Product Documentation

IP Router
Art. No.: IPR 200 REG

ALBRECHT JUNG GMBH & CO. KG
Volmestrasse 1
D-58579 Schalksmühle
GERMANY

Telephone: +49 2355 8060
Fax: +49 2355 806204
e-mail: kundencenter@jung.de
Internet: www.jung.de

1. Safety instructions

- Electrical equipment must only be installed and mounted by qualified electricians.
- When connecting KNX interfaces, detailed knowledge through KNX training is required.
- The manufacturer shall not be liable for any costs or damage incurred by the user or third party through the use this device, misuse or disturbances of the device or user equipment.
- Any unauthorized changes and modifications to the equipment will render the warranty null and void!
- The manufacturer shall not be liable for damage arising from improper use.

2. Installation and connection

Operation of the KNXnet/IP router requires:

- One of the following power supplies with at least 1 Watt power output:
  - Safety extra-low voltage of 20 to 30 VDC (direct voltage)
  - Safety extra-low voltage of 16 to 24 VAC (alternating voltage)
  - "Power over Ethernet" (IEEE 802.3af), Class 1
- A 10/100 Mbit compatible Ethernet connection
- A KNX/EIB bus connection

3. Commissioning

3.1 Description of functions

The interface has the following functionalities:

- LED display for communication, Ethernet communication and programming mode
- Configuration via ETS
- Max. 5 connections to IP terminal devices, e.g. for simultaneous visualisation and configuration
- Supply from network line – Power-over-Ethernet to IEEE 802.3af –, through separate voltage supply or the auxiliary voltage output of the KNX voltage supply.
- Electrical isolation between KNX and IP network

3.2 Configuration

In the ETS project, an appropriate device must be created and configured.

- Activate programming mode: Press programming button.
- The programming LED lights up.
- Program a physical address with the aid of the ETS.
- The programming LED goes out.
- Label the device with the physical address.
- Load application data into the device with the aid of the ETS.

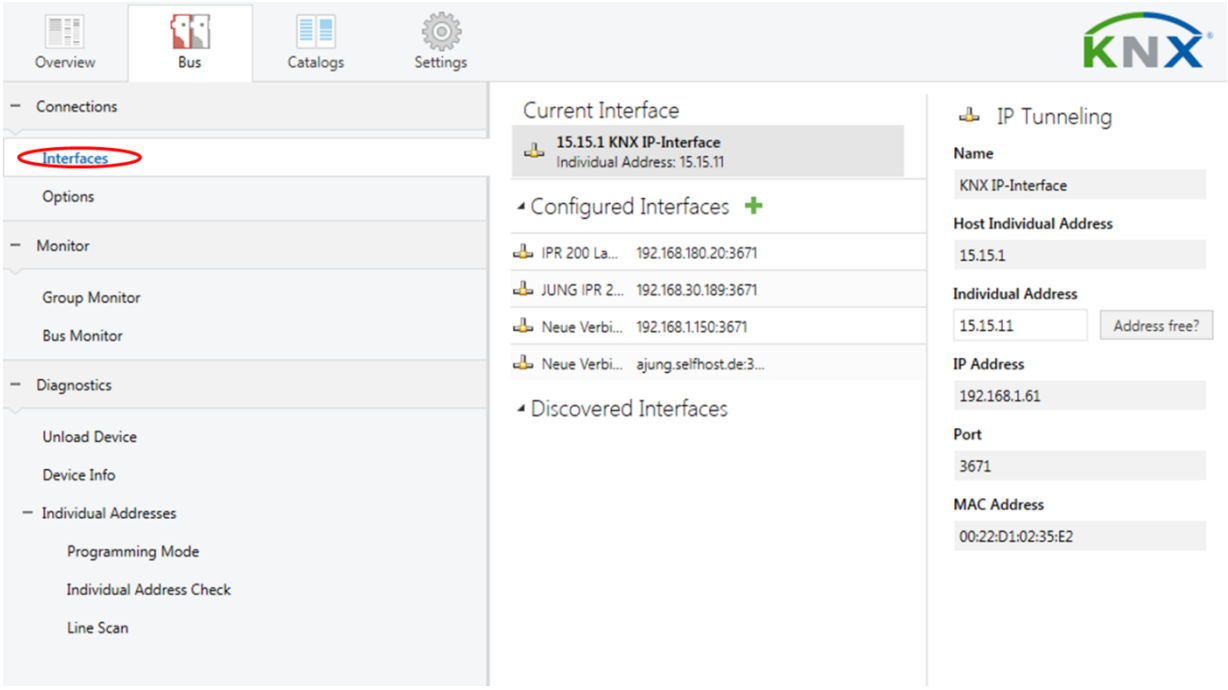
3.3 Physical address of the data interface

A direct connection to the KNX can be established from a PC or other data processing equipment (e.g. visualisation units) in the network via an IP data network and the KNX IP interfaces. This allows access to the bus from any point in the IP data network.

The ETS3 (from version 3.0c) enables the configuration of KNX installations via the existing IP data network and uses the IP interface such as a conventional serial RS232 or USB data interfaces for communication with the bus. This also includes the downloading of bus devices or the group bus monitor function (no support of the bus monitor mode).

For communication via KNXnet/IP Tunnelling and / or ObjectServer, the device must use a virtual physical address for each connection. These additional physical addresses must not be identical with the physical address of the device and must not be used by any other bus device either. In the ETS, the virtual physical addresses should be allocated by dummy devices. The additional addresses for the KNXnet/IP Tunnelling can either be assigned manually in the ETS by the communication settings or automatically by the device itself. To configure the communication interface (physical interface of the first tunnel connection) in the ETS 5, the following steps must be carried out.

In ETS 5, on the ***Bus*** tab, open the ***Connections -> Interfaces*** subitem

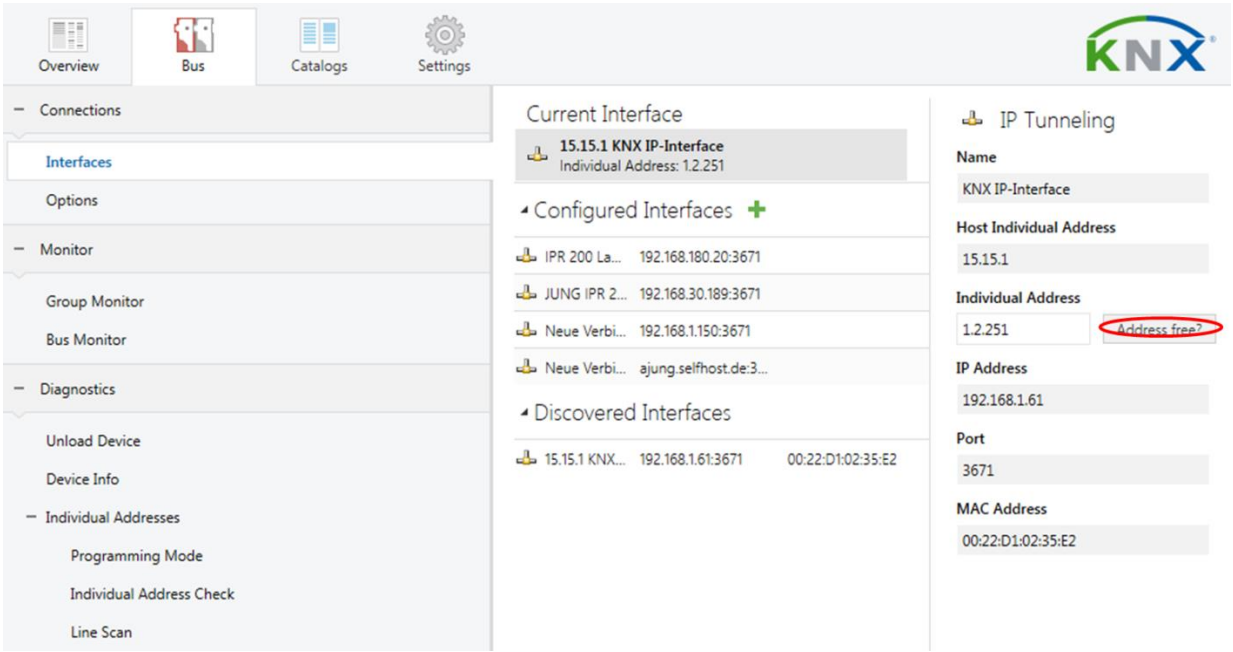


If the IP interface is online in the same network as the commissioning PC, this will already be shown here, otherwise it can be created using the "New" button.

An individual name for the interface, IP address, port and NAT mode can be set on the right-hand side of the menu.
An activated NAT mode in conjunction with the selected port (port 3671 is registered for this application worldwide by the KNXA, but can be set differently on an individual basis as well) enables remote access to the connected KNX system via the WAN (Internet).

This functionality should NOT be used without extensive network knowledge! For further information, please contact your network administrator or security administrator!

The physical address 15.15.1 is set by default.
It is absolutely essential to change this to an address that corresponds to the topological allocation of the IP data interface in the KNX installation.
Example: If the interface has the physical address 1.2.5, then the address for the function **must** read as data interface 1.2.xxx. Any address that has not yet been used must be selected from the value range xxx. For safety reasons, a scan should be initiated using the "Address free?" button in order to safeguard this, too.



To ensure correct documentation of the project, it is advisable to block the selected addresses in the project by using a virtual device. We recommend the dummy application for this.

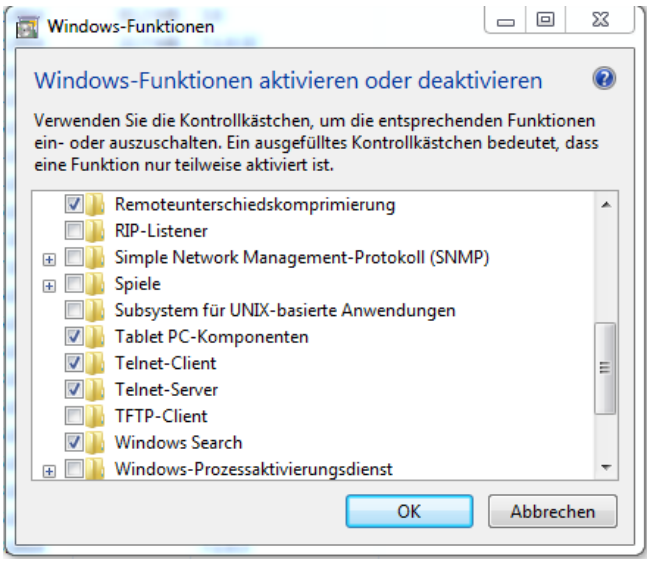
The IP interface can establish up to 5 such tunnel connections simultaneously and also needs 5 physical addresses for this. In the aforementioned process, only the address of the 1st connection can be configured. The device assigns addresses from 15.15.11 to 15.15.14 to the following 4 connections by default. These must always be adapted to the actual topological allocation of the device. This is implemented with the Telnet function.

If the physical address of the device is unloaded from ETS side, the device restarts by default with the physical address 15.15.255.

These 4 tunnel addresses can be set both via **TELNET** (1) and using the **software tool** (2).

4. Telnet server

Telnet is a common network protocol based on a TCP connection between a Telnet server (the KNX-IP router in this case) and a client (the commissioning PC in this case). For communication to be possible, it is necessary for the KNX-IP router to be administered in the network and to be reached by the commissioning PC via IP. Settings can then be made on the KNX-IP router (particularly status information) via Telnet as well as status information viewed without there being a connection to the ETS.
Telnet can either be activated as a function of the Windows operating system or used via a third party program, e.g. PuTTY.

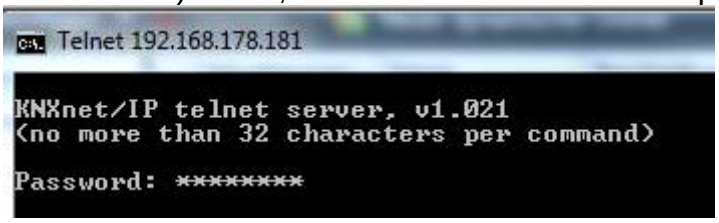


In Windows, Telnet is executed via command line commands.

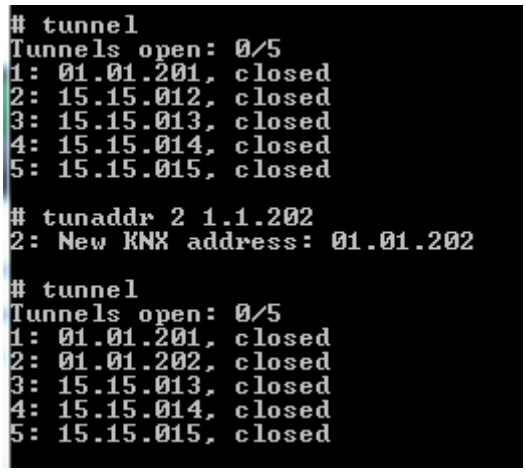
- The fastest way to start the Windows command line is to press [Windows]+[R], type in the command "cmd" and confirm by pressing "ENTER“.
- This is also possible via the start menu: Here, click on "All programs - Accessories - Command prompt", enter "cmd" and confirm with "ENTER"

In the window that then opens, type in **telnet [space][IP address of the IP router].**

- In Windows 7, it is also sufficient to enter Telnet in the input line (Programs/Search files). Then, enter the IP address in the opened window.



After entering the password (default: knxnetip), you can use the following commands and also change the KNX address of a tunnel among other things, e.g. **tunaddr 2 1.1.202** assigns the physical address 1.1.202 to the second tunnel connection.



Example:
The "tunaddr" command displays the physical address of the tunnel connections
The "tunaddr 2 1.1.202" command sets the second tunnel connection to 1.1.202
The "tunaddr" command displays the physical addresses after the change

4.1 Telnet commands

ifconfig	Displays network parameters
	Sys multicast: Multicastadresse for system-telegrams
	RT multicast: Multicastadresse for routing-telegrams
	`# ifconfig`
	`IP.............: 192.168.1.31`
	`Subnet mask...: 255.255.255.0`
	`Gateway.......: 192.168.1.1`
	`NTP server....: 192.168.1.1`
	`Sys multicast.: 224.0.23.12`
	`RT multicast..: 224.0.23.12`
	`Hardware addr.: 00:22:d1:02:0b:69`

tpconfig	Displays KNX parameters and serial number
	`# tpconfig`
	`KNX bus state.: up`
	`KNX address...: 15.15.000`
	`Serial number.: 00-04-00-00-0b-6a`
	KNX bus state: KNX bus detected (up) or not detected (down)
	KNX address: physical address of the device
	Serial number: Serial number of the device

lcconfig	KNXnet / IP displays routing settings:
	Telegrams to the following addresses:
	GA 0-13: group addresses of main groups 0 to 13
	GA 14-15: group addresses of main groups 14 to 15
	Ph. addr.: Physical addresses
	Broadcast: All devices
	Can be treated as follows:
	filter: forwarding by the filtertray
	route: always forward
	block: never forward
	Also displayed:
	PW fail. Mon.: Send telegram when KNX power supply fails
	`# lcconfig`
	`Coupler type.: line coupler`
	`IP -> KNX:`
	`GA  0-13......: filter`
	`GA 14-15......: route`
	`Ph. add.......: filter`
	`Broadcast.....: route`
	`KNX -> IP:`
	`GA  0-13......: filter`
	`GA 14-15......: route`
	`Ph. add.......: filter`
	`Broadcast.....: route`
	`PW fail. mon..: enabled`

stats	Shows statistics on telegram processing:
	`# stats`
	`uptime: 0:12`
	`KNX communication statistics:`
	`TX to IP (all): 811 (ca. 67 t/m)`
	`TX to KNX: 24 (ca. 2 t/m)`
	`RX from KNX: 228 (ca. 19 t/m)`
	`Overflow to IP: 3`
	`Overflow to KNX: 0`
	`TX tunnel re-req: 0`
	uptime: Runtime oft he Router
	TX to IP (all): Number of all transmitted IP telegrams
	TX to KNX: Number of all KNX telegrams sent to the bus
	RX from KNX: Number of all KNX telegrams received by the bus
	Overflow to IP: number of telegrams lost to IP, e.g. Because network is not was available
	Overflow to KNX: number of telegrams lost in the KNX direction, e.g. Because KNX bus was not available or persistent overload
	TX tunnel re-req: number of repeated KNXnet / IP tunneling telegrams, as an ACK telegram from the opponent

free	Display available disk space
	`# free help`
	`Free memory: 366 Bytes`
	`TP transmit buffer: 0 %`
	`TP transmit buffer max: 77 %`

tunnel [1..5]	Shows active tunnel connections (without argument), detailed information on the specified tunnel connection (Argument 1..5): Tunnel X: Shows whether tunnel is open and displays the CCID (identification number) of the tunnel KNX address: Tunnel address HPAI control: IP and port of the control end point of the remote control HPAI data: IP and port of the data terminal of the remote terminal Connect. Type: Connection type Tunnel or management connection TX tun req: Number of sent tunnel requests TX tun re-req: number of repeated tunnel requests due to remaining ACK RX tun req: Number of received tunnel requests RX tun re-req (identified): Number of received, repeated tunnel requests that could be detected by the sequence counter RX tun req (wrong seq.): Number of received tunnel requests with incorrect Sequence Counter

tunaddr 1..5 address
tunaddr reset
	Edit KNX address of a tunnel, e.g. Tunaddr 1 15.15.240
	Change KNX address of all tunnels, eg Tunaddr setall 15.15.240
	Reset the KNX addresses of all tunnels to the factory setting (Tunaddr reset)
	`# tunaddr setall 0.1.240`
	`Setting all tunnel KNX addresses...`
	`1: New KNX address: 00.01.240`
	`2: New KNX address: 00.01.241`
	`3: New KNX address: 00.01.242`
	`4: New KNX address: 00.01.243`
	`5: New KNX address: 00.01.244`
	`done`
	
	`# tunaddr reset`
	`Resetting all tunnel KNX addresses...`

tunmode	Read tunnel mode (without parameters) or set tunnel mode (tp or tpblk);
	tunmode tpblock:
	IP=> Forward KNX to TP with same Backbone Line Frame
	KNX=> Forward IP to TP with same Sub Line Frame
	`# tunmode help`
	`Usage: tunmode [std/tpblk]`

date	Displays the time and date (in UTC)
	`# date`
	`10:47:04 22.09.2017 (UTC)`

sntp [query I server IP]	Send request to the NTP server (sntp query) or IP of the NTP server (sntp server 192.168.1.1)
	`# sntp query`
	`Sending SNTP query to 192.168.1.1`
	
	`# sntp server 1.2.3.4`
	`NTP server...: 1.2.3.4`

lock [0 I 1]	Lock-Status query (without parameters) or the Lock-Status chanigng (0 = off, 1 = on)
	
	A router can prevent the forwarding of physically addressed telegrams by filtering, i. reprogramming devices across a line is not possible. This is of interest when using outside lines.
	However, e.g. a KNX-USB interface can be connected to an external line directly to the bus, and the router can be reprogrammed in the outside line itself so that it relays the physically addressed telegrams.
	With this Telnet function this can be prevented. If you set the telnet "lock" to 1, the router can no longer be programmed via the KNX line and appropriate activation of the routing via KNX TP is no longer possible.
	`# lock`
	`Lock Programming via TP 0 (off)`
	
	`# lock 1`
	`Lock Programming via TP 1 (on)`
	
	`# lock 0`
	`Lock Programming via TP 0 (off)`

routingcounter	Query or change routing counter handling (default / legacy behavior before 2018). This setting is identical to Activation Routing Algorithm <2018.
	`# routingcounter help`
	`Usage: routingcounter [standard/legacy]`

progmode [0 I 1]	Programming or changing the programming mode (0 = off, 1 = on)
	`# progmode`
	`Programming mode: off`
	
	`# progmode 1`
	`Programming mode: on`
	
	`# progmode 0`
	`Programming mode: off`

passwd oldpw newpw	Changes the current Telnet password
	`# passwd knxnetip 0000`
	`New password set.`

passwd oldpw	Deletes the current password
	`# passwd knxnetip`
	`Password deleted.`

passwd newpw	A new password, if none is currently set
	`# passwd knxnetip`
	`New password set.`

version	Check firmware version
	`# version help`
	`Firmware version: 1.049`

mask	Check mask version
	`# mask help`
	`Mask version: 0x091a`

factory_reset	Restore factory settings and restart `# factory_reset`
reboot	Rebooting `# reboot`
logout	Telnet-Session end. `# logout`

5. Software tool

The document describes the function of the software for simplified communication and configuration of the IP router (IPR200REG) and the IP interface (IPS200REG). You can find the software tool in the download area of our website.

5.1 System requirements

- PC with Windows operating system

  The following systems have been tested:
  - Microsoft Windows XP, Service Pack 3, 32 Bit
  - Microsoft Windows 7, Service Pack 1, 32 Bit
  - Microsoft Windows 7, Service Pack 1, 64 Bit
  - Microsoft Windows 8.1, 64 Bit
  - Microsoft Windows 10 , 64 Bit

- KNX-IP router / KNX-IP interface

5.2 Installation

- Unpack the downloaded file
- Start windows.exe

5.3 Functions

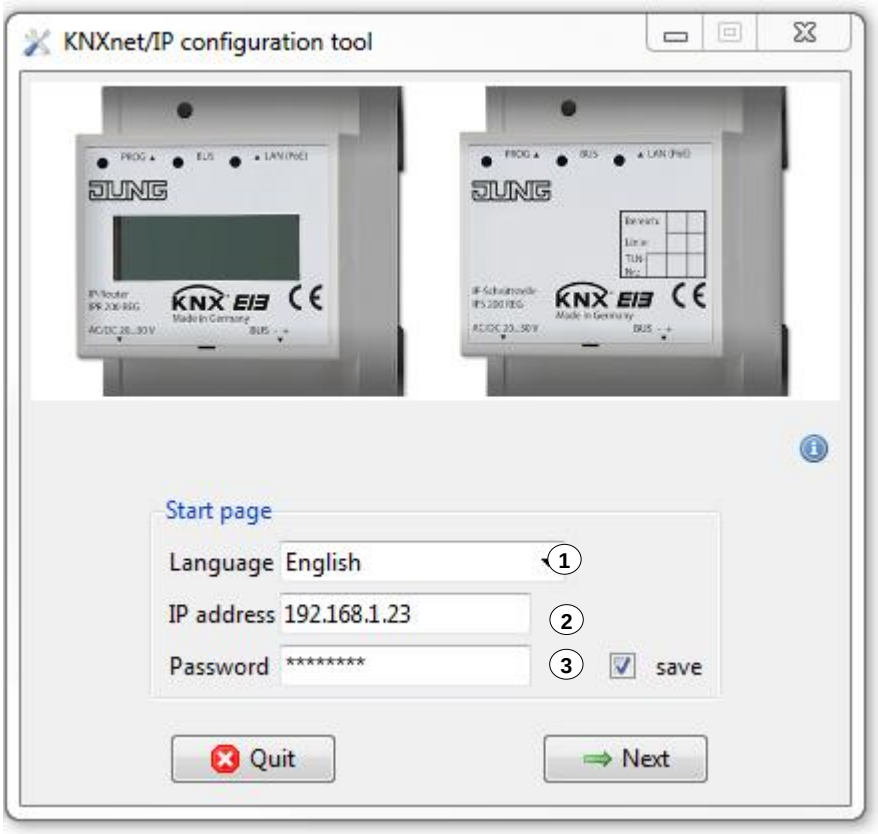
The software simplifies the configuration of the JUNG KNX-IP interfaces (IPR200REG / IPS200REG) and makes detailed information available if there is an error.

5.4 Access to the KNX IP interface

An authorised connection is essential for changing and reading out the device properties.
The following languages are available in the selection menu (1):

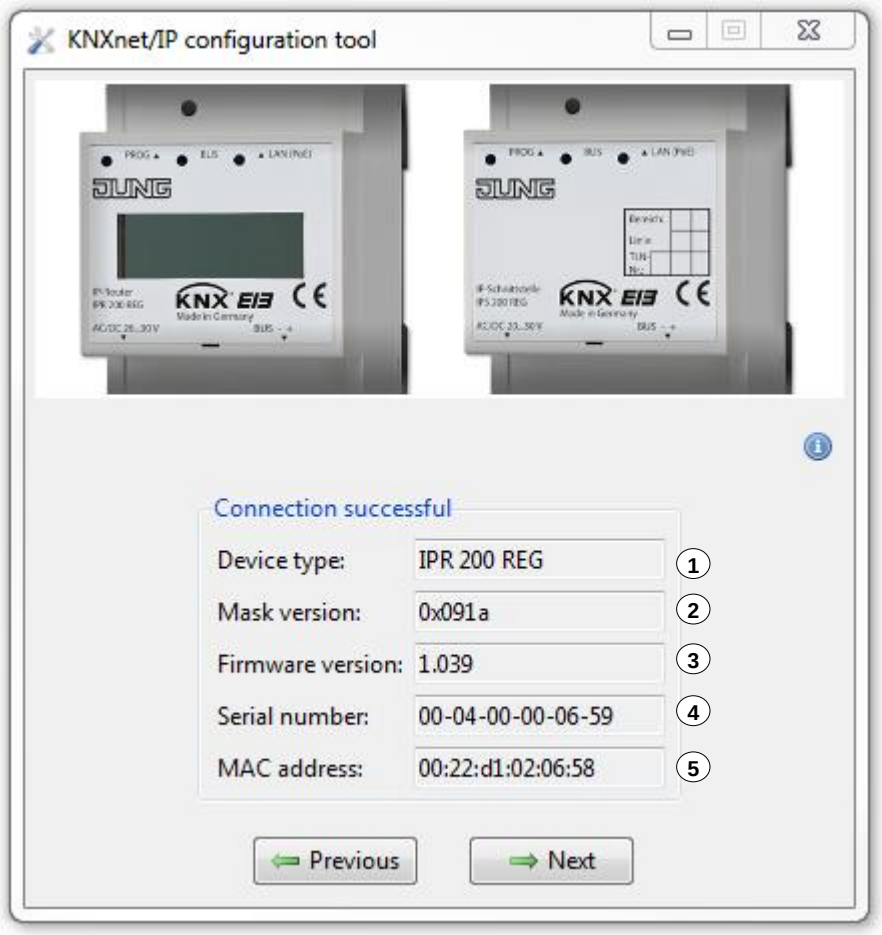
- German
- English

The software must be informed of the current IP address of the KNX-IP interfaces. The simplest way to do this is to determine them from the ETS configuration of the device (static IP address active) or from the network router (DHCP active). Enter the determined IP address of the KNX-IP interfaces in the "IP address" field (2).
Each KNX-IP address is protected with a password against unauthorized access. In the as-delivered state, the interfaces are protected with the password "**knxnetip**".
The optional storage of a password (3) means that reentering the password is not necessary.



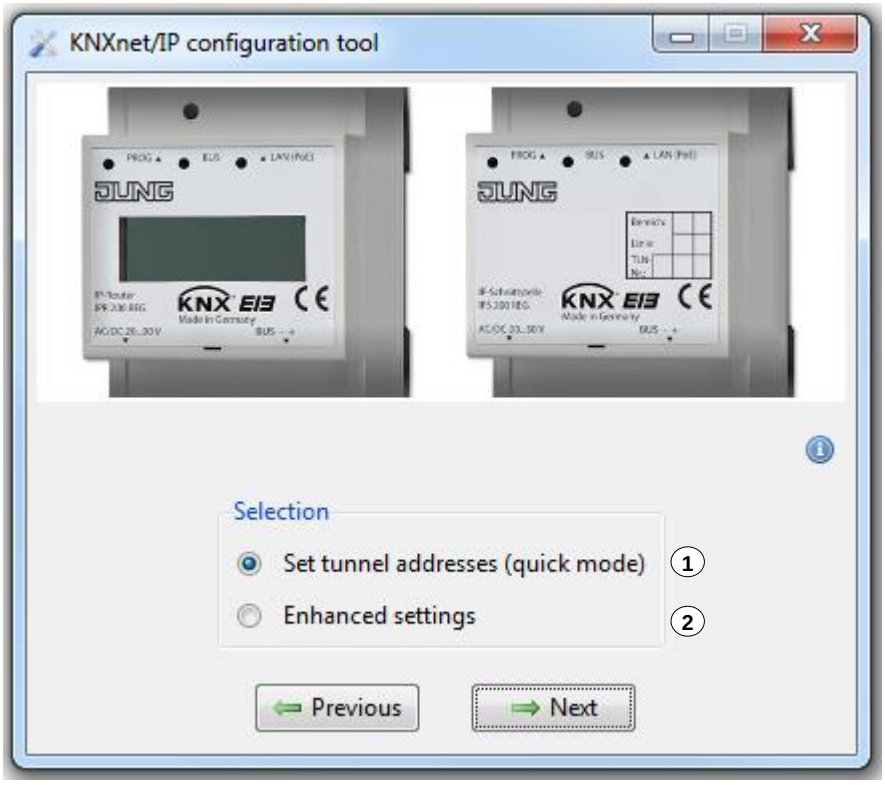
5.5 Device properties

After a successful connection, the device properties are initially listed. These contain basic information such as the device type (1), serial number (4) and the MAC address (5), but also variable properties such as the mask version (2) and firmware version (3).



5.6 Configuration options

Two configuration options are then available.

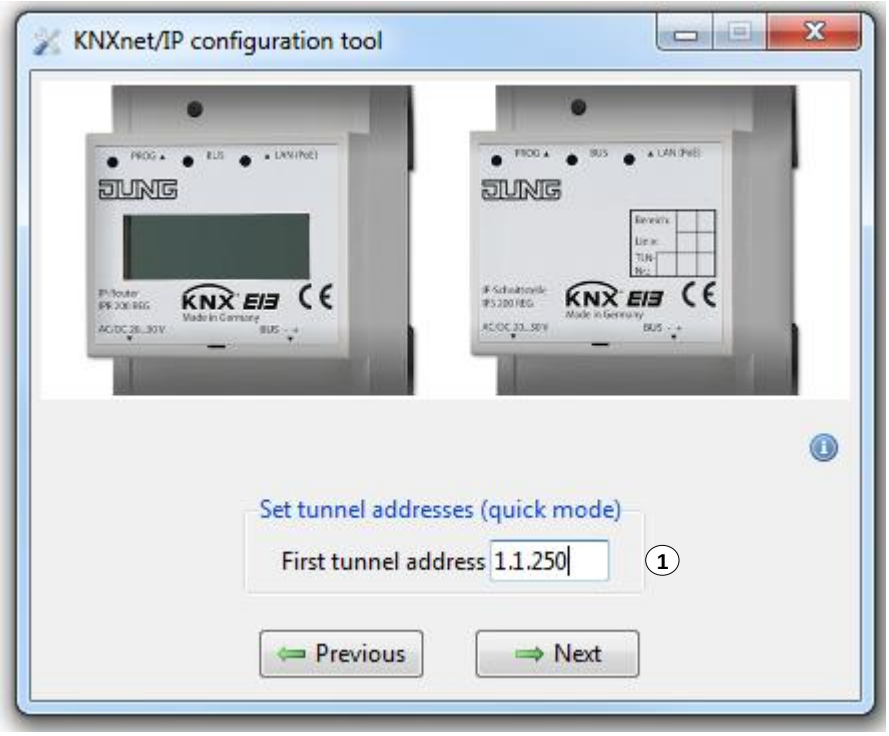


5.7 Quick tunnel address setting

In "Set tunnel addresses (quick mode)", the available tunnel addresses are addressed in consecutive order after entry of the first free tunnel address (1). For both devices (IPR200REG / IPS200REG), 5 tunnel addresses are available from firmware version ***1.0.39***.

Caution!

The software does **not** check for previously set tunnel addresses. 5 consecutive tunnel addresses (e.g. 1.1.250 … 1.1.254) must be previously unset. If there is an error, two devices possess an identical physical address.



5.8 Advanced settings

In the "Advanced settings", it is possible to remove the current password (1). On reconnection, leave the password field empty.
In addition, a new password can be entered or the existing one replaced (2). To prevent errors, enter the password again.
The "Query Support Data" button (3) collected detailed information about your device. This information allows a faster and more efficient error analysis. Collected information are stored in a text file incl. timestamp in the root directory of the software (e.g. C:\Users\XXX\Projekte\2016\KNXnetIP).
The "Restore Factory Settings" button (4) restores the default settings of the device. The software then restarts from the home page.