

IP Router

KNX IP Router (IP – TP)

ZSYIPR

USER MANUAL

Software Library Version: [1.0]

User Manual Version: [1.0]_a

www.zennio.com

Contents

1. IP Router 2

1.1. Features 2

1.2. Start-up and power loss 3

1.3. LED indicators 3

1.4. Buttons 4

1.5. Safe mode and factory reset 5

1.6. IP Tunnelling 6

1.7. KNX Security and Security Proxy 6

Configuration 7

2.1. General 7

2.1.1. Diagnostics 7

2.2. IP Medium 8

2.2.1. Received Telegrams (IP Medium) 8

2.3. TP Medium 9

2.3.1. Received Telegrams (TP Medium) 9

2.3.2. Sent Telegrams 10

Filter Table / Security Proxy Table 12

1. IP Router

IP Router manual, reference **ZSYIPR**

1.1. Features

IP Router is the Zennio solution for the **interconnection** of a KNX **twisted pair** (TP) line with a **KNX IP** network. The IP medium acts as the main line and the TP medium as the secondary line.

The main features of the **IP Router** are:

- Possibility of working as an **area coupler**.
- Possibility of working as a **line coupler**.
- Possibility of working as a **segment coupler**.
- Telegram filtering depending on the selected parameterisation options.
- **IP interface** with capacity for **10 simultaneous tunnelling connections**, plus a direct connection for programming the device itself from ETS.
- Support for **extended frames** with a **maximum APDU of 254 bytes**.
- **5 LED indicators**: one as programming mode indicator, two to indicate the status of the IP and TP media, another to indicate the operating mode of the coupler and another to indicate the IP address assignment method forced manually.
- **"IP Conf." button** to temporarily change the IP address assignment method (static, DHCP or AutoIP) without using ETS.
- **Manual control** to allow the routing of all telegrams by group address or by individual address.
- **KNX Security**: support for *KNX Data Security* and *KNX IP Security* (see section 1.7).
- **Security Proxy**: functionality that translates secure multicast telegrams from one medium into plain telegrams sent to the other medium.
- **Plug & Play**: with the factory configuration, the device routes telegrams without prior programming (see section 1.2).

> **Note**
>
> *The Security Proxy functionality is only available in ETS6. KNX Security must be enabled for it to work.*

> **Note**
>
> *The product information label includes a unique RESERVED KEY. It currently has no assigned use, but it is reserved for possible future use, so it is important to keep it.*

1.2. Start-up and power loss

This device has no specific configuration to be executed during start-up. In its factory state, the **IP Router** has the following configuration, which allows the installation to be commissioned without programming it first:

- Individual address **15.15.0**.
- Routing multicast address **224.0.23.12**.
- IP address assignment via **DHCP**. If there is no DHCP server on the network, the device keeps routing telegrams via multicast.
- Routing of broadcast telegrams enabled.
- Tunnelling service available as soon as the device has a valid IP address.

Regarding power failures, two cases must be considered:

- **Power failure on the TP line**: the device is powered from the KNX bus of the TP line. If a power failure occurs on this line, the device is no longer powered, any kind of telegram routing is interrupted and it cannot be accessed for programming through ETS.
- **Loss of connection to the IP network**: the device stops routing telegrams between both media and indicates it through the IP LED (see section 1.3).

The parameterisation and configuration of the device are retained after a power failure.

1.3. LED indicators

The **IP Router** has 5 LED indicators that make it easier to monitor its status and detect problems.

- **Programming LED**: red LED that lights up if the device is in programming mode and blinks if it is in safe mode.
- **IP LED**: indicates the status of the IP medium (main line):
  - **Off**: no Ethernet link and no IP address.
  - **Yellow (steady)**: Ethernet link and no IP address.
  - **Green (steady)**: Ethernet link and IP address.
  - **Green or yellow (blinking)**: sending or receiving KNX IP traffic (green if the device has a valid IP address; yellow otherwise).
  - **Red (steady)**: no Ethernet link and IP address.
  - **Red (blinking)**: no Ethernet link; an attempt to send a telegram over IP has failed.
- **TP LED**: indicates the status of the TP line (secondary line):
  - **Off**: no power supply.
  - **Green (steady)**: powered.
  - **Green (blinking)**: receiving or sending telegrams.

  - **Red (blinking)**: a communication error has occurred: telegram sent without acknowledgement, sending without connection to the KNX bus or reception of a faulty telegram.

- **Mode LED**: indicates the operating mode of the coupler.
  - **Off**: working as a line or area coupler.
  - **Green (steady)**: working as a segment coupler.
  - **Yellow (slow blinking, 500 ms period)**: "*Pass GA*" operation enabled.
  - **Yellow (fast blinking, 250 ms period)**: "*Pass IA*" operation enabled.
  - **Yellow (steady)**: "*Pass GA*" and "*Pass IA*" operation enabled.
- **IP Conf. LED**: indicates the IP address assignment method forced with the "IP Conf." button (see section 1.4):
  - **Off**: the method configured in ETS applies.
  - **Green (steady)**: DHCP assignment forced.
  - **Yellow (steady)**: AutoIP assignment forced.

> **Note**
>
> *The yellow colour of the Mode LED indicates that the "Pass IA/GA" button has been pressed and the associated functionality is active: routing all telegrams (individual and/or group). It does not reflect the parameterisation made in ETS, i.e. if the coupler is parameterised to route all telegrams but the button is not pressed, the LED will light up green or remain off.*

1.4. Buttons

The **IP Router** has 3 buttons that make it easier to control the device.

- **Programming button**: activates programming mode if the device is powered and, if the device is started with the button pressed, makes it enter safe mode (see section 1.5).
- **"Pass IA/GA" button**: provided that manual control has been enabled (see section 2.1), it allows all telegrams addressed to an individual address (*Pass IA*) and/or to a group address (*Pass GA*) to be routed to the other medium, regardless of the parameterised routing or filtering options. Starting with both modes inactive, successive presses go through the following sequence:
  - First press: *Pass IA* active.
  - Second press: *Pass GA* active.
  - Third press: *Pass IA* and *Pass GA* active.
  - Fourth press: *Pass IA* and *Pass GA* deactivated.

If **10 seconds or more** have elapsed with any mode active, a new press deactivates them directly, regardless of the point of the sequence the device is at. This way, the integrator can easily deactivate the mode when it is no longer needed.

The activated mode remains until one of the following occurs:

- The device restarts.
- The mode is deactivated by pressing the button again.
- The maximum duration parameterised in ETS for manual control elapses.

> **Note**
>
> *The "Pass IA/GA" button has no effect if manual control is disabled or if the device is in safe mode.*

- **"IP Conf." button**: allows the IP address assignment method of the device to be changed **temporarily**. Each **long press of 3 seconds** moves to the next method in the sequence:
  - **Static** → **DHCP** → **AutoIP** → **Static**…

The "IP Conf." LED indicates the forced method: green for DHCP, yellow for AutoIP and off when the method configured in ETS applies again (see section 1.3).

- If a **static IP address** has been configured in ETS, the sequence goes through the three methods.
- If **DHCP** has been configured in ETS, it is not possible to force a static IP address, as the device has no programmed IP address, subnet mask or default gateway. In this case, the sequence alternates between DHCP (LED off) and AutoIP (LED yellow).

> **Note**
>
> *The change is temporary: after a restart, the device always applies the assignment method configured in ETS again.*

1.5. Safe mode and factory reset

In **safe mode**, the device only keeps the functionality needed to reprogram or diagnose it:

- No telegram is routed from one medium to the other.
- Telegrams not addressed to the device itself are not acknowledged.
- It is still possible to establish a tunnelling connection.

Safe mode is indicated by **one blink per second of the programming LED**. It is entered in the following ways:

- Holding down the programming button while powering the device.
- Automatically, if the device restarts three times due to a malfunction with less than 10 seconds between restarts.

To **exit safe mode**, simply restart the device without holding down the programming button.

While in safe mode, a **long press of 10 seconds** on the programming button returns the device to its **factory state**, keeping its individual address. Outside safe mode it is not possible to reset the device manually, which prevents accidental resets.

> ⚠ **Important**
>
> *The factory reset erases the parameterisation and the KNX Security configuration of the device. It will be necessary to program it again from ETS.*

1.6. IP Tunnelling

The **IP Router** includes an IP interface that allows up to **10 simultaneous tunnelling connections**, for example, to program or monitor the installation from ETS over the IP network. Each tunnelling connection has its own individual address on the TP line.

In addition, the device supports a direct connection for its own programming from ETS, without the telegrams reaching the KNX bus.

The status of the tunnelling connections can be checked from ETS (see section 2.1.1).

1.7. KNX Security and Security Proxy

The **IP Router** is compatible with both types of KNX Security:

- **KNX Data Security**: protects the telegrams addressed to the device itself, for example, during its programming from ETS.
- **KNX IP Security**: protects communication on the IP medium, both tunnelling connections and multicast routing between IP routers.

The **Security Proxy** functionality translates secure multicast telegrams received from one medium into plain telegrams sent to the other medium, and vice versa. It also allows additional routing rules to be added for non-multicast telegrams.

For detailed information about the KNX Security functionality and configuration, please refer to the specific user manual “KNX Security”.

Configuration

2.1. General - IP Router

After importing the corresponding database into ETS and adding the device to the topology of the desired project, the configuration process begins by assigning an individual address **X.Y.Z**. Depending on the use of the device, the configuration will be as follows:

- **Area coupler**: it must have individual address **X.0.0**.
- **Line coupler**: it must have individual address **X.Y.0**.
- **Segment coupler**: it must have individual address **X.Y.Z**.

The “General” tab (Figure 1) contains the following parameters:

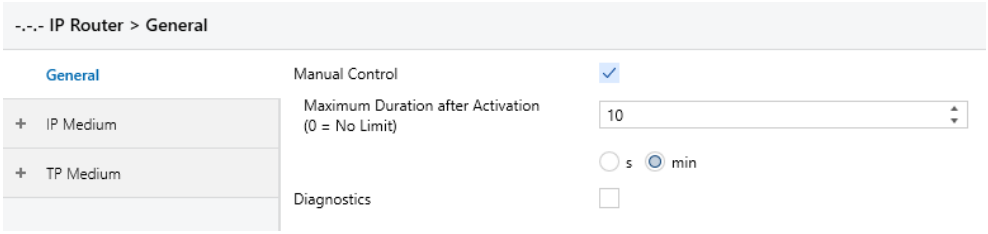


Figure 1. General.

- **Manual Control** [*disabled / enabled*]: prevents or allows the use of the “Pass IA/GA” button (see section 1.4).
  - **Maximum Duration after Activation (0 = No Limit)** [*0…10…60*] [*min*] / [*0…600…3600*] [*s*]: maximum time during which the *Pass IA* or *Pass GA* functionality remains active after its activation. The functionality can be deactivated before this time by pressing the button again.
- **Diagnostics**: enables the “Diagnostics” tab (see section 2.1.1).

2.1.1. Diagnostics

From this tab (Figure 2) it is possible to check the status of the tunnelling addresses of the device: which ones are in use and the IP address of the client connected to each one.

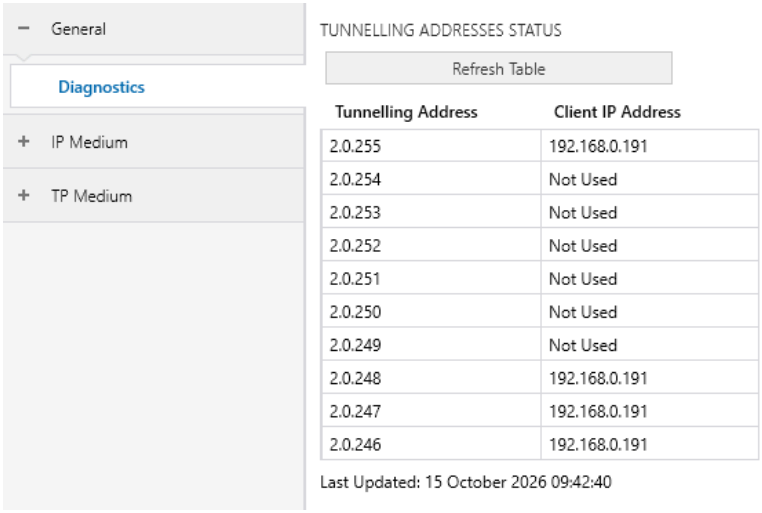


Figure 2. Diagnostics.

The information is not updated in real time: the “Refresh Table” button must be pressed to read it from the device. The data read is saved in the ETS project, so the date and time of the last update are shown, in the regional format of the PC.

2.2. IP Medium

The IP medium tabs determine the behaviour of the **IP Router** with the telegrams received from the IP network (main line).

2.2.1. Received Telegrams (IP Medium)

For telegrams received from the IP medium, there are three possible routing configurations:

- **Block**: the telegram never passes to the TP medium.
- **Route**: the telegram always passes to the TP medium.
- **Filter**: whether the telegram passes to the TP medium depends on its destination, as detailed for each parameter.

> **Note**
>
> *The restrictions are added to those of Security Proxy. If routing is set to **“Block”**, all telegrams are blocked and the Security Proxy exceptions no longer take effect. If routing is set to **“Filter”** / **“Route”**, in order to communicate with a device blocked by Security Proxy, ETS must activate a temporary exception of 60 seconds (renewed automatically every ~50 s during programming).*

The available parameters are shown in Figure 3.

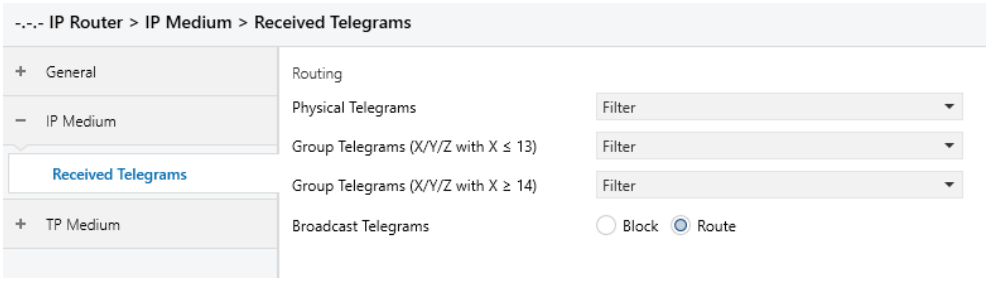


Figure 3. Received Telegrams (IP Medium).

Routing:

- **Physical Telegrams** [*Block / Route / Filter*]: telegrams addressed to an individual address, such as those sent while programming a device. With “Filter”, the telegram is only routed if the recipient is located on the TP medium.
- **Group Telegrams (X/Y/Z with X ≤ 13)** [*Block / Route / Filter*]: group telegrams whose main group is 13 or lower. With “Filter”, the telegram is only routed if at least one device on the TP medium uses that group address (see chapter 3).
- **Group Telegrams (X/Y/Z with X ≥ 14)** [*Block / Route / Filter*]: same as the previous one, for telegrams whose main group is 14 or higher.
- **Broadcast Telegrams** [*Block / Route*].

> **Note**
>
> *Telegrams addressed to the **IP Router** itself are always accepted and never routed to the other medium, regardless of this configuration.*

There are no telegram acknowledgement options on the IP medium.

2.3. TP Medium

The TP medium tabs determine the behaviour of the **IP Router** with the telegrams received and sent on the TP line (secondary line).

2.3.1. Received Telegrams (TP Medium)

Routing follows the same logic as in section 2.2.1, but in the opposite direction: it determines which telegrams pass from the TP medium to the IP medium (Figure 4).

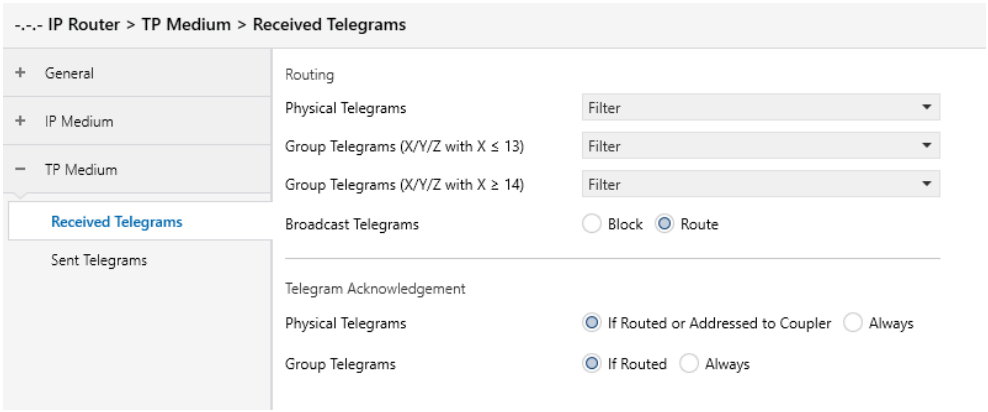


Figure 4. Received Telegrams (TP Medium).

Routing:

- **Physical Telegrams** [*Block / Route / Filter*].
- **Group Telegrams (X/Y/Z with X ≤ 13)** [*Block / Route / Filter*].
- **Group Telegrams (X/Y/Z with X ≥ 14)** [*Block / Route / Filter*].
- **Broadcast Telegrams** [*Block / Route*].

Telegram Acknowledgement:

- **Physical Telegrams** [*If Routed or Addressed to Coupler / Always*]: determines in which cases the device acknowledges a physical telegram received from the TP medium.
- **Group Telegrams** [*If Routed / Always*]: determines in which cases the device acknowledges a group telegram received from the TP medium.

> **Note**
>
> *The "Always" option makes the telegram appear as acknowledged (avoiding repetitions in the case of faulty projects, etc.) even if no device has received it. In the event of a reception error, the NACKs sent by the devices overwrite this acknowledgement, so no data is lost.*

> **Note**
>
> *While any tunnelling connection is open, the device always acknowledges the group telegrams received from the TP medium, as they can be captured by the tunnelling client.*

2.3.2. Sent Telegrams

This tab (Figure 5) determines the behaviour of the **IP Router** when sending telegrams coming from the IP medium to the TP line. It is possible to select which telegrams are repeated if no acknowledgement has been received or a NACK / BUSY has been received.

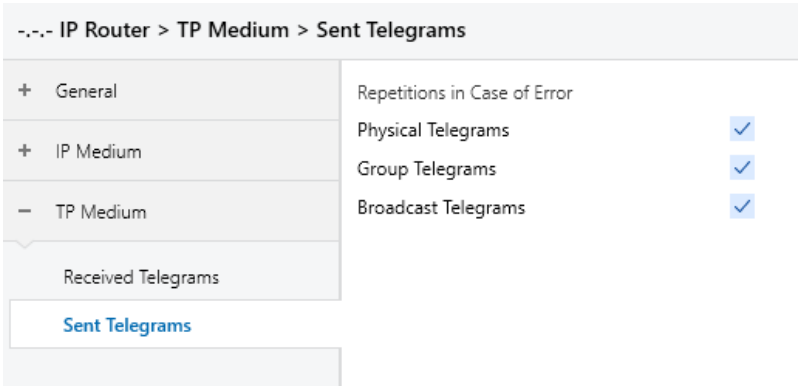


Figure 5. Sent Telegrams.

Repetitions in Case of Error:

- **Physical Telegrams** [*disabled / enabled*].
- **Group Telegrams** [*disabled / enabled*].
- **Broadcast Telegrams** [*disabled / enabled*].

> **Note**
>
> *This configuration does not apply to the responses of the device itself to telegrams addressed to it.*

> **Note**
>
> *With repetitions enabled, the device may dynamically suppress unnecessary repetitions in tunnelling connections to avoid overloading the bus.*

3. Filter Table / Security Proxy Table

The filter table is created automatically in ETS. The group addresses of the telegrams that must be routed by the coupler are included in this table. The content of this table can be checked through the preview, which also shows the Security Proxy tables.

To open the preview, right-click on the **IP Router** and, in the drop-down menu, select “Filter Table Preview” (Figure 6). A window like the one in Figure 7 will be displayed, with the group addresses routed by the coupler, organised by main group and middle group.

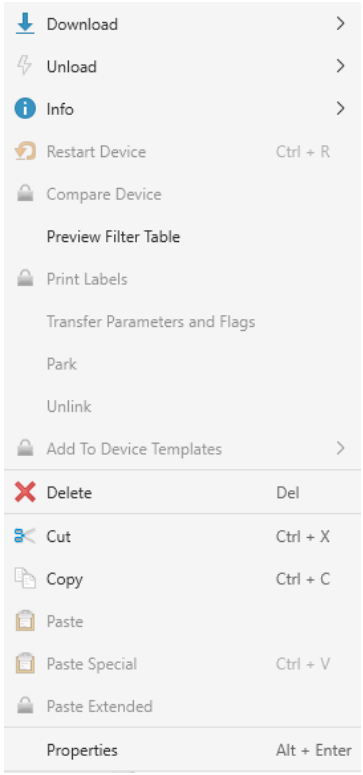


Figure 6. Device menu in ETS.

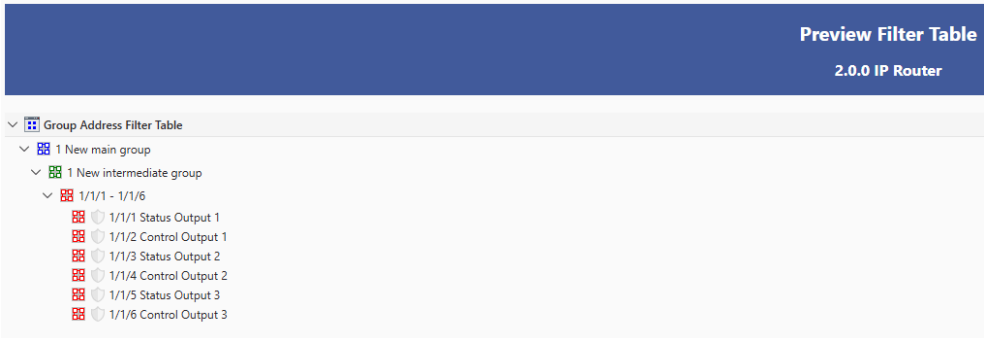


Figure 7. Filter table.

If the installation uses **KNX Security**, secure group addresses are identified in the preview by a filled shield icon, as shown in Figure 8.

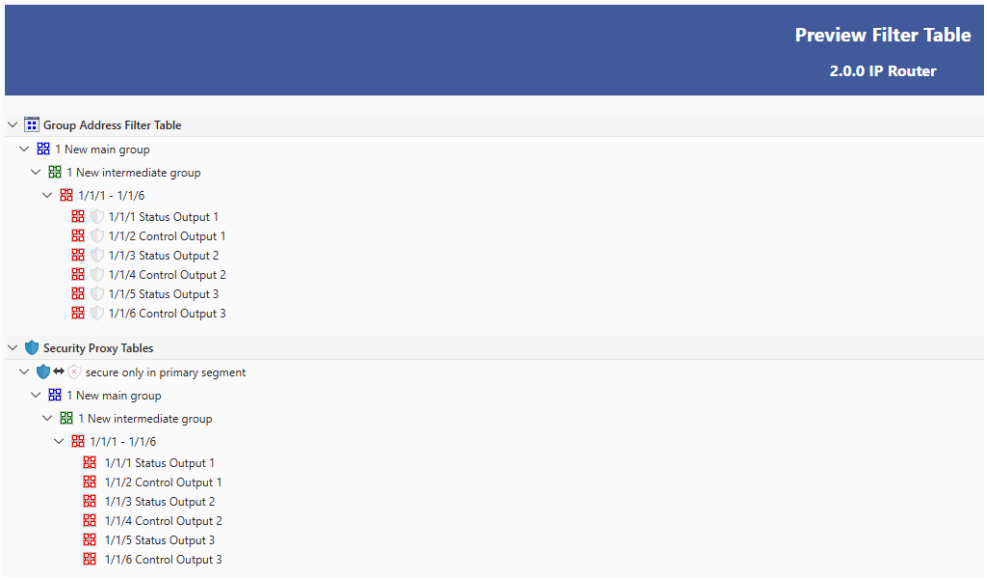


Figure 8. Filter table with secure group addresses.

Join and send us your inquiries about Zennio devices: https://support.zennio.com

Zennio Avance y Tecnología S.L.
C/ Río Jarama, 132. Nave P-8.11 45007 Toledo, Spain
Tel. +34 925 232 002
www.zennio.com
info@zennio.com