

IPsecure Router KNX 9070770 Product Manual



IPsecure Router KNX

Contents

Contents	Page
1 General.....	3
1.1 Using the product manual	3
1.2 KNXnet/IP Security	3
1.2.1 Notes.....	4
1.3 Product and functional overview	5
1.3.1 Monitoring for bus voltage failure.....	6
1.3.2 Overview of versions	6
2 Device technology.....	7
2.1 Technical data	7
2.2 Connection diagram	9
2.3 Dimension drawing	10
2.4 Mounting and installation	11
2.5 Description of inputs and outputs.....	14
2.6 Operating controls.....	15
2.7 Display elements	15
3 Commissioning.....	17
3.1 Overview.....	17
3.2 Parameters	18
3.2.1 Parameter window <i>KNX -> LAN</i>	18
3.2.1.1 Parameter window <i>LAN -> KNX</i>	21
3.2.1.2 Parameter window <i>IP settings</i>	24
3.3 Group objects	30
3.4 Use of the integrated tunneling servers	30
3.4.1 Settings in ETS 5.....	31
3.5 KNX Secure.....	32
4 Planning and application	33
4.1 The IPsecure Router in the network	33
4.1.1 Assignment of IP address	33
4.1.2 KNX telegrams in the network	34
4.1.3 Monitoring.....	35
4.1.4 System broadcast	35
4.1.5 IGMP	35
4.1.6 IPsecure Router as an area coupler	36
4.1.7 IPsecure Router as a line coupler	37
4.1.8 Mixed topology.....	38
4.2 The IP Tool	39
5 Contact	41
6 Open source software components (OSS).....	43

IPsecure Router KNX

General

1 General

The Theben IPsecure Router connects the KNX bus with an Ethernet network. KNX telegrams can be sent to or received from other devices via the network. The device supports the KNX Secure protocol (KNXnet/IP Security).

1.1 Using the product manual

This manual provides detailed technical information on the function, installation and programming of the Theben KNX device. The application is explained using examples.

This manual is divided into the following chapters:

Chapter 1	General
Chapter 2	Device technology
Chapter 3	Commissioning
Chapter 4	Planning and application
Chapter A	Appendix

1.2 KNXnet/IP Security

The device should always be operated in KNX Secure mode. This ensures security for runtime communication on the IP backbone, for the tunneling servers and for commissioning the device itself.

See also chapter, [KNX Secure](#).

1.2.1

Notes

Notes and safety instructions are represented as follows in this manual:

Note

Tips for usage and operation

Examples

Application examples, installation examples, programming examples

Important

These safety instructions are used as soon as there is danger of a malfunction without risk of damage or injury.

Attention

These safety instructions are used as soon as there is danger of a malfunction without risk of damage or injury.

 Danger

These safety instructions are used if there is a danger to life and limb with inappropriate use.

 Danger

These safety instructions are used if there is an extreme danger to life with inappropriate use.

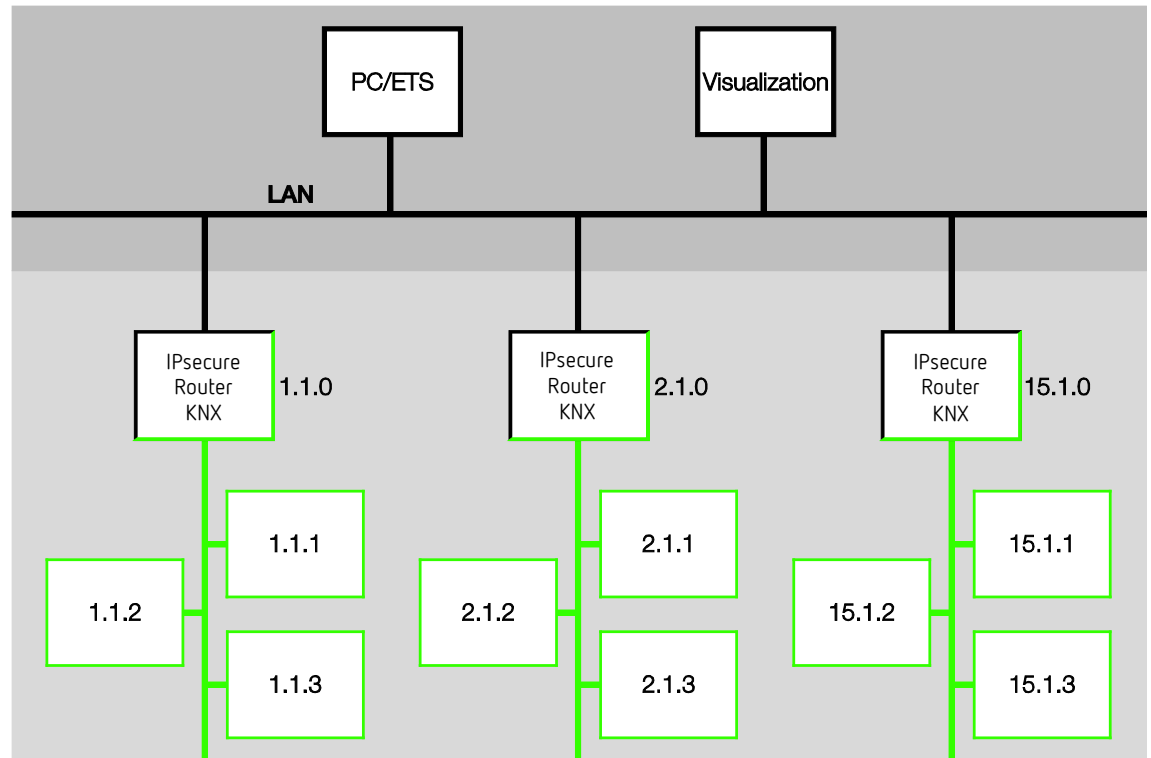
IPsecure Router KNX

General

1.3 Product and functional overview

The Theben IPsecure Router connects the KNX bus with an Ethernet network. KNX telegrams can be sent to or received from other devices via the network.

The device uses the KNXnet/IP protocol from the KNX Association (routing and tunneling) for communication.



The Router features five tunneling servers, see chapter [Use of the integrated tunneling servers](#). They support both bus monitor and group monitor mode. The tunneling servers can be operated in KNX Secure mode.

In addition to KNX standard multicast communication, up to ten Theben IP Routers KNX can communicate with each other via the unicast protocol, see chapter [KNX telegrams in the network](#). KNX Secure mode is not available in this case. The power supply can be implemented via PoE (Power over Ethernet) according to IEEE 802.3af class 1 or via a supply voltage.

The Theben IP Tool is available for the IPsecure Routers. It allows the Routers to be found in the network (IP discovery), the settings to be made for unicast communication and the firmware to be updated if necessary, see chapter [The Theben IP Tool](#).

An ETS app (KNX Bus Update) is available for the firmware update. If KNX Secure mode is not activated for the devices, a firmware update can also be performed with the IP Tool.

During the update process, the KNX bus (TP) must be connected in addition to the IP network (LAN) so that the KNX parameters can be restored correctly. Otherwise, the update process will fail.

It must be ensured that no voltage failure (KNX or IP) occurs during the update process, otherwise the device can be destroyed.

The device supports the KNX standard function "Monitoring for bus voltage failure". This is a network management function, which is used by visual display systems, for example (see chapter [Monitoring for bus voltage failure](#)).

IPsecure Router KNX

General

1.3.1 Monitoring for bus voltage failure

The IPsecure Router monitors the KNX TP bus for voltage failure. When the status of the bus voltage changes, a broadcast command of the type "NetworkParameterWrite" is sent on the IP network.

The following values are sent:

- Bus voltage failure: "00063301" (hex)
- Bus voltage recovery: "00063300" (hex)

These telegrams can be evaluated, e.g. by a visual display system.

Type	Info	Meaning
NetworkParameterWrite	00 06 33 01	TP1 bus voltage failure
NetworkParameterWrite	00 06 33 00	TP1 bus voltage recovery

1.3.2 Overview of versions

Device	IPsecure Router KNX	
Application	IPsecure Router KNX	IPsecure Router KNX
ETS	ETS 4/5	ETS 5
Properties of IP Router		
Number of tunneling servers	5	5
Number of unicast connections	10	10
Monitoring for bus voltage failure (see chapter Monitoring for bus voltage failure .)	■	■
Filter Group telegrams main group 0...31	■	■
IP discovery (IP Tool)	■	■
Firmware update (IP Tool)	■	■*
Firmware update with KNX Bus Update app	-	■
Unicast parameterization (IP Tool)	■	■*
KNX secure	-	■
Power over Ethernet	■	■
KNXSecure	-	■

■ = property applies

- = property does not apply

* Only if the device is not operated in KNX Secure mode

IPsecure Router KNX

Device technology

2 Device technology



IPsecure Router KNX

IPsecure Router is the interface between KNX installations and IP networks. It can be used as a line coupler or area coupler and can utilize the local network (LAN) for exchange of telegrams between lines/areas.

KNX devices can be programmed via LAN using ETS (five tunneling servers are available). The device uses the KNXnet/IP protocol from the KNX Association (routing and tunneling).

Alternatively, the device can communicate via unicast.

The device is powered by 12 to 30 V DC or PoE (Power over Ethernet) to IEEE 802.3af class 1.

2.1 Technical data

Supply	Auxiliary voltage U_s	12...30 V DC (+10% / -15%) or PoE (IEEE 802.3af class 1)
	Power dissipation	Maximum 1.8 W
	Auxiliary voltage, current consumption	Maximum 120 mA at 12 V
	Rated voltage U_n	12 V DC
	Current consumption KNX	< 10 mA
Connections	KNX	Bus connection terminal
	Operating voltage	Plug-in terminal
	LAN	RJ45 socket for 10/100BaseT, IEEE 802.3 networks, AutoSensing
Operating and display elements	Red LED and button	For assignment of the physical address
	Green "On" LED	Operation readiness indicator
	Yellow "LAN/Link" LED	Network connection indicator
	Yellow "Telegram" LED	KNX telegram traffic indicator
Protection degree	IP 20	To DIN EN 60 529
Protection class	II	To DIN EN 61 140
Isolation category	Overvoltage category	III according to DIN EN 60 664-1
	Pollution degree	2 according to DIN EN 60 664-1
KNX safety extra low voltage	SELV 30 V DC	
Temperature range	Operation	-5...+45 °C
	Storage	-25...+55 °C
	Transport	-25...+70 °C
Ambient conditions	Maximum air humidity	95 %, no condensation allowed
	Atmospheric pressure	Atmosphere up to 2,000 m

IPsecure Router KNX

Device technology

Design	Modular installation device (MDRC)	Modular installation device, ProM
	Overall dimensions	90 x 36 x 64 mm (H x W x D)
	Mounting width	2x 18 mm modules
	Mounting depth	68 mm
Installation	On 35 mm mounting rail	To DIN EN 60 715
Mounting position	Any	
Weight	0.1 kg	
Housing, color	Plastic, halogen free, gray	
Approvals	KNX to EN 50 090-1, -2	
CE mark	In accordance with the EMC directive and low voltage directive	

Device type	Application	Maximum number of communication objects	Maximum number of group addresses	Maximum number of assignments
IPsecure Router KNX	IPsecure Router / ...*	0	0	0

* ... = Current version number of the application. Please refer to the software information on our website for this purpose.

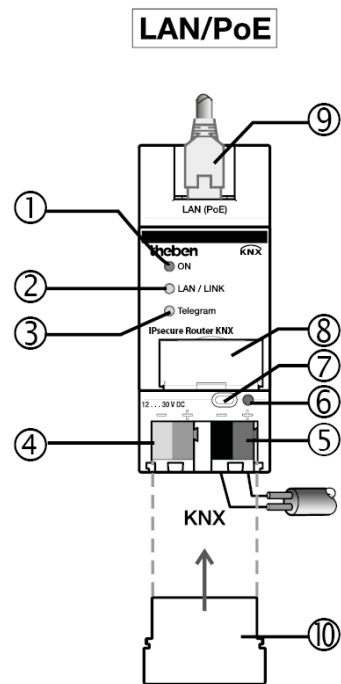
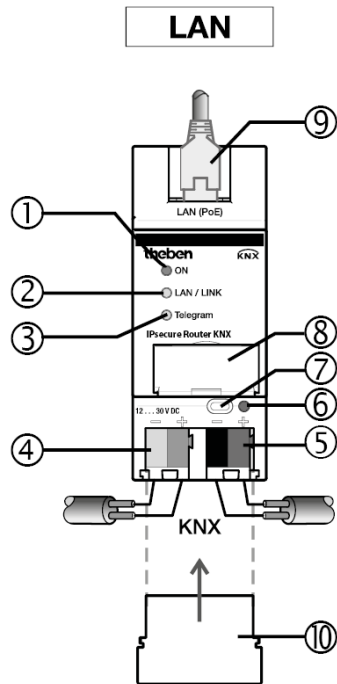
Note
ETS 5 and the current version of the device application are required for programming. If the device is to be operated in KNX Secure mode, the commissioning key (FDSK; see chapter, KNX Secure) on the side of the unit will be required as well. The latest version of the application and corresponding software information are available for download from www.theben.de/en/downloads_en. After import into ETS, it appears in the <i>Catalogs</i> window under <i>Manufacturers/THEBEN AG/System components/IP Router</i>. The device does not support the locking function of a KNX device in ETS. If you use a <i>BCU code</i> to inhibit access to all the project devices, it has no effect on this device. Data can still be read and programmed. Exception: When KNX Secure mode is activated, the device can no longer be programmed with a different ETS.

IPsecure Router KNX

Device technology

2.2

Connection diagram

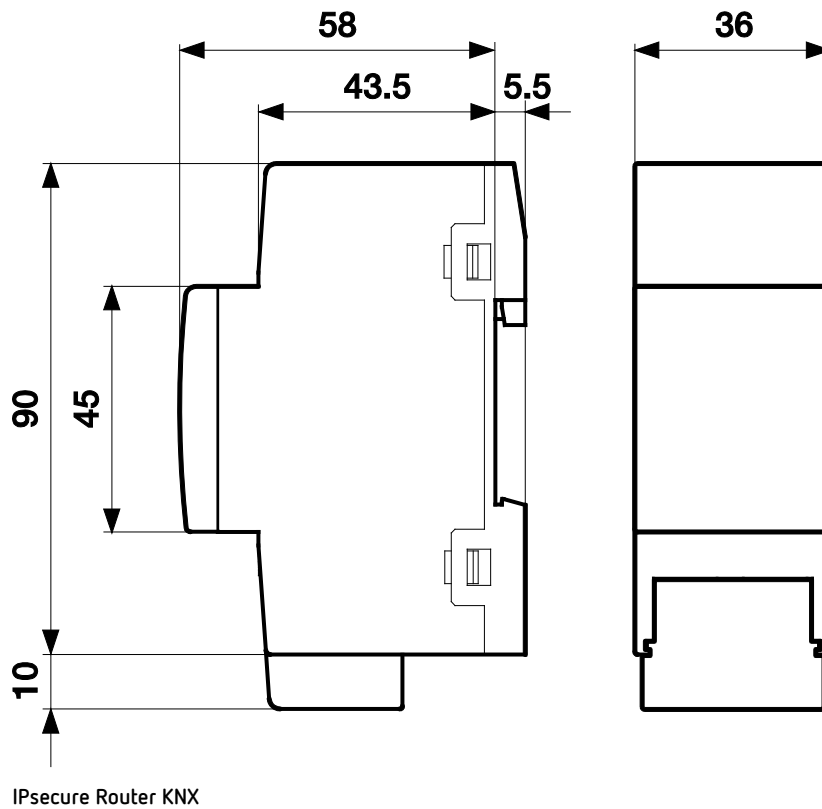


IPsecure Router KNX

- 1 *ON* LED
- 2 *LAN / LINK* LED
- 3 *Telegram* LED
- 4 Power supply connection
- 5 KNX connection

- 6 *Programming* LED
- 7 *Programming* button
- 8 Label carrier
- 9 LAN or LAN/PoE connection
- 10 Cover cap

2.3 Dimension drawing



2.4 Mounting and installation

The device is a modular installation device for quick installation in distribution boards on 35 mm mounting rails to DIN EN 60 715.

The installation position can be selected as required.

The connection to the bus is implemented using the supplied bus connection terminal. The terminal assignment is located on the housing.

The device is ready for operation after connecting the bus voltage and the auxiliary voltage.

Accessibility to the device for the purpose of operation, testing, visual inspection, maintenance and repair must be provided compliant to DIN VDE 0100-520.

Commissioning requirement

A PC with the latest version of ETS 5 and a supply voltage of 12 to 30 V DC are required in order to commission the device. Alternatively, the device can be powered via PoE (Power over Ethernet) to IEEE 802.3af class 1.

The device is ready for operation after connection to the bus voltage and auxiliary voltage.

Mounting and commissioning may only be carried out by electrical specialists. The appropriate standards, directives, regulations and specifications for the appropriate country should be observed when planning and setting up electrical installations and security systems for intrusion and fire detection.

- Protect the device from damp, dirt and damage during transport, storage and operation.
- Only operate the device within the specified technical data!
- The device should only be operated in an enclosed housing (distribution board)!
- The voltage supply to the device must be switched off before mounting work is performed.



Danger

To avoid dangerous touch voltages which originate through feedback from differing phase conductors, all poles must be disconnected when extending or modifying the electrical connections.

Supplied state

The device is supplied with the physical address 15.15.0. All physical tunneling connection addresses are set to 15.15.100 in the supplied state. In other words, only one tunnel is visible to the outside. The tunneling connection addresses set in the ETS will be adopted only after the first download.

The IP address is set to automatic IP assignment (DHCP/AutoIP).

Note

The device is supplied with the option *Route*. This is not the default setting in the application, but it simplifies commissioning. See chapter [Parameter window KNX -> LAN](#).
The programmed setting will be adopted after the first download.

Assignment of the physical address

The physical addresses and parameters are assigned and programmed in ETS.

The device features a *Programming* button for assignment of the physical address. The red *Programming* LED lights up after the button has been pressed. It goes off as soon as ETS has assigned the physical address or the *Programming* button is pressed again.

IPsecure Router KNX

Device technology

Download reaction

The device can be programmed in various ways: via one of the integrated tunneling servers ("local download"), via KNXnet/IP routing or via another programming interface (USB or IP).

Note
Any USB interface used for programming a KNX Secure device must support "long frames." One suitable USB interface is the USB interface from Theben.

There must be a connection to the KNX TP (twisted pair) in order to program the device.

After the download is complete, the device reboots and closes all open tunneling connections. If the device's IP address was changed during the download, the tunneling connections must be reconfigured manually in the tunneling clients. Tunneling clients establish the connection to the server via the IP address.

The data programmed with ETS is adopted approx. 30-60 seconds after the download.

Unloading the device and resetting to factory settings

The device can be reset to the factory settings. This is a secure device, so the following information must be observed:

When the device is operated in KNX Secure mode, it can be reset via the ETS only if the ETS uses the project with which the device was parameterized or if the commissioning key is available in the project.

The device can be unloaded by right-clicking it in the ETS.

Option: Unloading the application

- The IP address and IP configuration will be retained
- Any unicast configuration will be retained
- The passwords and IP addresses of the tunneling servers will be deleted
- The key for multicast communication ("backbone key") will be retained
- The tool key assigned by the ETS will be retained. In other words, the FDSK will not be needed for reprogramming
- The physical address will be retained

Option: Unloading the physical address and the application

- The device will be reset to the factory state
- The FDSK will be needed for re-commissioning unless it is still available in the ETS project from the original commissioning process

IPsecure Router KNX

Device technology

The reset to factory settings can also be performed directly on the device. This is not a security risk, because the device will no longer be part of the system afterward.

- Press the Programming button when the KNX bus is not connected
- Hold the Programming button down and plug on the bus terminal. The Programming LED flashes (2 Hz)
- Press the button, hold it for at least 5 s and then release it. The Programming LED goes out, and the device reboots with the factory settings

The Router can be reprogrammed if the ETS connects with the device after reset and if the device's FDSK key is still known to the ETS. The ETS will report that the device was reset in this case.

See chapter [KNX Secure](#), for more information about the FDSK (Factory Default Setup Key).

Cleaning

The voltage supply to the device must be switched off before cleaning. If devices become dirty, they can be cleaned using a dry cloth or a cloth dampened with a soapy solution. Corrosive agents or solutions should never be used.

Maintenance

The device is maintenance-free. In the event of damage (e.g. during transport and/or storage), repairs must not be carried out.

2.5 Description of inputs and outputs

Supply voltage input 12 to 30 V DC

Only a DC voltage in a range of 12 to 30 V may be connected to the power supply input. We recommend using a power supply 640 mA T KNX from our range.

Caution
The supply voltage must be 12 to 30 V DC, or the device is powered via PoE (Power over Ethernet) according to IEEE 802.3af class 1. Connecting the device to 230 V may destroy it!

KNX connection

The supplied bus connection terminal is used to connect to the KNX bus.

Note
The latest ETS 5 version is required for programming.

LAN connection

The network connection is carried out via an Ethernet RJ45 interface for LAN networks. The network interface can be operated with a transmission speed of 10/100 Mbit/s. Network activity is indicated by the LAN/LINK LED on the front of the device.

2.6 Operating controls

There are no operating controls located on the IPsecure Router.

2.7 Display elements

Three indicator LEDs are located on the front of the IPsecure Router:



ON



LAN/LINK



Telegram

ON

- The LED lights for a few seconds after connection of the supply voltage.
- After the auxiliary voltage is connected, the LED initially lights up continuously. After approx. 40 seconds, the LED starts flashing until the startup process is complete and the LED lights up continuously again. Depending on the size of the filter table, this can take 5 to 60 seconds.

LAN/LINK

- The LED lights up when the auxiliary voltage is present and the Router is connected to an Ethernet network.
- The LED flashes when the device detects activity on the network, e.g. when data is exchanged.

Telegram

- The LED lights up when the Router is connected to a TP network and the startup process is complete (see "On" LED).
- The LED flashes when the device detects activity on the KNX subline TP1 (twisted pair 1), e.g. when data is exchanged.

IPsecure Router KNX Commissioning

3 Commissioning

The IPsecure Router is parameterized using the application and the Engineering Tool Software ETS.

The application can be found under *THEBEN AG/System components/Routing*.

For parameterization purposes, a PC or laptop with ETS and a connection to KNX are required.

3.1 Overview

The IPsecure Router is parameterized using the Engineering Tool Software (latest ETS 5 version).

Some functions (Unicast) are parameterized via a separate tool (IP Tool).

IPsecure Router KNX Commissioning

3.2 Parameters

This chapter describes the parameters of the IPsecure Router using the parameter windows.

The parameter windows feature a dynamic structure so that further parameters or whole parameter windows may be enabled depending on the parameterization and the function of the outputs.

The default values of the parameters are underlined, e.g.:

Options: Yes
 No

3.2.1 Parameter window *KNX -> LAN*

In the parameter window *KNX -> LAN* it is possible to define the processing of telegrams from the KNX system to the LAN network.

Note

The device is supplied with the option *Route*. This is not the default setting in the application, but it simplifies commissioning.

The programmed setting will be adopted after the first download.

KNX->LAN

LAN->KNX

IP settings

Group telegrams
main groups 0...13

Group telegrams
main groups 14...31

Physically addressed telegrams

Broadcast telegrams

Telegram confirmation
for group telegrams

If free group address structure is used:

Main group 0...13 => 1...28,671

Main group 14...31 => 28,672...65,535

Filter

Filter

☒ Filter ☐ Block

☒ Route ☐ Block

☒ Only if routed ☐ Always

<--- NOTE

IPsecure Router KNX

Commissioning

Group telegrams main groups 0...13

Options: [Filter](#)
Route
Block

This parameter defines whether telegrams with group addresses of the main groups 0 to 13 are filtered, routed or blocked.

- *Filter*: Telegrams with the group addresses of the main groups 0 to 13 from KNX to LAN are filtered in accordance with the filter table, which is automatically calculated by ETS.
- *Route*: All group telegrams of main groups 0 to 13 are routed without considering the filter table settings.

Important

This setting is only useful for commissioning and diagnostics. It should not be used during normal operation. As this setting can overload the KNX lines, a loss of telegrams could occur.

- *Block*: All group telegrams from KNX to LAN are blocked without considering the filter table settings.

Group telegrams main groups 14...31

Options: [Filter](#)
Route
Block

This parameter defines whether telegrams with group addresses of the main groups 14 to 31 are filtered, routed or blocked.

- *Filter*: Telegrams with the group addresses of the main groups 14 to 31 from KNX to LAN are filtered in accordance with the filter table, which is automatically calculated by ETS.
- *Route*: All group telegrams of main groups 14 ... 31 are routed without considering the filter table settings.

Important

This setting is only useful for commissioning and diagnostics. It should not be used during normal operation. As this setting can overload the KNX lines, a loss of telegrams could occur.

- *Block*: All group telegrams of main groups 14 ... 31 are blocked without considering the filter table settings.

IPsecure Router KNX Commissioning

Physically addressed telegrams

Options: Filter
Block

This parameter defines whether physically addressed telegrams are filtered or blocked.

- *Filter*: Only telegrams from KNX to LAN that are to exit the line of the IPsecure Router to LAN are sent.
- *Block*: Physically addressed telegrams are not processed by the IP Router. It is not possible to send physically addressed telegrams from a line below the IPsecure Router to another line, e.g. during programming.

Broadcast telegrams

Options: Route
Block

This parameter defines whether broadcast telegrams are routed or blocked.

- *Route*: Broadcast telegrams are routed.
- *Block*: Broadcast telegrams are not processed by the IP Router. It is not possible to send broadcast telegrams from a line below the IPsecure Router to another line, e.g. during programming.

The *Broadcast telegrams* parameter applies to "system broadcast telegrams" as well. See chapter, [System broadcast](#), for details.

Telegram confirmation for group telegrams

Options: Only if routed
Always

This parameter defines whether the IPsecure Router is to acknowledge group telegrams.

- *Only if routed*: The group telegrams are acknowledged (send ACK) only if they are also routed by the IPsecure Router to LAN. Thus, only telegrams that are in the IPsecure Router filter table are acknowledged.
- *Always*: All group telegrams on KNX are acknowledged by the IP Router.

If free group address structure is used:

Main group 0...13 => 1...28,671

Main group 14...31 => 28,672...65,535

Note

In the ETS 5 it is possible to not just assign two- or three-stage group addresses; it is possible to assign them freely. If the free group address view is selected, main group 0...13 corresponds to subgroup range 1...28,671 and main group 14...31 corresponds to subgroup range 28,672...65,535. Relevant details can be found in the help for the ETS.

IPsecure Router KNX Commissioning

3.2.1.1

Parameter window LAN -> KNX

In the parameter window LAN -> KNX it is possible to define the processing of telegrams from the LAN network to the KNX system.

KNX->LAN	Group telegrams main groups 0...13	Filter
LAN->KNX	Group telegrams main groups 14...31	Filter
IP settings	Physically addressed telegrams	☒ Filter ☐ Block
	Broadcast telegrams	☒ Route ☐ Block
	In case of errors repeat telegrams	Yes
	If free group address structure is used:	<--- NOTE
	Main group 0...13 => 1...28,671 Main group 14...31 => 28,672...65,535	

Group telegrams main groups 0...13

Options: Filter
Route
Block

This parameter defines whether telegrams with group addresses of the main groups 0 to 13 are filtered, routed or blocked.

- *Filter*: Telegrams with the group addresses of the main groups 0 to 13 from LAN to KNX are filtered in accordance with the filter table, which is automatically calculated by ETS.
- *Route*: All group telegrams of main groups 0 to 13 are routed without considering the filter table settings.

Important

This setting is only useful for commissioning and diagnostics. It should not be used during normal operation. As this setting can overload the KNX lines, a loss of telegrams could occur.

- *Block*: All group telegrams from LAN to KNX are blocked without considering the filter table settings.

IPsecure Router KNX

Commissioning

Group telegrams main groups 14...31

Options: Filter
 Route
 Block

This parameter defines whether telegrams with group addresses of the main groups 14 to 31 are filtered, routed or blocked.

- *Filter*: Telegrams with the group addresses of the main groups 14 to 31 from LAN to KNX are filtered in accordance with the filter table, which is automatically calculated by ETS.
- *Route*: All group telegrams of main groups 14 ... 31 are routed without considering the filter table settings.

Important
This setting is only useful for commissioning and diagnostics. It should not be used during normal operation. As this setting can overload the KNX lines, a loss of telegrams could occur.

- *Block*: All group telegrams of main groups 14 to 31 from LAN to KNX are blocked.

Physically addressed telegrams

Options: Filter
 Block

This parameter defines whether physically addressed telegrams are filtered or blocked.

- *Filter*: Only telegrams from LAN to KNX that are to exit the line of the IPsecure Router to LAN are sent.
- *Block*: Physically addressed telegrams are not processed by the IPsecure Router. With this setting it is not possible to send physically addressed telegrams from a line of a lower level than the IPsecure Router to another line, e.g. during programming.

Broadcast telegrams

Options: Route
 Block

This parameter defines whether broadcast telegrams are routed or blocked.

- *Route*: Broadcast telegrams are routed.
- *Block*: Broadcast telegrams are not processed by the IPsecure Router. It is not possible to send broadcast telegrams from a line of a lower level than the IPsecure Router to another line, e.g. during programming.

IPsecure Router KNX Commissioning

In case of errors repeat telegrams

Options: Yes
No
User-defined

- *Yes*: If an error is detected when a telegram is transmitted, the telegram is repeated up to three times.
- *No*: The telegram is not repeated.
- *User-defined*: The reaction can be set individually for different types of telegram.

The following dependent parameters appear when the *User-defined* option is selected:

Repeat group addressed telegrams

Options: Yes
No

- *Yes*: If an error is detected when a group addressed telegram is transmitted, the telegram is repeated up to three times.
- *No*: The telegram is not repeated.

Repeat physically addressed telegrams

Options: Yes
No

- *Yes*: If an error is detected when a physically addressed telegram is transmitted, the telegram is repeated up to three times.
- *No*: The telegram is not repeated.

Repeat broadcast telegrams

Options: Yes
No

- *Yes*: If an error is detected when a broadcast telegram is transmitted, the telegram is repeated up to three times.
- *No*: The telegram is not repeated.

If free group address structure is used:

Main group 0...13 => 1...28,671

Main group 14...31 => 28,672...65,535

Note

In the ETS 5 it is possible to not just assign two- or three-stage group addresses; it is possible to assign them freely. If the free group address view is selected, main group 0...13 corresponds to subgroup range 1...28,671 and main group 14...31 corresponds to subgroup range 28,672...65,535. Relevant details can be found in the help for the ETS.

IPsecure Router KNX Commissioning

3.2.1.2 Parameter window *IP settings*

Parameter window *IP settings* is used to set how the IPsecure Router communicates via IP.

KNX->LAN	Type of IP communication	☒ Multicast ☐ Unicast
LAN->KNX	The device name, IP address and tunneling servers are set in the Properties window of ETS.	<--- NOTE ▾
IP settings		

Type of IP communication

Options: Multicast
 Unicast

The type of IP communication defines the type of telegrams that the IPsecure Router sends on the IP network.

- *Multicast*: This is the standard communication using KNX-IP devices for KNXnet/IP from the KNX Association. This setting should only be changed if the existing network demands that telegrams are sent as unicast.

For setting the routing multicast address, see [Routing multicast address](#).

- *Unicast*: The routing for the device is switched off.

This special communication type does not comply with the KNXnet/IP specification. The Theben Tool is required for configuration.

The *Unicast* type of communication cannot be used when the device is operated in KNX Secure mode. If *Unicast* is selected when KNX Secure mode is active, the ETS switches to *Multicast*. The *Unicast* parameterization in the application will be ignored in this case.

KNX Secure mode must be switched off in the ETS in order to be able to use the *Unicast* type of communication.

Note
A description of the functions can be found in the online Help of the IP Tool.

The following message appears if *Multicast* or *Unicast* is selected:

The device name, IP address and tunneling servers are set in the Properties window of ETS.

IPsecure Router KNX Commissioning

The following note also appears with the selection *Unicast*:

Attention! This setting switches off routing for the device.

The IP telegrams will now be sent as unicast to up to nine target addresses.

Unicast configuration is performed with the Theben IP Tool.

See description of unicast communication, chapter [KNX telegrams in the network](#).

The IP Tool can be downloaded for free from our website (www.theben.de/en/downloads_en).

No ETS or installation of Falcon is required for the IP Tool.

System requirements: system with Windows 7 operating system (service pack 3) or later and .NET Framework 4.0.

The integrated Falcon 5.0 supports only USB and IP interfaces (no RS232).

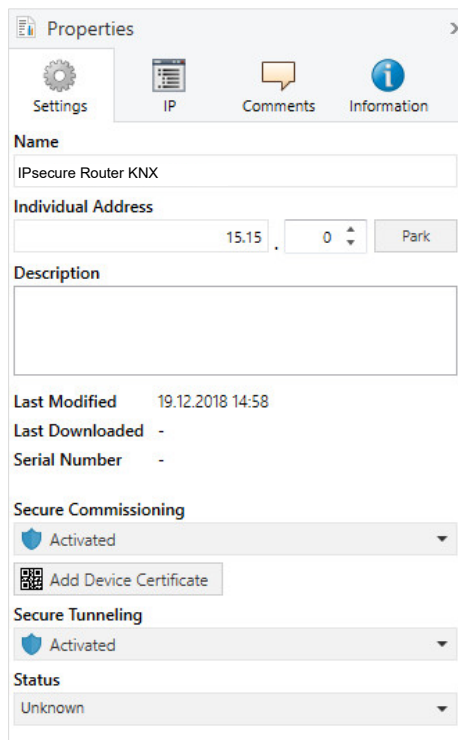
Note
A description of the functions can be found in the online Help of the IP Tool.

Important
Unicast communication cannot be used when KNX Secure mode is activated. If KNX Secure mode is activated and the parameter <i>Type of IP communication</i> is set to <i>Unicast</i> , multicast communication will be activated anyway. A corresponding message will be displayed when the unicast addresses are parameterized via the IP Tool.

IPsecure Router KNX

Commissioning

The remaining configuration of the IP parameters (device name, assignment of the IP address by DHCP or static) takes place in the Properties window of the ETS takes place in the corresponding Properties window of ETS.



The screenshot shows the 'Properties' window in ETS, specifically the 'Settings' tab. The 'Name' field is set to 'IPsecure Router KNX'. The 'Individual Address' is set to '15.15'. The 'Description' field is empty. The 'Last Modified' date is '19.12.2018 14:58'. The 'Last Downloaded' and 'Serial Number' fields are empty. The 'Secure Commissioning' dropdown is set to 'Activated'. There is a button labeled 'Add Device Certificate'. The 'Secure Tunneling' dropdown is also set to 'Activated'. The 'Status' dropdown is set to 'Unknown'.

The device name can be entered in the *Settings* Properties window. The device name loaded into the device can be changed in the *Name* field.

The device name is used for identification of the device on LAN. After a search query, e.g. by ETS, every KNXnet/IP device reports its name and can be allocated accordingly. For example, the installation location can be identified by the names assigned to the devices, e.g. IP Router, HALL, SUB7, etc.

Note

The default device name on delivery is "IPsecure Router". After the first download, the device name entered in the Properties window of ETS is loaded into the device.

Caution

Only the first 30 characters of the device name are loaded into the device; the rest is truncated.

IPsecure Router KNX Commissioning

The IP address can be defined in the *IP* Properties window.

Properties

Settings IP Comments Information

☐ Obtain an IP address automatically

☒ Use a static IP address

IP Address
127.0.0.1

Subnet Mask
255.255.255.255

Default Gateway
127.0.0.1

MAC Address
Unknown

Multicast Address
224.0.23.12

Commissioning Password
Wrrr!0Q;
Good

Authentication Code
_eT3j_o>
Good

The following options are available for setting the IP address:

Options: Obtain an IP address automatically
Use the following IP address

- *Obtain an IP address automatically:* In the default setting the IPsecure Router expects the assignment of an IP address by a DHCP (dynamic host configuration protocol) server. This server responds to a request by assigning a free IP address to the device. If a DHCP server is not available in the network or it does not respond within 30 seconds, the device starts an auto IP procedure. It assigns itself an address from the reserved range for auto IP addresses (169.254.1.0 to 196.254.254.255).

For information about DHCP: see chapter [Assignment of IP address](#).

- *Use a static IP address:* If no DHCP server is installed on the network or if the IP address should remain the same, it can be assigned as static.

When assigning static IP addresses, ensure that each device receives a different IP address.

IPsecure Router KNX

Commissioning

Note
The routing multicast address is displayed only here. For setting the routing multicast address, see Multicast address

Note
The MAC address is read from the device after a download. The MAC address is additionally labeled on the device, or it can be determined via the IP Tool.

Note
A description of the functions can be found in the online Help of the IP Tool.

IPsecure Router KNX Commissioning

Routing multicast address (default = 224.0.23.12)

Options: 224.0.23.12

The routing multicast address defines the target address of the IP telegrams of the IP Router. The preset address 224.0.23.12 is the defined address for the KNXnet/IP from the KNX Association in conjunction with IANA for KNX-IP devices. This address should be retained and only changed if the existing network demands that another address from the range 224.0.0.0 to 239.255.255.255 (reserved range for multicast addresses) be used.

The routing multicast address is set in ETS in the view *Topology* (topology selection; the routing multicast address can then be set on the *Settings* tab in the Properties window):

The screenshot shows the 'Properties' window in ETS with the 'Settings' tab active. The window contains several configuration fields:

- Backbone Name:** Backbone area
- Description:** (Empty text box)
- Status:** Unknown
- Backbone Medium:** IP
- Network Latency:** WLAN (< 1s)
- Multicast Address:** 224.0.23.12
- Security:** Automatic
- Bus Connection:** None

Important

All IPsecure Routers or other KNXnet/IP devices that are required to exchange telegrams on the IP network must use the same routing multicast address.

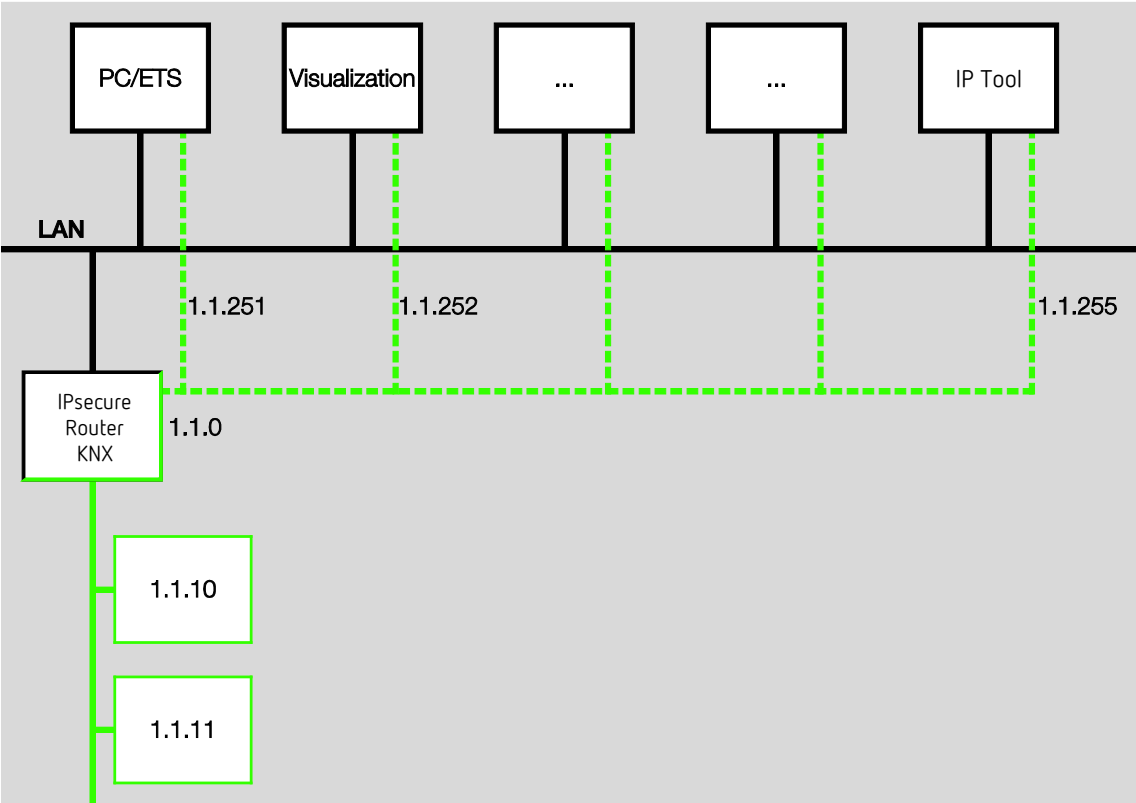
IPsecure Router KNX Commissioning

3.3 Group objects

The IPsecure Router has no KNX group objects.

3.4 Use of the integrated tunneling servers

The IPsecure Router offers five additional physical addresses, which can be used for a tunneling connection. These so-called tunneling servers can be used with ETS as a programming interface or with another client, e.g. a visual display system.



Tunneling involves a client connecting to a bus line. The tunneling process uses UDP, but includes a data link layer so that telegrams are repeated in the event of an error.

Tunneling V2 is supported from ETS 5. TCP is used instead of UDP here, and the TCP's data link layer is used for transmission

Note
The physical address for the tunneling connection must fit the topology. Therefore, the addresses must be selected from the address range of the subordinate line. On delivery, all tunneling servers have the address 15.15.100. In ETS 5, the first five free addresses in the line are assigned automatically after the Router has been inserted into a line.

The tunneling servers can also be encrypted with KNX Secure. When KNX Secure mode is activated, a client will need the password assigned in the ETS. For details, see chapter, [KNX Secure](#).

IPsecure Router KNX Commissioning

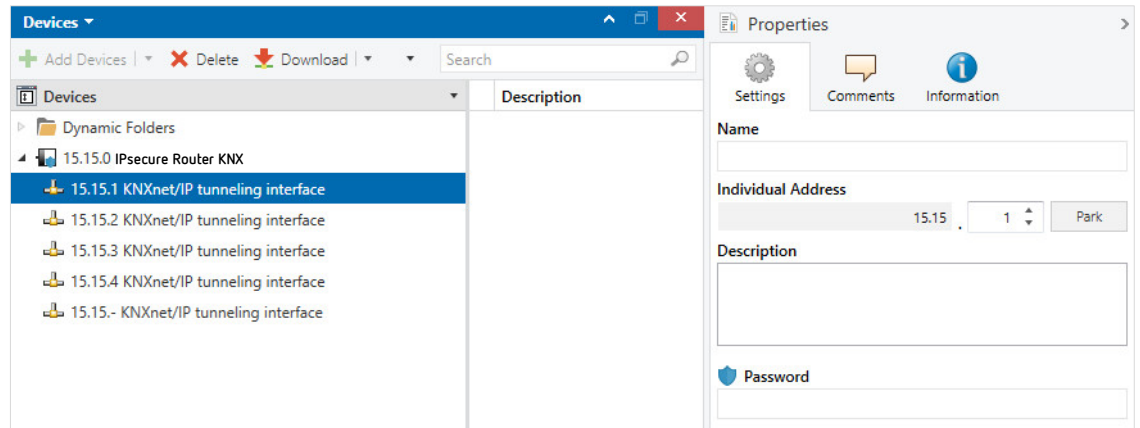
3.4.1 Settings in ETS 5

An additional Properties window is available in ETS for setting the additional physical addresses.

After insertion of the Router into the line, the ETS automatically reserves the first five free addresses of this line for the tunneling servers of the Router. This is a property of the ETS and cannot be changed.

The addresses will be available in the device after the first download.

If this is not desired, the setting can be changed manually in the Properties window.



To change the address, mark the current device address or additional address and then select the desired numeral using the up or down arrow key. The changed address is saved when another address is marked.

The changed addresses are adopted by the device only after a download.

Park

If the option Park is activated for a tunnel, this tunnel will receive the address 15.15.255.

If the option Park is selected for all tunneling servers, all tunneling servers will be assigned the address 15.15.255. Only one tunneling server is available as a result.

IPsecure Router KNX

Commissioning

3.5 KNX Secure

The IPsecure Router is a KNX device according to the KNX Secure standard. In other words, the device can be put into operation in a secure manner. Communication on the IP backbone is secure (all KNX IP devices must support the KNXnet/IP Security protocol for this purpose), and the tunneling connections are encrypted.

The following information must therefore be taken into account during device commissioning:

- It is essential to assign a project password as soon as a KNX Secure device is imported into a project. This will protect the project against unauthorized access.
The password must be kept in a safe place – access to the project is not possible without it (not even the KNX Association or Theben will be able to access it)!
- A commissioning key is required when commissioning a KNX Secure device (first download). This key (FDSK = Factory Default Setup Key) is included on a sticker on the side of the device, and it must be imported into the ETS prior to the first download.
 - On the first download of the device, a window opens in the ETS to prompt the user to enter the key. The certificate can also be read using a QR scanner (recommended).
 - Alternatively, the certificates of all Secure devices can be entered in the ETS beforehand. This is done on the "Security" tab on the project overview page.
 - Two FDSK stickers are applied on the device. One of them can be used for the project documentation, and the other one can remain on the device.
Without the FDSK, it will no longer be possible to operate the device in KNX Secure mode after a reset.

The FDSK is required only for initial commissioning. The ETS then assigns new keys. The FDSK will be required again only if the device was reset to its factory settings (e.g. If the device is to be used in a different system with a different ETS project).

The ETS assigns the "backbone" key to all KNX IP Secure devices in the project, and also generates separate passwords for each tunneling server. The passwords can be changed as required. ETS generates and administers the keys. Keys and passwords can be exported as needed (e.g. if a client would like to access one of the tunnels).

The Router can be reset to its factory settings if necessary, see chapter, [Unloading the device and resetting to factory settings](#).

IPsecure Router KNX

Planning and application

4 Planning and application

4.1 The IPsecure Router in the network

The IPsecure Router is designed for use in 10/100 BaseT networks compliant to IEEE 802.3. The device features an AutoSensing function and sets the baud rate (10 or 100 Mbit) automatically.

4.1.1 Assignment of IP address

DHCP/AutoIP

The IP address of the device can be received from a DHCP server. For this purpose the automatic assignment setting of the IP address in ETS is required, see [IP settings](#). If no DHCP server is found with this setting, the device starts an AutoIP procedure and autonomously assigns itself an IP address from the range 169.254.xxx.yyy.

The IP address that the device receives (via DHCP or AutoIP) during startup will be retained until

- the next reboot (switching off/on or reprogramming).
- a DHCP server is available.
- the DHCP lease expires.

No DHCP server available during start-up:

If no DHCP server is available during startup of the IP Router Secure, the device will assign itself an AutoIP address. The Router then cyclically (three telegrams at intervals of 3 seconds, followed by a pause of 20 seconds) searches for a DHCP server. As soon as a server is available again, the address assigned by the DHCP server is used.

DHCP server fails (device has already received IP address from the DHCP):

Requests to extend the utilization rights for this IP address remain unanswered until the end of the lease time (IP address validity time; this is defined by the DHCP server during assignment of the IP address). The IP address continues to be used.

At the end of the lease time or after a download, the device searches for an AutoIP address.

Static IP address

If the IP address of the IPsecure Router is to have a fixed assignment, a static IP address (as well as a subnet mask and a default gateway) can be set in the ETS, see parameter window [IP settings](#).

IPsecure Router KNX

Planning and application

4.1.2

KNX telegrams in the network

Note

When designing the KNX system it is important to note that the number of transferred telegrams is also limited when the IPsecure Router is used. Due to the high baud rate on the IP side (10/100 Mbit/s), telegrams may be lost with high levels of data exchange on the TP1 line (9.6 kbit/s) for system reasons.

Multicast

Multicast designates communication of a transmitter with a group of receivers. The IPsecure Router sends the KNX telegrams packaged as UDP/IP telegrams on the IP network, and all IPsecure Router devices parameterized with the same multicast address receive and evaluate these telegrams. If a telegram is intended for the corresponding subline, the IPsecure Router routes the telegram into the line. Otherwise, it is rejected.

The IPsecure Router sends telegrams from the KNX to the IP network in accordance with the KNXnet/IP protocol specification. These telegrams are sent in the default setting as multicast telegrams to the multicast IP address 224.0.23.12 port 3671. This multicast IP address is the defined address for the KNXnet/IP from the KNX Association in conjunction with IANA for KNX IP devices. This address should be retained. It should be changed only if the existing network demands that another address be used.

In order for several IPsecure Router devices to communicate with one another in a network, multicast communication must be possible between the devices. Depending on the type of network and the setting of the network components used, e.g. routers, switches or firewalls, the multicast IP address 224.0.23.12 may need to be enabled explicitly beforehand. Please discuss the topic with your network administrator.

For further information, see chapter, [Parameter window IP settings](#).

Unicast

If multicast communication is not possible in a network, the Theben IP Routers can also communicate with each other via unicast. Up to ten Theben IP Routers can be combined to form a unicast group. Each Router is then assigned nine IP addresses to which it sends its telegrams.

Unicast generally refers to communication between a transmitter and a receiver. In other words, the Router sets up a communication connection to every IPsecure Router within the unicast group.

Automatic configuration of this unicast group is simple with the Theben IP Tool.

It is also possible to link a client (e.g. a visual display system) with this unicast group. In this case, one of the ten unicast addresses is used by the client and up to nine IP Routers can be linked.

The exact description of how configuration with the IP Tool works can be found in the Help of the IP Tool (see chapter [The IP Tool](#)).

Note

As soon as the parameter is changed to *Unicast* under Type of IP communication in the ETS, the function *Multicast* is deactivated. The devices can then no longer be programmed via multicast routing; they can be programmed only via one of the integrated tunneling servers or a separate programming interface. However, the type of communication will be changed only when parameterization with the IP Tool has taken place. Until then, the Router will remain internally set to multicast. This offers the advantage of programming the Router via multicast.

For more information, see parameter window [IP settings](#).

Note

A description of the functions can be found in the online Help of the IP Tool.

IPsecure Router KNX

Planning and application

Note

- If unicast is used as the type of communication, it must be ensured that the IP address of the Router does not change during operation. For this purpose, either a static IP address should be assigned or a corresponding setting should be made for the DHCP server.
- With the ETS, all IP parameters are also updated when the physical address is changed. In other words, even if only the option *Programming physical address* is selected in the ETS, the device name, the multicast address, the type of IP communication (DHCP, AutoIP, fixed), the IP address, the subnet mask, the default gateway and all tunneling addresses are loaded again. If the IP address changes in the process, unicast configuration with the IP Tool must be repeated.

The *Unicast* type of communication cannot be used when the device is operated in KNX Secure mode. If *Unicast* is selected when KNX Secure mode is active, the ETS switches to *Multicast*. The *Unicast* parameterization in the application will be ignored in this case.

KNX Secure mode must be switched off in the ETS in order to be able to use the *Unicast* type of communication.

4.1.3

Monitoring

An active tunneling connection should be monitored via a "CONNECTIONSTATE_REQUEST", but this is also possible via T-Connect. Monitoring a device via T-Connect can have drawbacks, e.g. in case of monitoring, programming or scanning processes in the line.

4.1.4

System broadcast

All IP devices that are to communicate with each other in a KNX system must use the same multicast address. The address 224.0.23.12 port 3671 is used by default; see [Multicast](#).

Changing the multicast address in a system could lead to problems during commissioning. If the multicast address of the closest Router is changed first, for example, it will switch to the new multicast address after programming. It will then no longer be able to access the rest of the system, and the remaining Routers in the system can no longer be programmed.

ETS can then reach these devices via the "system broadcast address." The system broadcast address can be used to change the multicast address of all KNX IP devices, as well as the backbone key. This will work only if the device is not operated in KNX Secure mode or if the backbone key is known to the ETS.

Routing of system broadcast telegrams can be set via the parameter *Route/Block broadcast telegrams*. In other words, this parameter is effective for (standard) broadcast telegrams and system broadcast telegrams.

4.1.5

IGMP

The device supports IGMP snooping version V3.

IGMP snooping is the capability of routing multicast routing traffic only to where it is actually needed. The IT infrastructure and the device must use the same IGMP version, otherwise this IGMP mechanism will not work.

To enable a multicast address, the device logs in at this multicast address with a membership report.

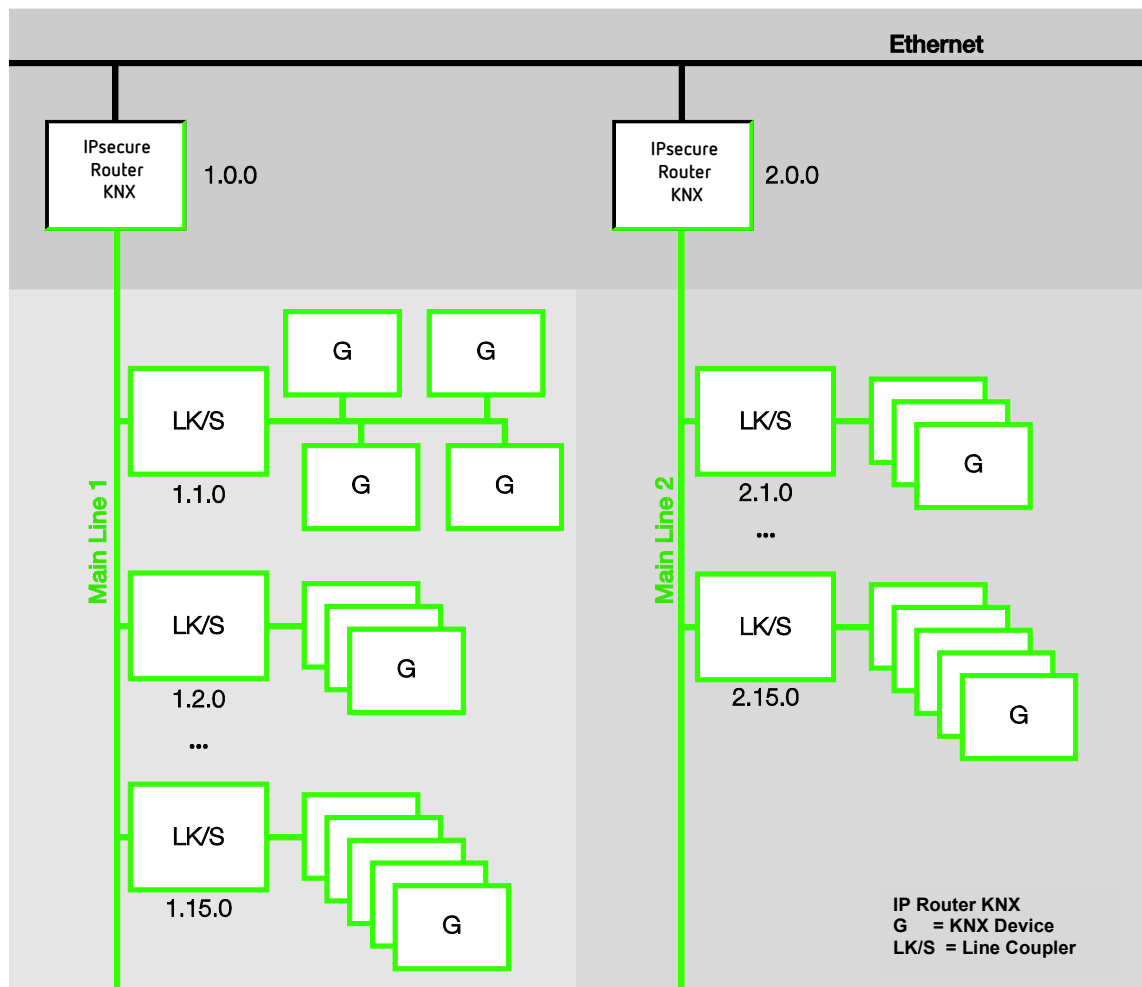
IPsecure Router KNX

Planning and application

4.1.6 IPsecure Router as an area coupler

The IPsecure Router in a KNX system can assume the function of an area coupler in a KNX system. For this purpose it must receive the physical address of an area coupler (1.0.0...15.0.0). Up to 15 areas can be defined with area couplers in an ETS project.

The following figure shows this topology with IP Router Secure devices as area couplers and KNX Line Couplers (LK/S).



IPsecure Router KNX

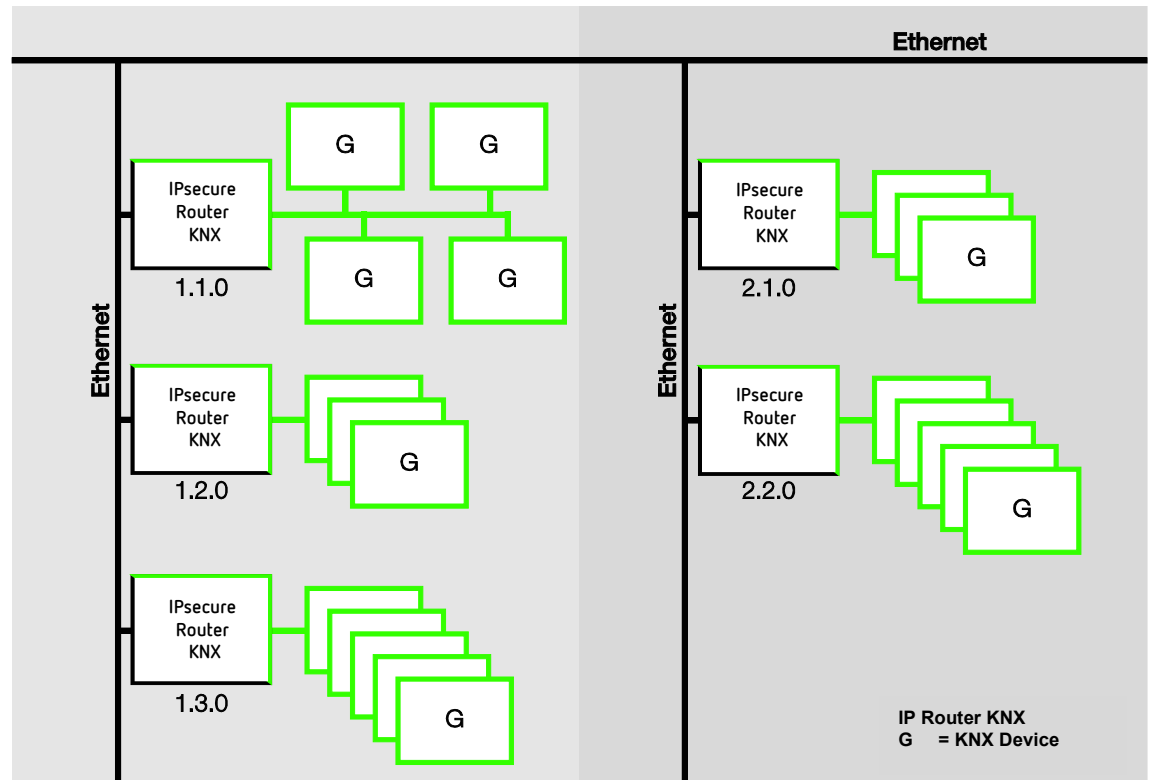
Planning and application

4.1.7

IPsecure Router as a line coupler

The IPsecure Router in a KNX system can assume the function of a line coupler. To do this it must be given the physical address of a line coupler (1.1.0...15.15.0).

The following illustration shows the topology with IPsecure Routers as line couplers.



IPsecure Router KNX

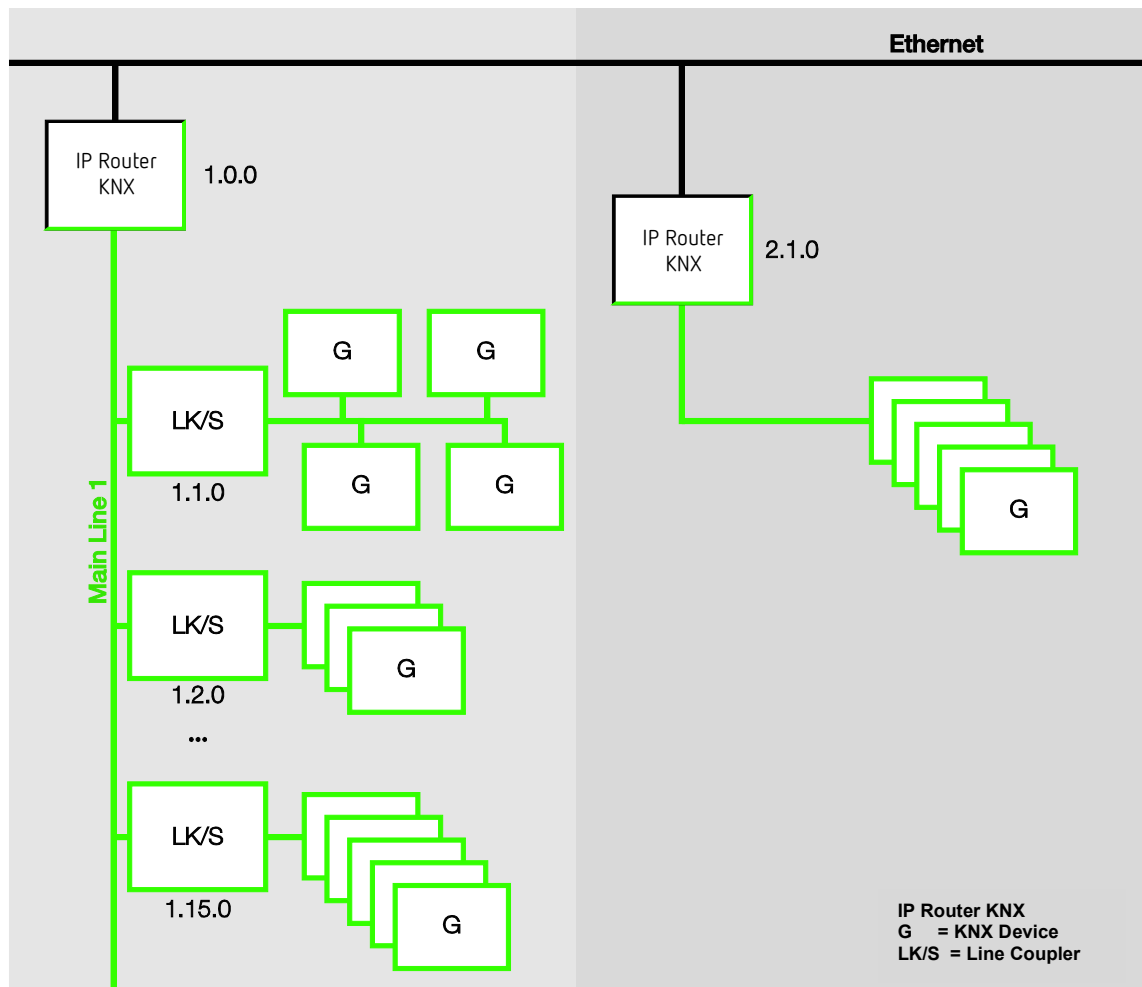
Planning and application

4.1.8

Mixed topology

If it is necessary in a KNX system to use the IPsecure Router as an area coupler at one point, e.g. office complex, and as a line coupler at another point, e.g. a remote underground garage, this is possible.

It is only necessary to ensure that the IPsecure Router as the line coupler uses the line coupler address from a free area, e.g. 2.1.0 in the figure.



IPsecure Router KNX

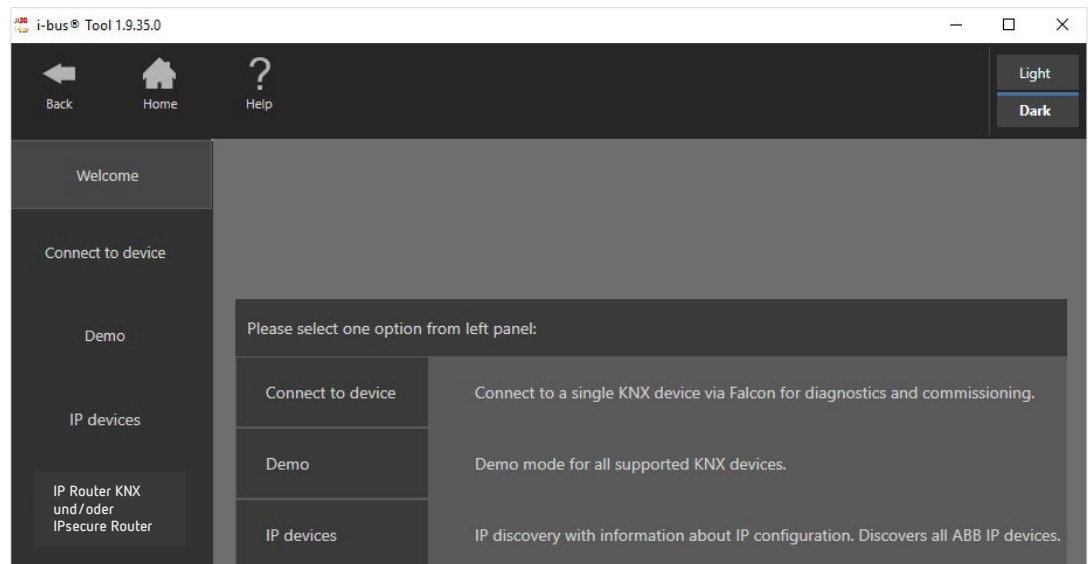
Planning and application

4.2 The IP Tool

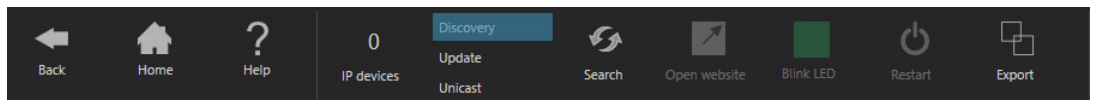
The Theben IP Tool is required in order to set certain functions of the Theben IP devices.

It simplifies commissioning on the IP side.

Go to the start page of the IP Tool, click *Connect* and then click *IP devices* in the window that then appears.



Ribbon: switching between Discovery, Firmware Update and Unicast



Click the corresponding button to select *Discovery* or *Unicast* mode.

Discovery

Select *Discovery* mode in the ribbon area. This function serves to find and display Theben IP devices in the network. Not all information is displayed when the IPsecure Router is operated in KNX Secure mode.

Note

A description of the functions can be found in the online help of the IP Tool.

Firmware update

The device cannot be updated with the IP Tool in KNX Secure mode. In this case, the firmware update will be possible only with the ETS app "KNX Bus Update." The app can be loaded free of charge from the KNX Online Shop.

Select *Update* mode in the ribbon area. If this should become necessary, the firmware can be updated using this function.

Important

The firmware must be downloaded from the Internet first (www.theben.de/en/downloads_en). For this purpose the IP Tool connects to a server **if an Internet connection is available**.
An Internet connection is then no longer necessary in order to update the system devices.

IPsecure Router KNX

Planning and application

Important

During the update process, the KNX bus (TP) must be connected in addition to the IP network (LAN) so that the KNX parameters can be restored correctly. Otherwise, the update process will fail.
It must be ensured that no voltage failure (KNX or IP) occurs during the update process, otherwise the device can be destroyed.

Note

A description of the functions can be found in the online help of the IP Tool.

Note

The IP Tool must be run with administrator rights for the update process.

Unicast

Select *Unicast* mode in the ribbon area.

This function is available only if the parameter [Type of IP communication](#) has been set to *Unicast* in the ETS application first.

Note

A description of the functions can be found in the online Help of the IP Tool.

5 Contact

Theben AG

Hohenbergstraße 32
72401 Haigerloch
GERMANY

Tel.: +49 7474 692-0
Fax: +49 7474 692-150
e-mail: info@theben.de

Further information and local contacts:

www.theben.de

Note:

We reserve the right to make technical changes or modify the contents of this document without prior notice.

The agreed properties are definitive for any orders placed.

Theben AG does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Reproduction, transfer to third parties or processing of the content – including sections thereof – is not permitted without prior expressed written permission from Theben AG.

Copyright© 2020 Theben AG
All rights reserved

6 Open source software components (OSS)

A list of the open source components used is available on the Internet at:

<https://www.theben.de/OSS>