JUNG

Product documentation

IP router
Ref.-no.: IPR 300 SREG

IP interface
Ref.-no.: IPS 300 SREG

Table of Contents

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
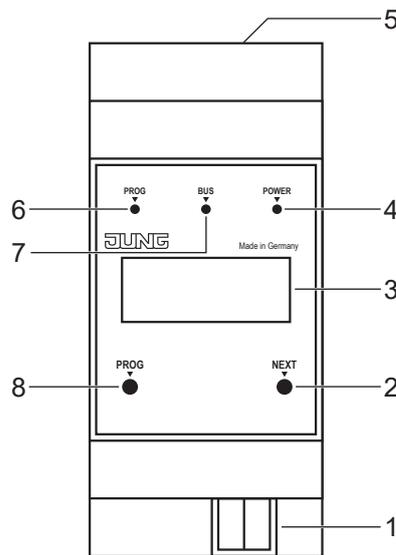
Fig. 1: Device components

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

The device can be updated. Firmware can be easily updated.

The device is KNX Data Secure capable. KNX Data Secure offers protection against manipulation in building automation and can be configured in the ETS project. Detailed specialist knowledge is required. A device certificate, which is attached to the device, is required for safe commissioning. During mounting, the certificate must be removed from the device and stored securely.

Planning, installation and commissioning of the device are carried out with the aid of the ETS, version 5.7 and above.

2.2 Intended use

2.2.1 IP router and IP interface

- Connection between KNX devices and PC or other data processing devices via IP
- Mounting on DIN rail according to EN 60715 in distribution boxes

2.2.2 IP interface

- Operation as data interface

2.2.3 IP router

- Operation as KNX area/line coupler or data interface

2.3 Product characteristics

2.3.1 IP router and IP interface

- Support of KNX Data Secure from ETS version 5.7 upwards
- Support of KNX IP Secure from ETS version 5.7 upwards
- 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

2.3.2 IP router

- KNXnet/IP routing for communication between KNX lines, areas and systems via IP network
- Telegram forwarding and filtering according to physical address or group address

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
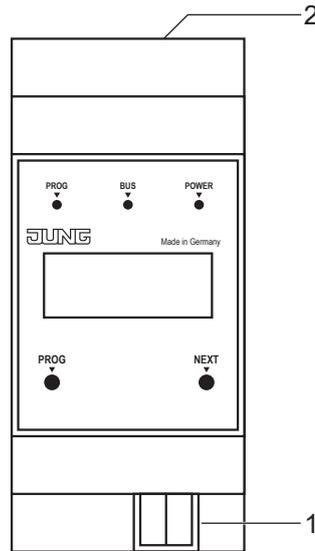
Fig. 2: Connection

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
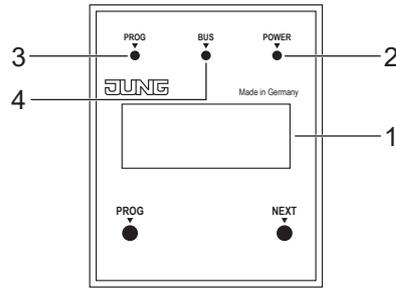
Fig. 3: Commissioning

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
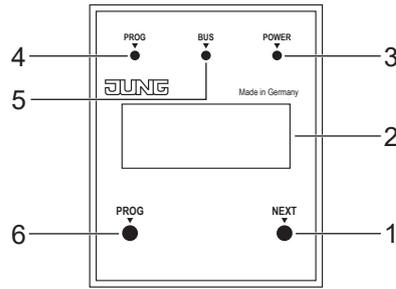
Fig. 4: Operation

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 IP Secure FDSK (Factory Default Setup Key)
  This is only displayed if the device is still in the delivery state.
- Page 5:
  Displaying the Data Secure FDSK (Factory Default Setup Key)
  This is only displayed if the device has not yet been set to secure mode.
- Page 6:
  Displaying the device time
  This is only displayed if the device has loaded the additional application.

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 lights up 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 Programming mode

Program device:

• Press PROG button.
  PROG LED lights up red.

Program product application:

• Press the PROG button again.
  PROG LED flashes red.

Terminate programming mode:

• Press the PROG button again.

5.4 Master reset

• Ensure that the device is switched off (disconnect bus voltage and power supply).
• Press PROG button, hold it and connect device.
  Device switches on.
• Hold PROG button until PROG LED flashes slowly (approx. 1 Hz).
• Release PROG button.
• Press PROG button again and hold it until PROG LED flashes fast (approx. 4 Hz).
  The master reset starts.
• Release PROG button.

6 Configuration

The devices comprise a combination of the following:

- KNX IP interface
- KNX IP interface - additional functions

or

- KNX IP router
- KNX IP router - additional functions

The additional functions can, for example, be used for the timer.

Both the devices are configured using ETS 5.

To use the complete functionality, product applications are necessary for both devices.

Both devices require a unique physical address.

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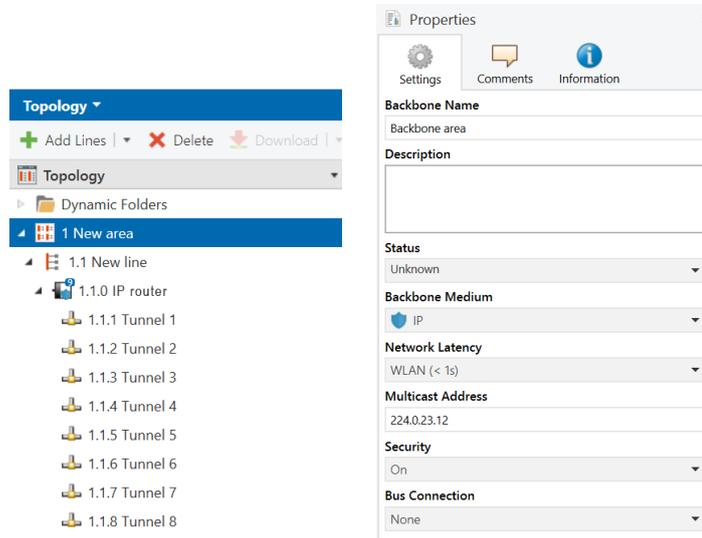
Fig. 5: Topology (left) and properties of the backbone

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
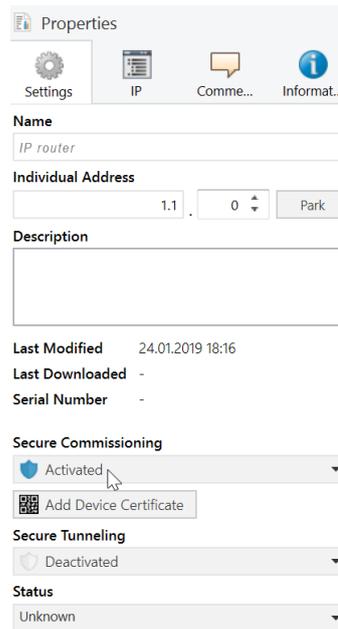
Fig. 6: Properties of the device

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
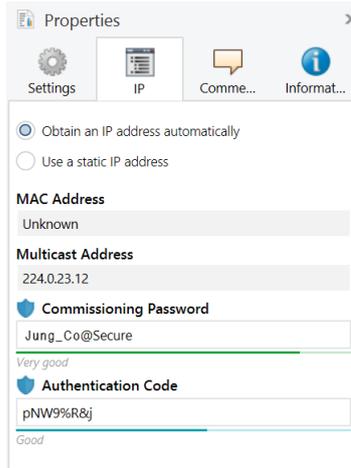
Fig. 7: IP Properties of the device

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.

ⓘ Document all passwords and store them securely.

6.2.4 KNX Data Secure

KNX Data Secure signs and encrypts the communication in KNX networks and provides a secured data transmission of telegrams.

The communication at commissioning processes with the ETS and the runtime communication between devices and visualisations is protected by KNX Data Secure. This ensures all KNX telegrams or just selected KNX telegrams to be authentificated and encrypted independent from the medium. The communication between transmitter and receiver can neither be interpreted nor manipulated.

Requirements:

- ETS 5.7.4 or higher
- FDSK entered/scanned or device certificate added

For KNX Secure commissioning, a device certificate is required, which is attached to the side of the device. Existing equipment which does not have a device certificate attached (IP Secure/Data Secure), show the certificate on the display. Further information can be found in the chapter "Display".

6.2.5 Additional functions
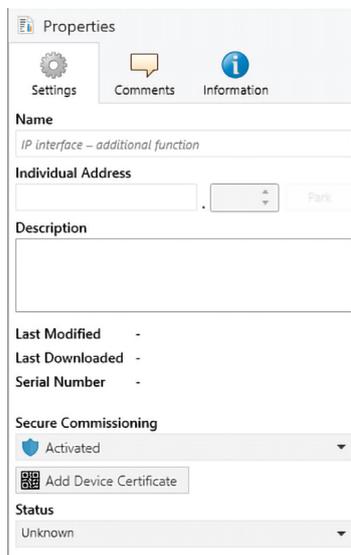
Fig. 8: Additional functions, properties of the device

Function	Description
Name	Any name can be assigned, max. 50 characters
Secure Commissioning	If activated, the encryption is active for commissioning: all parameters are then transmitted in encrypted form, although e.g. tunnel connections are still unencrypted.

Further functionalities are provided by the additional application.

- Timer
- Remote maintenance - IP interface only
- Mapper

Timer

- External timer server (NTP) as the source of time synchronisation when commissioning
- External time server can be set to a static IP address or via pool.ntp.org
- Status for the availability of the external time server
- Status for the validity of the internal clock (e.g. after power failure)
- User-controlled synchronisation with external time server

The timer synchronises the time of the integrated real time clock via the internet with pool.ntp.org or with another local source. This time can be issued to the KNX bus as a time or date telegram. When power fails, the device will buffer the time for approx. 36 hours. Every 48 hours and when restarting, the time automatically synchronises with the NTP server. Via a communisation object (referred to as KO below), the synchronisation can be requested manually by the user.

The "validity" of the time is issued via a separate KO. As long as the real time clock is power supplied, the time is valid. If, e.g., in normal operation a synchronisation is not possible because the internet connection is interrupted, the internal time continues to be valid. The last synchronisation failure can be checked via a separate KO using a reading request. If the status changes, this change will be issued on the bus.
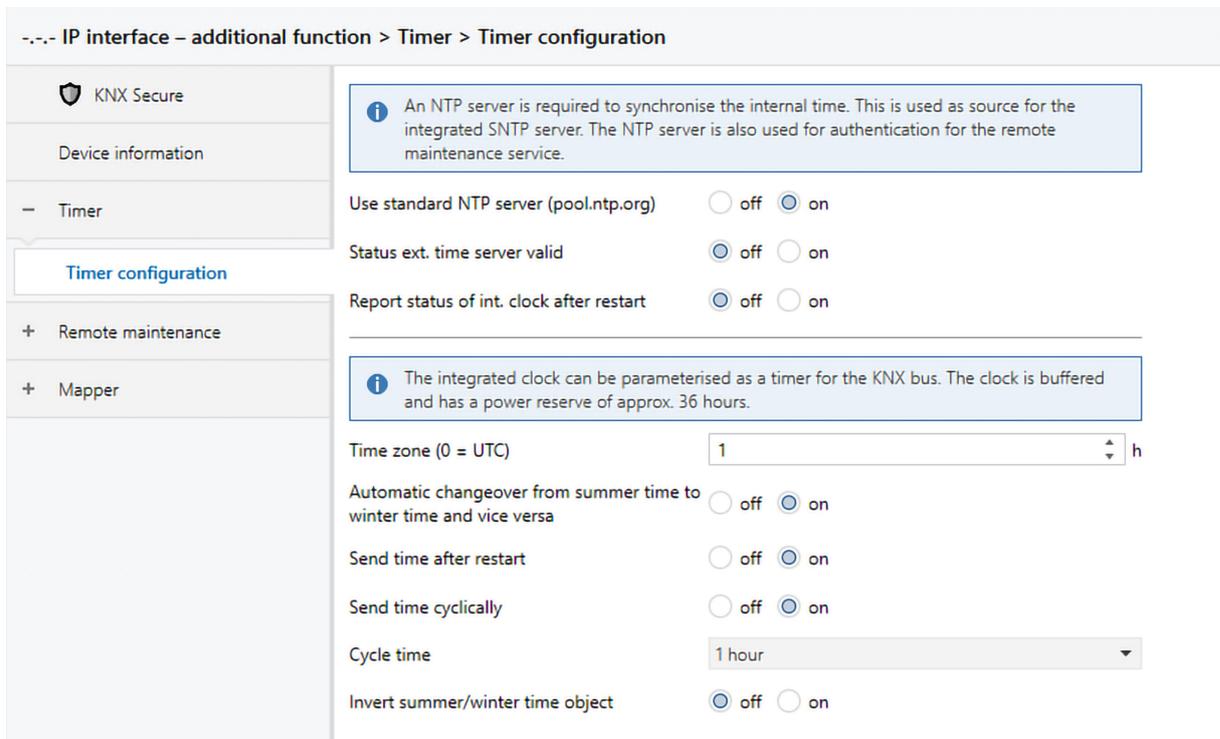
Fig. 9: Additional functions, Timer

Function	Options	Description
Use standard NTP server (pool.ntp.org)	off/<u>on</u>	See parameter dialogue If "off" is chosen here, an input field for the IP address of the own external time server is displayed.
Status ext. time server valid	<u>off</u>/on	Notification via KO1
Report status of int. clock after restart	<u>off</u>/on	Notification via KO2
Time zone (0 = UTC)	-12 ... <u>1</u> ... +14	Time lapse between internal time to UTC
Automatic changeover from summer to winter time and vice versa	off/<u>on</u>	
Send time after restart	off/<u>on</u>	Display of time and date via KO3, KO4, KO5

Function	Options	Description
Send time cyclically	off/<u>on</u>	
Cycle time	24 hours 12 hours <u>3 hours</u> 1 hour 30 minutes 15 minutes	Cyclical display of time and date via KO3, KO4, KO5

When shipping the device, the internal clock is invalid. Therefore the communication object KO2 is false [0]. The internal clock becomes valid (value = true [1]) once the device can reach an external time server (NTP server).

This happens after every restart but at least once a week automatically. For this to work, the NTP server specified has to be available.

After a restart or an ETS programming operation of the device, the time continues to be valid.

Only it the power reserve of the internal clock is low because the power was off for more than 36 hours, the time will again become invalid.

The internal clock can deviate approx. 1 second per 2 days from real time.

Mapper
- Translation of secure to plain communication objects.
- Mapping of up to 20 communication objects.
- Size of every communication object configurable between 1 bit, 2 bit, 4 bit , 8 bit, 16 bit, 24 bit, 32 bit, 6 bytes, 8 bytes and 14 bytes.

The mapper serves to translate secure to plain communication objects. For this, the mapper provides 20 channels, which communicate bidirectionally. The user can configure the communication objects in such a way that the group addresses have different lengths (max. 14 bytes).
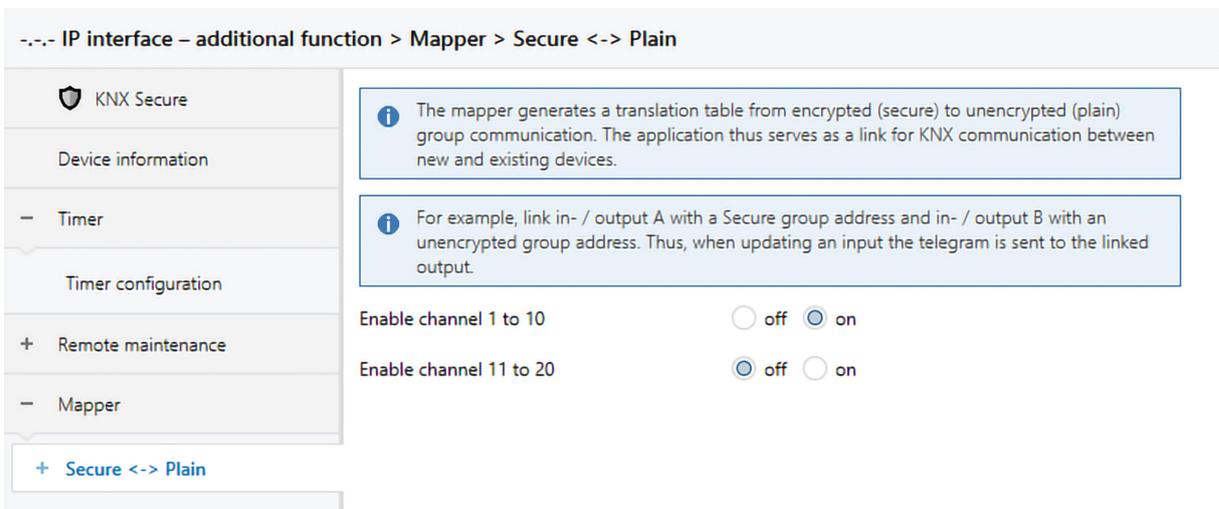
Fig. 10: Additional functions, Mapper

Function	Options	Description
Enable channel 1 to 10	off/<u>on</u>	see below
Enable channel 11 to 20	<u>off</u>/on	see below

The mapper serves to translate secure to plain communication objects. For this, the mapper provides 20 channels, which communicate bidirectionally. The user can configure the communication objects in such a way that the group addresses have different lengths (max. 14 bytes). The length can be configured between 1 bit, 2 bit, 4 bit , 8 bit, 16 bit, 24 bit, 32 bit, 6 bytes, 8 bytes and 14 bytes.

Mapper A → B

1/0/0 ——→ A   B • —→ 16/0/0

Mapper A ← B

1/0/0 ←—— • A   B • ←— 16/0/0
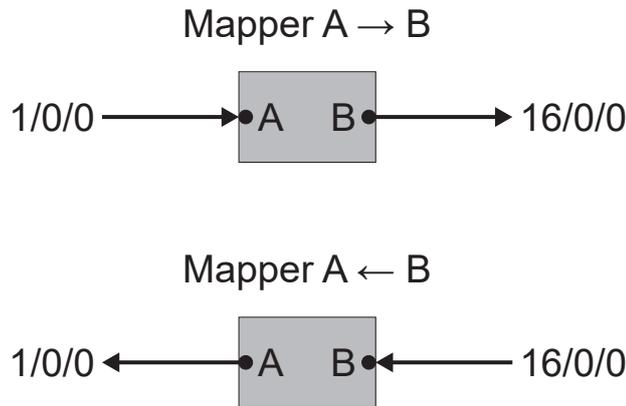
Fig. 11: Mapper writes on group addresses

Figure 11 shows the functionality described. Writing (or answering) to 1/0/0 (input/output A) triggers writing to 16/0/0 (input/output B). Therefore it is irrelevant whether 1/0/0 or 16/0/0 are encrypted or not. 1/0/0 could, for example, be an encrypted group address and 16/0/0 an unencrypted address. This way, one (or more) encrypted group addresses can be sent via an unencrypted one. The same is true the other way round. If several links according to the KNX regulation are used, it is important that a maximum of one group address is sending.

Mapper A → B

1/0/0 ⇄ A   B • —→ 16/0/0

Mapper A ← B

1/0/0 ←—— • A   B • ←⇄ 16/0/0
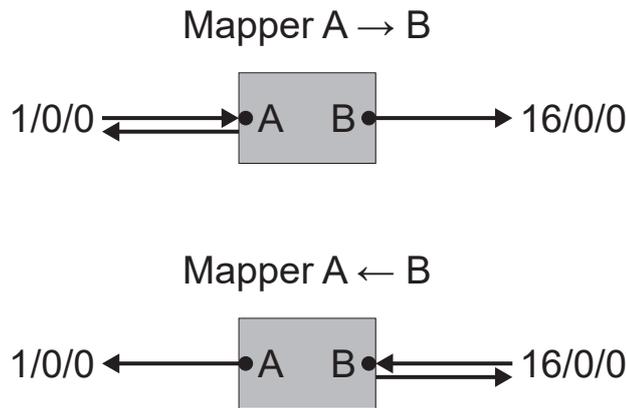
Fig. 12: Mapper reads on group addresses

Figure 12 shows the functionality described for reading. Reading via 1/0/0 (input/output A) triggers reading via 16/0/0 (input/output B). If the reading flag for input/output A is placed, the request of input/output A is answered with an answer telegram. If afterwards, the communication partners involved send an answer telegram, it will be treated as in figure 11. Therefore it is irrelevant whether 1/0/0 or 16/0/0 are encrypted or not. 1/0/0 could, for example, be an encrypted group address and 16/0/0 an unencrypted address. This way, a reading request of an encrypted group address can follow an unencrypted one. The same is true the other way round.

The application combines the mapper into the channels 1 to 10 and 11 to 20 for reasons of better overview. Every channel, containing both entries/exits A and B, can be configured to the length of choice.

ℹ️ The mapper only works with group addresses which are connected to another device. Group addresses which are connected to own communication objects, e.g. KO1 to KO13 will not be treated by the mapper in the way described.

Data length of mapper obj. 1	1 bit
Data length of mapper obj. 2	1 bit ✓
Data length of mapper obj. 3	2 bit
Data length of mapper obj. 4	4 bit
Data length of mapper obj. 5	1 byte
Data length of mapper obj. 6	2 byte
Data length of mapper obj. 7	3 byte
Data length of mapper obj. 8	4 byte
	6 byte
	8 byte
	14 byte
Data length of mapper obj. 9	1 bit
Data length of mapper obj. 10	1 bit
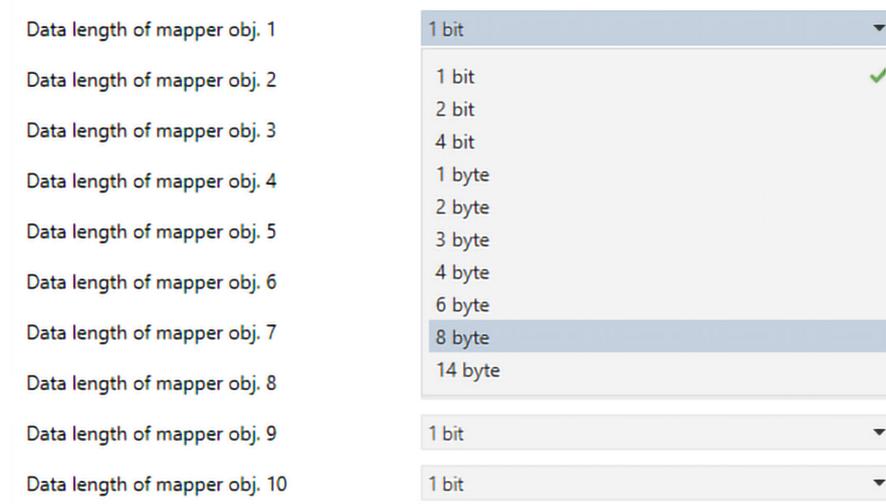
Fig. 13: Data length of mapper

Directions of communication:

Using the flags of the group addresses, directing group addresses through the mapper can be set to be dependant on the direction and on the kind of communication (reading or writing), The communication flags will have to be set as described in the table.

The communication flags for channel A are in column "Flags A" and for channel B in column "Flags B". Flags not listed do not have to be set. The direction of the arrows show in which direction the communication (reading or writing) is possible. A → B: A to B is the mapper direction possible as described in the table. There is no mapping of group addresses from B to A.

The communication flags found in ETS are sketched in figure 14.

In the table, the letters describe the same flags as in the ETS. C for example, for communication, R for reading etc.
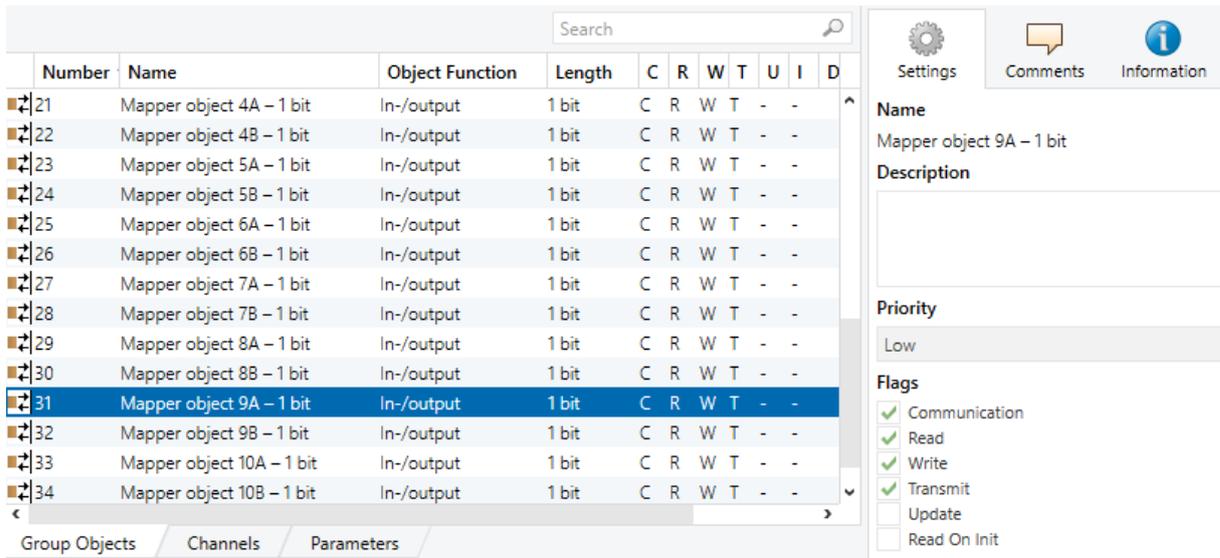
Fig. 14: Mapper flags

Directions	Reading	Writing	Flags A	Flags B
A ↔ B	yes	yes	CRWT--	CRWT--
A ↔ B	yes	–	CR-T--	CR-T--
A ↔ B	–	yes	C-WT--	C-WT--
A → B	yes	yes	CRW--	C-WT--
A → B	yes	–	CR----	C-WT--
A → B	–	yes	C-W---	C-WT--
A ← B	yes	yes	C-WT--	CRW---
A ← B	yes	–	C-WT--	CR----
A ← B	–	yes	C-WT--	C-W---

6.3 Device-specific parameters

6.3.1 IP interface

General settings

Fig. 15: 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	<u>off</u>/on	Advanced functions to ensure a maximum of flexibility.

Advanced settings

Fig. 16: 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.

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

Fig. 18: Preferred IP for Tunnelling

Function	Options	Description
Slow connection	off/on	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	1,0 ... 8,0 sec	Setting of timeout for tunnel connection over UDP
Preferred IP for tunnel X	off/on	Tunnel X should preferably be used for communication with the parametrized IP address.
End device IP	(IP-V4 address)	IP adress of end device

Additional function remote maintenance

Remote maintenance enables remote access via the KNX bus or connected KNX devices in place via an internet connection after customer approval.

In order to use it, a remote access license "IPS-L" will have to be purchased.

The connection is established via the IP interface. The data is completely encrypted and cannot be interpreted or changed. Remote maintenance works independent of the kind of internet connection (IPv4, IPv6) and requires no configuration of the local network environment.

The IP interface establishes a connection to the remote access server (RAS) after it is enabled via a communication object.

The ETS app JUNG IPS-Remote also automatically connects with the server and establishes the according connection. To establish an encrypted connection between the ETS and remote IP interface, the new data interface "IPS-Remote" can be used.

Further commissioning information can be found in the quick start guide on our website.

- Secure Tunnelling (encrypted) according to the KNX standard for the remote maintenance connection
- Switching between encrypted and unencrypted tunnelling without restart
- Maintaining connection when switching
- Status objects for Commissioning
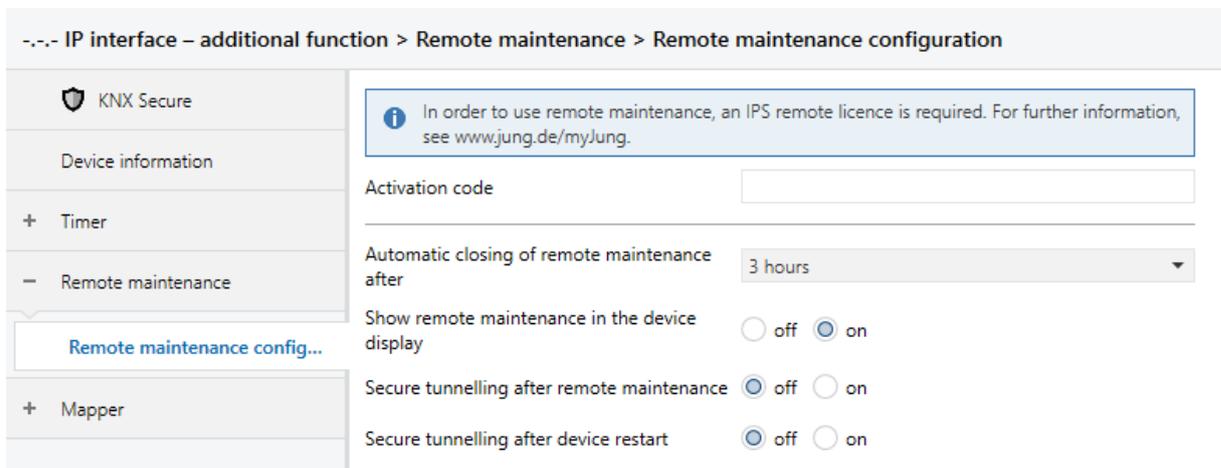
Fig. 19: Additional function remote maintenance

Function	Options	Description
Activation code	64 characters	available via MyJUNG
Automatic closing of remote maintenance	24 hours 12 hours 3 hours 1 hour 30 minutes 15 minutes	
Display remote maintenance on device	off/on	Notification via KO1
Secure tunnelling after remote maintenance	off/on	see below
Secure tunnelling after device restart	off/on	see below

In order to use remote maintenance, the main application of the IP interface has to be installed using secure commissioning. Secure tunnelling also has to be activated.

ⓘ Secure Tunnelling is required for remote maintenance.
  Establishing a connection with the solutions of visualisation continues to be possible as before.

• Activate secure commissioning under properties and add the device certificate.
• Then, activate secure tunnelling.

Further conditions for remote maintenance:

- uninterrupted internet connection on the PC used for commissioning and in the system in which the IP interface was installed
- firmware update of the IP interface to version 1.0.55 or higher was run
- licence for IPS-Remote (IPS-L) was purchased
- IP interface was securely commissioned (IP Secure)
    - Secure Tunnelling is active
- additional application loaded, physical address and application program transferred
    - Activation code for IPS-Remote transferred
    - Communication object 9: remote maintenance enabled and object connected
    - Communication object 2: internal clock valid
- ETS application for IPS-Remote loaded
    - synchronised locally with the IP interface for the first time
    - connected to IP interface after enabled via communication object

Expert knowledge:

When the power supply is interrupted, the remote maintenance connection is logged off or deactivated.

If enabled, the connection will be reestablished automatically after a restart.

The status of the remote maintenance can be seen of the display of the device (see figure 15).

If remote maintenance is active, the standard pages of the device will be shown (see chapter "Display")

During remote maintenance the display is active to show detailed information at any point in time.

When starting remote maintenance, the display shows:

Remote Access active
====================

If applicable, Secure Tunnelling will be turned on (automatically) and then the connection to the relay server will be established. If not, the device will try to establish the connection every 30 seconds until the time configured for "Automatic closing of remote maintenance" is up (see figure 15). At the same time, the display shows:

Remote Access active
====================
→ **RAS wait for reconnect**

If the connection to the relay server was established successfully, the display shows:

Remote Access active
====================
→ **Device secured**
→ **RAS opened**

If the ETS app IPS-Remote of the remote maintenance logs onto the device, the display additionally shows the following line:

Remote Access active
====================
→ **Device secured**
→ **RAS opened**
→ **Remote ETS opened**

If the ETS app JUNG IPS-Remote logs off (updating time lapse as for KO13, see there), the display shows:

Remote Access active
====================
→ **Device secured**
→ **RAS opened**
→ **Remote ETS closed**

In this case, the connection to the server is still established.

When remote maintenance via KO9 is turned off, the standard display of the device will become visible again (see chapter "Display").

6.3.2 IP router

General settings

Fig. 20: 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	<u>off</u>/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)   50   t/s

Fig. 21: 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).

Fig. 22: Preferred IP for Tunnelling

Function	Options	Description
Slow connection	off/on	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	1,0 ... 8,0 sec	Setting of timeout for tunnel connection over UDP
Preferred IP for tunnel X	off/on	Tunnel X should preferably be used for communication with the parametrized IP address.
End device IP	(IP-V4 address)	IP adress of end device

Advanced settings routing

1.1.0 KNX IP router > Advanced settings > Routing

IP settings	**Check of topology**
Advanced settings	ℹ️ 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.
Properties of the subline	
Standard tunnelling	ℹ️ The erroneous KNX address will be shown in the Telnet interface and on the display. The erroneous telegram will not be routed.
Routing	Check topology ⦿ off ◯ on
Filter	**Routing (before 2018)**
Physical address filter	ℹ️ If enabled, the router acts according to specification before 2018. This means different behaviour of routing count algorithm.
Group telegram filter	
Routing	ℹ️ If the router is used as replacement in existing installations, the old routing model might be necessary.
Tunnelling	Enable routing algorithm (<2018) ⦿ off ◯ on

Fig. 23: Routing

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

Physical address filter

1.1.0 KNX IP router > Filter > Physical address filter

IP settings	**Physically addressed telegrams**	
Advanced settings	IP => KNX	filter (default) ▼
Properties of the subline	KNX => IP	filter (default) ▼
Standard tunnelling	**Block broadcast telegrams**	
Routing	IP => KNX	⦿ off ◯ on
Filter	KNX => IP	⦿ off ◯ on
Physical address filter		
Group telegram filter		

Fig. 24: Physical address filter

Function	Options	Description
Physically addressed telegrams	<u>filter</u>, 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	<u>off</u>/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	IP => KNX
Advanced settings	Main group 0..13 — route
Properties of the subline	Main group 14..15 — filter
Standard tunnelling	Main group 16..31 — filter
Routing	Extended group address filter — ( ) off (●) on
Filter	KNX => IP
Physical address filter	Main group 0..13 — route
Group telegram filter	Main group 14..15 — filter
Ext. filter IP => KNX	Main group 16..31 — filter
Ext. filter KNX => IP	Extended group address filter — ( ) off (●) on
Routing	
Tunnelling	

Fig. 25: 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</u>/on	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</u>/on	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

Fig. 26: 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

6.4 Communication objects

ℹ️ Depending on the configuration, some object may not be available.

ID	Name	Object function	Length	Type	Flags
1	External time server valid – output	**Status**	1 bit	[1.2] DPT_Bool	CR-T--

Shows whether the external time server pool.ntp.org can be reached by the device. The DNS Server 9.9.9.9 is responsible for the name resolution. For more information, go to www.quad9.net. If using an own NTP time server, the IP address has to be known. In this case, the KO does not send. Every 2 days, the time is automatically synchronised with the external NTP server or when initiated by KO7. It the time server was not reachable during the last synchronisation, the status will be issued via this KO on the bus.

ID	Name	Object function	Length	Type	Flags
2	Internal clock valid – output	**Status**	1 bit	[1.2] DPT_Bool	CR-T--

Shows whether the internal clock is valid. Value true [1] represents valid, value false [0] invalid. The communication object can be sent automatically after every restart via the configuration.

When shipping the device, the communication object is false [0]. The clock becomes valid [value = true [1]) if the device can synchronise its time via an NTP server. After a restart or an ETS programming operation of the device, the value continues to be true [1]. Only if the internal buffer capacitor is too low on power because the power was off for several days, the time will again become invalid (value = false [0]).

ID	Name	Object function	Length	Type	Flags
3	Time – output	**Time output**	3 bytes	[10.001] DPT_ TimeOf Day	CR-T--

Communication object for outputting the current time to the bus. The internal clock is buffered internally for approx. 1.5 days (via supercap capacitor). The internal clock can deviate approx. 1 second per 2 days from real time. A reading telegram always delivers the current time.

ID	Name	Object function	Length	Type	Flags
4	Date – output	**Date output**	3 bytes	[11.001] DPT_ Date	CR-T--

Communication object for issuing the calendar of the internal clock.

ID	Name	Object function	Length	Type	Flags
5	Date and time – output	**Date and time output**	8 bytes	[19.001] DPT_ DateTime	CR-T--

Time and date for outputting the current time and date to the bus.

ID	Name	Object function	Length	Type	Flags
6	Date/time – input	**Requesting**	1 bit	[1.017] DPT_ Trigger	C-WT--

Trigger for writing of KO3, KO4 and KO5. It triggers writing with 0 as well as 1.

ID	Name	Object function	Length	Type	Flags
7	NTP server synch. – input	**Requesting**	1 bit	[1.017] DPT_ Trigger	C-WT--

Every 2 days, the internal clock is automatically synchronised with the external NTP server or when initiated by this KO. It triggers writing with 0 as well as 1.

ID	Name	Object function	Length	Type	Flags
8	Summer / winter time - output	**Status**	1 bit	[1.xxx]	CR-T--
	If summer time is active, this KO is set to 0, if winter time to 1. This KO is therefore directly usable for the change to winter configuration of heating systems.				

ID	Name	Object function	Length	Type	Flags
9	Enable remote maintenance – input	**Switching**	1 bit	[1.002] DPT_ Switch	CRWT--
	Turning on remote maintenance (1) or stopping remote maintenance (0): When the user opens the remote maintenance access via this KO, Secure Tunnelling is enabled for this duration. The interface connects to the relay server. There is no decryption on the cloud. The customer's connection can be either IPv4 or IPv6.				

ID	Name	Object function	Length	Type	Flags
10	Activation code valid – output	**Status**	1 bit	[1.2] DPT_Bool	CR-T--
	Shows true [1] if the device was fed with a valid activation code at least once and if remote maintenance is generally possible. Otherwise the value is false [0].				

ID	Name	Object function	Length	Type	Flags
11	Secure mode active – output	**Status**	1 bit	[1.2] DPT_Bool	CR-T--
	Shows true [1] if the IPS 300 SREG was commissioned securely and secure (encrypted) tunnelling in the interface application was activated. Otherwise the value is false [0].				

ID	Name	Object function	Length	Type	Flags
12	Server connection – output	**Status**	1 bit	[1.2] DPT_Bool	CR-T--
	If the connection to the relay server is established, this KO turns true [1] otherwise false [0].				

ID	Name	Object function	Length	Type	Flags
13	Secure tunnelling active – output	**Status**	1 byte	[5.1] DPT_ Scaling	CR-T--
	Status of Secure Tunnellings: false [0] = inactive, true [1] = active Inactive means that the unencrypted tunnelling connection can be established.				

ID	Name	Object function	Length	Type	Flags
14	Programming of remote maintenance active – output	**Status**	1 bit	[1.2] DPT_Bool	C--T--
	If remote maintenance is established to the IPS 300 SREG from the computer of the installer (ETS), this is true [1], otherwise false [0]. In general, it takes approx. 10 seconds for the connection to the device to be completely closed. Normally, a time lapse can be observed between the output of the KOs and the display in the group monitor.				

ID	Name	Object function	Length	Type	Flags
15	MapperObjekt channel A - Field length	**In-/output**	1 bit to 14 bytes	n/a	CRWT--
When writing or answering on this KO, the value will be written on the KO of channel B on the bus. Here, the encryption of the individual channels is taken into consideration. When reading is requested, the request will be answered. At the same time a reading request is issued to channel B.					

ID	Name	Object function	Length	Type	Flags
16	MapperObjekt channel B - Field length	**In-/output**	1 bit to 14 bytes	n/a	CRWT--
When writing or answering on this KO, the value will be written on the KO of channel A on the bus. Here, the encryption of the individual channels is taken into consideration. When reading is requested, the request will be answered. At the same time a reading request is issued to channel B.					

7 Advanced configuration

7.1 Configuration tool

This software simplifies the configuration of the device and provides detailed information about the device for error analysis.

If the device is in secure mode, the configuration tool can not connect to the device.

7.1.1 IP router and IP interface

Device connection
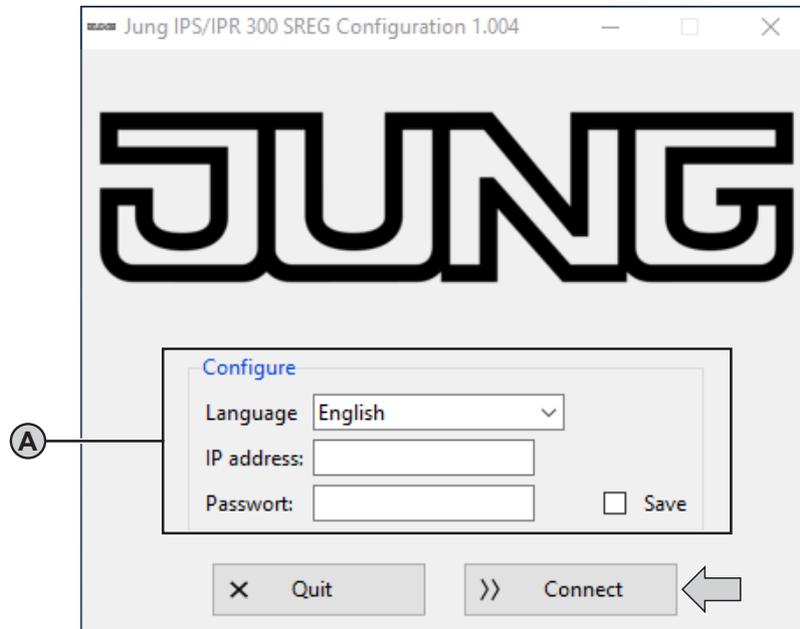
Fig. 27: Device connection

Requirements:
- device connected and booted
- configuration tool started

Configure (A)

Changing language:

- Select language.
  Configuration tool is shown in selected language.

Connecting device for device configuration:

- Enter IP address of device.
  The IP address is shown on the display of the device or can be located as follows:
  Static IP address: see ETS
  Dynamic IP address: see DHCP server
- Enter password.
  The default password is "knxsecure".
  The entered password can be saved, so it must not be entered again after the next start of the configuration tool.
- Select "Connect".
  Device is connecting.
  Device configuration is shown.

Device configuration

The IP router provides more configuration possibilities than the IP interface.

Therefore the following figure exemplarily shows the configuration of the IP router only.
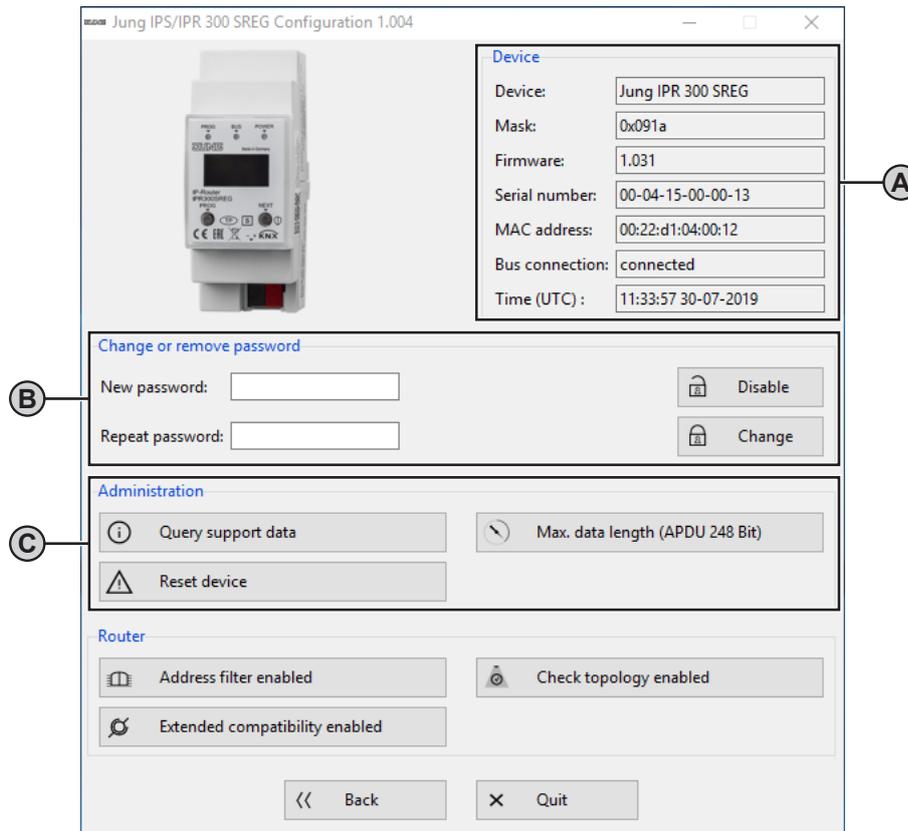
Fig. 28: Device configuration – IP router and IP interface

Requirement:

- device connected

Device (A)

Shows current properties of the device.

Change or remove password (B)

Changing password:

- Enter new password and repeat input.
- Confirm new password with "Change".
  Password is changed.

Removing password:

- Select "Disable".
  Password is removed.

Administration (C)

Saving device information for error correction:

- Select "Query support data".
  A text file with device information is saved in the main folder of the software.
  Example path: C:\Programs\ConfigTool\

Performing master reset for restoring of default settings:

- Select "Reset device".
  Master reset is performed.
  Configuration tool is restarting.

Selecting min. / max. length of telegrams for error correction of third party products:

- Select "Max. data length (APDU 248 Bit)" or "Min. data length (APDU 55 Bit)".
  Telegram length is adjusted.

7.1.2 IP router

Device configuration
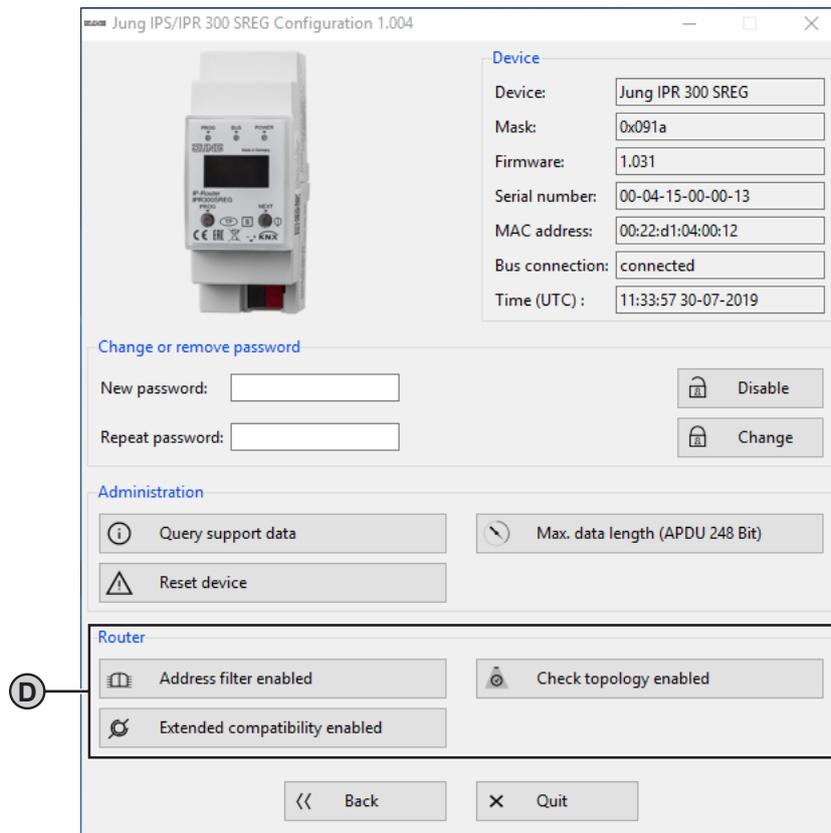
Fig. 29: Device configuration – IP router

Router (D)

ⓘ This area will only be shown, if the configuration tool is connected with an IP router.

Deactivating address filters <u>temporary</u> for error correction:

- Select "Address filter enabled".
  Address filters are deactivated.
- Correct cause of error.
- Select "Address filter disabled".
  Address filters are activated.

Checking physical addresses of all devices in the line:

- Select "Check topology enabled".
  All devices in the line are checked.
  Incorrect physical address is shown in telnet interface, on the display of the device and is saved in the text file with device information.
  Telegram is forwarded independent of address filters.

Improving compatibility to third party products:

- Select "Extended compatibility enabled".
  Compatibility to third party products is improved.

7.2 Use cases

7.2.1 IP router and IP interface

Mapper

The practical use of the mapper is outlined in the following scenario:

A system comprises an inner and outer line. To increase the security of the system, it was decided to convert the outer line to Secure. Opening or closing a garage door, for example, is done via KNX and secure communication. In this example the group addresses 17/2/1, 17/2/2 und 17/2/3 are used. These are inserted into the inner line via two routers. The devices are these functions in the group communication 1/2/1, 1/2/2 und 1/2/3. The inner line, however, only has unencrypted actuators and sensors. The mapper maps the group addresses 17/2/1 to 1/2/1, 17/2/2 to 1/2/2 and 17/2/3 to 1/2/3. For this reason, only the devices on the inner line can only communicate with the outer line. Routing the main group 17 but main group 2 is blocked can be set via the routing. In this way, the security of the outer line can be combined with the inner line easily.

7.2.2 IP interface

Remote maintenance

An encrypted or normal access via the tunnelling connection can be ensured setting the parameters "Secure Tunnelling after device restart" or "Secure Tunnelling after remote maintenance". The visualisation has be activated consciously and has to support all attributes of the encrypted tunnelling connection.

For the usual access (e.g. Smart Visu Server) both parameters have to be set to "off".

For encrypted access (e.g. JUNG Visu Pro), both parameters have to be set to "on".

7.3 Telnet interface

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.

7.3.1 IP router and IP interface

Telnet input	Description
`help`	Displays all available commands

`ifconfig`	Displays network parameters
	
	```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```
	
	Sys multicast: Multicast address for System telegrams
	
	RT multicast: Multicast address für routingt telegrams

`ifconfig [help|dhcp|ip |mask]`	Set network parameters via the telnet interface.
	Expamples:
	
	Setting IP Addresse with DHCP:
	  `ifconfig dhcp`
	Statically set the IP address to 192.168.1.2 (in this case, the gateway and mask should also be adapted, see below)
	  `ifconfig ip 192.168.1.2`
	Set the gateway to 192.168.1.1:
	  `ifconfig gw 192.168.1.1`
	Set the mask to 255.255.255.0:
	  `ifconfig mask 255.255.255.0`

Telnet input	Description

`tpconfig`	Shows KNX parameters
	
	`KNX bus state.: up`
	`KNX address...: 15.15.000`
	`Serial number.: 00-a6-00-00-00-01`

`tpconfig [help|set]`	Set KNX parameters via the telnet interface. Set the TP address to 1.1.0: `tpconfig set 1.1.0`
`progmode [0|1]`	Query or change programming mode (0 = off, 1 = on)

`apdu [55..248]`	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.
	
	`# apdu`
	`maximal len of a KNX telegram 248.`
	`Usage: apdu [55 .. 248]`

`tpratemax [5..50]`	Read or configure maximum telegram rate (IP => TP); 50 T / s corresponds to 100 % bus load.
	
	`# tpratemax`
	`no limit, sending with maximum performance to TP.`
	`Usage: tpratemax [5 .. 50]`

`stats`	Shows various statistics on device and bus status
	
	`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 %)`
	
	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)

Telnet input	Description

`free [clear]`	Shows statistics about the memory usage
	
	`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 %`
	
	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
	
	Clear the buffer statistics:
	`free clear`

Telnet input	Description
`tunnel [1..8]`	Shows active tunnel connections (without argument) or detailed information about the specified tunnel connection (with argument 1..8) ```# 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 HPAI control.............: 192.168.22.252:4808 HPAI 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``` 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.
`version`	Firmware version
`mask`	Mask version
`display [0|1]`	Query or change the display mode (0 = standard, 1 = inverted)

`tunaddr 1..8 address`
`tunaddr reset`
`tunaddr setall`
`tunaddr help`
	KNX address of a tunnel read (`tunaddr`) or change, e.g. `tunaddr 1 15.15.240`, set all tunnel addresses consecutively from a certain start address (`tunaddr setall 15.15.15`), or reset the KNX addresses of all tunnels to factory settings (tunaddr reset)
	
	``# 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```

`tunmode [std/tpblk]`	Read tunnel mode (without parameters) or set (`tp` or `tpblk`); `tunmode tpblock`: IP => KNX If same backbone forward to line frame KNX => IP If same sub line send to backbone

Telnet input	Description
`lock [0|1]`	Query lock status (without further parameters) or change (0 = off, 1 = on). Setting is identical to programming lock TP page, figure 13. 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. 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. 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.

`topology [0|1]`	Query or change "topology check" (0 = off, 1 = on). Setting is identical to "Topology check", figure 15
	
	`Subline Topology has been violated with 1.2.3`
	`Last logged at 18:28:31 09-11-2018`
	
	`Mainline Topology has been violated with 1.2.3`
	`Last logged at 18:24:31 09-11-2018`

`Tunneltime [1.0..8.0]`	Query or change timeout for tunnel connection (1.0 to 8.0). Setting is identical to "slow connection", figure 14
`tunudp`	Query or change the type of tunnel connection for the ETS (0 = default, 1 = UDP only).
`date`	Show date and time
`busload`	Shows the busload of the last minute / last 5 minutes / last 15 minutes / since start and also the maximum load with date and time
`sntp [query|server IP]`	Send request to the NTP server (sntp query) or set the IP of the NTP server (`sntp server 1.2.3.4`)
`logmem`	Event memory in the device. Suitable for the development of clients. Read out for support requests.

`passwd oldpw newpw`
`passwd oldpw`
`passwd newpw`
	Changes the current Telnet password (passwd), deletes the current password (old passwd) or sets a new password if none is currently set (new passwd)

`factory_reset`	Reset to factory settings and reboot
`reboot`	Reboot
`logout`	End Telnet session

7.3.2 IP router

Telnet input	Description

`lcconfig`	```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```

`systembc [0|1]`	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. ```Wrong handling of bits in system broadcasts is 1 (on)```
`sendack [0|1]`	Querying or changing every telegram (ACK). Setting is identical to the documentation to figure 13.
`blockfilter [0|1]`	Disable all group address filters (i.e., forward all) regardless of the settings of the ETS. Query or change (0 = off, 1 = on).
`routingcounter [0|1]`	Query or change routing counter handling (0 = default, 1 = behavior before 2018). This setting is identical to Enable routing algorithm (<2018), figure 15

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.
Secure Tunnelling	Secure Tunnelling means that the tunnelling connection can be transferred as encrypted.
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: • 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: • KNX IP Secure Routing
Ambient temperature	−5 ... +45 °C
Storage/transport temperature	−25 ... +70 °C
Relative humidity	max. 95 %
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 specialty 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.}