

IP Router

Router IP KNX (IP – TP)

ZSYIPR

MANUAL DE USUARIO

Versión de la librería software: [1.0]

Edición del manual: [1.0]_a

www.zennio.com

Índice

1. IP Router 2

1.1. Características 2

1.2. Inicialización y fallo de tensión 3

1.3. Indicadores LED 3

1.4. Botones 4

1.5. Modo seguro y reset de fábrica 5

1.6. IP Tunneling 6

1.7. Seguridad KNX y Security Proxy 6

Configuración 7

2.1. General 7

2.1.1. Diagnósticos 7

2.2. Medio IP 8

2.2.1. Telegramas recibidos (medio IP) 8

2.3. Medio TP 9

2.3.1. Telegramas recibidos (medio TP) 9

2.3.2. Telegramas enviados 10

Tabla de filtros / Tabla de security proxy 12

1. IP Router

Manual de **IP Router** con referencia **ZSYIPR**

1.1. Características

IP Router constituye la solución Zennio para la **interconexión** de una línea KNX de **par trenzado** (TP) con una red **KNX IP**. El medio IP actúa como línea principal y el medio TP como línea secundaria.

Las características principales del **IP Router** son:

- Posibilidad de funcionar como **acoplador de área**.
- Posibilidad de funcionar como **acoplador de línea**.
- Posibilidad de funcionar como **acoplador de segmentos**.
- Filtrado de telegramas en función de las opciones de parametrización seleccionadas.
- **Interfaz IP** con capacidad para **10 conexiones de túnel** simultáneas, además de una conexión directa para la programación del propio dispositivo desde ETS.
- Soporte de **tramas extendidas** con una **APDU máxima de 254 bytes**.
- **5 indicadores LED**: uno como indicador de modo programación, dos para indicar el estado de los medios IP y TP, otro para indicar el modo de funcionamiento del acoplador y otro para indicar el método de asignación de dirección IP forzado manualmente.
- **Botón "IP Conf."** para cambiar temporalmente el método de asignación de dirección IP (estática, DHCP o AutoIP) sin necesidad de ETS.
- **Control manual** para permitir el enrutado de todas las tramas por dirección de grupo o por dirección individual.
- **Seguridad KNX**: soporte de *KNX Data Security* y *KNX IP Security* (ver sección 1.7).
- **Security Proxy**: funcionalidad que permite traducir telegramas seguros multicast desde un medio a telegramas en plano enviados al otro medio.
- **Plug & Play**: con la configuración de fábrica, el dispositivo enruta telegramas sin necesidad de programación previa (ver sección 1.2).

> **Nota**
>
> *La funcionalidad de Security Proxy solo se encuentra disponible para ETS6. Debe estar habilitada la Seguridad KNX para su funcionamiento.*

> **Nota**
>
> *En la etiqueta de información de producto se incluye una RESERVED KEY única, actualmente no tiene un uso asignado, pero queda reservada para un posible uso futuro por lo que es importante que sea conservada.*

1.2. Inicialización y fallo de tensión

Este dispositivo no dispone de configuraciones específicas para ejecutar durante el arranque. En estado de fábrica, el **IP Router** presenta la siguiente configuración, que permite poner en marcha la instalación sin programarlo previamente:

- Dirección individual **15.15.0**.
- Dirección multicast de enrutamiento **224.0.23.12**.
- Asignación de dirección IP mediante **DHCP**. Si no hay servidor DHCP en la red, el dispositivo sigue enrutando telegramas por multicast.
- Enrutamiento de telegramas broadcast habilitado.
- Servicio de túnel disponible en cuanto el dispositivo dispone de una dirección IP válida.

Respecto a los fallos de tensión, deben considerarse dos casos:

- **Fallo de tensión en la línea TP**: el dispositivo se alimenta del bus KNX de la línea TP. Si se produce un fallo de tensión en esta línea, el dispositivo deja de estar alimentado, interrumpiendo cualquier tipo de enrutamiento de tramas, y no podrá ser accesible para su programación a través de ETS.
- **Pérdida de conexión con la red IP**: el dispositivo deja de enrutar tramas entre ambos medios y lo indica mediante el LED IP (ver sección 1.3).

La parametrización y la configuración del dispositivo se conservan tras un fallo de tensión.

1.3. Indicadores LED

El **IP Router** dispone de 5 indicadores LED que facilitan el seguimiento del estado y la detección de problemas.

- **LED de programación**: LED rojo que se enciende si el dispositivo se encuentra en modo programación y parpadea si está en modo seguro.
- **LED IP**: indica el estado del medio IP (línea principal):
  - **Apagado**: sin conexión Ethernet y sin dirección IP.
  - **Amarillo (sólido)**: con conexión Ethernet y sin dirección IP.
  - **Verde (sólido)**: con conexión Ethernet y con dirección IP.
  - **Verde o amarillo (parpadeo)**: envía o recibe tráfico KNX IP (verde si el dispositivo tiene una dirección IP válida; amarillo en caso contrario).
  - **Rojo (sólido)**: sin conexión Ethernet y con dirección IP.
  - **Rojo (parpadeo)**: sin conexión Ethernet; se ha intentado enviar un telegrama por IP y no ha sido posible.
- **LED TP**: indica el estado de la línea TP (línea secundaria):
  - **Apagado**: sin alimentación.

- **Verde (sólido)**: recibe alimentación.
- **Verde (parpadeo)**: recibe o envía telegramas.
- **Rojo (parpadeo)**: se ha producido un error de comunicación: telegrama enviado sin confirmación, envío sin conexión con el bus KNX o recepción de un telegrama con errores.

- **LED Mode**: indica el modo de funcionamiento del acoplador.
  - **Apagado**: funcionamiento como acoplador de línea o área.
  - **Verde (sólido)**: funcionamiento como acoplador de segmentos.
  - **Amarillo (parpadeo lento, periodo 500 ms)**: funcionamiento "*Pass GA*" activado.
  - **Amarillo (parpadeo rápido, periodo 250 ms)**: funcionamiento "*Pass IA*" activado.
  - **Amarillo (sólido)**: funcionamiento "*Pass GA*" y "*Pass IA*" activado.
- **LED IP Conf.**: indica el método de asignación de dirección IP forzado con el botón "IP Conf." (ver sección 1.4):
  - **Apagado**: se aplica el método configurado en ETS.
  - **Verde (sólido)**: asignación por DHCP forzada.
  - **Amarillo (sólido)**: asignación por AutoIP forzada.

> **Nota**
>
> *El color amarillo del LED Mode indica que se ha pulsado el botón "Pass IA/GA" y se ha activado la funcionalidad asociada: enrutar todas las tramas (individuales y/o de grupo). No refleja la parametrización realizada en ETS, es decir, si se parametriza el acoplador para enrutar todos los telegramas, pero no se pulsa el botón, el LED se encenderá en verde o se mantendrá apagado.*

1.4. Botones

El **IP Router** dispone de 3 botones que facilitan el control del dispositivo.

- **Botón de programación**: activa el modo programación si el dispositivo está alimentado y, en caso de arrancar el dispositivo con el botón pulsado, hace que entre en modo seguro (ver sección 1.5).
- **Botón "Pass IA/GA"**: siempre que el control manual haya sido habilitado (ver sección 2.1), permite enrutar al otro medio todas las tramas dirigidas a una dirección individual (*Pass IA*) y/o a una dirección de grupo (*Pass GA*), independientemente de las opciones de enrutado o filtrado parametrizadas. Partiendo de ambos modos inactivos, las pulsaciones sucesivas recorren la siguiente secuencia:
  - Primera pulsación: *Pass IA* activo.
  - Segunda pulsación: *Pass GA* activo.
  - Tercera pulsación: *Pass IA* y *Pass GA* activos.
  - Cuarta pulsación: *Pass IA* y *Pass GA* desactivados.

Si han transcurrido **10 segundos o más** con algún modo activo, una nueva pulsación los desactiva directamente, independientemente del punto de la secuencia en que se encuentre el dispositivo. De esta forma, el integrador puede desactivar el modo fácilmente cuando ya no lo necesite.

El modo activado permanece hasta que ocurra alguno de los siguientes casos:

- El dispositivo se reinicia.
- Se desactiva el modo pulsando el botón de nuevo.
- Transcurre la duración máxima parametrizada en ETS para el control manual.

> **Nota**
>
> *El botón "Pass IA/GA" no tiene efecto si el control manual está inhabilitado o si el dispositivo se encuentra en modo seguro.*

- **Botón "IP Conf."**: permite cambiar **temporalmente** el método de asignación de dirección IP del dispositivo. Cada **pulsación larga de 3 segundos** pasa al siguiente método de la secuencia:
  - **Estática → DHCP → AutoIP → Estática**…

El LED "IP Conf." indica el método forzado: verde para DHCP, amarillo para AutoIP y apagado cuando se aplica de nuevo el método configurado en ETS (ver sección 1.3).

- Si en ETS se ha configurado **dirección IP estática**, la secuencia recorre los tres métodos.
- Si en ETS se ha configurado **DHCP**, no es posible forzar la dirección IP estática, ya que el dispositivo no dispone de dirección IP, máscara de subred ni puerta de enlace programadas. En este caso, la secuencia alterna entre DHCP (LED apagado) y AutoIP (LED amarillo).

> **Nota**
>
> *El cambio es temporal: tras un reinicio, el dispositivo vuelve a aplicar siempre el método de asignación configurado en ETS.*

1.5. Modo seguro y reset de fábrica

En **modo seguro**, el dispositivo mantiene solo la funcionalidad necesaria para poder reprogramarlo o diagnosticarlo:

- No se enruta ningún telegrama de un medio al otro.
- No se confirman telegramas que no vayan dirigidos al propio dispositivo.
- Sigue siendo posible establecer una conexión de túnel.

El modo seguro se indica con **un parpadeo por segundo del LED de programación**. Se entra en él de las siguientes formas:

- Manteniendo pulsado el botón de programación al alimentar el dispositivo.

- De forma automática, si el dispositivo se reinicia tres veces por un fallo de funcionamiento en menos de 10 segundos entre reinicios.

Para **salir del modo seguro**, basta con reiniciar el dispositivo sin mantener pulsado el botón de programación.

Estando en modo seguro, una **pulsación larga de 10 segundos** en el botón de programación devuelve el dispositivo a su **estado de fábrica**, manteniendo su dirección individual. Fuera del modo seguro no es posible resetear el dispositivo manualmente, lo que evita resetearlo por accidente.

> ⚠ **Importante**
>
> *El reset de fábrica borra la parametrización y la configuración de seguridad KNX del dispositivo. Será necesario volver a programarlo desde ETS.*

1.6. IP Tunneling

El **IP Router** incorpora una interfaz IP que permite hasta **10 conexiones de túnel** simultáneas, por ejemplo, para programar o supervisar la instalación desde ETS a través de la red IP. Cada conexión de túnel dispone de su propia dirección individual en la línea TP.

Además, el dispositivo admite una conexión directa para su propia programación desde ETS, sin que los telegramas lleguen al bus KNX.

El estado de las conexiones de túnel puede consultarse desde ETS (ver sección 2.1.1).

1.7. Seguridad KNX y Security Proxy

El **IP Router** es compatible con los dos tipos de seguridad KNX:

- **KNX Data Security**: protege los telegramas dirigidos al propio dispositivo, por ejemplo, durante su programación desde ETS.
- **KNX IP Security**: protege la comunicación en el medio IP, tanto las conexiones de túnel como el enrutado multicast entre routers IP.

La funcionalidad **Security Proxy** permite traducir telegramas seguros multicast recibidos por un medio a telegramas en plano enviados al otro medio, y viceversa. También permite añadir reglas adicionales de enrutado para telegramas que no son multicast.

Para obtener información detallada acerca de la funcionalidad y configuración de la seguridad KNX, consúltese el manual de usuario específico “Guía de seguridad KNX”.

Configuración

2.1. General - IP Router

Tras importar la correspondiente base de datos en ETS y añadir el dispositivo a la topología del proyecto deseado, el proceso de configuración comienza adjudicando una dirección individual **X.Y.Z**. Dependiendo del uso del dispositivo, la configuración será la siguiente:

- **Acoplador de área**: deberá tener dirección individual **X.0.0**.
- **Acoplador de línea**: deberá tener dirección individual **X.Y.0**.
- **Acoplador de segmentos**: deberá tener dirección individual **X.Y.Z**.

La pestaña “General” (Figura 1) contiene los siguientes parámetros:

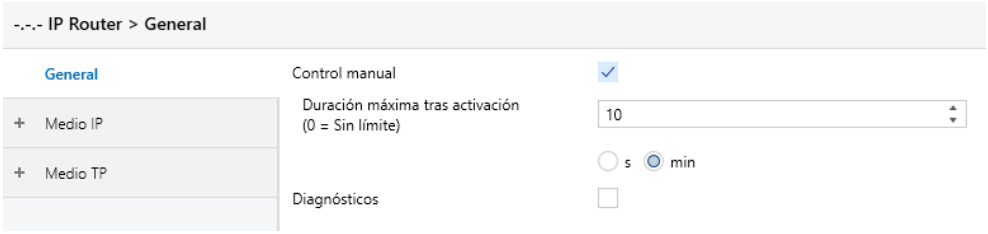


Figura 1. General.

- **Control manual** [*inhabilitado / habilitado*]: impide o permite el uso del botón “Pass IA/GA” (ver sección 1.4).
  - **Duración máxima tras activación (0 = Sin límite)** [*0…10…60*] [*min*] / [*0…600…3600*] [*s*]: tiempo máximo durante el que se mantiene activa la funcionalidad *Pass IA* o *Pass GA* tras su activación. La funcionalidad puede desactivarse antes de este tiempo pulsando el botón de nuevo.
- **Diagnósticos**: habilita la pestaña “Diagnósticos” (ver sección 2.1.1).

2.1.1. Diagnósticos

Desde esta pestaña (Figura 2) se puede comprobar el estado de las direcciones de túnel del dispositivo: cuáles están en uso y la dirección IP del cliente conectado a cada una.

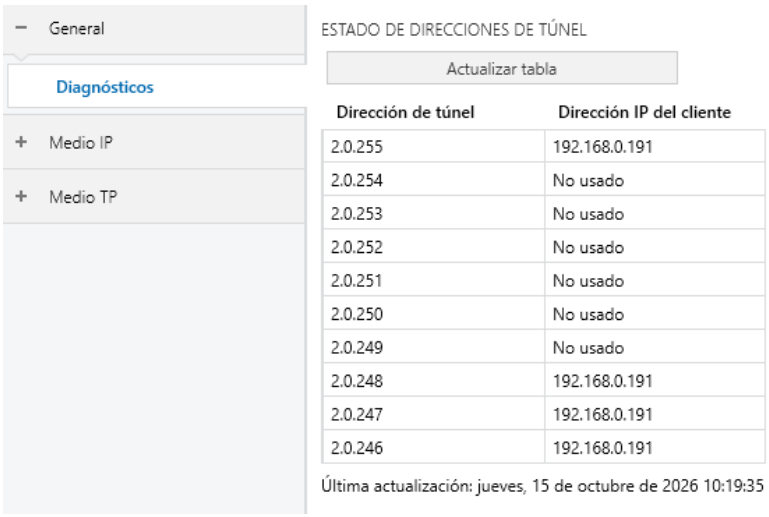


Figura 2. Diagnósticos.

La información no se actualiza en tiempo real: debe pulsarse el botón “Actualizar tabla” para leerla del dispositivo. Los datos leídos se guardan en el proyecto de ETS, por lo que se indica la fecha y la hora de la última actualización, en el formato regional del PC.

2.2. Medio IP

Las pestañas del medio IP determinan el comportamiento del **IP Router** con los telegramas recibidos por la red IP (línea principal).

2.2.1. Telegramas recibidos (medio IP)

Para los telegramas recibidos por el medio IP, existen tres posibles configuraciones de enrutado:

- **Bloquear**: el telegrama nunca pasa al medio TP.
- **Enrutar**: el telegrama siempre pasa al medio TP.
- **Filtrar**: el telegrama pasa o no al medio TP en función de su destino, como se detalla en cada parámetro.

> **Nota**
>
> *Las restricciones se suman a las de Security Proxy. Si tenemos enrutado en **“Bloquear”**, se bloquean todos los telegramas y dejan de tener efecto las excepciones de Security Proxy. Si se tiene el enrutado en **“Filtrar”** / **“Enrutar”**, para poder comunicar con un dispositivo bloqueado por Security Proxy, ETS debe activar una excepción temporal de 60 segundos (renovados automáticamente cada ~50s durante la programación).*

Los parámetros disponibles se muestran en la Figura 3.

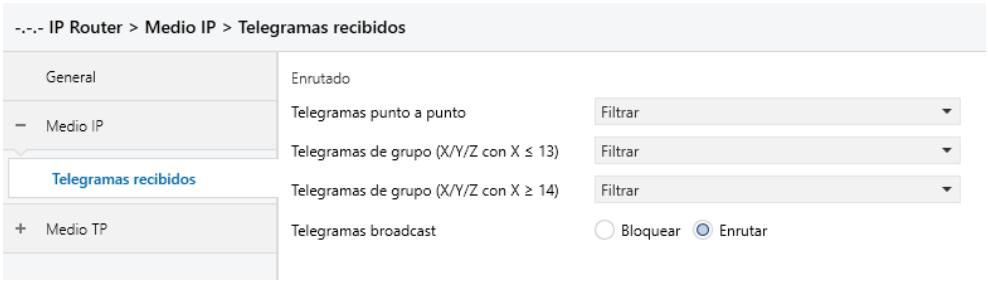


Figura 3. Telegramas recibidos (medio IP).

Enrutado:

- **Telegramas punto a punto** [*Bloquear / Enrutar / Filtrar*]: telegramas dirigidos a una dirección individual, como los enviados durante la programación de un dispositivo. Con «Filtrar», el telegrama se enruta solo si el destinatario se encuentra en el medio TP.
- **Telegramas de grupo (X/Y/Z con X ≤ 13)** [*Bloquear / Enrutar / Filtrar*]: telegramas de grupo con grupo principal igual o inferior a 13. Con «Filtrar», el telegrama se enruta solo si en el medio TP existe al menos un dispositivo que utilice esa dirección de grupo (ver capítulo 3).
- **Telegramas de grupo (X/Y/Z con X ≥ 14)** [*Bloquear / Enrutar / Filtrar*]: igual que el anterior, para telegramas con grupo principal igual o superior a 14.
- **Telegramas broadcast** [*Bloquear / Enrutar*].

> **Nota**
>
> *Los telegramas dirigidos al propio **IP Router** siempre se aceptan y nunca se enrutan al otro medio, independientemente de esta configuración.*

No existen opciones de confirmación de telegramas en el medio IP.

2.3. Medio TP

Las pestañas del medio TP determinan el comportamiento del **IP Router** con los telegramas recibidos y enviados por la línea TP (línea secundaria).

2.3.1. Telegramas recibidos (medio TP)

El enrutado sigue la misma lógica que en la sección 2.2.1, pero en sentido inverso: se decide qué telegramas pasan del medio TP al medio IP (Figura 4).

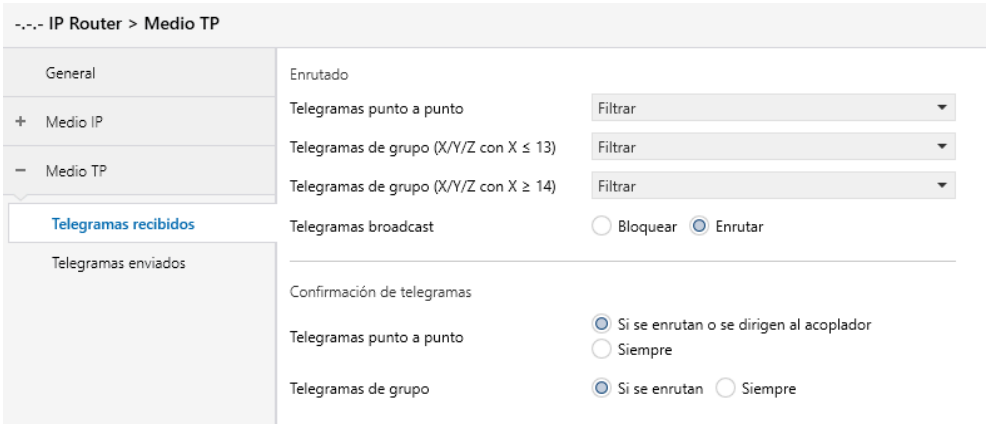


Figura 4. Telegramas recibidos (medio TP).

Enrutado:

- **Telegramas punto a punto** [*Bloquear / Enrutar / Filtrar*].
- **Telegramas de grupo (X/Y/Z con X ≤ 13)** [*Bloquear / Enrutar / Filtrar*].
- **Telegramas de grupo (X/Y/Z con X ≥ 14)** [*Bloquear / Enrutar / Filtrar*].
- **Telegramas broadcast** [*Bloquear / Enrutar*].

Confirmación de telegramas:

- **Telegramas punto a punto** [*Si se enrutan o se dirigen al acoplador / Siempre*]: determina en qué casos el dispositivo confirma un telegrama punto a punto recibido por el medio TP.
- **Telegramas de grupo** [*Si se enrutan / Siempre*]: determina en qué casos el dispositivo confirma un telegrama de grupo recibido por el medio TP.

> **Nota**
>
> *La opción «Siempre» permite que el telegrama aparezca como confirmado (evitando repeticiones en el caso de proyectos defectuosos, etc.) incluso aunque ningún dispositivo lo haya recibido. En el caso de un error de recepción, los NACK enviados por los dispositivos sobrescriben esta confirmación, por lo que no se producen pérdidas de datos.*

> **Nota**
>
> *Mientras haya alguna conexión de túnel abierta, el dispositivo confirma siempre los telegramas de grupo recibidos por el medio TP, ya que pueden ser capturados por el cliente del túnel.*

2.3.2. Telegramas enviados

Esta pestaña (Figura 5) determina el comportamiento del **IP Router** al enviar a la línea TP telegramas procedentes del medio IP. Es posible seleccionar qué telegramas se repiten si en el envío no se ha recibido confirmación o se ha recibido NACK / BUSY.

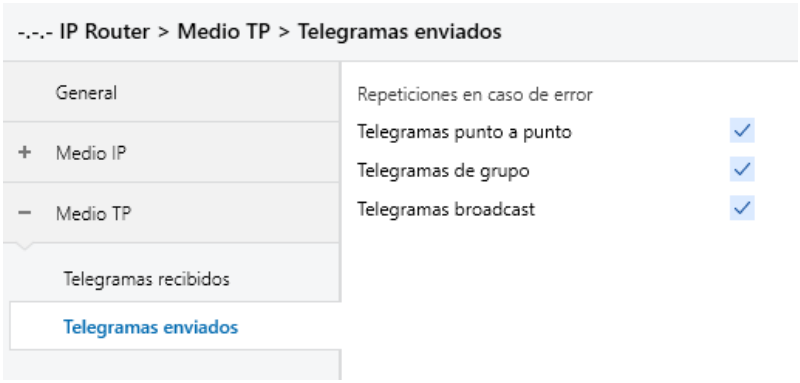


Figura 5. Telegramas enviados.

Repeticiones en caso de error:

- **Telegramas punto a punto** [*inhabilitado / habilitado*].
- **Telegramas de grupo** [*inhabilitado / habilitado*].
- **Telegramas broadcast** [*inhabilitado / habilitado*].

> **Nota**
>
> *Esta configuración no se aplica a las respuestas del propio dispositivo a telegramas dirigidos a él.*

> **Nota**
>
> *Con las repeticiones habilitadas, el dispositivo puede suprimir dinámicamente las repeticiones innecesarias en conexiones de túnel para no saturar el bus.*

3. Tabla de filtros / Tabla de security proxy

La tabla de filtros se crea automáticamente en ETS. Las direcciones de grupo de los telegramas que deben ser enrutados por el acoplador se incluyen en esta tabla. El contenido de esta tabla puede consultarse a través de la vista previa, donde también se muestran las tablas de Security Proxy.

Para acceder a la previsualización, hacer clic derecho sobre el **IP Router** y, en el menú desplegable, seleccionar «Vista Previa de la Tabla de Filtros» (Figura 6). Se mostrará una ventana como la de la Figura 7, con las direcciones de grupo que el acoplador enruta, organizadas por grupo principal y grupo intermedio.

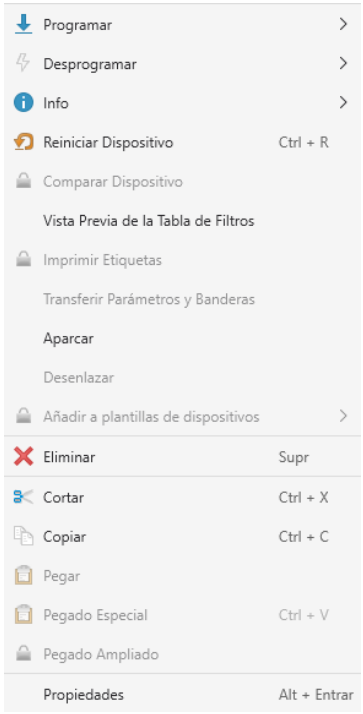


Figura 6. Menú del dispositivo en ETS.

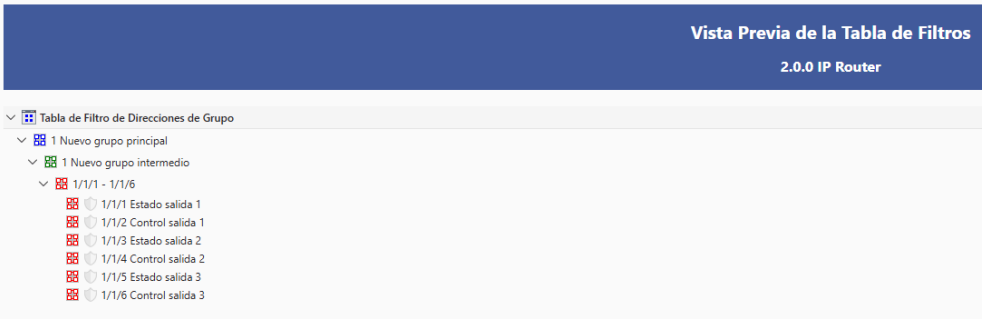


Figura 7. Tabla de filtros.

Si la instalación utiliza **seguridad KNX**, las direcciones de grupo seguras se identifican en la vista previa con el icono de escudo relleno, como se muestra en la Figura 8.

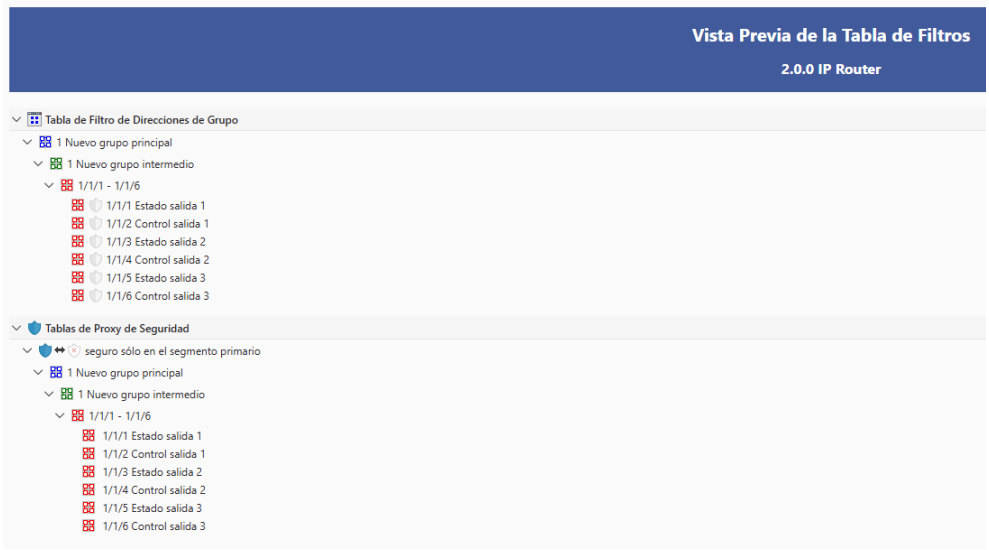


Figura 8. Tabla de filtros con direcciones de grupo seguras.

Únete y envíanos tus consultas sobre los dispositivos Zennio: https://support.zennio.com

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