

Product documentation



IP router

Ref.-no.: IPR 300 SREG

IP interface

Ref.-no.: IPS 300 SREG

ALBRECHT JUNG GMBH & CO. KG

Volmestraße 1
58579 Schalksmühle
GERMANY

Tel. +49 2355 806-0
Fax +49 2355 806-204
kundencenter@jung.de
www.jung.de

Table of Contents

1	Safety instructions and device components	3
1.1	Safety instructions.....	3
1.2	Device components	3
2	Function	3
2.1	System information	3
2.2	Intended use.....	3
2.3	Product characteristics	4
3	Information for electrically skilled persons	4
3.1	Installation and electrical connection.....	4
3.2	Mounting.....	4
3.3	Connection	4
4	Commissioning	5
4.1	Switching on.....	5
4.2	Boot procedure	5
5	Operation	6
5.1	Display	6
5.2	LED displays	6
5.3	Factory settings / reset.....	7
6	Configuration.....	7
6.1	Topology	7
6.1.1	IP interface.....	7
6.1.2	IP router	7
6.2	Device properties	8
6.2.1	General	8
6.2.2	IP properties.....	9
6.2.3	KNX IP Secure.....	9
6.3	Device-specific parameters	10
6.3.1	IP interface.....	10
6.3.2	IP router	12
7	Telnet	18
7.1	IP router and IP interface.....	18
7.2	IP router	22
8	Terms	23
9	Technical data.....	24
10	Warranty	24
11	Open Source Software.....	25
11.1	LWIP	25

1 Safety instructions and device components

1.1 Safety instructions



Electrical equipment may only be fitted and connected by electrically skilled persons.

Serious injuries, fire or property damage possible. Please read and follow manual fully.
 These instructions are an integral part of the product and must remain with the end customer.
 This product is only intended for use in dry rooms.

1.2 Device components

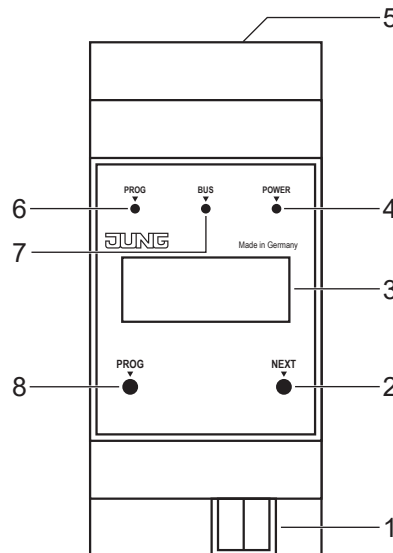


Fig. 1: Device components

1	KNX connection	5	LAN connection
2	NEXT button	6	PROG LED
3	Display	7	BUS LED
4	POWER LED	8	PROG button

2 Function

2.1 System information

This device is a product of the KNX system and conforms to the KNX Directives. Detailed knowledge attained through KNX training is a prerequisite for understanding.

The device function is software-dependent.

Detailed information about software versions and the respective function scope, as well as the software itself can be found in the manufacturer's product database.

The device is planned, installed and commissioned by means of KNX-certified software. Full functionality with KNX commissioning software version ETS 5.7 f onwards.

An updated version of the product database, technical descriptions and conversion programs and other auxiliary programs are available on our Internet website.

2.2 Intended use

- Connection between KNX devices and PC or other data processing devices via IP
- Operation as KNX area/line coupler or data interface
- Mounting on DIN rail according to EN 60715 in distribution boxes

2.3 Product characteristics

- KNXnet/IP routing for communication between KNX lines, areas and systems via IP network
- Support of KNX Data Secure from ETS version 5.7 upwards
- Support of KNX IP Secure from ETS version 5.7 upwards
- Telegram forwarding and filtering according to physical address or group address
- Max. 48 telegrams per second in IP secure mode
- LED display for KNX communication, Ethernet communication and programming mode
- Configuration via ETS, Telnet or software tool
- SNTP server, buffered
- Commissioning with display support
- Max. 8 connections to IP terminal devices, e.g. for simultaneous visualisation and configuration
- Outage message of the KNX system to the IP system
- Electrical isolation between KNX and IP network
- Power consumption max. 1 W

3 Information for electrically skilled persons

3.1 Installation and electrical connection



DANGER

Electrical shock on contact with live parts in the installation environment.

Electrical shocks can be fatal.

Before working on the device, disconnect the power and cover live parts in the area!

3.2 Mounting

Mount IP router on DIN rail according to EN 60715 in distribution boxes.

3.3 Connection

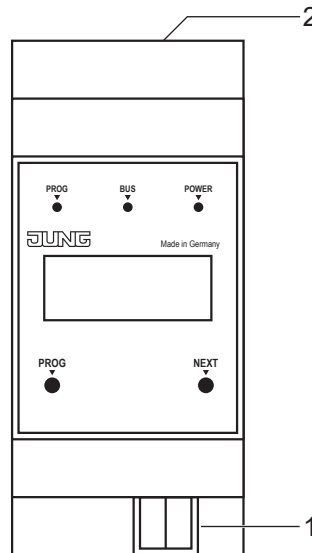


Fig. 2: Connection

1 KNX connection

2 LAN connection

Requirements:

- one Ethernet connection with 10/100 Mbit
- one KNX/EIB bus connection

For position of the connections see device components.

- Connect LAN and KNX.

4 Commissioning

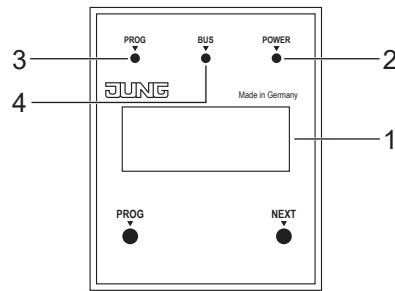


Fig. 3: Commissioning

- | | | | |
|---|-----------|---|----------|
| 1 | Display | 3 | PROG LED |
| 2 | POWER LED | 4 | BUS LED |

4.1 Switching on

After connecting, the device is switched on automatically. The product name and assigned IP address appear on the display when switching on.

4.2 Boot procedure

The automatic boot procedure starts after switching on. The three LEDs flash on the front of the device as a running light during the boot procedure.

PROG LED – red

BUS LED – yellow

POWER LED – green

The duration of the boot procedure is prolonged if the IP address is assigned to the IP router via DHCP. DHCP is specified by the factory settings. The green POWER LED flashes during the assignment of the IP address.

The IP address of the device appears in the display at the end of the boot procedure.

5 Operation

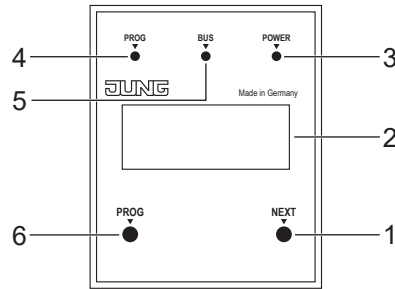


Fig. 4: Operation

1	NEXT button	4	PROG LED
2	Display	5	BUS LED
3	POWER LED	6	PROG button

5.1 Display

The display switches itself off automatically after one minute.

Switching on display:

- Press NEXT button.

Scrolling through menu:

- Press NEXT button repeatedly while the display is switched on.

Menu structure:

- Page 1:
Displaying the firmware version, IP address, physical address, serial number and tunnel connections used
- Page 2:
Displaying all IP settings
Displaying the boot-up time
- Page 3:
Information on the telegram rate
- Page 4:
Displaying the FDSK (Factory Default Setup Key)
This is only displayed if the device is still in the delivery state.

5.2 LED displays

There are three LEDs on the front of the device. The LEDs indicate the following device statuses during operation:

- PROG LED lights up red:
Device is in programming mode.
- BUS LED flashes yellow:
Device bus is active.
- POWER LED flashes green:
Device is ready for operation.

There are two other LEDs next to the LAN connection. The LEDs indicate the following device statuses during operation:

- green LED:
Connection to another IP device or switch is established.
- yellow LED:
IP data transfer is active.

5.3 Factory settings / reset

Restoring factory settings:

- Press PROG button for 10 seconds.
 PROG LED flashes red.
 Device is in programming mode.
 Factory settings are restored automatically.
 Boot procedure is started.

6 Configuration

6.1 Topology

6.1.1 IP interface

To insert the interface into an ETS project, a TP line must exist.

6.1.2 IP router

To insert the router into an ETS project, it must have an IP backbone.

Example:

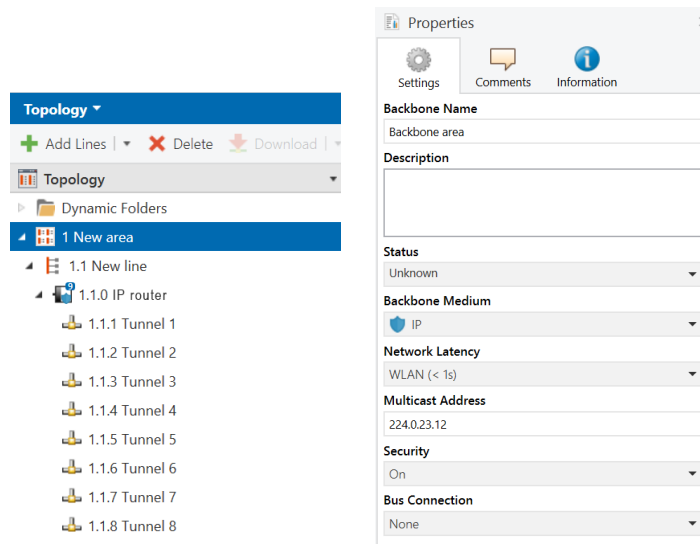


Fig. 5: Topology (left) and properties of the backbone

Line 1: Backbone Medium IP

Line 1.1: Line Medium TP

In the Properties Diagram of the Backbone (NOTE: For this click on Topology, directly above “Dynamic Folders”, see figure 5), you will find the settings for the Multicast of the Backbone. Network latency (see figure 5) can be changed if the routing is over a large distributed system. In this case, increase the time constant.

The KNX IP Secure Router supports up to eight KNX (Secure) IP tunnel connections and can be used as a line or area coupler.

6.2 Device properties

6.2.1 General

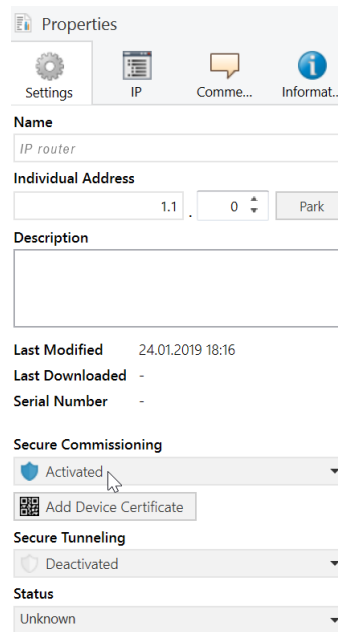


Fig. 6: Properties of the device

Function	Description
Name	Any name can be assigned, max. 30 characters
Secure Comissioning	If activated, the encryption is active for commissioning: all parameters are then transmitted in encrypted form, although e.g. Tunnel connections are still unencrypted.
Secure Tunneling	If activated, the tunnel connections can only be established via KNX Secure Tunneling.

6.2.2 IP properties

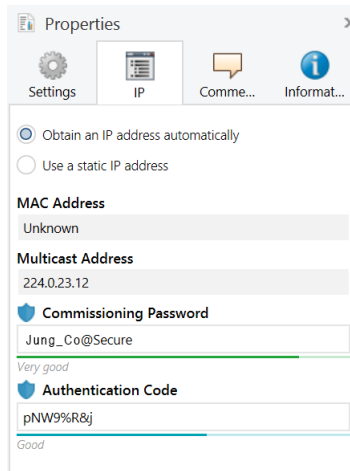


Fig. 7: IP Properties of the device

Function	Description
Obtain an IP address automatically	The device requires a DHCP server for IP address assignment.
Use a static IP address	The user specifies the IP settings.
Comissioning Password	A password from which the ETS generates a key. This is the key to secure commissioning (see above).
Authentication Code	With the authentication password, the user proves that he has access to the project.
MAC Address	Is a device property.
Multicast Address	Is given by the backbone configuration (see figure 5).

6.2.3 KNX IP Secure

Requirements:

- Safe commissioning activated
- FDSK entered/scanned or device certificate added

Configuration of KNX IP Secure:

- Activate secure tunneling.
- Define a password for each tunnel (max. 8 tunnels).
- Define a password for commissioning and authentication code.

i Document all passwords and store them securely.

6.3 Device-specific parameters

6.3.1 IP interface

General settings

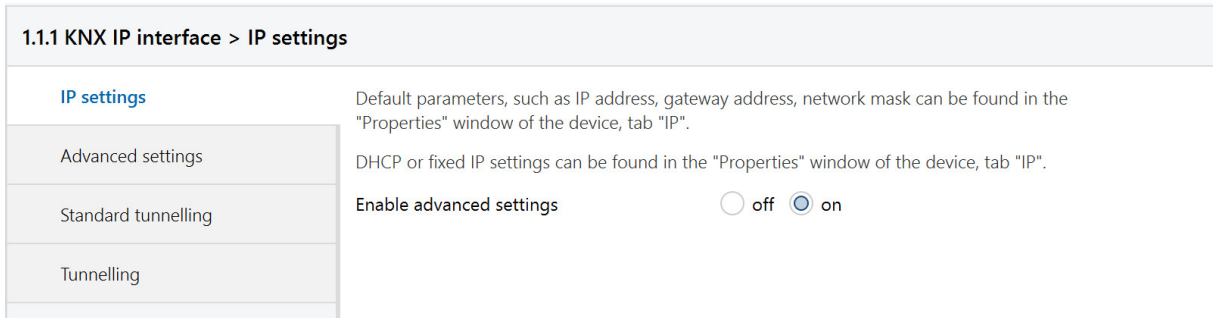


Fig. 8: General settings of the device

Function	Options	Description
(Text)		The ETS has manufacturer-independent uniform parameter descriptions for various settings. To simplify the application, a note text is displayed here.
Enable advanced settings	off/on	Advanced functions to ensure a maximum of flexibility.

Advanced settings

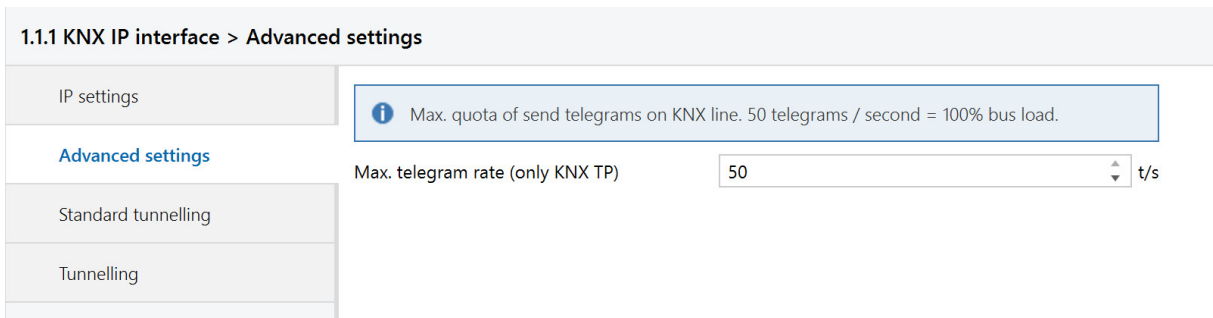


Fig. 9: Advanced settings of the device

Function	Options	Description
Max. number of telegrams to KNX TP	5 .. <u>50</u>	See parameter description

Advanced settings standard tunnel preferred IP

For standard tunnel connections (before 2019) it is possible to assign each of these tunnel connections to an IP address. In the analysis of group telegrams, this makes it easier to assign the telegrams to the sender which „sits“ behind the tunnel, as e.g. Visualizations or smartphone apps.

i This assignment can be resolved at any time by the ETS or a new so-called extended tunnel connection (as of 2019).

1.1.1 KNX IP interface > Standard tunnelling

IP settings

Advanced settings

Standard tunnelling

Tunnelling

Slow connection (UDP connections only) off on

UDP connection timeout sec

The standard timeout (1 second) may be too low for a connection, e.g. via the Internet.
Parameter range is [1.0 ... 8.0] seconds

i A standard tunnelling connection (so called BasicCRI, devices up to ETS4) does not differentiate which tunnel is used for a connection. This setting assigns the tunnel of the BasicCRI connection to an IP address.

i Note: ETS connections or extended CRI connections will override this assignment.

Preferred IP for tunnel 1 off on

Preferred IP for tunnel 2 off on

End device IP

Preferred IP for tunnel 3 off on

Preferred IP for tunnel 4 off on

Preferred IP for tunnel 5 off on

Preferred IP for tunnel 6 off on

Preferred IP for tunnel 7 off on

Preferred IP for tunnel 8 off on

Fig. 11: Preferred IP for Tunnelling

Function	Options	Description
Slow connection	<u>off/on</u>	The tunnel connections over UDP are controlled by default with a connection timeout of 1 second. This may be too short for connections over the Internet.
UDP connection timeout	<u>1,0 ... 8,0</u> sec	Setting of timeout for tunnel connection over UDP
Preferred IP for tunnel X	<u>off/on</u>	Tunnel X should preferably be used for communication with the parametrized IP address.
End device IP	(IP-V4 address)	IP address of end device

6.3.2 IP router

General settings

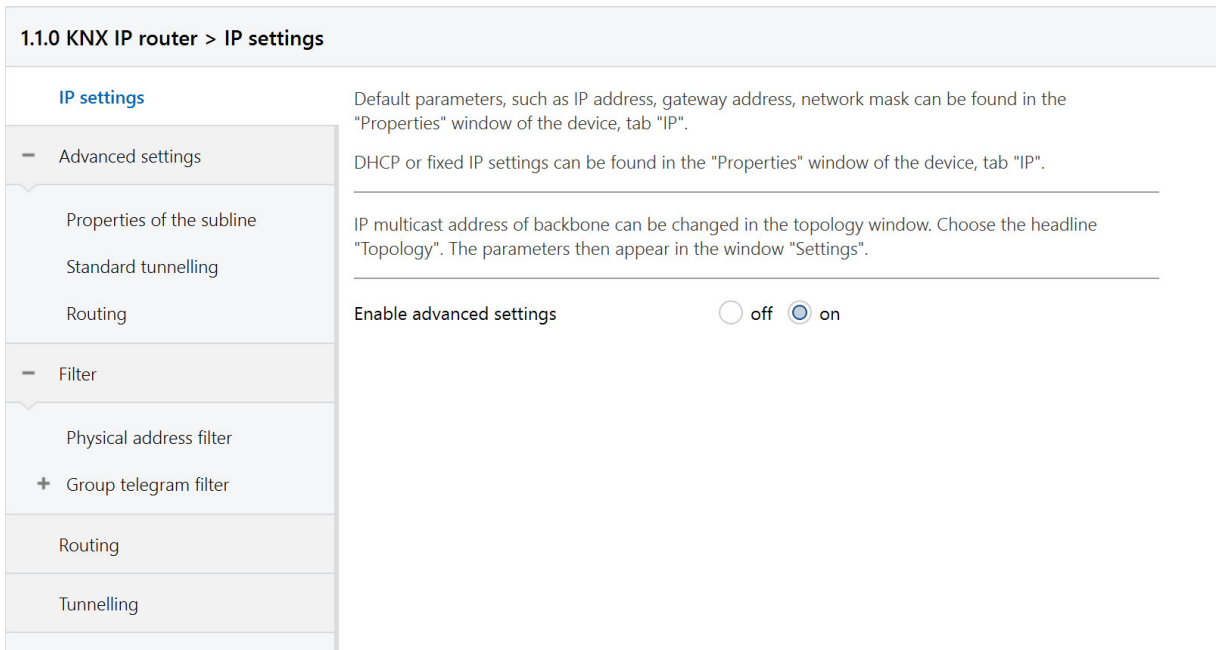


Fig. 12: General settings of the device

Function	Options	Description
(Text)		The ETS has manufacturer-independent uniform parameter descriptions for various settings. To simplify the application, a note text is displayed here.
Enable advanced settings	off/on	Advanced functions to ensure a maximum of flexibility.

Advanced settings properties of the subline

1.1.0 KNX IP router > Advanced settings > Properties of the subline

IP settings

Advanced settings

Properties of the subline

Standard tunnelling

Routing

Filter

Physical address filter

Group telegram filter

Routing

Tunnelling

i Note: If a tunnel connection is used, every telegram is acknowledged (ACK). Therefore, this setting is only useful for routers that do not use the tunnel connections.

ACK for every telegram off on

TP device -> KNX IP router

ACK for routed telegrams only off on

KNX IP router -> TP device

Repeat routed telegrams if not acknowledged off on

i If the TP line is easily accessible (e.g. KNX line outside), the router can be locked, so that it can not be reprogrammed via the KNX bus. This adds extra security. Programming via IP is still possible.

Programming disabled for TP side off on

i Max. quota of send telegrams on KNX line. 50 telegrams / second = 100% bus load.

Max. telegram rate (only KNX TP) t/s

Fig. 13: Properties of the subline

Function	Options	Description
ACK for every telegram	off/on	The router acknowledges each telegram, even if it does not forward this telegram (TP only)
ACK for routed telegram only	off/on	The router only confirms the telegrams that it forwards (TP only)
Repeat routed telegrams if not ACKed	off/on	The router repeats unconfirmed individually addressed telegrams (TP only)
Inhibit programming from TP side	off/on	See parameter description
Max. number of telegrams to KNX TP	5 .. 50	See parameter description

Advanced settings standard tunnel preferred IP

For standard tunnel connections (before 2019) it is possible to assign each of these tunnel connections to an IP address. In the analysis of group telegrams, this makes it easier to assign the telegrams to the sender which „sits“ behind the tunnel, as e.g. Visualizations or smartphone apps.

i This assignment can be resolved at any time by the ETS or a new so-called extended tunnel connection (as of 2019).

1.1.0 KNX IP router > Advanced settings > Standard tunnelling

IP settings

Advanced settings

Properties of the subline

Standard tunnelling

Routing

Filter

Physical address filter

Group telegram filter

Routing

Tunnelling

Slow connection (UDP connections only) off on

UDP connection timeout sec

The standard timeout (1 second) may be too low for a connection, e.g. via the Internet.
Parameter range is [1.0 .. 8.0] seconds.

i A standard tunnelling connection (so called BasicCRI, devices up to ETS4) does not differentiate which tunnel is used for a connection. This setting assigns the tunnel of the BasicCRI connection to an IP address.

Note: ETS connections or extended CRI connections will override this assignment.

Preferred IP for tunnel 1 off on

Preferred IP for tunnel 2 off on

End device IP

Preferred IP for tunnel 3 off on

Preferred IP for tunnel 4 off on

Preferred IP for tunnel 5 off on

Preferred IP for tunnel 6 off on

Preferred IP for tunnel 7 off on

Preferred IP for tunnel 8 off on

Fig. 14: Preferred IP for Tunnelling

Function	Options	Description
Slow connection	<u>off/on</u>	The tunnel connections over UDP are controlled by default with a connection timeout of 1 second. This may be too short for connections over the Internet.
UDP connection timeout	<u>1,0</u> ... 8,0 sec	Setting of timeout for tunnel connection over UDP
Preferred IP for tunnel X	<u>off/on</u>	Tunnel X should preferably be used for communication with the parametrized IP address.
End device IP	(IP-V4 address)	IP address of end device

Advanced settings routing

1.1.0 KNX IP router > Advanced settings > Routing

IP settings

Advanced settings

Properties of the subline

Standard tunnelling

Routing

Filter

Physical address filter

Group telegram filter

Routing

Tunnelling

Check of topology

i If enabled, the router will detect an error in topology and send a message (A_Network_Parameter_Response) on the KNX bus or IP line, respectively. The telegram is sent on the line which violates the topology rules.

i The erroneous KNX address will be shown in the Telnet interface and on the display. The erroneous telegram will not be routed.

Check topology off on

Routing (before 2018)

i If enabled, the router acts according to specification before 2018. This means different behaviour of routing count algorithm.

i If the router is used as replacement in existing installations, the old routing model might be necessary.

Enable routing algorithm (<2018) off on

Fig. 15: Routing

Function	Options	Description
Check of topology	off/on	See parameter description
Enable routing algorithm (<2018)	off/on	See parameter description

Physical address filter

1.1.0 KNX IP router > Filter > Physical address filter

IP settings

Advanced settings

Properties of the subline

Standard tunnelling

Routing

Filter

Physical address filter

Group telegram filter

Physically addressed telegrams

IP => KNX filter (default) ▼

KNX => IP filter (default) ▼

Block broadcast telegrams

IP => KNX off on

KNX => IP off on

Fig. 16: Physical address filter

Function	Options	Description
Physically addressed telegrams	filter, block, route	The physically addressed telegrams (e.g., actuator programming) may be routed, blocked, or filtered via the routing. This affects all communication related to the device address.
Block broadcast telegrams	off/on	Broadcast telegrams (e.g., searching for actuators in programming state) can be routed or blocked through the router.

Group telegram filter

1.1.0 KNX IP router > Filter > Group telegram filter

IP settings

Advanced settings

Properties of the subline

Standard tunnelling

Routing

Filter

Physical address filter

Group telegram filter

Ext. filter IP => KNX

Ext. filter KNX => IP

Routing

Tunnelling

IP => KNX

Main group 0..13 route

Main group 14..15 filter

Main group 16..31 filter

Extended group address filter off on

KNX => IP

Main group 0..13 route

Main group 14..15 filter

Main group 16..31 filter

Extended group address filter off on

Fig. 17: Group telegram filter

Function	Options	Description
IP => KNX		Direction: Telegrams from the IP side to the KNX side
Main group 0 to 13	filter, block, <u>route</u>	Group telegrams can be routed, blocked or filtered via the routing. The groups 0 to 13 are summarized here to a block.
Main group 14 to 15	<u>filter</u> , block, route	Group telegrams can be routed, blocked or filtered via the routing. Groups 14 and 15 are grouped together to form a block.
Main group 16 to 31	<u>filter</u> , block, route	Group telegrams can be routed, blocked or filtered via the routing. The groups 16 and 31 are here combined to form a block.
Extended group address filter	<u>off/on</u>	In addition to the block-oriented filtering of group address telegrams, each group can also be separately routed, blocked or filtered via the routing. With this function, the parameter dialog can be opened for this purpose.
KNX => IP		Direction: Telegrams from the KNX side to the IP side
Main group 0 to 13	filter, block, <u>route</u>	Group telegrams can be routed, blocked or filtered via the routing. The groups 0 to 13 are summarized here to a block.
Main group 14 to 15	<u>filter</u> , block, route	Group telegrams can be routed, blocked or filtered via the routing. Groups 14 and 15 are grouped together to form a block.

Function	Options	Description
Main group 16 to 31	<u>filter</u> , block, route	Group telegrams can be routed, blocked or filtered via the routing. The groups 16 and 31 are here combined to form a block.
Extended group address filter	<u>off/on</u>	In addition to the block-oriented filtering of group address telegrams, each group can also be separately routed, blocked or filtered via the routing. With this function, the parameter dialog can be opened for this purpose.

Extended group telegram filter

1.1.0 KNX IP router > Filter > Group telegram filter > Ext. filter IP => KNX

IP settings

Advanced settings

Properties of the subline

Standard tunnelling

Routing

Filter

Physical address filter

Group telegram filter

Ext. filter IP => KNX

Ext. filter KNX => IP

Routing

Tunnelling

Extended filter for direction IP => KNX

i You can define a filter for each main group. This overrides the respective settings of the group filters (0..13, 14..15, or 16..31). If the individual filter is disabled, the group filter is active.

Main group 00	disabled (default)
Main group 01	disabled (default)
Main group 02	disabled (default)
Main group 03	disabled (default)
Main group 04	disabled (default)
Main group 05	block
Main group 06	route
Main group 07	disabled (default)
Main group 08	disabled (default)
Main group 09	disabled (default)
Main group 10	disabled (default)
Main group 11	disabled (default)
Main group 12	disabled (default)
Main group 13	disabled (default)
Main group 14	disabled (default)

Fig. 18: Extended group telegram filter

Function	Options	Description
Main group 00	<u>inactive</u> , filter, block, forward	Group telegrams of this main group can be routed, blocked or filtered via the routing. If the filter is not active, the behavior of the parameters of figure 10 and figure 11, respectively.
Main group NN NN = 1 ... 31	See above	See above

7 Telnet

Telnet is a common network protocol based on a TCP connection between a Telnet server (the device in this case) and a client (the commissioning PC in this case).

For communication to be possible, it is necessary for the device to be administered in the network and to be reached by the commissioning PC via IP. Settings can then be made on the device (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.

Telnet access is factory-protected with the password "knxsecure".

Once the device is in secure mode, the telnet interface is disabled.

7.1 IP router and IP interface

Telnet input	Description
<code>help</code>	Displays all available commands
<code>ifconfig</code>	<p>Displays network parameters</p> <pre>IP mode.....: DHCP IP.....: 192.168.33.142 Subnet mask...: 255.255.0.0 Gateway.....: 192.168.33.1 NTP server....: 192.53.103.108 Sys multicast.: 224.0.23.12 RT multicast..: 224.0.23.12 Hardware addr.: 00:50:c2:79:3f:ff</pre> <p>Sys multicast: Multicast address for System telegrams RT multicast: Multicast address für routing telegrams</p>
<code>ifconfig [help dhcp ip mask]</code>	<p>Set network parameters via the telnet interface. Expamples:</p> <p>Setting IP Adresse with DHCP: <code>ifconfig dhcp</code></p> <p>Statically set the IP address to 192.168.1.2 (in this case, the gateway and mask should also be adapted, see below) <code>ifconfig ip 192.168.1.2</code></p> <p>Set the gateway to 192.168.1.1: <code>ifconfig gw 192.168.1.1</code></p> <p>Set the mask to 255.255.255.0: <code>ifconfig mask 255.255.255.0</code></p>
<code>tpconfig</code>	<p>Shows KNX parameters</p> <pre>KNX bus state.: up KNX address...: 15.15.000 Serial number.: 00-a6-00-00-00-01</pre>
<code>tpconfig [help set]</code>	<p>Set KNX parameters via the telnet interface.</p> <p>Set the TP address to 1.1.0: <code>tpconfig set 1.1.0</code></p>
<code>progmode [0 1]</code>	Query or change programming mode (0 = off, 1 = on)
<code>apdu [55..248]</code>	<p>Read or configure the maximum length of the KNX TP telegrams. This may be necessary if there is an incorrect implementation of a TP stack. In that case the ETS may try to use telegrams with 248 bytes payload, but the TP device can not process (e.g. Zennio Z35i). Default is 248 and should only be changed if necessary.</p> <pre># apdu maximal len of a KNX telegram 248. Usage: apdu [55 .. 248]</pre>

Telnet input	Description
<pre>tpratemax [5..50]</pre>	<p>Read or configure maximum telegram rate (IP => TP); 50 T / s corresponds to 100% bus load.</p> <pre># tpratemax no limit, sending with maximum performance to TP. Usage: tpratemax [5 .. 50]</pre>
<pre>stats</pre>	<p>Shows various statistics on device and bus status</p> <pre>uptime: 114 days, 2:19 KNX communication statistics: TX to IP (all)..: 333729 (ca. 233 t/m) TX to KNX.....: 23244 (ca. 16 t/m) RX from KNX.....: 94559 (ca. 66 t/m) Overflow to IP..: 0 Overflow to KNX.: 0 TX tunnel re-req: 260 TP bus voltage..: 28.95 V TX TP rate.....: 50 T/s (= 100 %)</pre> <p>Uptime: Runtime of the interface since last restart TX to IP (all): Number of all telegrams sent on IP TX to KNX: Number of all telegrams sent on KNX RX from KNX: number of telegrams received from the KNX bus Overflow to IP: Number of telegrams that could not be sent to IP Overflow to KNX: Number of telegrams that could not be sent to the KNX bus TX tunnel re-req: Number of telegrams that had to be repeated in the tunnel connections TP bus voltage: Current bus voltage (at the time of calling stats) TX TP rate: maximum telegram rate (TP)</p>
<pre>free [clear]</pre>	<p>Shows statistics about the memory usage</p> <pre>Used stack memory...: 14 % Allocated memory....: 64 % Unused memory.....: 35 % TP-Tx buffer.....: 0 % TP-Tx buffer max....: 0 % TP-Rx buffer max....: 0 % Tunnel-T8 buffer max: 92 %</pre> <p>Used stack memory: Function stack utilization Allocated memory: Allocated device memory Unused memory: Unused device memory TP-Tx buffer: Currently used TP send buffer TP-Tx buffer max:Max. Utilization of TP send buffer (IP => TP) since system startup TP-Rx buffer max:Max. Utilization TP receive buffer (IP <= TP) since system startup Tunnel-XX (XX=1..8) buffer max:Max. Utilization of the tunneling buffer. Only tunnels whose buffer was used at all will be displayed</p> <p>Clear the buffer statistics: <pre>free clear</pre></p>

Telnet input	Description
<pre>tunnel [1..8]</pre>	<p>Shows active tunnel connections (without argument) or detailed information about the specified tunnel connection (with argument 1..8)</p> <pre># tunnel Tunnels open: 1/8 1: 00.02.246, closed 2: 00.02.247, open (CCID: 82) 3: 00.02.248, closed 4: 00.02.249, closed 5: 00.02.250, closed 6: 00.02.251, closed 7: 00.02.252, closed 8: 00.02.253, closed # tunnel 2 Tunnel 2.....: open (CCID 82) KNX address.....: 00.02.247 HPI control.....: 192.168.22.252:4808 HPI data.....: 192.168.22.252:4808 Connect. type.....: TUNNEL CONNECTION Communication.....: UDP CONNECTION TX tun req.....: 23169 TX tun re-req.....: 0 RX tun req.....: 821 RX tun re-req (identified): 0 RX tun req (wrong seq.)...: 0 Current tunnel buffer.....: 0 % Connected since (UTC).....: 16:26:16 29-01-2019</pre> <p>CCID: Connection ID of the tunnel connection KNX address: Tunneling address HPAI control: Control endpoint of the connection partner HPAI data: Data endpoint of the connection partner Connect. Type: Connection type tunnel or management connection Communication: UDP or TCP Connection TX tun req: Number of telegrams sent to the tunnel connection TX tun re-req: Number of telegrams that had to be repeated in the tunnel connections RX tun req: Number of telegrams received from the tunnel connections RX tun re-req: Number of telegrams received twice by the tunnel connections RX tun req (wrong seq.): number of frames received from the tunnel connections with wrong sequence number Current tunnel buffer: Utilization currently of the IP buffer of the tunnel Connected since (UTC): Time since the tunnel connection has been established.</p>
<pre>version</pre>	<p>Firmware version</p>
<pre>mask</pre>	<p>Mask version</p>
<pre>display [0 1]</pre>	<p>Query or change the display mode (0 = standard, 1 = inverted)</p>
<pre>tunaddr 1..8 address tunaddr reset tunaddr setall tunaddr help</pre>	<p>KNX address of a tunnel read (<code>tunaddr</code>) or change, e.g. <code>tunaddr 1 15.15.240</code>, set all tunnel addresses consecutively from a certain start address (<code>tunaddr setall 15.15.15</code>), or reset the KNX addresses of all tunnels to factory settings (<code>tunaddr reset</code>)</p> <pre># tunaddr 1: KNX address: 15.15.010 2: KNX address: 15.15.011 3: KNX address: 15.15.012 4: KNX address: 15.15.013 5: KNX address: 15.15.014 6: KNX address: 15.15.015 7: KNX address: 15.15.016 8: KNX address: 15.15.017</pre>
<pre>tunmode [std/tpblk]</pre>	<p>Read tunnel mode (without parameters) or set (<code>tp</code> or <code>tpblk</code>); <code>tunmode tpblock</code>: IP => KNX If same backbone forward to line frame KNX => IP If same sub line send to backbone</p>

Telnet input	Description
lock [0 1]	<p>Query lock status (without further parameters) or change (0 = off, 1 = on). Setting is identical to programming lock TP page, figure 13.</p> <p>A router can prevent the forwarding of physically addressed telegrams by filtering, i. It is not possible to reprogram devices across a line. This becomes interesting when using outdoor lines.</p> <p>However, e.g. if a KNX-USB interface is connected to an outdoor line directly to the bus, the router itself could be re-programmed, so that it forwards the physically addressed telegrams. With that, any access to the internal line is possible.</p> <p>This can be prevented with this telnet function. If you set telnet "lock" to 1, the router can no longer be programmed via the KNX line and corresponding activation of forwarding via KNX TP is no longer possible.</p>
topology [0 1]	<p>Query or change "topology check" (0 = off, 1 = on). Setting is identical to "Topology check", figure 15</p> <p>Subline Topology has been violated with 1.2.3 Last logged at 18:28:31 09-11-2018</p> <p>Mainline Topology has been violated with 1.2.3 Last logged at 18:24:31 09-11-2018</p>
Tunneltime [1.0..8.0]	<p>Query or change timeout for tunnel connection (1.0 to 8.0). Setting is identical to "slow connection", figure 14</p>
tunudp	<p>Query or change the type of tunnel connection for the ETS (0 = default, 1 = UDP only).</p>
date	<p>Show date and time</p>
sntp [query server IP]	<p>Send request to the NTP server (sntp query) or set the IP of the NTP server (sntp server 1.2.3.4)</p>
logmem	<p>Event memory in the device. Suitable for the development of clients. Read out for support requests.</p>
passwd oldpw newpw passwd oldpw passwd newpw	<p>Changes the current Telnet password (passwd), deletes the current password (old passwd) or sets a new password if none is currently set (new passwd)</p>
factory_reset	<p>Reset to factory settings and reboot</p>
reboot	<p>Reboot</p>
logout	<p>End Telnet session</p>


7.2 IP router

Telnet input	Description
lcconfig	<pre> Coupler type...: line coupler IP -> KNX: GA 0-13.....: route GA 14-15.....: filter GA 16-31.....: block Ph. addr.....: filter Broadcast.....: route KNX -> IP: GA 0-13.....: route GA 14-16.....: filter GA 16-31.....: block Ind.addr.....: filter Broadcast.....: route Check IA rout.: disabled Ind.Addr.tlg...: individually addressed telegrams are 3 times repeated </pre>
systembc [0 1]	<p>Set certain bits in the system broadcasts so that IP routing is possible even on older devices. By default, this compatibility mode is turned on.</p> <p>Wrong handling of bits in system broadcasts is 1 (on)</p>
sendack [0 1]	<p>Querying or changing every telegram (ACK). Setting is identical to the documentation to figure 13.</p>
blockfilter [0 1]	<p>Disable all group address filters (i.e., forward all) regardless of the settings of the ETS. Query or change (0 = off, 1 = on).</p>
routingcounter [0 1]	<p>Query or change routing counter handling (0 = default, 1 = behavior before 2018). This setting is identical to Enable routing algorithm (<2018), figure 15</p>

8 Terms

Term	Description
Backbone	For IP routers and IP interfaces, this is always the IP network.
Backbonekey	The routing protocol communicates in secure mode with encrypted telegrams. The key for encryption must be the same for all participants and is loaded into the device. The ETS generates the necessary backbone key on its own.
Encryption, encrypted	If devices send data information via the TP bus or IP network, they are generally readable by third parties. These only require access to the TP bus or IP network for reading. Encryption of the data in this context means that the contents of the telegrams are no longer to be interpreted if the encryption parameters (for example passwords) are unknown.
Key, Key Parameter	A series of numbers known only to the ETS project. These numbers are used to transform the data in both directions: encryption and decryption.
FDSK (Factory Default Setup Key)	The initial factory key. This key is used when commissioning the initial programming. A new key is loaded into the device, whereby this process is encrypted with the FDSK. The FDSK key is then no longer valid. It is reactivated only when resetting to factory settings.
Multicast	An IP address in the network over which all the routers of a backbone communicate. Tunnel connections do not need this address. Multicast connections are always established with the UDP protocol. Unlike TCP communication, an UDP telegram can always be lost. This is e.g. for WLAN connections very likely. Therefore, the routing backbone should always be realized with an Ethernet cable connection, as this is almost 100 % transmission safe.
Tunneling	A KNX point-to-point connection on the TCP / IP network, which is established with UDP or TCP protocol. Tunneling communication is reliable and has incorporated a link layer for that purpose. Therefore independent of the Ethernet connection, e.g. Cable or WLAN, and regardless of the TCP / IP protocol (UDP or TCP), no data is lost. With UDP, however, the restriction is that the data link layer works with a one-second timeout. This timeout can be adjusted in the advanced setup.
Telnet	A simple TCP server on port 23 that enables direct text-based communication with the IP device. Telnet is a de facto standard used at the window level, e.g. with "PuTTY" is addressed.
Abgesicherter Modus, Secure Mode	If the device is parameterized via the ETS so that the communication is only encrypted, this is referred to as secure mode.
Nicht abgesicherter Modus, Plain Mode	If the device is parameterized via the ETS so that the communication is only unencrypted, this is called unsecured mode.

9 Technical data

Symbols	 Must not be disposed of with household waste.
Rated voltage KNX	DC 21 ... 32 V SELV
KNX connection	Connection terminal
Current consumption	max. 20 mA
Power consumption	max. 1 W
IP communication	Ethernet 10/100 BaseT (10/100 Mbit/s)
IP connection	1 x RJ45
Resolution	128 x 64, OLED display
KNX Functions	IP router and IP interface: <ul style="list-style-type: none"> • KNX IP Secure Tunneling • Up to 48 telegrams per second • AES 128 encryption • Asymmetric key exchange for tunnel connections • UDP and TCP communication • Up to 8 tunnel connections • Up to 62 group address filters • APDU 248, parameterizable between 55 and 248 • TP telegram rate limit • TP bus voltage measurement (display telnet or display) IP router and IP interface: <ul style="list-style-type: none"> • KNX IP Secure Routing
Ambient temperature	-5 ... +45 °C
Installation width	36 mm (2 rail units)
Outer dimensions	35.0 mm x 89.6 mm x 62.9 mm (L x W x H)

10 Warranty

The warranty follows about the speciality store in between the legal framework as provided for by law.

11 Open Source Software

This product uses third-party software from the following authors:

Adam Dunkels adam@sics.se

Marc Boucher <marc@mbsi.ca> and David Haas dhaas@alum.rpi.edu

Guy Lancaster <lancasterg@acm.org>, Global Election Systems Inc.

Martin Husemann <martin@NetBSD.org>

Van Jacobson (van@helios.ee.lbl.gov)

Paul Mackerras, paulus@cs.anu.edu.au,

Christiaan Simons christiaan.simons@axon.tv

Jani Monoses jani@iv.ro

Leon Woestenberg <leon.woestenberg@gmx.net>

11.1 LWIP

Source: <https://savannah.nongnu.org/projects/lwip/>

Copyright (c) 2001-2004 Swedish Institute of Computer Science.

All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. 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.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR '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 AUTHOR 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. }