



enertexbayern gmbh
simulation entwicklung consulting

Manual and Configuration

Enertex® KNX IP Secure Router



Note

The content of this document may not be reproduced, distributed, distributed or stored in any form whatsoever, in whole or in part, without the prior written consent of Enertex® Bayern GmbH.

Enertex® is a registered trademark of Enertex® Bayern GmbH. Other product and company names mentioned in this manual may be trademarks or trade names of their respective owners.

This manual is subject to change without notice or announcement and does not claim to be complete or correct.

Inhalt

Security Notes.....	3
Assembly and connection.....	3
Comissioning.....	3
<i>Boot</i>	<i>3</i>
<i>Displays.....</i>	<i>3</i>
<i>Reset.....</i>	<i>4</i>
Functional Overview.....	4
ETS Parameter.....	4
<i>Terms.....</i>	<i>4</i>
<i>ETS 5.6.6 and ETS 5.7.0.....</i>	<i>5</i>
Version requirements.....	5
Special behavior	5
<i>Topology.....</i>	<i>5</i>
<i>Device Properties.....</i>	<i>7</i>
General.....	7
IP Properties	7
<i>Device-specific parameters.....</i>	<i>8</i>
General.....	8
Special Functions.....	8
Behavior of the KNX side.....	8
Standard tunnel preferred IP.....	9
Routing.....	11
Physical address filter.....	11
Group address filter.....	11
Standard.....	12
Extended Group Address Filter.....	13
Telnet.....	15
Latest documentation and Software.....	18
Specification.....	18
Open Source Software.....	19
<i>LWIP</i>	<i>19</i>

Security Notes

- Installation and assembly of electrical equipment may only be carried out by qualified electricians.
- When connecting KNX / EIB interfaces, KNX TM training is required.
- Failure to observe this instruction may result in damage to the unit, fire or other hazards.
- This guide is part of the product and must remain with the end user.
- The manufacturer is not liable for costs or damages caused to the user or third parties by the use of this device, misuse or interference of the connection, malfunctions of the device or of the subscriber devices.
- The opening of the housing, other unauthorized modifications and / or conversions to the device will void the guarantee!
- The manufacturer shall not be liable for any inappropriate use.

Assembly and connection

To operate the Enertex® KNX IP Secure Router, you need:

- A 10/100 Mbit compatible Ethernet connection
- KNX / EIB bus connection

Comissioning

Boot

When powered the display shows the product name. The default for the network is DHCP. The boot time is about 2 seconds. During this time, the green / red / yellow LEDs operate as running light for a short time. At the end of the boot process, the IP address of the device is shown in the display.

If the IP address assignment is done via DHCP server, the boot time is extended accordingly. As soon as "KNX Ready" appears in the display, the device can be addressed via the bus and, for example, alternatively be programmed via a USB interface. The green LED flashes every second with a duty cycle of 1:30.

Displays

After one minute, the display turns off automatically.

To turn this on again, the DISPLAY button on the front panel must be pressed briefly. When the display is activated, pressing the DISPLAY button will scroll through various pages of information.

Page 1 shows the firmware version, IP address, physical address, serial number, bus voltage and used tunnel connections.

Page 2 shows all IP settings, as well as the boot time.

Page 3 gives information about the telegram load.

Page 4 shows the FDSK as long as the device has not been set to the secure state.

There are three LEDs on the front. The green LED flashes every second with a duty cycle of 1:30 and indicates ready for operation. The red LED indicates the programming mode, the yellow LED indicates bus activity.

In the LAN socket two further LEDs are installed. The green indicates a connection to another IP

device or switch ("Link"), the yellow LED shows the IP data transfer.

Reset

If the device is to be reset to the factory settings, the PROG button on the front panel must be pressed for 10 seconds. After this time, the red LED starts to flash - then the PROG key can be released and the device carries out the reset to the delivery condition.

Functional Overview

The device has the following functions:

- KNX IP Secure
 - Eight independent KNXnet / IP tunnel connections
 - Communication via TCP or UDP KNX IP routing for communication between KNX lines, areas and systems
 - KNX IP routing in encrypted (secure) mode.
 - KNX IP tunneling in encrypted (secure) mode.
 - Telegram forwarding and filtering according to physical address
 - Telegram forwarding and filtering according to group address with up to 62 filter blocks
- Displays
 - LED displays for KNX communication, Ethernet communication and programming mode
 - Power indicator
 - OLED display for status messages, parameter displays etc.
- Special functions
 - Configuration via ETS and Telnet
 - SNTP server
 - Measurement of the TP bus voltage (Telnet, OLED display)
 - Maximum TP APDU packet length of the KNX bus (248 bytes)
 - Maximum TP packet length adjustable (Telnet) between 55 and 248 bytes (APDU)
 - Simulation of UDP tunnels for ETS communication (Telnet)
- Performance
 - Specification of a max. TP data rate for writing KNX telegrams
 - Buffering up to 256 telegrams per tunnel (2048 in total) in the device on the IP side
 - Buffering up to 1024 telegrams for telegrams from IP to TP

ETS Parameter

Terms

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.

Backbone For IP routers, this is always the IP network.

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.

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.

Tunnelling 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. For Enertex devices, this timeout can be adjusted in the advanced setup.

Telnet A simple TCP server on port 23 that enables direct text-based communication with the IP device. Telnet is a de facto standard used at the window level, e.g. with "Putty" is addressed.

Secure Mode If the device is parameterized via the ETS so that the communication is only encrypted, this is referred to as secure mode.

Plain Mode If the device is parameterized via the ETS so that the communication is only unencrypted, this is called unsecured mode.

ETS 5.6.6 and ETS 5.7.0

Version requirements

For error-free operation of the devices in secure mode, ETS 5.7.x or higher is required.

In plain mode, the device can basically be programmed as of ETS 5.6.6. Although the secure mode can be parameterized, it is not fully implemented in this version. If the device is therefore to be operated secure, we recommend working with version 5.7 or higher.

Special behavior

If you program the individual address in the ETS 5.6.6 with its own and a tunnel connection, the ETS will throw an error message at the end. This is to be ignored, the assignment of the address has nevertheless been made.

If no tunnel addresses are assigned in the application, all tunnels are set by the ETS to 15.15.255. Communication via the tunnel connection can then be considerably disturbed or not possible.

If the device is integrated in a secure project, the ETS saves the parameterization of this particular device including secure parameters. If the device is reset to factory settings, the ETS (5.6 or 5.7) only addresses the device in encrypted form. Therefore, communication with the ETS can no longer be established. In this case, only deleting the application and restarting the ETS will help.

If an update of Windows runs in the background, strange phenomenon can occasionally occur with the communication between the device and the ETS. In this case, wait for the end of the update and restart Windows.

Topology

To insert the router into an ETS project, it must have an IP backbone. Example: the following ETS topology:

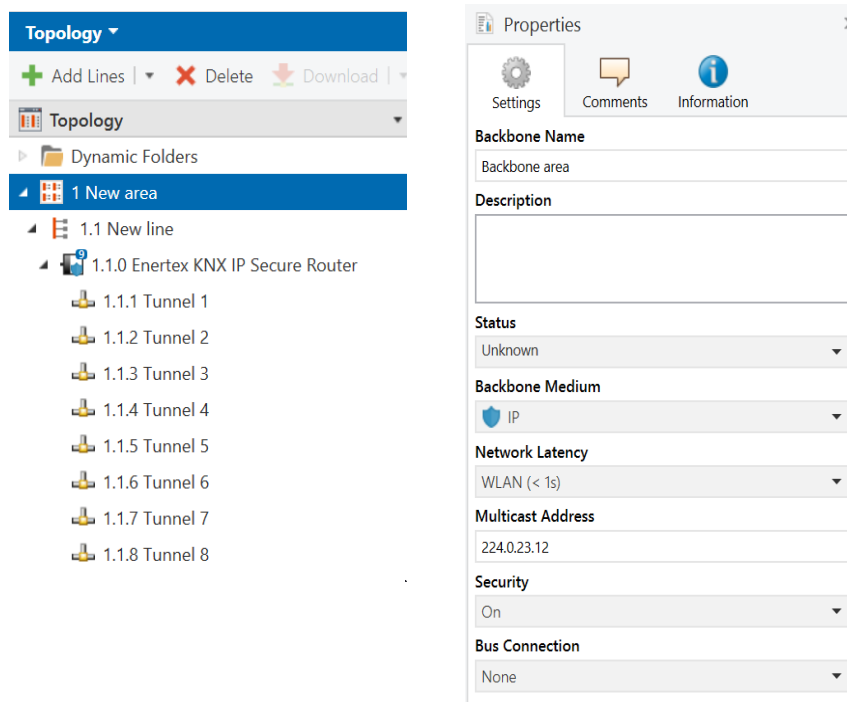


Figure 1: Topology (left) and properties of the backbone

Lines:

1: Backbone Medium IP

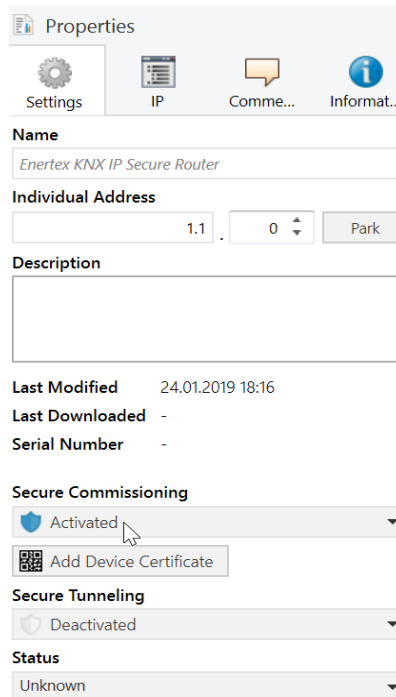
1.1: Line Medium TPium TP

In the Properties Diagram of the Backbone (NOTE: For this click on Topology, directly above "Dynamic Folders", see Figure 1), you will find the settings for the Multicast of the Backbone. Network latency (see Figure 1) can be changed if the routing is over a large distributed system. In this case, increase the time constant.

The device is parameterized with the ETS 5.6.6 or higher. The KNX IP Secure Router supports up to eight KNX (Secure) IP tunnel connections and can be used as a line or area coupler.

Device Properties

General



Properties

Settings IP Comme... Informat...

Name
Enertex KNX IP Secure Router

Individual Address
1.1 . 0 Park

Description

Last Modified 24.01.2019 18:16
Last Downloaded -
Serial Number -

Secure Commissioning
 Activated
 Add Device Certificate

Secure Tunneling
 Deactivated

Status
 Unknown

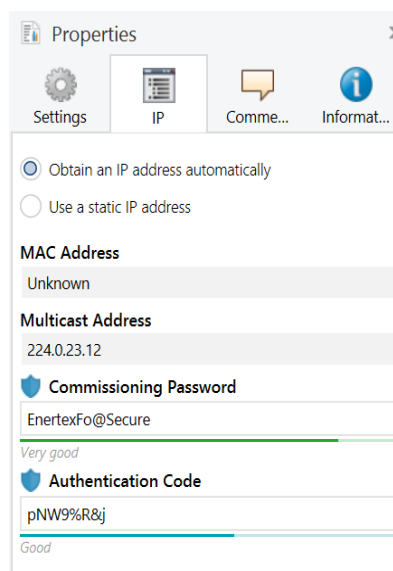
Figure 2: Properties of the device

Name Any name can be assigned, max. 30 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.

Secure Tunneling If activated, the tunnel connections can only be established via KNX Secure Tunneling.

IP Properties



Properties

Settings IP Comme... Informat...

☒ Obtain an IP address automatically
☐ Use a static IP address

MAC Address
 Unknown

Multicast Address
 224.0.23.12

Commissioning Password
 EnertexFo@Secure

Very good

Authentication Code
 pNW9%R&j

Good

Abbildung 3: IP Einstellungen des Geräts

Obtain an IP address automatically The device requires a DHCP server for IP address assignment

Use a static address The user specifies the IP settings.

Commissioning 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 1).

Device-specific parameters

General

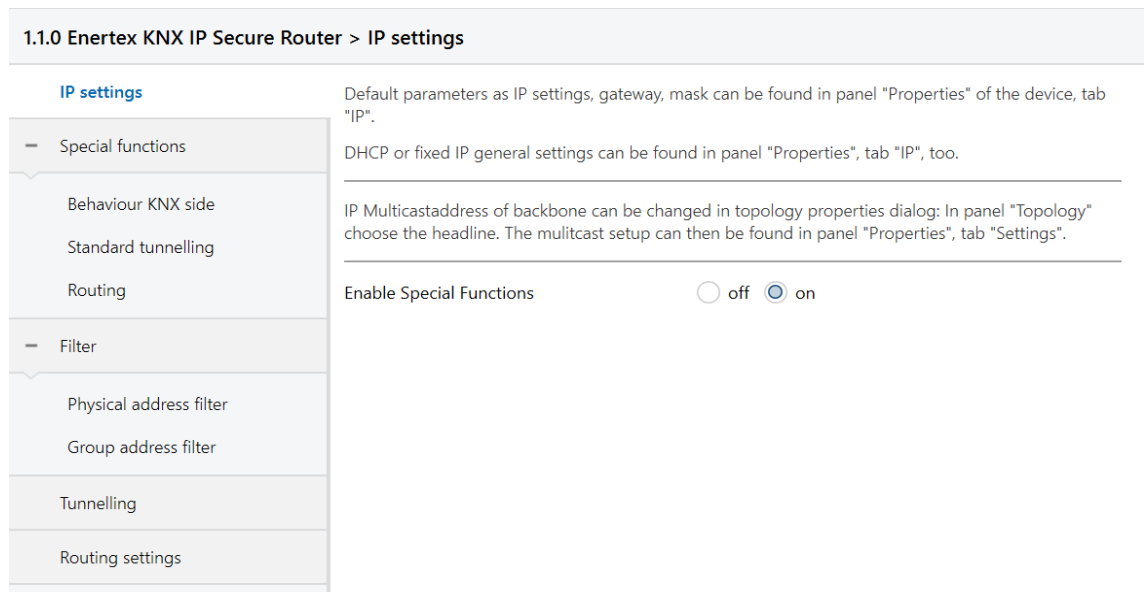


Figure 4: General settings of the device

Name	Options	Description
(Text)		The ETS has manufacturer-independent uniform parameter dialogs for various settings. To simplify the application, a note text is displayed here.
Enable Special Functions	<u>off</u> /on	Enertex® devices offer special functions to ensure a maximum of flexibility.

Special Functions

Behavior of the KNX side

1.1.0 Enertex KNX IP Secure Router > Special functions > Behaviour KNX side

IP settings	Note: If a tunnelling connection is used, every telegram is acked in any case. Therefore this setting is useful if using the device as router only.
Special functions	ACK for every telegram <input checked="" type="radio"/> off <input type="radio"/> on
Behaviour KNX side	Direction: device as receiver (KNX side)
Standard tunnelling	ACK for routed telegrams only <input checked="" type="radio"/> on <input type="radio"/> off
Routing	Direction: device as sender (KNX side)
Filter	Repeat routed telegrams if not ACKed <input type="radio"/> off <input checked="" type="radio"/> on
Physical address filter	If a line is easily accessible (e.g. KNX line for outside), the router can be locked, so it can not be reprogrammed by KNX bus at all but only from IP. This adds extra security to your installation.
Group address filter	Inhibit programming from KNX side <input checked="" type="radio"/> off <input type="radio"/> on
Tunnelling	Telegram rate limit for sending (TP side only). 50 Telegrams per second equals 100% bus load.
Routing settings	Max. number of telegrams to KNX TP <input type="text" value="50"/> T/s

Figure 5: Behavior of the KNX side

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

Standard tunnel preferred IP

Enertex® devices offer the possibility for standard tunnel connections (before 2019) 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.

Note:

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

1.1.0 Enertex KNX IP Secure Router > Special functions > Standard tunnelling

IP settings	Slow Connection (UDP Clients only) <input type="radio"/> off <input checked="" type="radio"/> on
Special functions	UDP Connection Timeout <input type="text" value="1"/> sec
Behaviour KNX side	If a connection is running e.g. over the Internet the normal timeout (1s) can be too small. Parameter range is [1.0 .. 8.0] seconds.
Standard tunnelling	<p>A standard tunnelling connection (so called BasicCRI, devices upto ETS4) can not determine which tunnel to be used for a connection request. With this feature the tunnels are preferably assigned to an IP address.</p> <p>Note, this is a weak assignment. Management connections or (new) extended CRI connections will override this assignment.</p> <p>Preferred IP for Tunnel 1 <input type="radio"/> off <input checked="" type="radio"/> on</p> <p>End device IP <input type="text" value="192.168.1.131"/></p> <p>Preferred IP for Tunnel 2 <input checked="" type="radio"/> off <input type="radio"/> on</p> <p>Preferred IP for Tunnel 3 <input checked="" type="radio"/> off <input type="radio"/> on</p> <p>Preferred IP for Tunnel 4 <input checked="" type="radio"/> off <input type="radio"/> on</p> <p>Preferred IP for Tunnel 5 <input checked="" type="radio"/> off <input type="radio"/> on</p> <p>Preferred IP for Tunnel 6 <input checked="" type="radio"/> off <input type="radio"/> on</p> <p>Preferred IP for Tunnel 7 <input checked="" type="radio"/> off <input type="radio"/> on</p> <p>Preferred IP for Tunnel 8 <input checked="" type="radio"/> off <input type="radio"/> on</p>
Routing	
Filter	
Physical address filter	
Group address filter	
Tunnelling	
Routing settings	

Figure 6: Preferred IP for Tunnelling

Name	Options	Description
Slow Connection	<u>off</u> /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	<u>1,0</u> ... 8,0 sec	Tunnel X should preferably be used for communication with the parametrized IP address.
Preferred IP for Tunnel X	<u>off</u> /on	
End device IP	(IP-V4 Address)	

Routing

1.1.0 Enertex KNX IP Secure Router > Special functions > Routing

IP settings	Check of topology
Special functions	If enabled, the router will detect an error in topology and send A_Network_Parameter_Response on KNX or IP line, respectively. This telegram is sent on the line, which violates the KNX rules for routing topology.
Behaviour KNX side	If enabled, the detected errors will be shown on display and in telnet interface. The erroneous telegrams will not be routed.
Standard tunnelling	Check topology <input checked="" type="radio"/> off <input type="radio"/> on
Routing	
Filter	Legacy routing
Physical address filter	If enabled, the router acts as KNX routers built before 2018. This means different behaviour of routing count algorithm. This legacy routing has higher vulnerability to certain attacks.
Group address filter	If router used as replacement in existing installations, this might be necessary.
Tunnelling	Enable old routing behaviour <input checked="" type="radio"/> off <input type="radio"/> on
Routing settings	

Figure 7: Routing

Name	Options	Description
Check of topology	<u>off</u> /on	See parameter dialog
Legacy routing	<u>off</u> /on	See parameter dialog

Physical address filter

1.1.0 Enertex KNX IP Secure Router > Filter > Physical address filter

IP settings	Physically addressed
Special functions	IP => KNX <input type="text" value="filter (default)"/>
Behaviour KNX side	KNX => IP <input type="text" value="filter (default)"/>
Standard tunnelling	Block Broadcast Telegrams
Routing	IP => KNX <input checked="" type="radio"/> off <input type="radio"/> on
Filter	KNX => IP <input checked="" type="radio"/> off <input type="radio"/> on
Physical address filter	

Figure 8: Physical address filter

Name	Options	Description
Physically addressed	<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 address filter

Standard

1.1.0 Enertex KNX IP Secure Router > Filter > Group address filter

IP settings	IP => KNX	
Special functions	Main Group 0..13	route
	Main Group 14..15	filter
	Main Group 16..31	filter
	Extended Group Address Filter	<input type="radio"/> off <input checked="" type="radio"/> on
Behaviour KNX side		
Standard tunnelling		
Routing		
Filter	KNX => IP	
Physical address filter	Main Group 0..13	route
	Main Group 14..15	filter
	Main Group 16..31	filter
	Extended Group Address Filter	<input type="radio"/> off <input checked="" type="radio"/> on
Group address filter		
Ext. filter IP => KNX		
Ext. filter KNX => IP		

Figure 9: Standard Filter Group address

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

Main Group 14 to 15	<u>filter</u> , block, route	Group telegrams can be routed, blocked or filtered via the routing. Groups 14 and 15 are grouped together to form a block.
Main Group 16 to 31	<u>filter</u> , block, route	Group telegrams can be routed, blocked or filtered via the routing. The groups 16 and 31 are here combined to form a block.
Extended Group Address Filter	<u>off/on</u>	In addition to the block-oriented filtering of group address telegrams, each group can also be separately routed, blocked or filtered via the routing. With this function, the parameter dialog can be opened for this purpose.

Extended Group Address Filter

For both directions, in addition to the block-oriented filtering of group address telegrams, each group can also be individually routed, blocked or filtered via the routing. Therefore, there are the links in the navigation bar when activated (see Figure 8 and Figure 9, respectively) „ext. filter IP=>KNX“ and „ext. filter KNX=>IP“.

For each of these entries, there are 32 more group address filters that work independently of the block-oriented filters. The settings of the 32 group address filters override those of the block-oriented filter.

1.1.0 Enertex KNX IP Secure Router > Filter > Group address filter > Ext. filter IP => KNX

IP settings	Advanced filter for direction IP => KNX	
Special functions	You can add a filter for each single main group . This overrides the cumulative settings of the group address filter (0..13, 14..15, or 16..31). If disabled, the standard filter is active.	
Behaviour KNX side	Main Group 00	disabled (default)
Standard tunnelling	Main Group 01	disabled (default)
Routing	Main Group 02	disabled (default)
Filter	Main Group 03	disabled (default)
Physical address filter	Main Group 04	disabled (default)
Group address filter	Main Group 05	disabled (default)
Ext. filter IP => KNX	Main Group 06	disabled (default)
Ext. filter KNX => IP	Main Group 07	route block filter disabled (default) ✓
Tunnelling	Main Group 08	disabled (default)
Routing settings	Main Group 09	disabled (default)
	Main Group 10	disabled (default)
	Main Group 11	disabled (default)
	Main Group 12	disabled (default)
	Main Group 13	disabled (default)
	Main Group 14	disabled (default)
	Main Group 15	disabled (default)
	Main Group 16	disabled (default)
	Main Group 17	disabled (default)
	Main Group 18	disabled (default)

Figure 10: Extended Group Address Filter

Name	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 8 and Figure 9, respectively.
Main Group NN NN= 1.. 31	See above	See above

Telnet

Telnet can be used to request additional information from the IP router. Telnet access is factory-protected with the password "knxsecure".

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

Although it can be enabled for developer purposes prior to programming the secure mode, this is a security risk.

<code>help</code>	Displays all available commands
<code>ifconfig</code>	Displays network parameters <pre>IP mode.....: DHCP IP.....: 192.168.33.142 Subnet mask...: 255.255.0.0 Gateway.....: 192.168.33.1 NTP server....: 192.53.103.108 Sys multicast.: 224.0.23.12 RT multicast..: 224.0.23.12 Hardware addr.: 00:50:c2:79:3f:ff</pre> <p>Sys multicast: Multicast address for System telegrams RT multicast: Multicast address für routing telegrams</p>
<code>ifconfig [help dhcp ip mask]</code>	Set network parameters via the telnet interface. Expamples Setting IP Adresse with DHCP: <pre>ifconfig dhcp</pre> <p>Statically set the IP address to 192.168.1.2 (in this case, the gateway and mask should also be adapted, see below)</p> <pre>ifconfig ip 192.168.1.2</pre> <p>Set the gateway to 192.168.1.1: <pre>ifconfig gw 192.168.1.1</pre> <p>Set the mask to 255.255.255.0: <pre>ifconfig mask 255.255.255.0</pre></p></p>
<code>tpconfig</code>	Show KNX parameters <pre>KNX bus state.: up KNX address...: 15.15.000 Serial number.: 00-a6-00-00-00-01</pre>
<code>tpconfig [help set]</code>	Set KNX parameters via the telnet interface. Set the TP address to 1.1.0: <pre>tpconfig set 1.1.0</pre>
<code>lcconfig</code>	Coupler type..: line coupler IP -> KNX: <pre>GA 0-13.....: route GA 14-15.....: filter GA 16-31.....: block Ph. addr.....: filter Broadcast.....: route KNX -> IP: GA 0-13.....: route GA 14-16.....: filter GA 16-31.....: block Ind.addr.....: filter Broadcast.....: route Check IA rout.: disabled Ind.Addr.tlg..: individually addressed telegrams are 3 times repeated</pre>
<code>systembc [0 1]</code>	Set certain bits in the system broadcasts so that IP routing is possible even on older devices (e.g. Gira Homerserver). By default, this compatibility mode is turned on. Wrong handling of bits in system broadcasts (necessary for e.g. Gira Homerserver) is 1 (on)
<code>progmode [0 1]</code>	Query or change programming mode (0 = off, 1 = on)
<code>apdu [55..248]</code>	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. <pre># apdu maximal len of a KNX telegram 248. Usage: apdu [55 .. 248]</pre>

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


<code>tunnel [1..8]</code>	<p>Shows active tunnel connections (without argument) or detailed information about the specified tunnel connection (with argument 1..8)</p> <pre># tunnel Tunnels open: 1/8 1: 00.02.246, closed 2: 00.02.247, open (CCID: 82) 3: 00.02.248, closed 4: 00.02.249, closed 5: 00.02.250, closed 6: 00.02.251, closed 7: 00.02.252, closed 8: 00.02.253, closed # tunnel 2 Tunnel 2.....: open (CCID 82) KNX address.....: 00.02.247 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</pre> <p>CCID: Connection ID of the tunnel connection KNX address: Tunnelling address HPAI control: Control endpoint of the connection partner HPAI data: Data endpoint of the connection partner Connect. Type: Connection type tunnel or management connection Communication: UDP or TCP Connection TX tun req: Number of telegrams sent to the tunnel connection TX tun re-req: Number of telegrams that had to be repeated in the tunnel connections RX tun req: Number of telegrams received from the tunnel connections RX tun re-req: Number of telegrams received twice by the tunnel connections RX tun req (wrong seq.): number of frames received from the tunnel connections with wrong sequence number Current tunnel buffer: Utilization currently of the IP buffer of the tunnel Connected since (UTC): Time since the tunnel connection has been established.</p>
<code>version</code>	Firmware-Version
<code>mask</code>	Mask-Version
<code>display [0 1]</code>	Query or change the display mode (0 = standard, 1 = inverted)
<code>tunaddr 1..8 address</code> <code>tunaddr reset</code> <code>tunaddr setall</code> <code>tunaddr help</code>	<p>KNX address of a tunnel read (<code>tunaddr</code>) or change, e.g. <code>tunaddr 1 15.15.240</code>, set all tunnel addresses consecutively from a certain start address (<code>tunaddr setall 15.15.15</code>), or reset the KNX addresses of all tunnels to factory settings (<code>tunaddr reset</code>)</p> <pre># tunaddr 1: KNX address: 15.15.010 2: KNX address: 15.15.011 3: KNX address: 15.15.012 4: KNX address: 15.15.013 5: KNX address: 15.15.014 6: KNX address: 15.15.015 7: KNX address: 15.15.016 8: KNX address: 15.15.017</pre>
<code>tunmode [std/tpblk]</code>	<p>Read tunnel mode (without parameters) or set (<code>tp</code> or <code>tpblk</code>); <code>tunmode tpblock:IP => KNX</code> If same backbone forward to line frame <code>KNX=> IP</code> if same sub line send to backbone</p>
<code>lock [0 1]</code>	<p>Query lock status (without further parameters) or change (0 = off, 1 = on). Setting is identical to programming lock TP page, Figure 5.</p> <p>A router can prevent the forwarding of physically addressed telegrams by filtering, i. It is not possible to reprogram devices across a line. This becomes interesting when using outdoor lines.</p> <p>However, e.g. if a KNX-USB interface is connected to an outdoor line directly to the bus, the router itself could be re-programmed, so that it forwards the physically addressed telegrams. With that, any access to the internal line is possible.</p> <p>This can be prevented with this telnet function. If you set telnet "lock" to 1, the router can no longer be programmed via the KNX line and corresponding activation of forwarding via KNX TP is no longer possible.</p>
<code>topology [0 1]</code>	<p>Query or change "topology check" (0 = off, 1 = on). Setting is identical to "Topology check", Figure 7</p> <pre>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</pre>
<code>Tunneltime [1.0..8.0]</code>	Query or change timeout for tunnel connection (1.0 to 8.0). Setting is identical to "slow connection", Figure 6

tunudp	Query or change the type of tunnel connection for the ETS (0 = default, 1 = UDP only).
date	Show 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)
sendack [0 1]	Querying or changing every telegram (ACK). Setting is identical to the documentation to Figure 5.
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 Legacy Routing Algorithm <2018, Figure 7
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)
secure [0 1]	Display or change the behavior of the Telnet interface in secure mode (0 = disable, default, 1 = enable) Note: Although it can be enabled for developer purposes prior to programming the secure mode, this is a security risk.
factory_reset	Reset to factory settings and reboot
die	Test hardware watchdog. Executes reset.
reboot	reboot
logout	end Telnet-Session

Latest documentation and Software

Under <http://www.enertex.de/d-produkt.html> you will find the current ETS database file as well as the current product description.

Specification

Symbols	 — Must not be disposed of with household waste.
KNX (Powersupply)	DC 21 ... 32 V SELV current consumption < 20 mA
Ethernet-Interface	Rj45-connector 10M/100MBit Ethernet
Display	Graphical OLED, 128x64 Programming LED (red), Bus Activity LED (yellow), Voltage LED (green flashing) Network link (green), network activity (yellow)
KNX Functions	<ul style="list-style-type: none"> • KNXIP Secure Tunneling and Routing • 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)
Environment	-5 ... +45° C
Installation	<ul style="list-style-type: none"> • Only for use in dry interiors. • Only for installation in distributor according to DIN 43880 on DIN rail 35mm according to EN 50022. • Degree of protection IP20
Outer dimensions	35,0 mm x 89,6 mm x 62,9 mm (L x B x H)

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>

LWIP

Quelle: <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.