

Using of the application program

Product family: System device
Product type: IP-Router
Manufacturer: IPAS GmbH

Name: 3622-IPRouter Pro_V1.1.0
Order No: 3622-141-18

Content:

FUNCTION	1
GENERAL	1
KNX SECURE	1
KNX IP SECURE FOR THE ROUTER FUNCTION	1
KNX IP SECURE FOR THE INTERFACE FUNCTION.....	1
KNX DATA SECURE FOR THE DEVICE	2
KNX DATA SECURE FOR GROUP TELEGRAMS	2
COUPLER FUNCTION (KNXNET/IP ROUTING)	2
KNX INTERFACE (KNXNET/IP TUNNELING)	3
INSTALLATION AND COMMISSIONING	4
MOUNTING	4
KNX PROGRAMMING MODE	4
MANUAL OPERATION AND STATUS DISPLAY	4
RESET TO FACTORY SETTINGS	5
ETS CONFIGURATION	5
INTERFACE SETTINGS	5
APPLICATION	5
PROJECT PASSWORD	6
DEVICE CERTIFICATE.....	6
PROPERTIES DIALOGUE	6
<i>Tunnel connections.....</i>	<i>6</i>
<i>Properties.....</i>	<i>6</i>
<i>IP.....</i>	<i>7</i>
<i>Commissioning password and authentication code.....</i>	<i>8</i>
ETS PARAMETER DIALOGUE	8
GENERAL SETTINGS.....	8
PROG. MODE ON FRONT PANEL.....	8
MANUAL CONTROL ON THE UNIT.....	8
ROUTING (KNX -> IP)	8
ROUTING (IP -> KNX)	9
PROGRAMMING	9
VIA THE KNX BUS	9
VIA KNXNET/IP TUNNELING	9
VIA KNXNET/IP ROUTING	10
VIA DIRECT IP CONNECTION.....	10

Function

General

The compact ComBridge IP Router Pro enables the forwarding of telegrams between different lines via a LAN (IP) as a fast backbone. The device also serves as a programming interface between a PC and the KNX bus (e.g. for ETS programming).

The device supports KNX Secure. The option can be activated in the ETS. As a secure router, the device enables the coupling of non-secure communication on a KNX TP line with a secure IP backbone.

KNX Secure also prevents unauthorised access to the system with the interface function (tunneling).

The IP address can be assigned via DHCP or through the ETS configuration. The device operates according to the KNXnet/IP specification using Core, Device Management, Tunneling and Routing.

The ComBridge IP Router Pro has an extended filter table for main group 0.31 and can buffer up to 150 telegrams. Power is supplied via the KNX bus.

KNX Secure

KNX Secure has been added to the KNX standard to protect KNX installations from unauthorised access. KNX Secure reliably prevents both eavesdropping on communication and manipulation of the installation.

The specification for KNX Secure distinguishes between KNX IP Secure and KNX Data Secure. KNX IP Secure protects the communication via IP while on KNX TP the communication remains unencrypted. Thus, KNX IP Secure can also be used in existing KNX installations and with non-secure KNX TP devices.

KNX Data Secure describes the encryption on telegram level. This means that the telegrams on the twisted pair bus are also encrypted.

KNX IP Secure for the router function

The coupling of individual KNX TP lines via IP is referred to as KNX IP routing. Communication between all connected KNX IP routers takes place via UDP multicast.

With KNX IP Secure, routing communication is encrypted. This means that only IP devices that know the key can decrypt the communication and send valid telegrams. A time stamp in the routing telegram ensures that no previously recorded telegrams can be imported. This prevents the so-called replay attack.

The key for routing communication is reassigned by the ETS for each installation. If KNX IP Secure is used for routing, all connected KNX IP devices must support Secure and be configured accordingly.

KNX IP Secure for the interface function

When using a KNX IP router as an interface to the bus, access to the installation is possible without Secure for all devices that have access to the IP network. With KNX Secure, a password is required. A secure connection is already established for the transmission of the password. All communication via IP is encrypted and secured.

KNX Data Secure for the device

The **CB IPR Pro** Router also supports KNX Data Secure to protect the device from unauthorised access from the KNX bus. If the KNX IP router is programmed via the KNX bus, this is done with encrypted telegrams.

i *Encrypted telegrams are longer than the previously used unencrypted ones. Therefore, for secure programming via the bus, it is necessary that the interface used (e.g. USB) and any intermediate line couplers support the so-called KNX long frames.*

KNX Data Secure for group telegrams

Telegrams from the bus that do not address the KNX IP router as a device are forwarded or blocked according to the filter settings (parameters and filter table). It does not matter whether the telegrams are unencrypted or encrypted. Forwarding is done exclusively on the basis of the destination address. The secure properties are checked by the respective recipient.

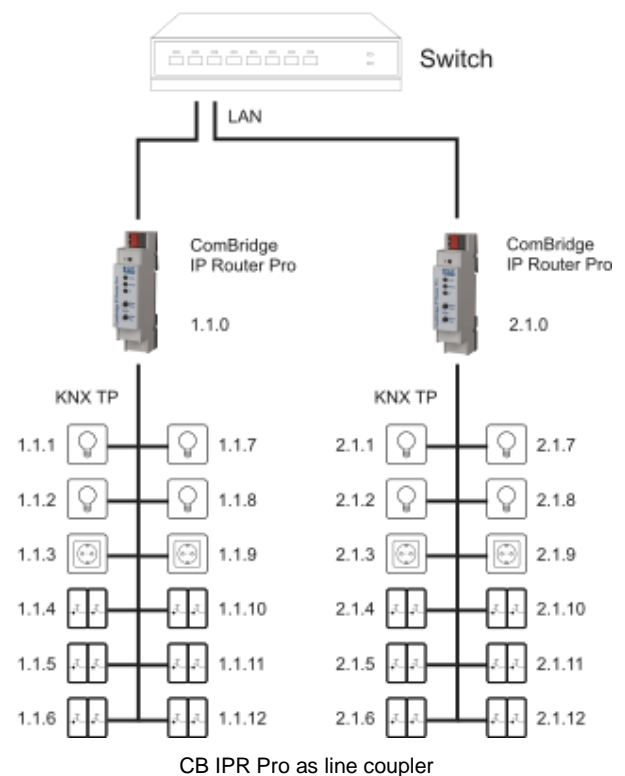
KNX Data Secure and KNX IP Secure can be used in parallel. In this case, for example, a KNX sensor would send a group telegram encrypted with KNX Data Secure to the bus. When forwarding via KNX IP with KNX IP Secure, the encrypted telegram would be encrypted again just like unencrypted ones. All devices on the KNX IP level that support KNX IP Secure can decode the IP encryption, but not the Data Secure. Thus, the telegram from the other KNX IP routers is transmitted again with KNX Data Secure to the destination line(s). Only devices that know the key used for Data Secure can interpret the telegram.

Coupler function (KNXnet/IP Routing)

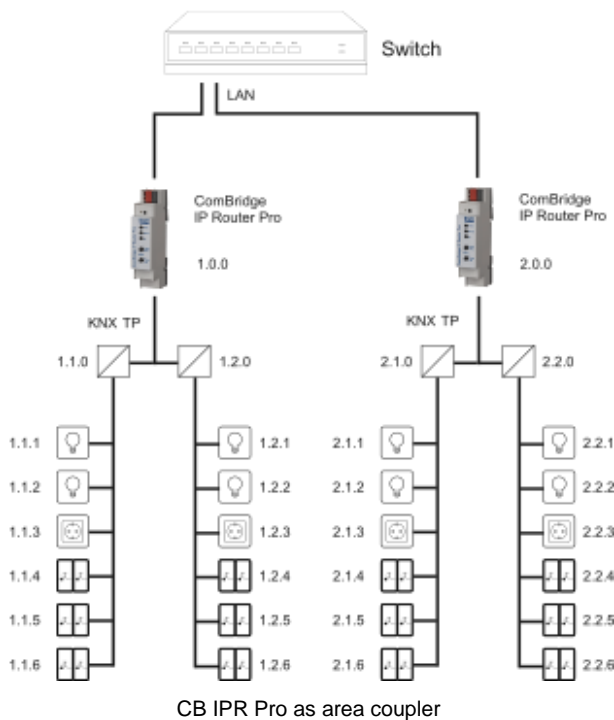
The **CB IPR Pro** can work as a line or area coupler. In both cases, the LAN (IP) is used as the backbone.

The following table shows the possible uses of the router in comparison to the classic topology:

	Classical Topology (without IP)	IP coupling of areas (IP area coupler)	IP coupling of lines (IP line coupler)
Area (Backbone)	TP	IP	IP
Coupling	KNX Line Coupler (max. 15 St.)	KNX IP Router (max. 15 St.)	Directly via LAN Switch
Main line	TP	TP	IP
Coupling	KNX Line Coupler (max. 15x15 St.)	KNX Line Coupler (max. 15x15 St.)	KNX IP Router (max. 225 St.)
Line	TP	TP	TP

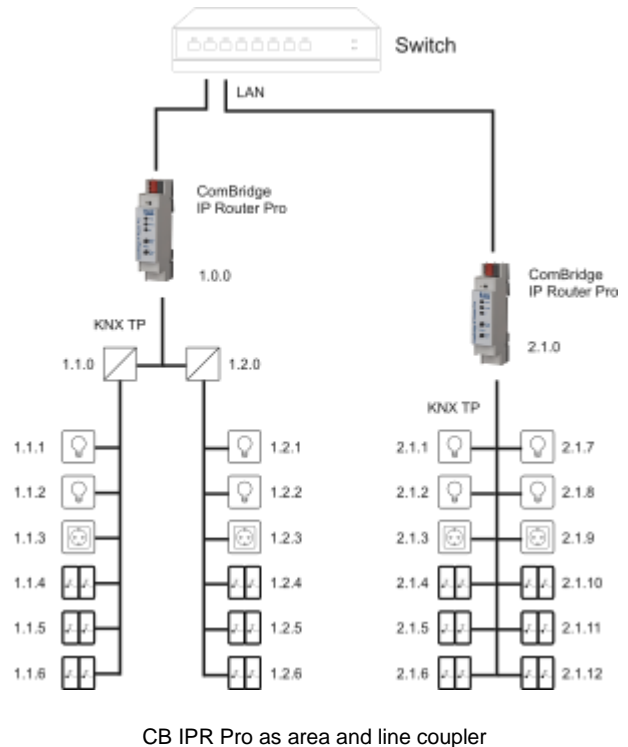


The assignment of the physical address of the CB IPR Pro decides whether the device works as a line or as a range coupler. If the physical address corresponds to the form x.y.0 (x, y: 1..15), the router functions as a line coupler. If the physical address is in the form x.0.0 (x: 1..15), it is a range coupler.



i If the CB IPR Pro is used as a range coupler (x.0.0), no KNX IP router may be located topologically below it. If, for example, a KNX IP router has the physical address 1.0.0, there must be no KNX IP router with the address 1.1.0.

i If the CB IPR Pro is used as a line coupler (x.y.0), no KNX IP router may be located topologically above it. If, for example, a KNX IP router has the physical address 1.1.0, there must be no KNX IP router with the address 1.0.0.



The KNX IP Router has a filter table and thus contributes to reducing the bus load. The filter table (8kB) supports the extended group address range (main groups 0..31) and is automatically generated by the ETS.

Due to the difference in speed between Ethernet (10/100 MBit/s) and KNX TP (9.6 kBit/s), considerably more telegrams can be transmitted on IP. If several telegrams for the same line follow each other in quick succession, they must be temporarily stored in the router in order to avoid telegram losses. For this purpose, the ComBridge IP Router Pro has memory space for 150 telegrams (from IP to KNX).

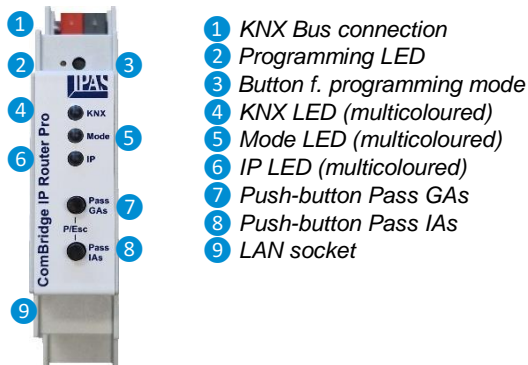
KNX interface (KNXnet/IP Tunneling)

The **CB IPR Pro** can be used as an interface to the KNX. The KNX bus can be accessed from any point in the LAN. For this purpose, an additional physical address must be assigned in each case. This is described in the following chapters.

Installation and commissioning

Mounting

The **ComBridge IP Router Pro** is mounted on a top-hat rail and has a space requirement of 1 TE (18 mm). It has the following operating elements and displays:



The connection of an external supply voltage is not necessary.



In the absence of bus voltage, the unit is without function.

KNX programming mode

The KNX programming mode is switched on or off via the recessed KNX programming button **3** or by pressing the buttons **7** and **8** simultaneously.

Manual operation and status display

The KNX LED **4** lights up green when KNX bus voltage is present. When this LED flickers, telegram traffic is taking place on the KNX bus.

Errors in communication (e.g. telegram repetitions or telegram fragments) are indicated by a brief colour change to red.

Overview of KNX LED states **4**:

LED Status	Meaning
LED lights green	KNX bus voltage present.
LED flickers green	Telegram traffic on the KNX Bus.
LED briefly red	Error in communication on the KNX Bus.

The IP LED **6** lights up when an Ethernet link is active. This LED is green if the unit has valid IP settings (IP address, subnet and gateway). If the IP settings are invalid or non-existent, this LED is red. This is also the case, for example, if the unit has not yet received the IP settings from the DHCP server.

When this LED flickers, IP telegram traffic takes place.

Overview of IP LED states **6**:

LED Status	Meaning
LED lights green	The device has an active Ethernet link and valid IP settings.
LED lights red	The device has an active Ethernet link and invalid IP settings or not yet received the IP settings by a DHCP server.
LED flickers green	IP telegram traffic

For test purposes (e.g. during commissioning), the parameterised routing settings (filter or block) can be bypassed via manual operation.

With the button Pass Gas **7** the forwarding of group-addressed telegrams can be activated.

With the button Pass IAs **8** the forwarding of physically addressed telegrams can be activated.

This is indicated by a single flash of the mode LED **5** (orange). If both modes are selected at the same time, the mode LED **5** flashes twice.

By pressing the buttons Pass GAs **7** and Pass IAs **8** again, these settings can be selected and deselected as desired. The manual operation can be terminated via the escape function (Esc) by simultaneously pressing the buttons Pass GAs **7** and Pass IAs **8**.

If neither programming mode nor manual operation is active, the mode LED **5** may indicate configuration errors.

Overview of Mode LED states **5**:

LED Status	Meaning
LED lights green	Device is working in standard operation mode.
LED lights red	Programming mode is active.
LED flashes 1x orange	Programming mode is not active. Manual operation is active: Forwarding IA or GA
LED flashes 2x orange	Programming mode is not active. Manual operation is active: Forwarding IA and GA
LED flashes rot	Programming mode is not active. Manual operation is not active. The device is not properly loaded e.g. after an interrupted download.

Factory settings

The following configuration is set by factory default:

Individual device address:	15.15.0
Number of configured KNXnet/IP tunneling con.:	1
Individual address of tunneling configuration:	15.15.240
IP address assignment:	DHCP
Initial Key (FDSK):	active
Security Mode:	not active

Reset to factory settings

It is possible to reset the device to its factory settings.

- Disconnect the KNX bus connector ① from device
- Press the KNX programming button ③ and keep it pressed down
- Reconnect the KNX bus connector ① of device
- Keep the KNX programming button ③ pressed for at least another 6 seconds
- A short flashing of all LEDs (② ④ ⑤ ⑥) visualizes the successful reset of the device to factory default settings.

ETS Configuration

Interface settings

In the ETS, interfaces can be selected and configured via the ETS menu "Bus - Interfaces".

The ETS can access configured KNX IP routers even without a database entry. If the KNX IP router configuration does not correspond to the conditions of the KNX installation, it must be configured via the ETS project. See the section ETS database.

In the delivery state, the IP address is assigned automatically via DHCP, i.e. no further settings are necessary for this. In order to use this function, a DHCP server must be located in the LAN (e.g. many DSL routers have a DHCP server integrated).

After the KNX IP Router has been connected to the LAN and the KNX bus, it should automatically appear from the ETS in the menu item "Bus" under "Found interfaces".

Clicking on the interface found selects it as the current interface. Connection-specific information and options then appear on the right-hand side of the ETS window.

The displayed device name and the "Host Physical Address" (physical address of the device) can then be changed within the ETS project.

Like all programmable KNX devices, the **CB IPR Pro** has a physical address with which the device can be addressed. This is used, for example, by the ETS when downloading the KNX IP router via the bus.

For the interface function, the unit uses additional physical addresses that can be set in the ETS. If a client (e.g. ETS) sends telegrams to the bus via the KNX IP

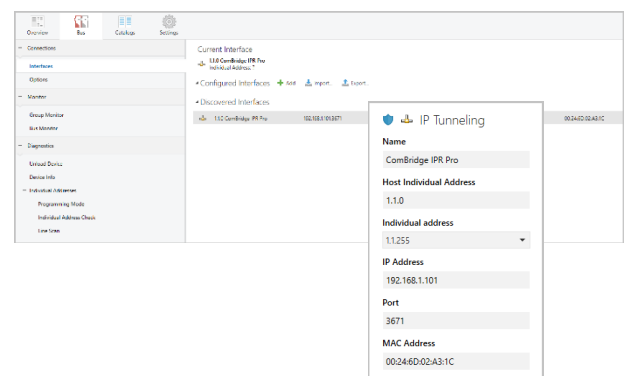
router, these contain one of the additional addresses as the sender address. Each address is assigned to a connection. In this way, response telegrams can be clearly forwarded to the respective client.

The additional physical addresses must be from the address range of the bus line in which the KNX IP Router is located and must not be used by another device.

Example:

Device adresse	1.1.0	(adresse within ETS topology)
Connection 1	1.1.240	(1. additional address)
Connection 2	1.1.241	(2. additional address)
Connection 3	1.1.242	(3. additional address)
Connection 4	1.1.243	(4. additional address)
Connection 5	1.1.244	(5. additional address)
Connection 6	1.1.245	(6. additional address)
Connection 7	1.1.246	(7. additional address)
Connection 8	1.1.247	(8. additional address)

In the "Physical address" section, the physical KNX address of the currently used KNXnet/IP tunneling connection can be selected.



The physical KNX device address as well as the physical KNX addresses for the additional tunneling connections can be changed within the ETS project after the device has been added to the project.

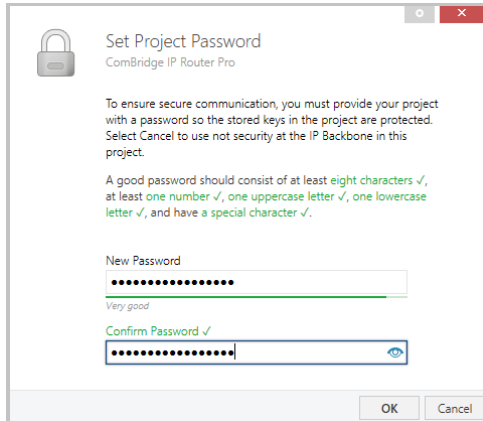
Application

The ETS application for the **ComBridge IP Router Pro** can be downloaded from our website at the link below or from the KNX Onlike catalogue of the ETS.

<https://www.ipas-products.com/en/products/produkt/knx-systemgeraete/ip-router-cb-ipr-pro/3622-141-18>

Project password

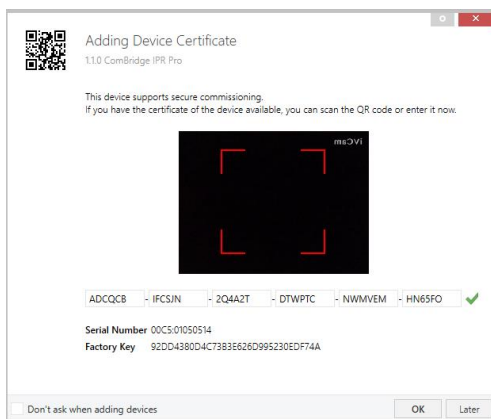
If the first product with KNX Secure is inserted into a project, the ETS prompts to enter a project password.



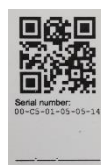
This password protects the ETS project from unauthorised access. This password is not a key used for KNX communication. The password entry can be bypassed with "Cancel", but this is not recommended for security reasons.

Device certificate

For each device with KNX Security that is created in the ETS, the ETS requires a device certificate. This certificate contains the serial number of the device and an initial key (FDSK = Factory Default Setup Key).



The certificate is printed as text on the device. It can also be conveniently scanned from the printed QR code via a webcam.



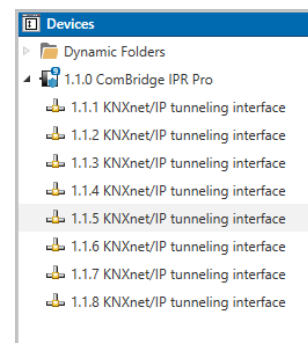
The list of all device certificates can be managed in the ETS window Overview - Projects - Security.

This initial key is required to safely put a device into operation right from the start. Even if the ETS download is recorded by a third party, the third party will not have access to the secured devices afterwards. During the first secure download, the initial key is replaced by the ETS with a new key that is generated individually for each device. This prevents people or devices who may know the initial key from accessing the device. The initial key is only reactivated after a master reset. The serial number in the certificate enables the ETS to assign the correct key to a device during a download.

Properties dialogue

Tunnel connections

In the ETS, some settings are displayed in addition to the parameter dialogue in the properties dialogue (at the edge of the screen). For example, the IP settings can be made here. The additional addresses for the interface connections are displayed in the topology view.



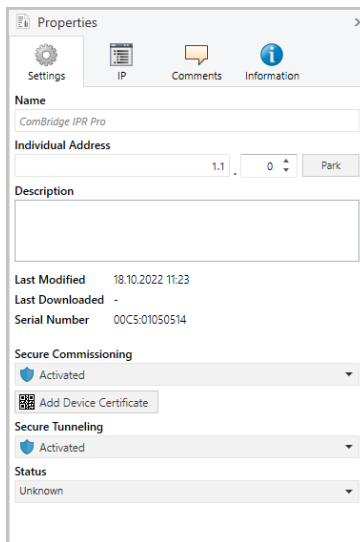
To change the individual addresses, select the corresponding entry in the list and enter the desired address in the text field. If the frame of the text field changes its colour to red after entry, this indicates that the address entered is already in use.

i Make sure that none of the above addresses are already used in your KNX installation.

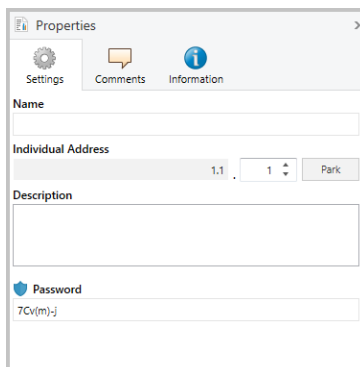
Properties

By marking the **ComBridge IPR Pro** in the tree structure of the topology view of the ETS project, the overview "Properties" appears on the right side of the ETS window. The device name of the **ComBridge IPR Pro** can be changed under Properties menu item „Settings“.

i The changes made in the properties menus only take effect after an application download.



If Secure Tunneling is activated, a password is automatically assigned for each tunnel. This password is displayed under menu item "Settings" when a tunnel is selected.

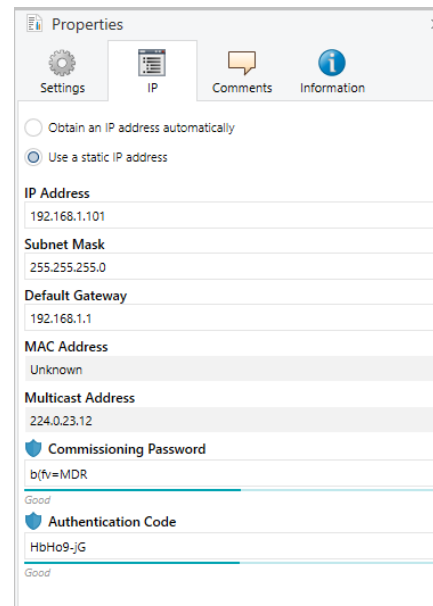


IP

By switching from "Obtain IP address automatically" (via DHCP) to "Use the following IP address" (static IP address), the IP address, subnet mask and standard gateway can be freely selected.

IP Address

Enter the IP address of the ComBridge IP Router Pro here. This is used to address the device via the IP network (LAN). The IP addressing should be coordinated with the administrator of the network.



Subnet mask

The subnet mask must be entered here. This mask is used by the unit to determine whether a communication partner is in the local network. If a partner is not in the local network, the unit does not send the telegrams directly to the partner, but to the gateway, which takes over the forwarding.

Default gateway

Enter the IP address of the gateway here, e.g. the DSL router of the installation.

Routing Multicast Adresse

This address is used for routing telegrams to IP. The multicast IP address 224.0.23.12 has been reserved for this purpose (KNXnet/IP) by the IANA (Internet Assigned Numbers Authority). If another multicast IP address is desired, it must be from the range 239.0.0.0 to 239.255.255.255.

Example for the allocation of IP addresses:

The **ComBridge IP Router Pro** is to be accessed with a PC.

IP adresse of the PCs: 192.168.1.30

Subnet of the PCs: 255.255.255.0

The **ComBridge IP Router Pro** is located in the same local LAN, i.e. it uses the same subnet. The subnet restricts the assignment of the IP address, i.e. in this example the IP address of the IP router must be 192.168.1.xx, xx can be a number from 1 to 254 (with the exception of 30, which has already been used). Care must be taken not to assign addresses twice.

IP adresse of the KNX IP Router: 192.168.1.31

Subnet of the KNX IP Router: 255.255.255.0

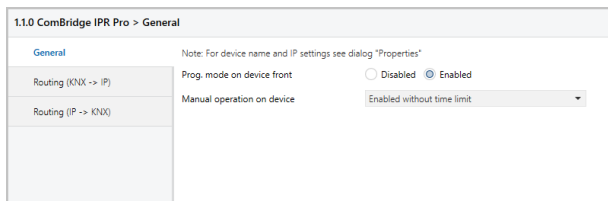
Commissioning password and authentication code

Under Properties menu item "IP", specific options such as the commissioning password and the authentication code of the **ComBridge IP Router Pro** can be changed.

ETS parameter dialogue

The following parameters can be set with the ETS.

General settings



1.1.0 ComBridge IPR Pro > General

Note: For device name and IP settings see dialog "Properties"

Prog. mode on device front: ☐ Disabled ☒ Enabled

Manual operation on device: Enabled without time limit

Prog. mode on front panel

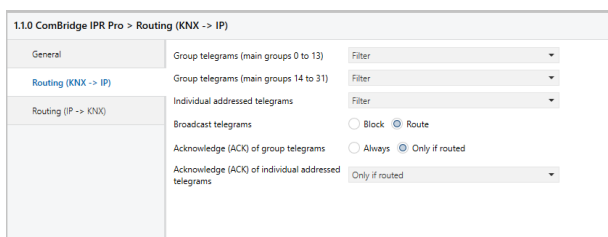
In addition to the normal programming button **3**, the unit allows you to activate the programming mode on the front panel without opening the panel cover. Programming mode can be activated and deactivated by pressing keys **7** and **8** simultaneously.

This function can be activated and deactivated via the parameter "Prog. Mode on front panel" parameter to switch this function on and off. The recessed programming key **3** (next to the programming LED **2**) is always activated and is not affected by this parameter.

Manual control on the unit

This sets the duration of the manual operation mode. When it ends, the normal operating mode is automatically carried out again.

Routing (KNX -> IP)



1.1.0 ComBridge IPR Pro > Routing (KNX -> IP)

General: Group telegrams (main groups 0 to 13): Filter

Routing (KNX -> IP): Group telegrams (main groups 14 to 31): Filter

Routing (IP -> KNX): Individual addressed telegrams: Filter

Broadcast telegrams: ☐ Block ☒ Route

Acknowledge (ACK) of group telegrams: ☐ Always ☒ Only if routed

Acknowledge (ACK) of individual addressed telegrams: Only if routed

Group telegrams (main groups 0 to 13)

Block: No group telegram of these main groups is forwarded to IP.

Route: All group telegrams of these main groups are forwarded to IP regardless of the filter table. This setting should only be used for test purposes.

Filter: Here, the filter table is used to check whether the received group telegram is forwarded to IP.

Group telegrams (main groups 14 to 31)

Block: No group telegram of the main groups 14 to 31 is forwarded to IP.

Route: All group telegrams of the main groups 14 to 31 are forwarded to IP.

Filter: Here, the filter table is used to check whether the received group telegram is forwarded to IP.

Physically addressed telegrams

Block: No physically addressed telegram is forwarded to IP.

Route: All physically addressed telegrams are forwarded to IP.

Filter: The physical address is used to check whether the received physically addressed telegram is forwarded to IP.

Broadcast telegrams

Block: No received broadcast telegram is forwarded to IP.

Route: All received broadcast telegrams are forwarded to IP.

Acknowledgement (ACK) of group telegrams

Always: An acknowledge is always generated for received group telegrams (from KNX).

Only if routed: For received group telegrams (from KNX), an acknowledge is only generated when forwarded to IP.

Acknowledge (ACK) of individual addressed telegrams

Always: An acknowledge is always generated for received individual addressed telegrams (from KNX).

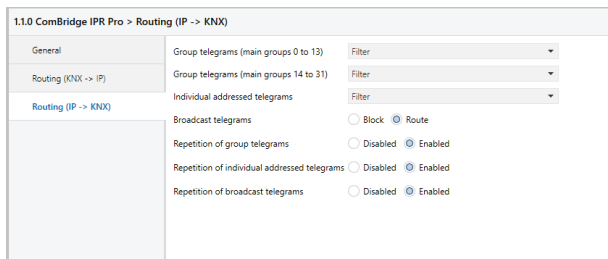
Only if routed: For received individual addressed group telegrams (from KNX), an acknowledge is only generated when forwarded to IP.

Answer with NACK: Each individual addressed telegram received (from KNX) is answered with NACK (Not Acknowledge), i.e. communication with individual addressed telegrams on the corresponding KNX line is no longer possible. Group communication (group telegrams) is not affected by this. This setting can be used to prevent manipulation attempts.



If the response is NACK, access to the device via KNX TP is no longer possible. The parameterisation must be carried out via IP.

Routing (IP -> KNX)



Group telegrams (main groups 0 to 13)

- Block:** No group telegram of these main groups is forwarded to KNX.
- Route:** All group telegrams of these main groups are forwarded to KNX regardless of the filter table. This setting should only be used for test purposes.
- Filter:** Here, the filter table is used to check whether the received group telegram is forwarded to KNX.

Group telegrams (main groups 14 to 31)

- Block:** No group telegram of the main groups 14 to 31 is forwarded to KNX.
- Route:** All group telegrams of the main groups 14 to 31 are forwarded to KNX.
- Filter:** Here, the filter table is used to check whether the received group telegram is forwarded to IP.

Individually addressed telegrams

- Block:** No individual addressed telegram is forwarded to KNX.
- Route:** All individual addressed telegrams are forwarded to KNX.
- Filter:** The individual address is used to check whether the received physically addressed telegram is forwarded to KNX.

Broadcast telegrams

- Block:** No received broadcast telegram is forwarded to KNX.
- Route:** All received broadcast telegrams are forwarded to KNX.

Repetition of group telegrams

- Deactivated:** The received group telegram is not sent repeatedly on the KNX bus in the event of an error..
- Activated:** The received group telegram is repeated up to three times in the event of an error.

Repetition of individually addressed telegrams

- Deactivated:** The received individual addressed telegram is not sent repeatedly on the KNX bus in the event of an error.
- Activated:** The received individual addressed telegram is repeated up to three times in the event of an error.

Repetition of broadcast telegrams

- Deactivated:** The received broadcast telegram is not sent repeatedly on the KNX bus in the event of an error.
- Activated:** The received broadcast telegram is repeated up to three times in the event of an error.

Programming

The **ComBridge IP Router Pro** can be programmed in different ways by the ETS:

Via KNX bus

For this, the device only needs to be connected to the bus. The ETS requires an additional interface (e.g. USB) to the bus. This way, both the physical address and the entire application including IP configuration can be programmed. Programming via the bus is recommended if no IP connection can be established.

Via KNXnet/IP Tunneling

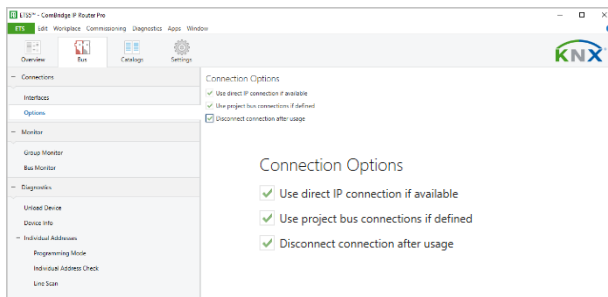
No additional interface is required here. Programming via KNXnet/IP tunneling is possible if the device already has a valid IP configuration (e.g. via DHCP). In this case, the device is displayed in the interfaces in the ETS and must be selected. The download is carried out from the ETS project as with other devices.

Via KNXnet/IP Routing

Programming via KNXnet/IP routing is possible if the device already has a valid IP configuration (e.g. via DHCP or Auto IP). The routing interface appears in the ETS if at least one device that supports routing is visible in the network. The name of the network interface in the PC appears as the designation. If routing is selected as the interface, programming is carried out from the ETS project as with other devices. In this case, the LAN is used as a KNX medium similar to TP. No additional interface device is required.

Via direct IP connection

While both KNXnet/IP Tunneling and KNXnet/IP Routing are limited to the speed of KNX TP, a direct IP connection allows the device to be loaded at high speed. The direct IP connection is possible if the device already has both a valid IP configuration and a physical address. To do this, the selection "Use direct IP connection if possible" must be selected in the ETS menu under "Bus - Connections - Options". The download then takes place directly in the device and is not visible in the ETS group monitor.



i Due to the significantly shorter transmission times, it is recommended to carry out downloads via IP.

Open Source Licenses

This product contains open source software licenses:
curve25519-donna: Curve25519 elliptic curve, public key function

Source: <http://code.google.com/p/curve25519-donna/>

Copyright 2008, Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



WARNING

- The device must be mounted and commissioned by an authorized electrician.
- The prevailing safety rules must be heeded.
- The device must not be opened.
- For planning and construction of electric installations, the relevant guidelines, regulations and standards of the respective country are to be considered.