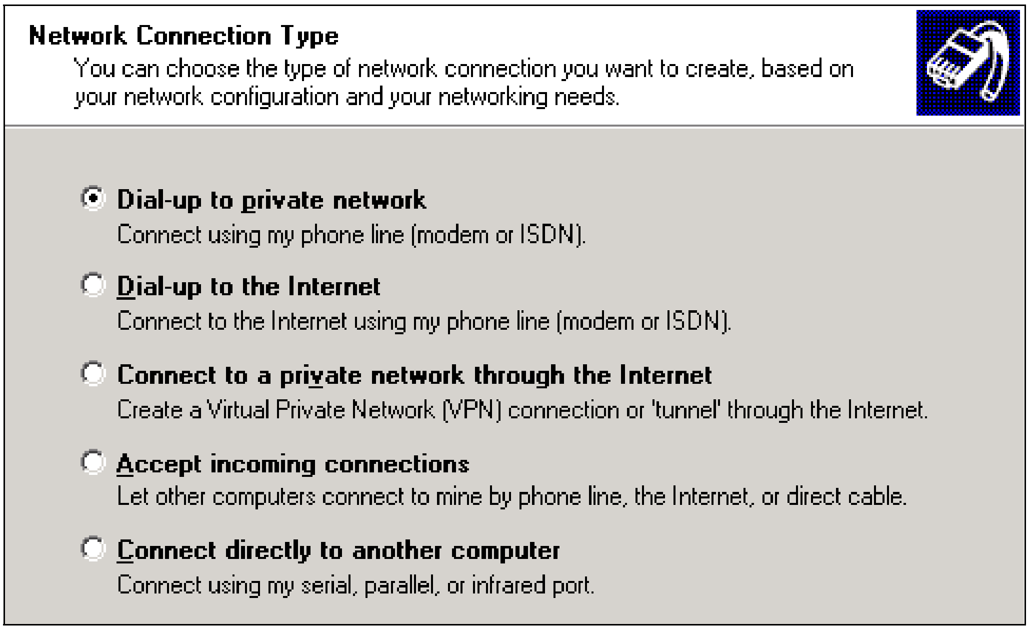
It is not relevant whether MS Windows or Linux is installed on your PC, because both operating systems include the required tools.

NOTE

The method described here pertains to Windows 2000 only.

Now go to `Control Panel`→`Network Connections` and start the "New Connection Wizard".

Choose "Connect directly to another computer" for the type of connection:



Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

● **Dial-up to private network**
Connect using my phone line (modem or ISDN).

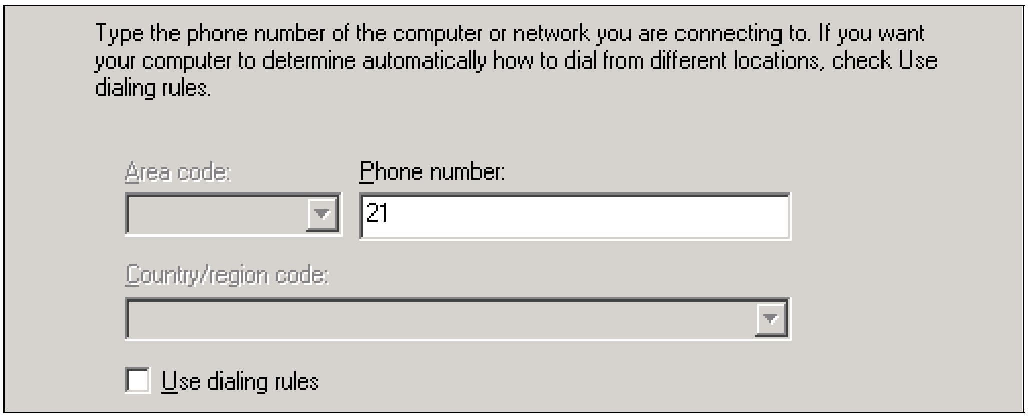
○ **Dial-up to the Internet**
Connect to the Internet using my phone line (modem or ISDN).

○ **Connect to a private network through the Internet**
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

○ **Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.

○ **Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

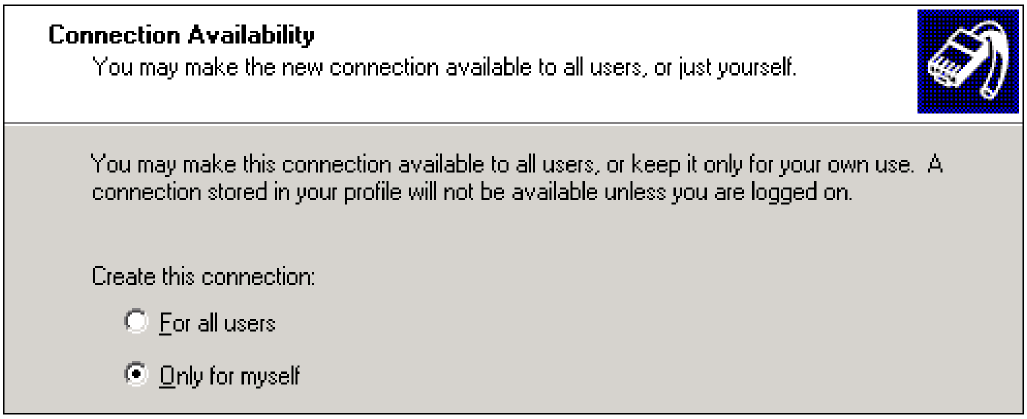
Enter the number of the telephone connection to which the router is connected:



Type the phone number of the computer or network you are connecting to. If you want your computer to determine automatically how to dial from different locations, check Use dialing rules.

Area code:
Phone number: 21
Country/region code:
□ Use dialing rules

If you are prompted to specify the availability of the connection, choose the option "Use connection exclusively":

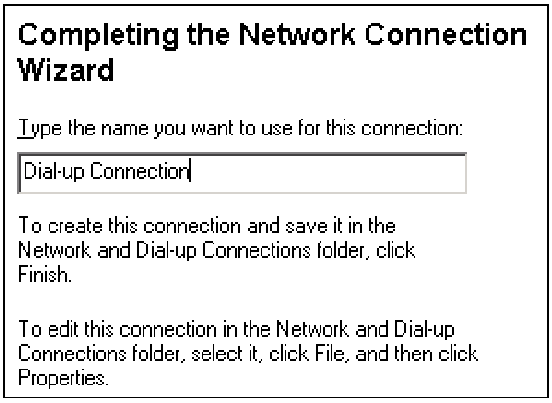


Connection Availability
You may make the new connection available to all users, or just yourself.

You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.

Create this connection:
○ For all users
● Only for myself

Enter a name for your connection (e.g.: "Zero modem"):



Completing the Network Connection Wizard

Type the name you want to use for this connection:

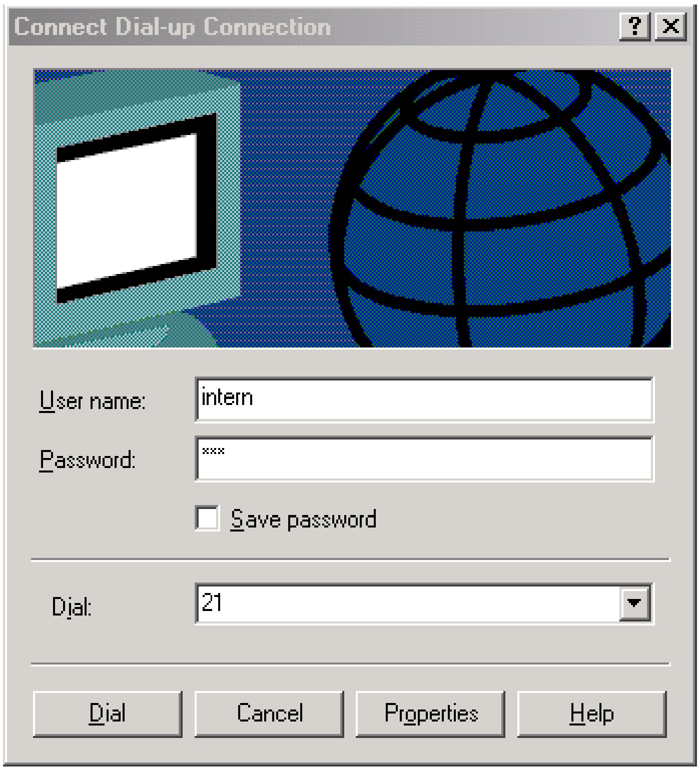
Dial-up Connection

To create this connection and save it in the Network and Dial-up Connections folder, click Finish.

To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.

If you are connected to a private telecommunications switching system, please note that no dialling tone is to be heart in the telephone. In this case, you must configure the modem such that it does not wait for the dialling tone. To this end, the initialisation command "ATX3" must additionally be entered in the tab "Advanced settings" in the modem configuration in the device manager of Windows 2000.

Use "Select" to establish a new connection:



Connect Dial-up Connection

User name: intern

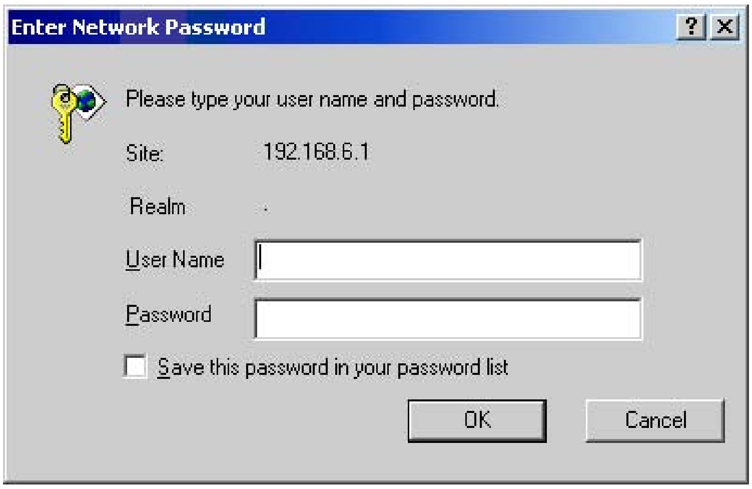
Password: ***

□ Save password

Dial: 21

Enter ’extern’ as the user name for yourself, too, and ’ctr’ for the password (default values). Now call a browser and type the following address: 192.168.6.1

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



Enter Network Password

Please type your user name and password.

Site: 192.168.6.1

Realm .

User Name

Password

□ Save this password in your password list

The welcoming text of the embedded web server will appear. Now you can proceed with Section 4.3.1 .

4.2.4 Configuring via the RS 232 interface

CAUTION

It is not recommended to use this type of configuration. It should only be used if you are absolutely conversant with the handling and programming of program commands in the terminal mode. Incorrect inputs or typing errors may result in the router no longer functioning.

If the router is configured incorrectly and no longer boots correctly, it is possible to restore the original default settings. To do so, press ENTER after you have been prompted to do so (on the console) while the router is booting. In this case, however, all settings you have made will be lost!

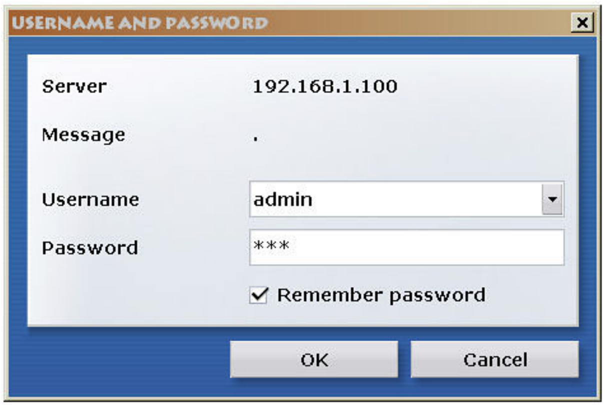
If you wish to configure the router using a browser, it is imperative that the router is installed in the same network with a network address not yet used. The default setting of the IP address is 192.168.1.100 with subnet mask 255.255.255.0. If you do not wish to set the IP address according to the local network, you can also set the IP address and the subnet mask via the serial interface to allow access via the network using a browser (see Section 4.1.1.1).

4.3 Configuration services

4.3.1 Web browser

You may use any browser which is able to handle frames as the configuration tool. The configuration has been tested successfully using Internet Explorer 5.x, Mozilla 1.x, Opera 7.x and Konquerer 3.x.

If the factory default settings have not been changed, the integrated web server of the router is started if you enter the IP address 192.168.6.1 (for modem) or 192.168.7.1 (for direct serial line) or 192.168.1.100 (for Ethernet) as the URL. The dialog box for you to enter your user name and the password is displayed:



USERNAME AND PASSWORD

Server 192.168.1.100

Message .

Username admin

Password ***

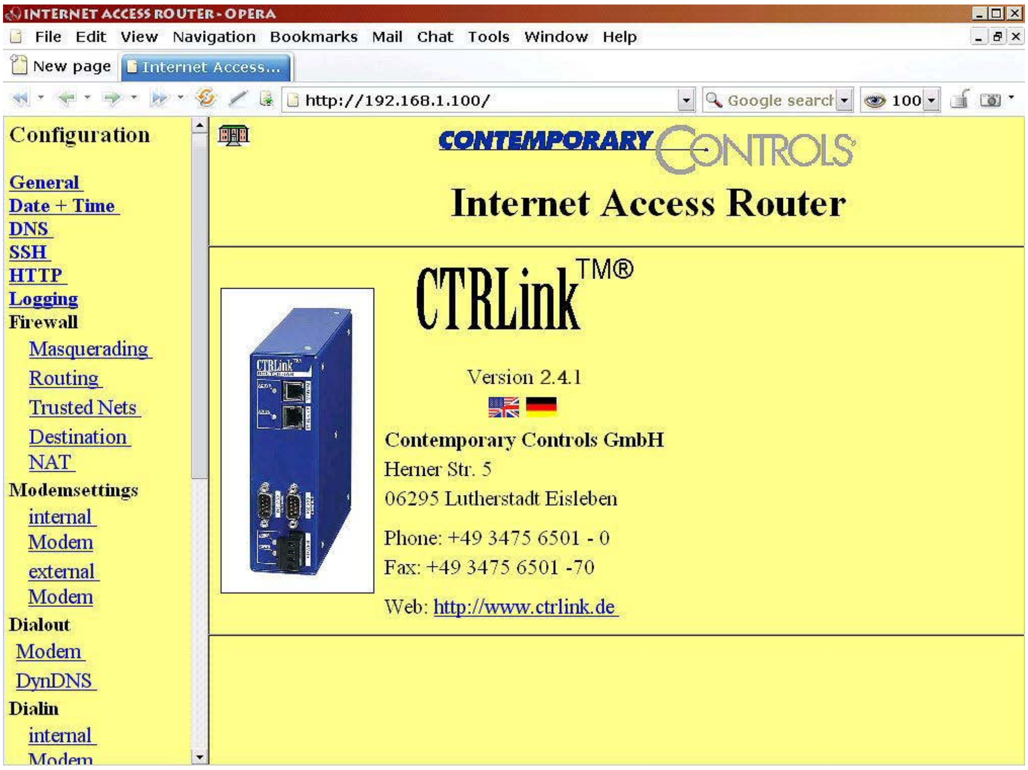
☑ Remember password

The default user name is "admin", and the default password is "ctr". The exact appearance of the interrogation dialog box depends on the browser you are using.

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

HINWEIS

The exact appearance of the browser window depends on the browser you are using and its settings. The colour, font type and font size, line length and line feeds may deviate from the illustrations shown here.



Internet Access Router

CTRLink™®

Version 2.4.1

Contemporary Controls GmbH
Herner Str. 5
06295 Lutherstadt Eisleben

Phone: +49 3475 6501 - 0
Fax: +49 3475 6501 -70

Web: http://www.ctrlink.de

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. The home page is called by clicking on the house 🏠 in the top right window (see illustration above).

The central area is the actual working area. The settings are made here and status information is also displayed. The dialog language for the menus and help texts can be selected by clicking on the appropriate flag on the home page. Currently, German and English are supported, default language is English.

If necessary, help texts are displayed for the individual configuration options.

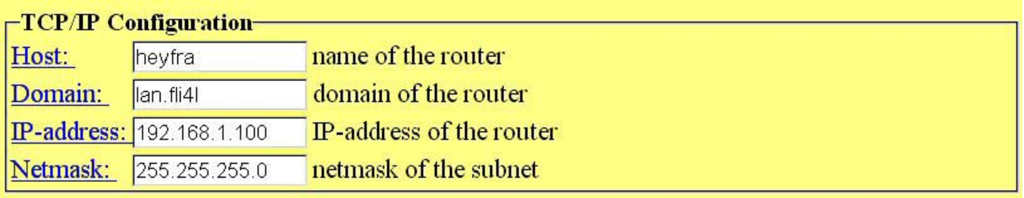
4.3.1.1 Menu option "General"

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

- the TCP/IP configuration
- the configuration of the administrator access
- the configuration of the serial console

These three configuration options will be explained in the following.

TCP/IP configuration



TCP/IP Configuration

Host:	heyfra	name of the router
Domain:	lan.fli4l	domain of the router
IP-address:	192.168.1.100	IP-address of the router
Netmask:	255.255.255.0	netmask of the subnet

Enter the host and the domain name, as well as the IP address and the subnet mask of your router here. To activate the online help for the individual items, simply click on the appropriate menu option.

Brief info IP addresses:

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

192.168.1.100

Number of network

Number of computer in network 192.168.1

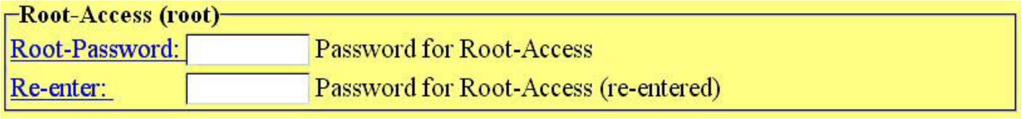
The size of the network portion may be varied via this IP address. It is determined by the network class. The example uses network class C, three numbers for the network, and one for the client.

CAUTION

For 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, either restore the factory default settings or set a valid network address using the serial console (see Section 4.2.4).

Make sure that the address you are setting is not already assigned within the Ethernet. The default setting 192.168.1.100 corresponds to client no. 100 in a C class network with no. 192.168.1. Make sure that the IP address is the same as that of the network address.

Configuring the administrator access



Root-Access (root)

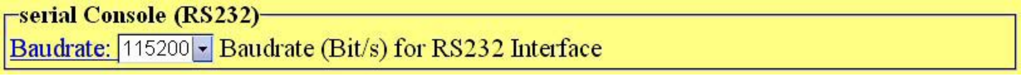
Root-Password:		Password for Root-Access
Re-enter:		Password for Root-Access (re-entered)

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.

CAUTION

It is strongly recommended to replace the default password ’ctr’ by your own password with 8 characters. Keeping the default password constitutes a significant breach in security.

Configuring the serial console



serial Console (RS232)

Baudrate: 115200 Baudrate (Bit/s) for RS232 Interface

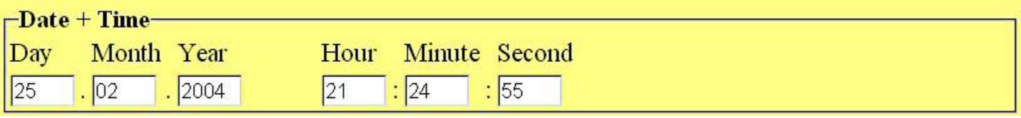
Here you can set the velocity of the serial console. If you connect the serial console to an IBM/PC (i386 or higher), you may keep the default value 115,200.

4.3.1.2 Menu option "Date & time"

This configuration menu is divided into two parts:

- Set local date and local time
- Configure the time zone / rules for daylight saving time

Configuring date & time

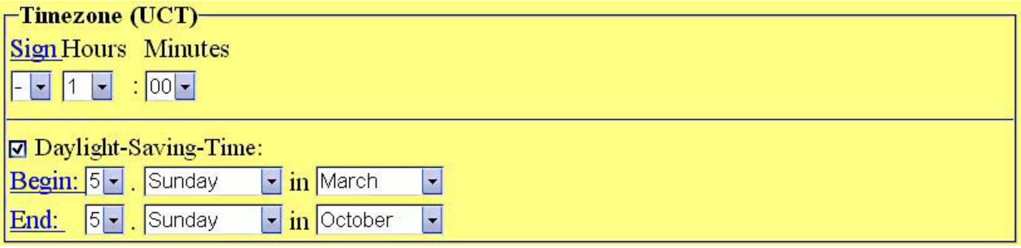


Date + Time

Day	Month	Year	Hour	Minute	Second
25	. 02	. 2004	21	: 24	: 55

Here you must enter the local date and the local time. Setting of the time is necessary, for example, if you want to use the recording capabilities of your router (see Section 4.3.1.7).

Configuring time zone and daylight saving time



Timezone (UCT)

Sign Hours Minutes

- 1 : 00

☑ Daylight-Saving-Time:

Begin: 5 . Sunday in March

End: 5 . Sunday in October

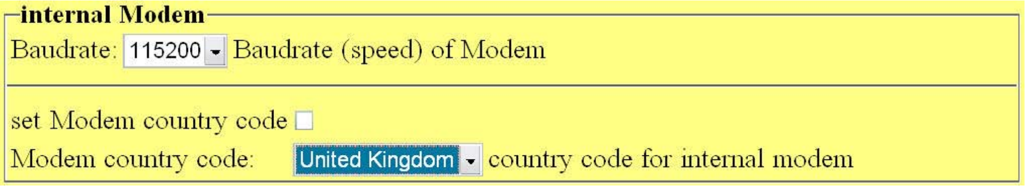
You can first enter here your time zone relative to the zero meridian (Greenwich). The sign will become negative (minus) if your time zone lies east of the zero meridian, and positive (plus) if it lies west. For Central Europe, for example, the value "-1" must be entered.

If switching between daylight saving time and standard time is required in the country where the router is used, select the relevant field. You may configure the rules applying in this country. In the European Union, daylight saving time always starts on the last Sunday in March, which can be set as the 5th Sunday in March. The return to standard time is on the last Sunday in October, which can be set as the 5th Sunday in October. If a month has only 4 Sundays, the time is nevertheless switched on the 4th (last) Sunday even if "5" has been chosen. In the USA, however, daylight saving time always starts on the 1st Sunday in April and must be configured accordingly.

4.3.1.3 General modem settings

The menu shown below can be used to make general settings for configuring your modem.

Configuring the internal modem analogue



internal Modem

Baudrate: 115200 Baudrate (speed) of Modem

set Modem country code □

Modem country code: United Kingdom country code for internal modem

The menu shown above can be used to configure the speed and the country code of your internal modem.

The country is selected via name of the country in the list box **Modem country code**.

The country code is set by placing a 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.

The internal modem supports the following country codes:

Australia	Great Britain	Korea	South Africa
Austria	Greece	Malaysia	Spain
Belgium	Hong Kong	Mexico	Sweden
Brazil	Hungary	New Zealand	Switzerland
China	India	Norway	Taiwan
Denmark	Ireland	Philippines	The Czech Republic
Finland	Israel	Poland	The Netherlands
France	Italy	Portugal	Turkey
Germany	Japan	Singapore	USA/Canada

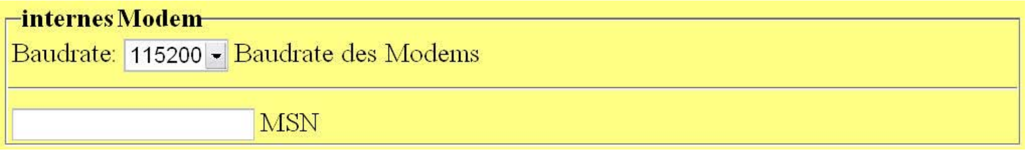
CAUTION

Always ensure that the modem has been assigned the correct country code; otherwise, you will not be allowed to dial in.

Please save your configuration immediately after changing the country code. Otherwise, all your settings are lost after a cold restart of your router.

To activate a changed country code, the router must be disconnected from the mains temporarily; a warm restart will not be sufficient.

Konfiguration des internen Modems ISDN



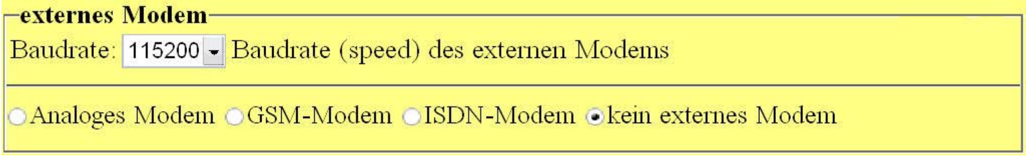
internes Modem

Baudrate: 115200 ▾ Baudrate des Modems

MSN

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

Configuring the external modem

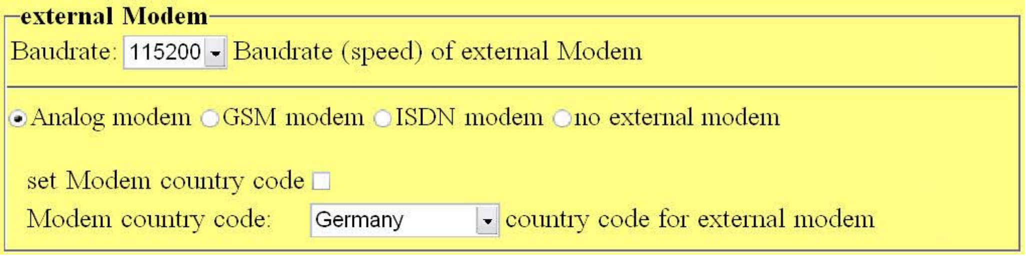


externes Modem

Baudrate: 115200 ▾ Baudrate (speed) des externen Modems

○ Analoges Modem ○ GSM-Modem ○ ISDN-Modem ● kein externes Modem

The configuration depends on the external modem you are using:



external Modem

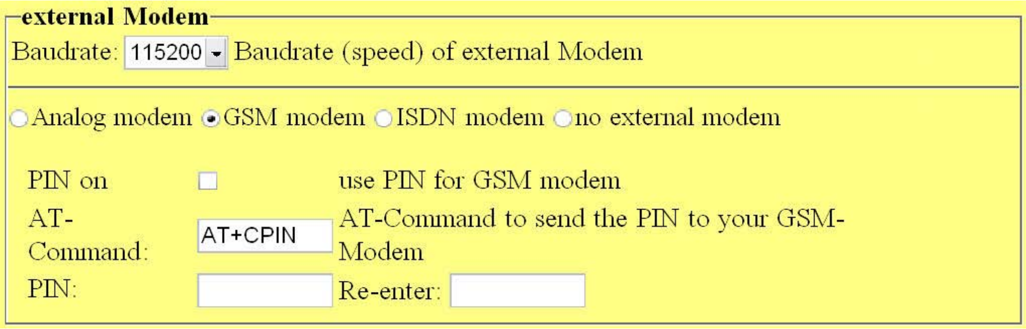
Baudrate: 115200 ▾ Baudrate (speed) of external Modem

● Analog modem ○ GSM modem ○ ISDN modem ○ no external modem

set Modem country code □

Modem country code: Germany ▾ country code for external modem

The menu shown above can be used to configure the speed and the country code of your external modem. For the country codes of the external modem, please refer to the manual 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.



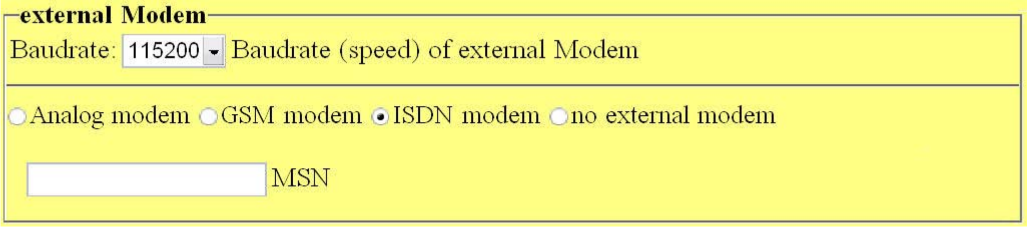
external Modem

Baudrate: 115200 Baudrate (speed) of external Modem

○ Analog modem ● GSM modem ○ ISDN modem ○ no external modem

PIN on	□	use PIN for GSM modem
AT-Command:	AT+CPIN	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.



external Modem

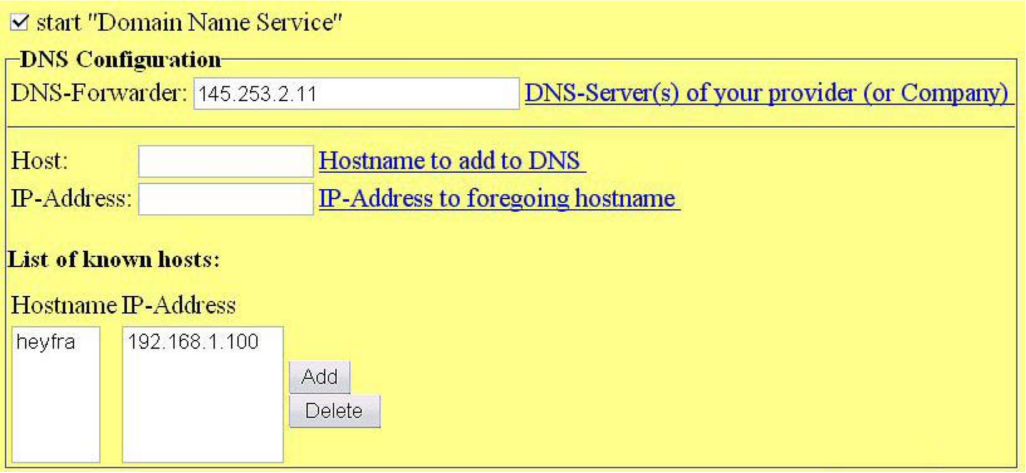
Baudrate: 115200 Baudrate (speed) of external Modem

○ Analog modem ○ GSM modem ● ISDN modem ○ no external 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.

4.3.1.4 Menu option "DNS"



☑ start "Domain Name Service"

DNS Configuration

DNS-Forwarder: 145.253.2.11 DNS-Server(s) of your provider (or Company)

Host: Hostname to add to DNS

IP-Address: IP-Address to foregoing hostname

List of known hosts:

Hostname	IP-Address
heyfra	192.168.1.100

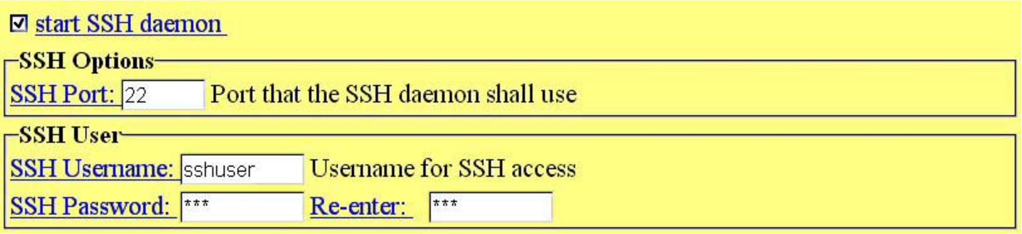
The domain name service serves to resolve the names in a network. Resolving names means that each IP address is assigned a name which is easy to remember. This service is offered by the server.

In order not to be compelled to enter all hosts of the entire company or even of the entire Internet here, the DNS forwarder concept has been created. Any addresses which cannot be resolved 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.

4.3.1.5 Menu option "SSH"

Here you can configure the SSH daemon.



☑ start SSH daemon

SSH Options

SSH Port: 22 Port that the SSH daemon shall use

SSH User

SSH Username: sshuser Username for SSH access

SSH Password: *** Re-enter: ***

If you want to use the SSH daemon, the appropriate field must be activated. You can define at which port the SSH daemon is to be addressed. This is port 22 by default.

For security reasons, you may also enter a different port. Please observe that the relevant port must also be communicated explicitly to the SSH client you are using, see chapter 4.3.3.

For details on how to do this, please refer to the appropriate documentation of your SSH client (a suitable and tested client for Windows is "putty", for example; http://www.chiark.greenend.org.uk/~sgtatham/putty/)

CAUTION

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

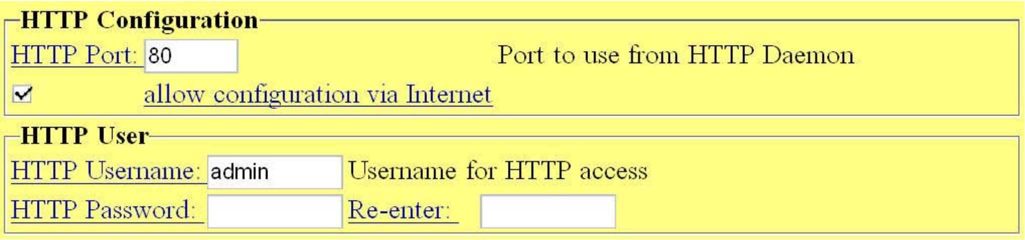
NOTE

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

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

4.3.1.6 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.



HTTP Configuration

HTTP Port: 80 Port to use from HTTP Daemon

☑ allow configuration via Internet

HTTP User

HTTP Username: admin Username for HTTP access

HTTP Password: Re-enter:

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.

NOTE

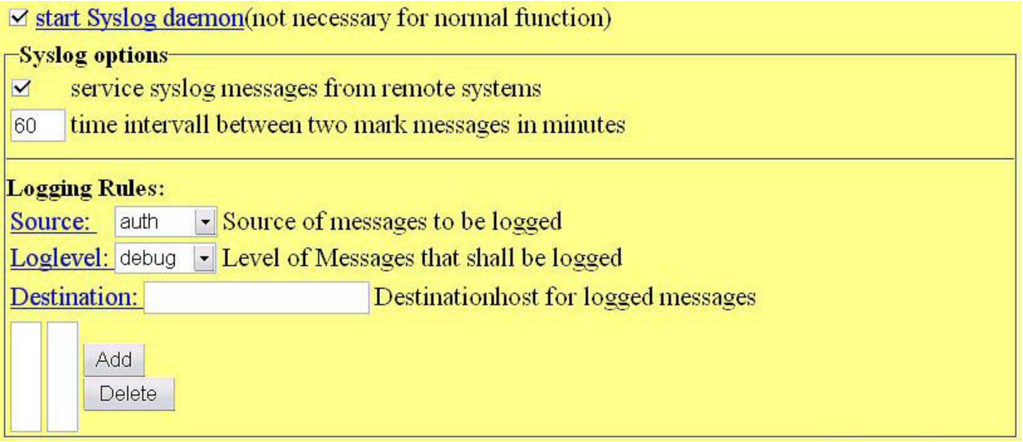
It is recommended to change both the user name and the password of the default user. Please note that the web server possesses its own user management so that neither the administrator (root), nor the SSH user have access to the web interface. Otherwise, the HTTP user specified here is not granted access to the router, neither via the serial console, nor via the SSH.

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.

CAUTION

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

4.3.1.7 Menu option "Logging"



☑ start Syslog daemon(not necessary for normal function)

Syslog options

☑ service syslog messages from remote systems

60 time intervall between two mark messages in minutes

Logging Rules:

Source: auth Source of messages to be logged

Loglevel: debug Level of Messages that shall be logged

Destination: Destinationhost for logged messages

If the logging service is activated, the router issues status messages regarding its current activities. All these status messages are generally output to the serial console. Additionally, you can configure here which status messages are to be forwarded to a so-called log-host (see below). The router can also forward status messages from computers in one 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 logged (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.
- **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 logging 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:

- **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 errors).
- **alert** Creates status messages with reference to things that should be corrected immediately (for example, errors in configuration files)
- **emerg** Creates status messages indicating that the appropriate service could either not be started or had to be cancelled.

4.3.1.8 Menu option "Firewall"

The firewall of the router offers two data filtering options:

- a packet filter
- a port filter

The packet filter always considers the IP addresses. It only passes IP packets with permitted IP addresses, and blocks packets of illegal addresses. As a rule, complete network(s) (areas) are enabled or disabled in order to prohibit or permit individual hosts selectively as required.

The router offers three preconfigured packet filters:

- Masqueraded 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 are 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 for which the access to the routed / masked networks is to be permitted / prohibited explicitly.

A port filter assesses packets not by their source or target address, but by their target port. For example, all packets aimed at a certain port are discarded, or all packets of a certain port are transferred to another computer.

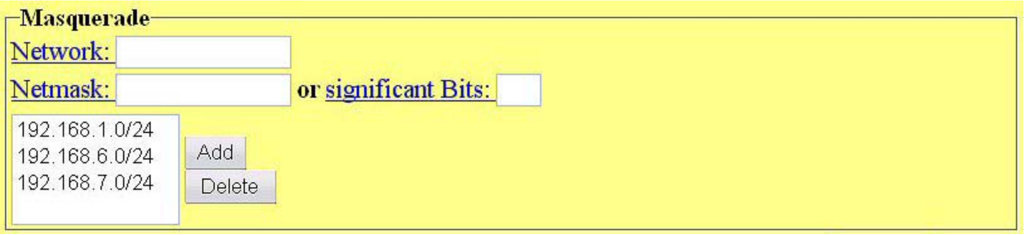
CAUTION

CAUTION !!!

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

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

4.3.1.9 Menu option "Firewall - Masquerading"



192.168.1.0/24
192.168.6.0/24
192.168.7.0/24

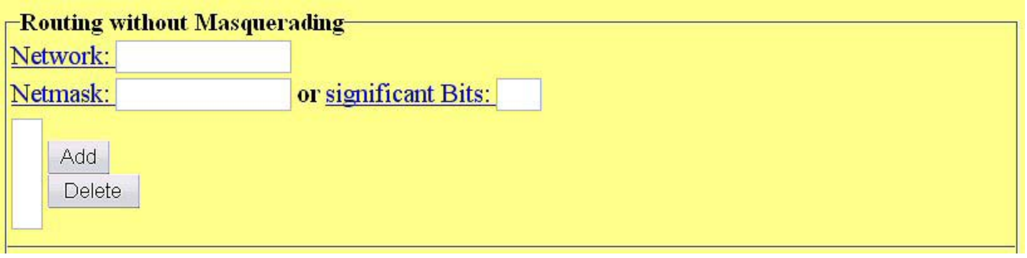
Specify the networks to be masked externally here. If you are using unofficial IP addresses, such as 192.168.x.x, and if the router is nevertheless to be used for access to the Internet, it is imperative to specify them here.

Please observe that any network addresses always contain "xxx.xxx.xxx.0" (i.e. always end with zero).

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

4.3.1.10 Menu option "Firewall - Routing"

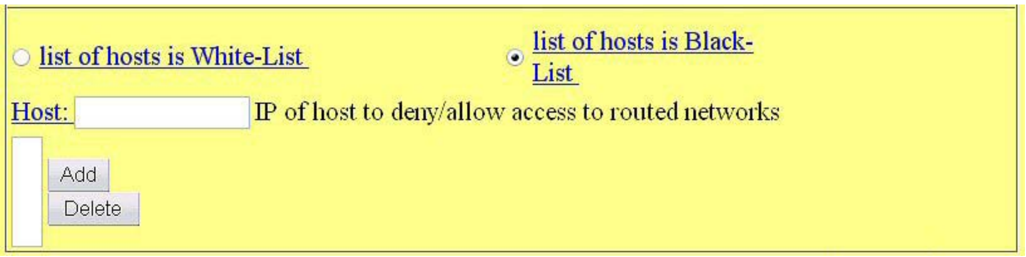
Routing



Packets belonging to connections established by hosts in these subnets are forwarded by the router. Furthermore, packets sent into these networks are not masked.

The same syntactic rules apply as for the masked networks.

Host filter



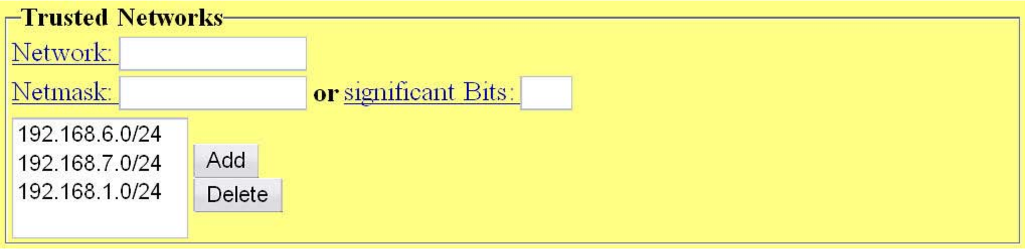
○ list of hosts is White-List ● list of hosts is Black-List

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

Certain computers may be granted access specifically to other networks (white list) or else, conversely, 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 else it will block precisely these.

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

4.3.1.11 Menu option "Firewall - Trusted Nets"



Trusted Networks

Network:

Netmask: or significant Bits:

192.168.6.0/24
192.168.7.0/24
192.168.1.0/24

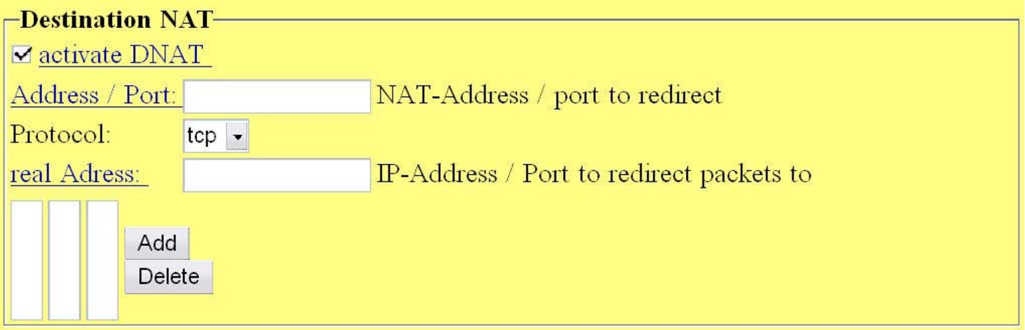
By using this configuration menu, the disabling of routing for certain ports (see below) and the black/white list can be disabled for certain networks. Here you can specify subnets which are trusted.

A typical example is the routing of NetBios ports (Windows enables) between two LANs which are assigned data via two network cards of the Linux fli4l router. In this case, all trusted networks must be specified.

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.

4.3.1.12 Menu option "Firewall – Destination NAT"

Destination NAT



Destination NAT

☑ activate DNAT

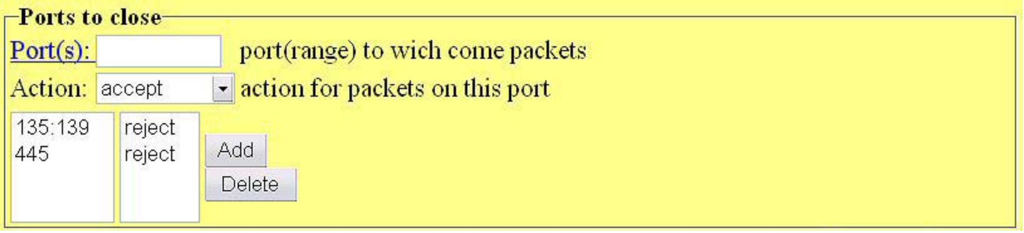
Address / Port: NAT-Address / port to redirect

Protocol: tcp

real Adress: IP-Address / Port to redirect packets to

For various Internet protocols it is imperative to divert a connection established for a computer from the outside to the internal network. If the network is masked externally ("IP masquerading", see 4.3.1.19), 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. This is called port forwarding or "Destination Network Address Translation", briefly "DNAT".

Port access



Ports to close

Port(s): port(range) to wich come packets

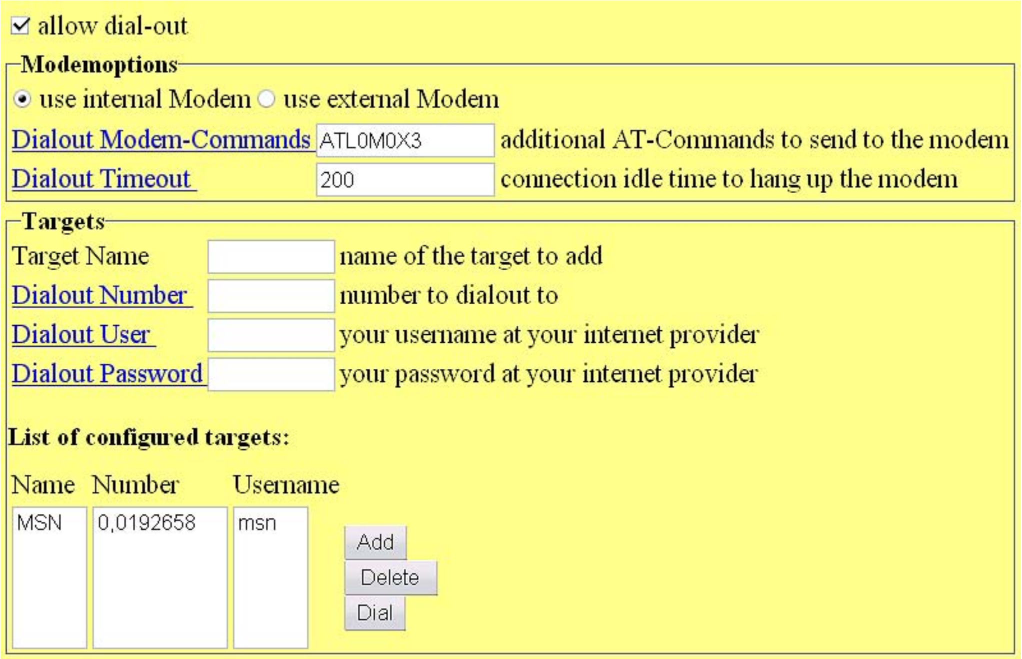
Action: accept action for packets on this port

135:139 reject
445 reject

The routing via certain IP ports can be prevented. For example, it makes sense to prohibit the routing for 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 4.3.1.11) can be specified between which the routing of these ports is nevertheless explicitly permitted.

4.3.1.13 Menu option "Dial-out - modem"



☑ allow dial-out

Modemoptions

● use internal Modem ○ use external Modem

Dialout Modem-Commands	ATL0M0X3	additional AT-Commands to send to the modem
Dialout Timeout	200	connection idle time to hang up the modem

Targets

Target Name		name of the target to add
Dialout Number		number to dialout to
Dialout User		your username at your internet provider
Dialout Password		your password at your internet provider

List of configured targets:

Name	Number	Username
MSN	0,0192658	msn

Dial-out (for example, into the Internet) is possible via the internal or the external modem. This dial-out into 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 not assign otherwise to any of its known networks.

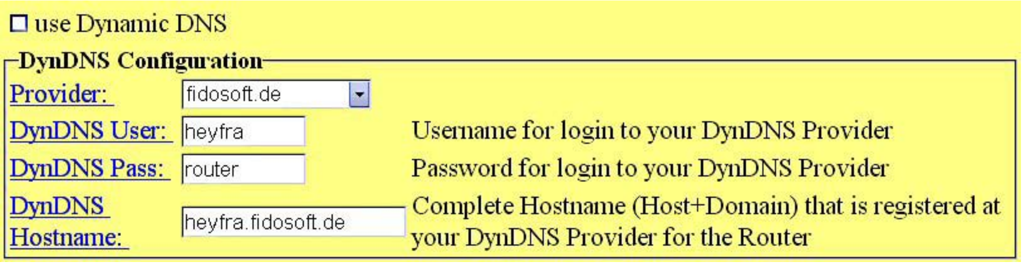
Instead of the internal modem, an external modem connected via the serial interface "Ext. modem" can also be used. The default dialling string can be changed in the field "Dial-out modem commands". For automatic hang-up, a wait time in seconds can be set in the field "Dial-out Timeout".

More than one destination can be defined. If more than one destination is defined the function "Dial on Demand" is deactivated. To dialout the button "Dial" must be activated manually. The manual activation also works if only one destination is defined and function "Dial on Demand" is activated accordingly.

With firmware version 2.2 or above the Dial-Out can be deactivated completely. Be aware then a Callback is not longer possible.

Either only the internal or only the external modem can be configured for dial-out at the same time. This, however, has no influence on the configuration for dial-in (see Section 4.3.1.15).

4.3.1.14 Menu option "Dial-out - DynDNS"



□ use Dynamic DNS

DynDNS Configuration

Provider:	fidosoft.de	
DynDNS User:	heyfra	Username for login to your DynDNS Provider
DynDNS Pass:	router	Password for login to your DynDNS Provider
DynDNS Hostname:	heyfra.fidosoft.de	Complete Hostname (Host+Domain) that is registered at your DynDNS Provider for the Router

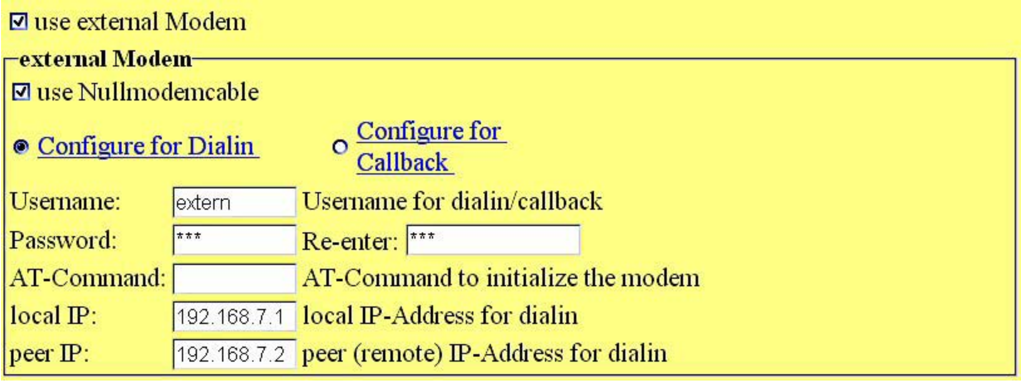
With version 2.0 and higher, the router offers the facility to register with a DynDNS provider in the Internet so that it can be addressed using a fixed host name. This possibility can be configured here.

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

- FreeDNS (http://freedns.afraid.org)
- CJB.NET (http://cjb.net/)
- Companity (http://www.staticip.de/)
- DHS International (http://www.dhs.org/)
- DNS2Go (http://dns2go.deerfield.com/)
- The Art of DNS (http://dnsart.com/)
- DtDNS (http://www.dtdns.com/)
- DynAccess (http://dynaccess.de/)
- DynDNS (http://dyndns.org/)
- DynDNS DK (http://dyndns.dk/)
- dyn.ee (http://dyn.ee/)
- eisfair.net (http://eisfair.net/)
- Fidosoft (http://fidosoft.de)
- hn.org (http://hn.org/)
- KONTENT (http://www.kontent.de/)
- Nerdcamp (http://nerdcamp.net/)
- No-IP (http://www.no-ip.com/)
- Regfish (http://www.regfish.com)
- SelfHost (http://selfhost.de/)
- ZoneEdit (http://zoneedit.com/)

Please note that the relevant DynDNS provider must be entered as the first name server on the client side to be able to resolve the host name of the router correctly.

4.3.1.15 Menu option "Dial-in"



☑ use external Modem

external Modem

☑ use Nullmodemcable

● Configure for Dialin ○ Configure for Callback

Username: extern Username for dialin/callback

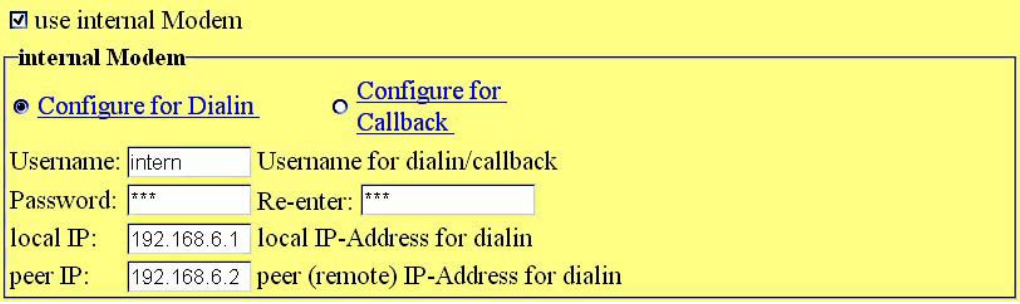
Password: *** Re-enter: ***

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

Dial-in can be performed either via the external or via the internal 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. It is also possible, however, that both modems wait for incoming calls simultaneously.



☑ use internal Modem

internal Modem

● Configure for Dialin ○ Configure for Callback

Username: intern Username for dialin/callback

Password: *** Re-enter: ***

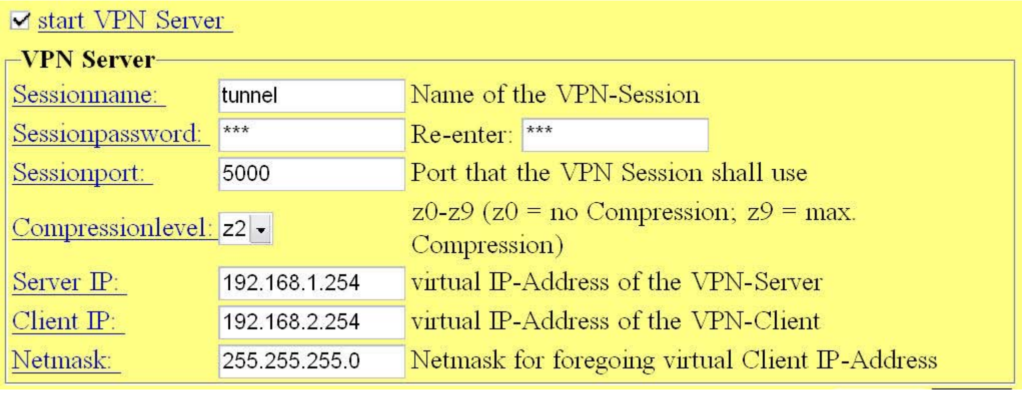
local IP: 192.168.6.1 local IP-Address for dialin

peer IP: 192.168.6.2 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. With call-back, the router recognises that it was dialled, hangs up immediately and either calls back or calls the Internet provider, depending on how it was configured in the dial-out (see Section 4.3.1.13).

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

4.3.1.16 Menu option "VPN server"



☑ start VPN Server

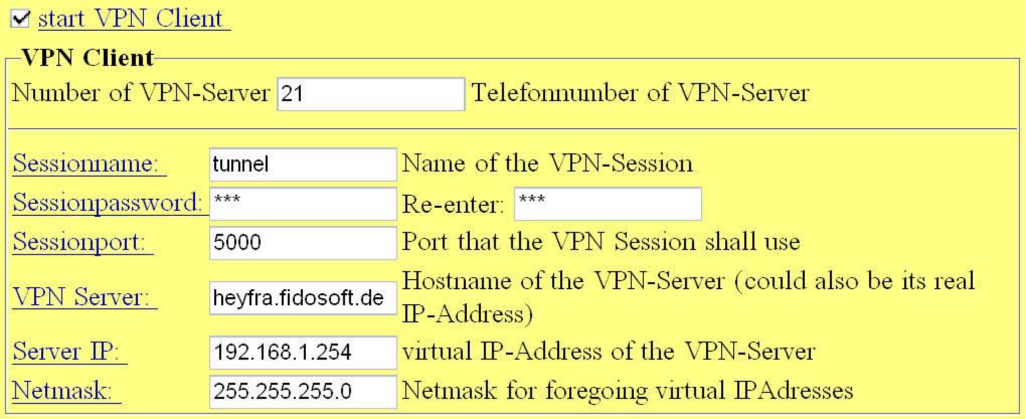
VPN Server

Sessionname:	tunnel	Name of the VPN-Session
Sessionpassword:	***	Re-enter: ***
Sessionport:	5000	Port that the VPN Session shall use
Compressionlevel:	z2	z0-z9 (z0 = no Compression; z9 = max. Compression)
Server IP:	192.168.1.254	virtual IP-Address of the VPN-Server
Client IP:	192.168.2.254	virtual IP-Address of the VPN-Client
Netmask:	255.255.255.0	Netmask for foregoing virtual Client IP-Address

The VPN server can be used to establish secure (encrypted; 128bit blowfish encryption) connections to the router. To this end, a VPN server must be started on the router which will then assign the router a virtual IP.

To be able to communicate with this server, a VPN client must be started on the opposite side. This can be either also a router (see Section 4.3.1.17) or a Linux PC on which the relevant software is installed (BSD, Solaris) (http://vtun.sourceforge.net/).

4.3.1.17 Menu option "VPN client



☑ start VPN Client

VPN Client

Number of VPN-Server 21 Telefonnumber of VPN-Server

Sessionname:	tunnel	Name of the VPN-Session
Sessionpassword:	***	Re-enter: ***
Sessionport:	5000	Port that the VPN Session shall use
VPN Server:	heyfra.fidosoft.de	Hostname of the VPN-Server (could also be its real IP-Address)
Server IP:	192.168.1.254	virtual IP-Address of the VPN-Server
Netmask:	255.255.255.0	Netmask for foregoing virtual IPAdresses

The VPN client can establish a connection to a VPN server and thus establish an encrypted connection across the Internet. To this end, either a second router can be used as server (see Section 4.3.1.16) or an appropriately configured Linux computer (BSD, Solaris) (http://vtun.sourceforge.net/).

4.3.1.18 Menu option "Save settings"

This menu option serves to save all changes made in the configuration permanently. Any changes are only held in the user memory until saving; they are lost when restarting the PC. The error LED of the router is lit in red during the saving process.

4.3.1.19 Menu option "Restarting the router"

This menu option can be used to restart the router. This process may take several minutes. The router is ready again for operation if the following LEDs are lit in green: "Power", "Error" and "Ethernet".

CAUTION

To activate a changed country code for the internal modem, the router must be disconnected from the mains temporarily; warm restart via the menu is not sufficient.

4.3.1.20 Menu option "Close PPP connections"

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

4.3.1.21 Menu option "Active network interfaces"

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

4.3.1.22 Menu option "Active VPN tunnel"

Use this menu option to display all VPN servers and VPN clients currently active, as well as all active connections.

4.3.2 Configuration via the serial console

CAUTION

This configuration method is not recommended. It should only be used if you are absolutely sure with the handling and programming of program commands in the terminal mode. Incorrect inputs or type errors may have the effect that the router does not function any more.

Log in to the system of the router as described in Section 4.2.4. After you have entered the command "e3em /etc/rc.cfg", an integrated editor opens. At the same time, the central configuration is displayed as plain text. Use the arrow keys for navigation.

Keyboard assignment of the integrated editor:

Ctrl + X, then F - Load file

Ctrl + X, then S - Save current file

Ctrl + X, then C - Quit editor

HINWEIS

Only the command "spiwr" will save all settings in the flash of your router. If you then reboot the system, your changes come into effect.

A large part of the configuration file consists of internal settings which should not be changed.

All entries which can be changed will be specified here. We will here forego an explanation of the principle of action; it corresponds to the appropriate menu options of the web interface. Each item specified here can also be addressed via the web interface which is therefore recommended for configuring.

4.3.2.1 Changing the network address

If you only wish to change the network address to grant a browser access to the router, change the following lines:

- IP_ETH_1_IPADDR='192.168.1.100'
- IP_ETH_1_NETMASK='255.255.255.0'
- MASQ_NETWORK='192.168.1.0/24 ...
- TRUSTED_NETS='192.168.1.0 ...

4.3.2.2 Basic configuration

HOSTNAME=’heyfra’

.... the host name of the router

DOMAIN_NAME='lan.fli4l'

.... the domain name of the router

PASSWORD='ctr'

.... the password of the administrator access of the router

IP_ETH_1_IPADDR='192.168.1.100'

.... the IP address of the router

IP_ETH_1_NETMASK='255.255.255.0'

.... the netmask of the router

SER_CONSOLE_RATE='115200'

.... the baud rate of the serial console

The country code of the modem cannot be controlled via the file </etc/rc.cfg>. To this end, the script <setCountry> is included in the scope of supply. The command "setCountry -h" in the command line indicates all country codes possible.

"setCountry device <code>" will set the modem specified in <device> to <code>. <device> must be either:

- **/dev/ttyS1** for the external modem, or
- **/dev/ttyS2** for the internal modem

If no <code> is specified, the script will simply output the country code currently set for the appropriate modem.

4.3.2.3 Configuring date and time

TIME_INFO='UCT-1UCST,M3.5.0,M10.5.0'

Configuring time zone and daylight saving time; meaning:

- UCT-1: Subtract an hour from the Greenwich Time.
- UCST: This time zone possesses a daylight saving time.
- M3.5.0: The daylight saving time starts on the last (5) Sunday (0) of the third (3) month.

- M10.5.0: The daylight saving time ends on the last (5) Sunday (0) of the third (10) month.
- In this file, date and time cannot be set. To this end, the commands "date" and "hwclock" which must be used on the console.

4.3.2.4 DNS configuration

START_DNS='yes'

.... corresponds to "Start DNS server?"

DNS_FORWARDERS='145.253.2.11'

.... corresponds to "External DNS server of provider / company"

HOST_1_NAME='kai'

.... first host name of the "LIST OF HOSTS FOR DNS"

HOST_1_IP='192.168.101.44'

.... the IP which is to be assigned to the appropriate host name (in this case, the first one)

HOSTS_N='2'

.... number of entries **in HOST**_X

4.3.2.5 SSH configuration

OPT_SSHD='yes'

.... corresponds to "Start DNS server?"

SSHD_PORT='22'

.... port to be used by the SSH server

SSHD_USERS_1_NAME='sshuser'

.... name of the SSH user

SSHD_USERS_1_PASSWD='ssh'

.... password of the SSH user

4.3.2.6 HTTP configuration

HTTPD_PORT='80'

.... web server to be used by the SSH server

HTTPD_USER_1='admin'

.... user name for the web server

HTTPD_PASS_1='ctr'

.... password for the web server

4.3.2.7 Firewall configuration

MASQ_NETWORK='192.168.1.0/24'

.... networks to be masked (separate by spaces)

ROUTE_NETWORK='192.168.6.0/24 192.168.7.0/24'

.... networks to be routed (separate by spaces)

TRUSTED_NETS=' '

.... trusted networks (separate by spaces; either at least 2 or none)

FORWARD_HOST_WHITE='no'

.... host list is white list or black list

OPT_PORTFW='yes'

.... Activate port forwarding?

PORTFW_N='0'

.... number of ports to be forwarded

PORTFW_1_SOURCE='1024'

.... first port to be forwarded

PORTFW_1_PROTOCOL='tcp'

.... protocol on the first port whose data are to be forwarded

PORTFW_1_TARGET='192.168.1.45'

.... target host for the data of the first port

FORWARD_DENY_PORT_N='1'

.... number of ports at which the acceptance of data is to be denied

FORWARD_DENY_PORT_1='445 reject'

.... port whose data are to be denied ("reject" is a keyword and is repeated in each entry).

4.3.2.8 Modem configuration

OPT_MODEM='yes'

.... Configure modem for dial-out?

MODEM_DEV='ttyS2'

.... If instead of the internal modem the external modem is to be used for dial-out, enter here "ttyS1", otherwise "ttyS2".

MODEM_SPEED='115200'

.... speed of the modem

MODEM_DIALOUT='0,0192658'

.... number of the Internet provider

MODEM_TIMEOUT='200'

.... time of inactivity after which the modem is to hang up

MODEM_USER='msn'

.... user name with the Internet provider

MODEM_PASSWD='msn'

.... password with the Internet provider

INT_DIALIN='yes'

.... Configure internal modem for dial-in?

INT_CALLBACK='no'

.... Configuring the internal modem for call-back (CAUTION: If both dial-in and call-back are activated, the modem will be configured to "Dial-in".)

INT_IPADDR='192.168.6.1'

.... local IP address to be assigned for dial-in

INT_PEER='192.168.6.2'

.... remote IP address to be assigned for dial-in

INT_USER='intern'

.... log-in name for dial-in / call-back

INT_PASS='ctr'

.... password for dial-in / call-back

EXT_DIALIN='yes'

.... Configure external modem for dial-in?

EXT_CALLBACK='no'

.... Configuring the external modem for call-back (CAUTION: If both dial-in and call-back are activated, the modem will be configured to "Dial-in".)

EXT_NULLMODEM='yes'

.... Instead of a modem, a zero-modem cable is connected to the external modem interface.

EXT_SPEED='38400'

.... speed of the external modem

EXT_IPADDR='192.168.7.1'

.... local IP address with dial-in

EXT_PEER='192.168.7.2'

.... remote IP address with dial-in

EXT_USER='extern'

.... user name for dial-in / call-back

EXT_PASS='ctr'

.... password for dial-in / call-back

4.3.2.9 DynDNS configuration

OPT_DYNDNS='yes'

.... Start dynamic DNS?

DYNDNS_N='1'

.... number of DynDNS providers you are using

DYNDNS_1_PROVIDER='FIDOSOFT'

.... name of the DynDNS provider; possible entries are:

- AFRAID for afraid.org
- CJB for cjb.net
- COMPANITY for Companity
- DHS for DHS International
- DNS2GO for DNS2Go
- DNSART for The Art of DNS
- DTDNS for DtDNS.net
- DYNACCESS for dynaccess.de
- DYNDNSDK for DynDNS.dk
- DYNDNS for DynDNS.org
- DYNEE for dyn.ee
- DYNEISFAIR for eisfair.net
- FIDOSOFT for fidosoft.de
- HAMMERNODE for hn.org
- KONTENT for Kontent.de
- NERDCAMP for nerdcamp.net
- NOIP for No-IP.com
- REGFISH for Regfish.com
- SELFHOST for SelfHost.de
- ZONEEDIT for zoneedit.com

DYNDNS_1_USER='heyfra'

.... log-in name with the DynDNS provider

DYNDNS_1_PASSWORD='router'

.... log-in password with the DynDNS provider

DYNDNS_1_HOSTNAME='heyfra.fidosoft.de'

.... host name to be to be registered with the DynDNS provider

4.3.2.10 VPN configuration

VTUND_SERVER_1_NAME='tunnel01'

.... name of the VPN server session

VTUND_SERVER_1_PASS='ctr'

.... password for the VPN server session

VTUND_SERVER_1_PORT='4326'

.... port of the VPN server

VTUND_SERVER_1_COMPRESS='z2'

.... compression rate of the VPN connection (min.: z0; max. z9)

VTUND_SERVER_1_SERVERIP='192.168.1.254'

.... virtual local IP address of the VPN server

VTUND_SERVER_1_CLIENTIP='192.168.2.254'

.... virtual remote IP address of the VPN client

VTUND_SERVER_1_CLIENTNETMASK='255.255.255.0'

.... virtual netmask of the VPN connection

VTUND_CLIENT_1_NAME='tunnel01'

.... name of the VPN server session

VTUND_CLIENT_1_PASS='ctr'

.... password for the VPN server session

VTUND_CLIENT_1_HOST='heyfra.fidosoft.de'

.... real host name of the computer on which the VPN server runs

VTUND_CLIENT_1_PORT='4326'

.... port to be used by the VPN client

VTUND_CLIENT_1_SERVERIP='192.168.1.254'

.... virtual local IP address of the VPN client

```
VTUND_CLIENT_1_SERVERNETMASK='255.255.255.0'
```

.... virtual netmask of the VPN connection

4.3.2.11 Logging configuration

```
OPT_SYSLOGD='yes'
```

.... Activate logging of status messages

```
SYSLOGD_REMOTE='yes'
```

.... Forward status messages of remote hosts

```
SYSLOGD_MARK_INTERVALL='60'
```

.... time interval for the logging time marks in minutes

```
SYSLOGD_DEST_N='1'
```

.... number of logging rules

```
SYSLOGD_DEST_2='*.* @192.168.1.123'
```

.... First logging rule: Structure: <source.type@targethost>. Which sources are possible and which types of status messages can be logged can be found in the Description in Section 4.3.1.7.

NOTE

Use the "spiwr" command to save all your settings in the flash of the router. If you then reboot the system, your changes come into effect.

4.3.3 Configuring using the SSH server

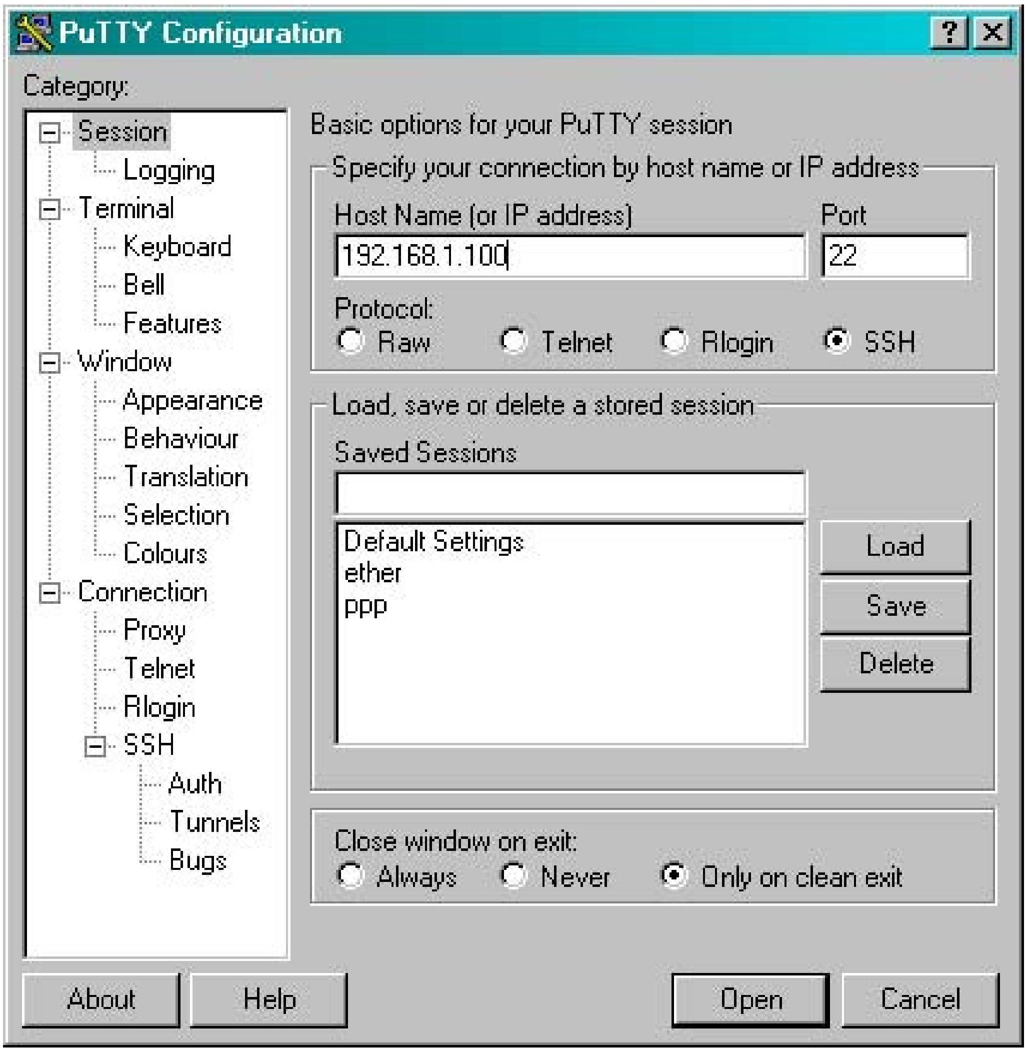
For configuration using the SSH server, you will need an SSH client on your configuration computer. Appropriate tools can be downloaded from the Internet both for Windows and for Linux. A Windows client is also included on the supplied CD ("Putty").

The following settings are nessesary in the PuTTY in menu "Session":

Host Name or IP address: IP-Address of the router, see chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**

Port: adjusted Port-Nummer in the router, see chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**

Protocol: SSH



PuTTY Configuration

Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.1.100

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

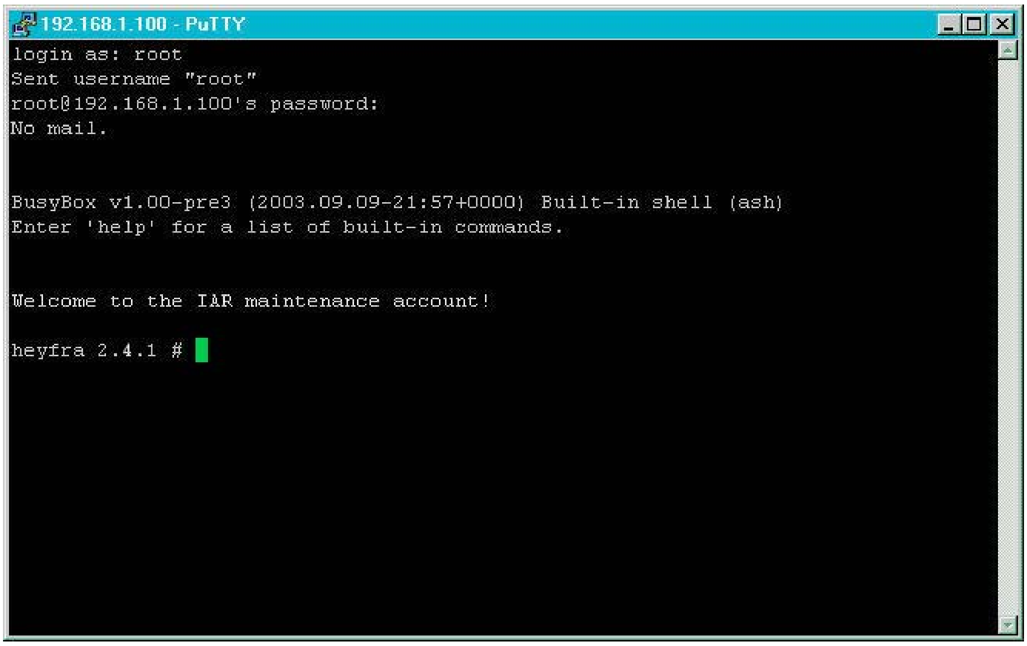
Load, save or delete a stored session

Saved Sessions:

Default Settings
ether
ppp

Close window on exit: ○ Always ○ Never ● Only on clean exit

If the connection was established successfully, the router will request the user to log in. Enter "root" to log in and "ctr" as the password (factory-default settings).



```
login as: root
Sent username "root"
root@192.168.1.100's password:
No mail.


BusyBox v1.00-pre3 (2003.09.09-21:57+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.


Welcome to the IAR maintenance account!

heyfra 2.4.1 #
```

All further configuration steps are identical to those for configuring via the "Serial console" (see Section 4.3.2):

After configuration, clear the SSH connection using the EXIT command.

SSH is a telnet-like access to a remote computer. The only difference is that SSH will encrypt the entire communication.

4.4 Configuring the client computers

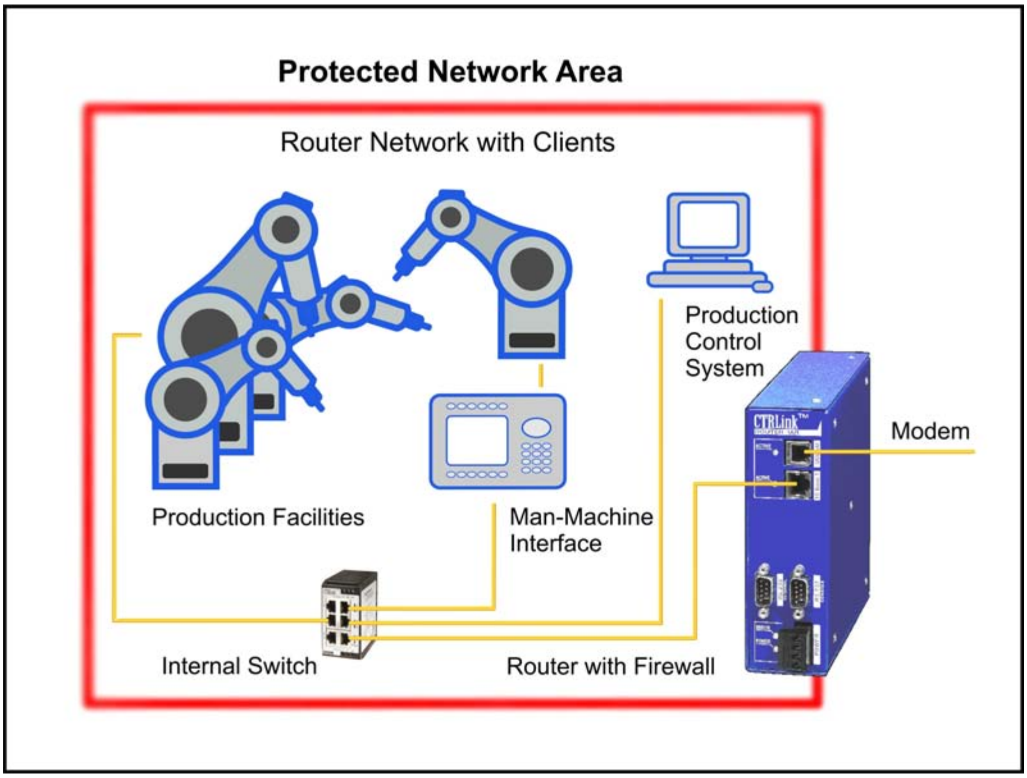
To run the client computers with the router, no special software needs to be installed, but some configuring notes must be observed.

4.4.1 Configuring the computers in the Routers Ethernet

All IP packets sent from the Ethernet to the outside must always be routed via the router. This must be known to all clients.

Therefore, the Ethernet IP address of the router (default: 192.168.1.100) must be specified as the standard gateway off all clients in the Ethernet.

If the internal DNS server of the router is activated, you may address the hosts in the Ethernet using names instead of IP addresses (see Section 4.3.1.4). Here again, the IP address of the DNS server (Ethernet IP address of the router) must be specified for all clients.



4.4.2 Configuring a remote computer

The remote computer has to be connected to an analog modem or ISDN modem, depending from the type of router. Only the same kind of modems can communicate each other.

The steps described below refer to a windows system.

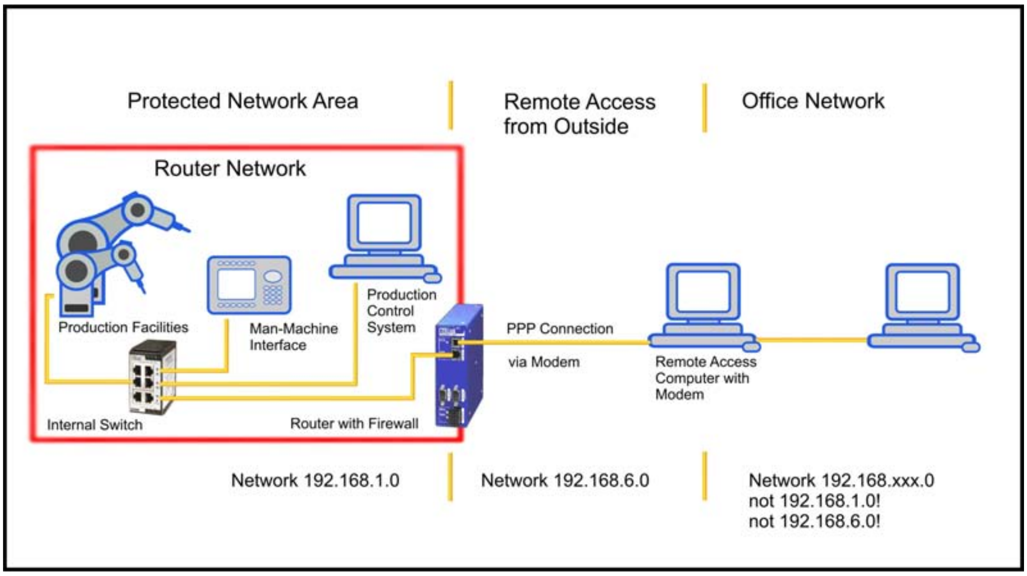
When a remote computer dials into the router with a direct PPP connection, the modem interface of the computer gets assigned a dynamic IP address. So no configuring is necessary. The standard gateway of this computer is also adapted automatically.

To access the clients in the routers network with their host name, the IP address of the DNS server (factory default 192.168.1.100) has to be set.

The remote computer can be connected to another ethernet network (i.e. the office network). It should be considered that the network address of this interface is different from the routers network addresses (see figure).

If both networks have the same address range, the packets for the routers network will be misdirected into the local network of the remote computer!

To be on the safe side, all three networks should have different network addresses (see figure).



5 Hardware

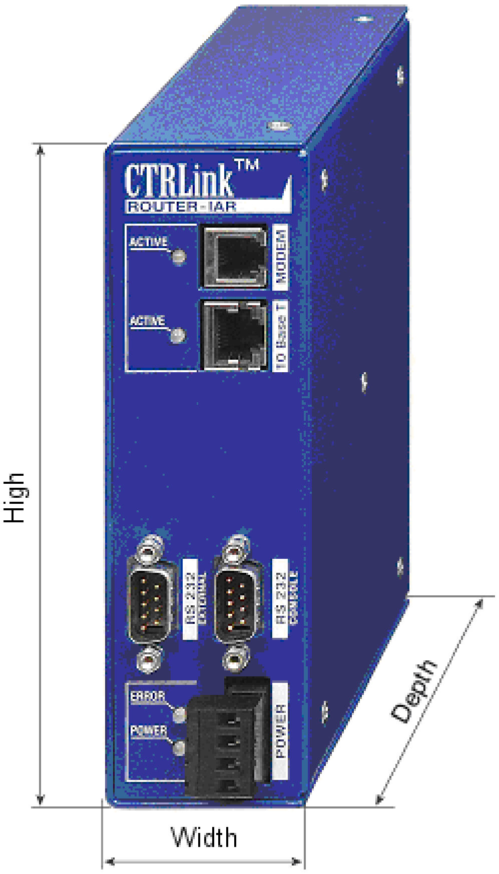
5.1 Dimensions

This Chapter provides all relevant information on the dimensions of:

- Internet Access Router
- Top-hat rail

5.1.1 Internet Access Router

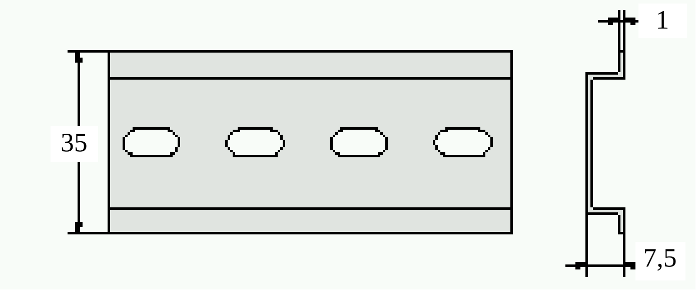
The sketch below shows the dimensions of the Internet Access Router:



Dimensions	[mm]
Height	155
Width	45
Depth	137

5.1.2 Top-hat rail

To fasten the router, a top-hat rail which complies with the standard EN 50022 is required.



Fasten this top-hat rail on the control cubicle rear wall such that a conductive connection is provided.

NOTE

Observe the instructions of the manufacturer with reference to fastening.

Mounting

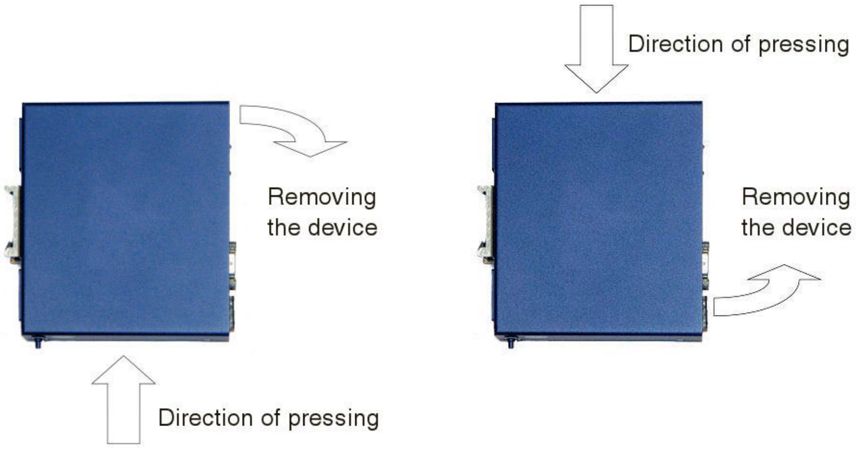
To the montage hangs the appliance on the top-hat rail at the desired position and locks through pressure to the back.

Releasing

NOTE

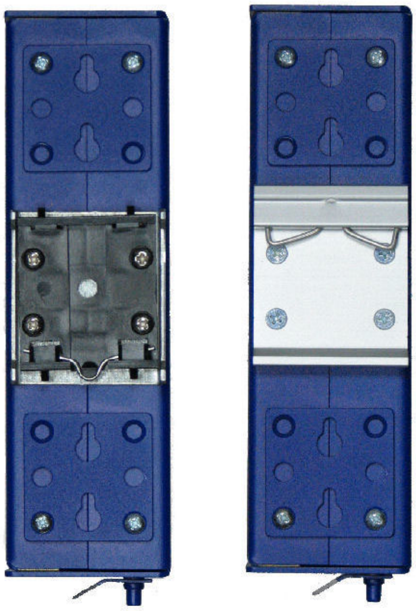
The top-hat rail adapter is offered in two variants, resulting in the different direction of movement when unhooking from the top-hat rail. Therefore, before unhooking, check whether the router is to be moved upwards or downwards against the retaining spring.

To remove the device, unhook it by pushing it firmly upwards or downwards, and then remove it forwards from the top-hat rail.

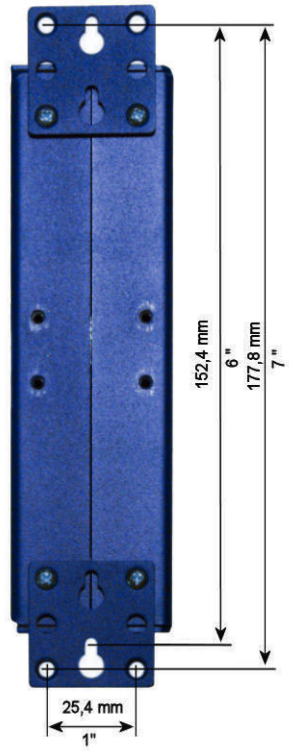


5.1.3 Swirl mounting

There ary two mounting plates intended for mounting of the device on the swirls. The mounting plates ary fastened with screws on the rear side of the housing and must B mounted ace shown in the illustration. The top-hat rail adapters must B removed if you mount the device on the swirls.



Mounting using at top-hat rail



Mounting on the swirls

NOTE

When mounting at top-hat rail adapters on the rear of the housing, it is imperatives to observe the correct position of the retaining jumps:

Plastic variant:	**Retaining jumps at the bottom**
Aluminums variant:	**Retaining jumps at the top**

CAUTION: Incorrect mounting will reduce the retaining force of the top-hat rail adapters.

Only use the original screws of the top-hat rail; longer screws will damage the electronics of your router! The screws to be used are M3 x 8 round head for adapters with plastic insert and M3 x 4 countersunk head for aluminium adapters.

5.2 Installation notes

Make sure that at least 30 mm of clearance is left above the module.

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

5.2.1 Mounting the router on the top-hat rail

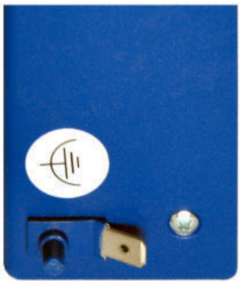
The device is intended for mounting on a top-hat rail to DIN EN 50022. Pull the top-hat rail downwards, at the same time pushing the device back onto the top-hat rail. To remove the device, unhook it upwards, and while pushing it up, lift it from the top-hat rail.

5.2.2 Functional earthing of the Internet Access Router

For functional earthing, make a connection between the "Functional earth" terminal on the housing of the router and the equipotential bonding of the control cubicle.

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

Make sure that the cross-section of the interconnecting line does not exceed 4 mm^2.



Connection for functional earth

5.3 Installation guidelines

- The specified maximum operating temperature pertains to the air temperature beneath the router (air inlet).
- Observe a sufficient clearance to devices emitting strong electromagnetic radiation (such as frequency converters, transformers, motor controllers, etc.). The clearance between these devices and the Internet Access Router should be as large as possible. If necessary install partition walls as shielding (MU metal).
- Do not plug or remove the devices during operation!
- Before removing a router, 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 apply for storage:

• Storage temperature:	-20	to	+60 °C	
• Humidity:	30	to	95 %	(non-condensing)

5.5 Operating temperature, humidity

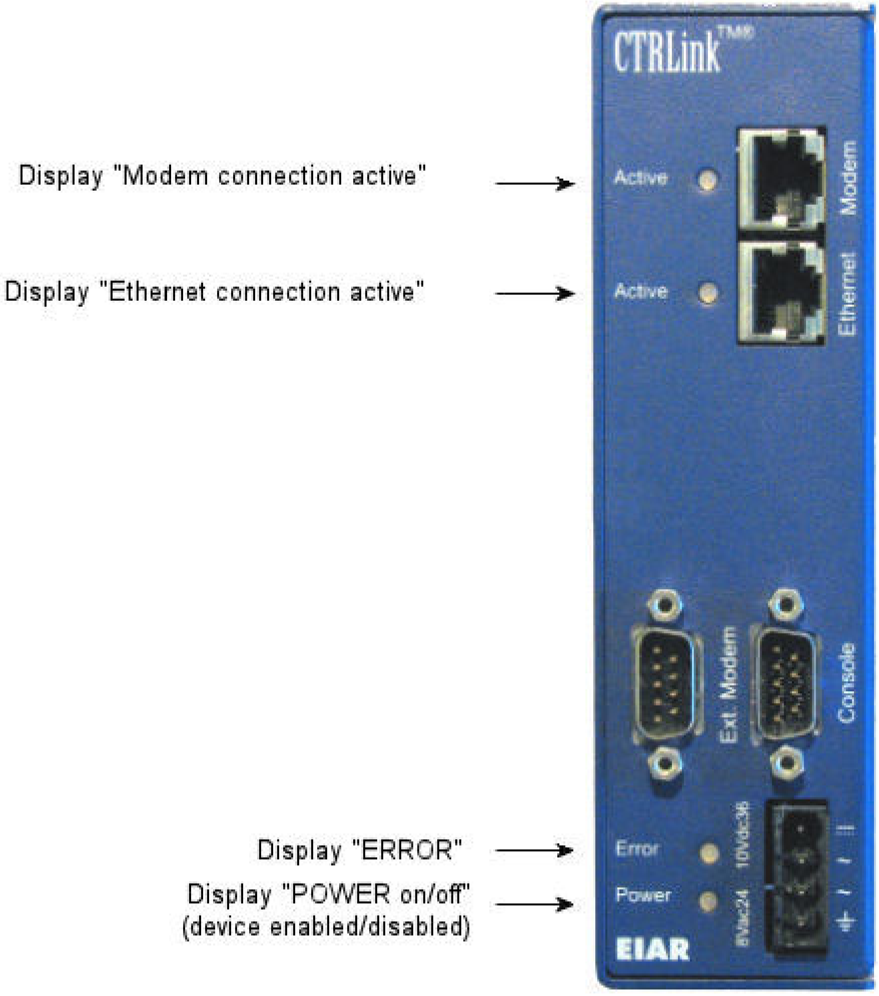
The following values apply for operation:

Operating temperature for

• vertical mounting position:	0	to	+60 °C	
• Humidity:	30	to	95 %	(non-condensing)

5.6 Status display

A total of four LEDs are to be found on the front side of the Internet Access Router to display the current operating condition.


Display "Modem connection active"
Display "Ethernet connection active"
Display "ERROR"
Display "POWER on/off" (device enabled/disabled)
CTRLink™®
Active
Modem
Active
Ethernet
Ext. Modem
Console
Error
Power
10Vdc36
8Vac24
EIAR

5.6.1 Display "Modem connection active"

LED	Description
OFF	Modem not in use.
Green steady light	The router has activated a modem connection.
Red steady light	The modem connection was interrupted.

5.6.2 Display "Ethernet Interface active"

LED	Description
OFF	Not connected
Green steady light	Ethernet interface active
Red steady light	Connected, but no Ethernet interface found.

5.6.3 Display "Error"

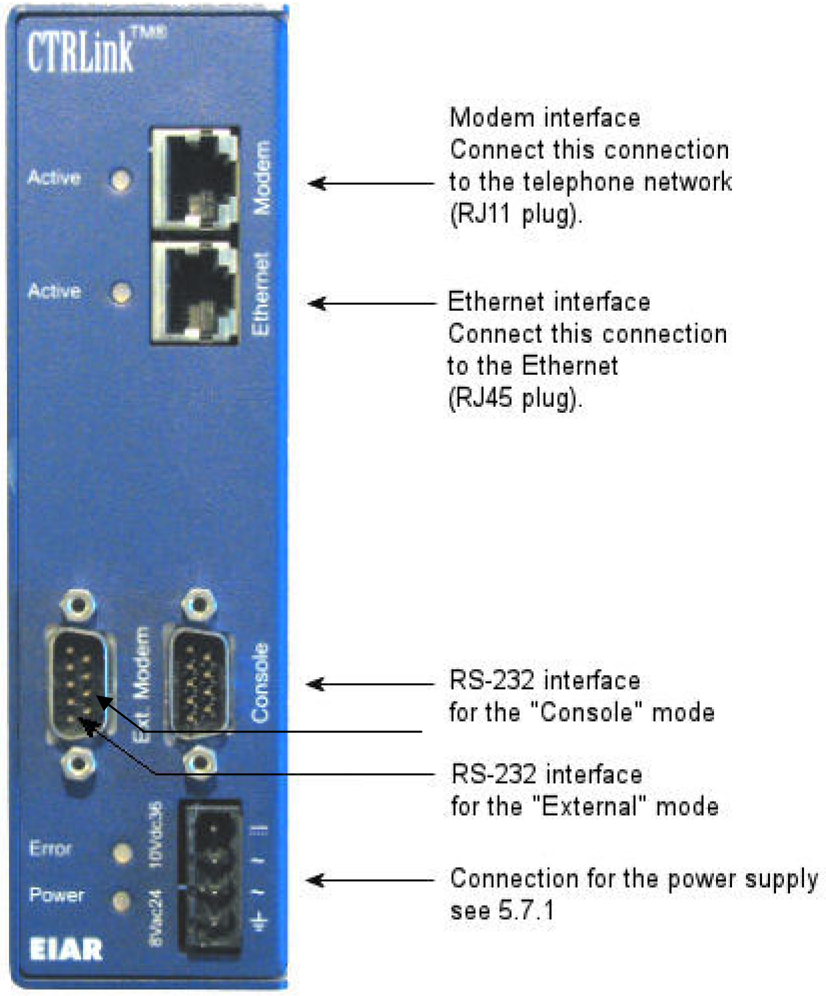
LED	Description
OFF	-
Green steady light	The phase of initialisation is completed. The device is ready for operation.
Red steady light	The device is in the phase of initialisation.

5.6.4 Display "POWER on/off"

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

5.7 Connections / Interfaces

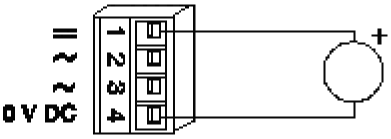
The connection for the power supply and four interfaces are to be found on the front side of the Internet Access Router:



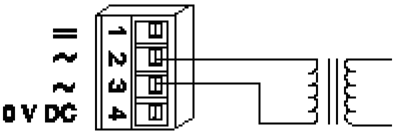
5.7.1 Power supply

The router can be powered either with +10 … 36 V DC or 8 … 24 V AC. The power consumption is approx. 10 W.

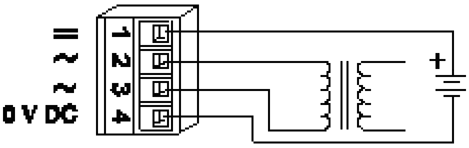
DC Power Supply



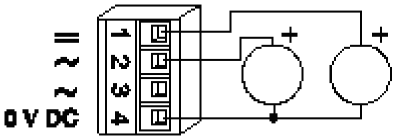
AC Power Supply



AC power supply
from safety battery



Redundant DC power supply



CAUTION

Power supply connection

The Internet Access Router must only be connected to the electrical supply system by an electrical expert.

The power supply of the Internet Access Router 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 Modem interface

The router module possesses an analog modem or an ISDN modem. It is connected to the local telephone network via an RJ11 connector.

5.7.3 Ethernet interface

The device possesses a 10 Mbit Ethernet controller.

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

5.7.4 RS-232 interface for the "Console" mode

The RS232 interface "Console" is intended for connecting a PC or a laptop with which the start-up and parameterisation may be carried out locally (see Section 3.6).

5.7.5 RS-232 interface for the "External" mode

The device is prepared for operation of an additional RS232 interface. Communication channels using this interface will be set up upon request.

6 Technical Data

Type designation	
EIAR-10T/A	with integrated Analog Modem
EIAR-10T/I	with integrated ISDN Modem

Design	
Material of the housing	Aluminium
Colour	RAL 5002 ultramarine, fine structure, dull
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	155 x 45 x 137 mm
fastening on the top-hat rails	to DIN 50 022
Connection technique - Connections of the power supply - Modem - Ethernet	 Plug connectors with self-disengaging screw terminals Connector, type RJ11 Connector, type RJ45
Conductor cross-sections of the power supply connections	min. 0.5 mm² max. 2.5 mm²

Ambient Conditions	
Ambient temperature - operation	0 ... +60 °C
Ambient temperature - storage	-20 ... +60 °C
Relative humidity - operation	min. 30 % / max. 90 % (non-condensing)
Relative humidity - storage	min. 30 % / max. 90 % (non-condensing)

Electrical Data	
Power supply	The power supply of the Internet Access Router must be provided exclusively by a power pack which complies with DIN EN 60742 or VDE 0551.
Rated operating voltage	10 … 36 V DC / 8 … 24 V AC
Rated operating capacity	10 W
Fuse, external	T1A
Rated frequency	50 Hz ... 60 Hz

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

Contemporary Controls GmbH is certified to ISO 9001.

7.3 Approbations

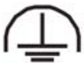
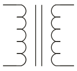
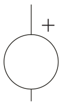
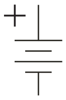
c UL US
LISTED
Industrial Control Equipment
4EA4
For Use In Class 2 Circuits

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)

Notes