KNX IP Router: **IPR 300 SREG**

Interface KNX IP: **IPS 300 SREG**

INDICE

1. DESCRIPCIÓN DE SU FUNCIÓN

El router IP interconecta las diferentes líneas y áreas del sistema KNX utilizando el protocolo IP. Implementa el estándar EIBnet/IP de tal forma que no solamente sirve para transmitir telegramas entre líneas KNX (Routing), sino que además permite acceder al sistema vía IP desde cualquier PC o dispositivo (Tunnelling). Se necesita la versión ETS 5.7.1. para programarlo con plena funcionalidad.

El uso de la red existente de datos para comunicación entre líneas está especialmente indicado para edificios terciarios, donde se puede conseguir una comunicación más rápida entre líneas KNX, extender un sistema KNX más allá de un edificio, o reprogramación del sistema KNX desde cualquier punto de la red.

En su función como acoplador de área o de línea (Routing), el router IP interconecta dos líneas KNX para formar un área lógica asegurando igualmente una separación eléctrica entre ambas líneas. Cada línea de bus de una instalación KNX es así independiente de las otras líneas. La función exacta de este dispositivo viene determinada por su dirección física.

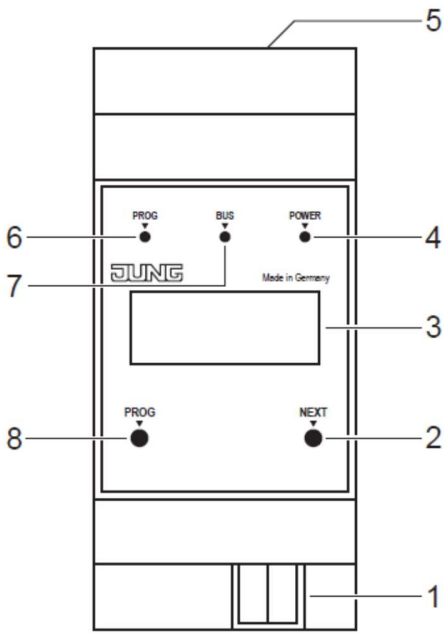
En su funcionamiento como módulo de comunicación (Tunnelling), el aparato ofrece hasta 8 conexiones KNXnet/IP simultáneas, de modo que, por ejemplo, podemos ejecutar una visualización al mismo tiempo que accedemos a la instalación a través del ETS. El aparato está preparado para comunicar tanto en IP Secure como en Data Secure.

La conexión con KNX se establece mediante terminal de conexión, y a la red IP se conecta mediante un conector RJ 45. El aparato no requiere una alimentación adicional.

Dispone de LED y botón de programación, además de un display de varias páginas donde podemos ver la IP del aparato, cuántas conexiones hay ocupadas en cada momento, así como su dirección física local o versión de firmware.

El interface IP (IPS …) es un aparato análogo al anterior, pero que solamente realiza la función de Tunnelling, por lo que no hace de acoplador de línea ni tiene tabla de filtros. Este aparato IPS cuenta con una aplicación adicional que le permite interactuar con la App del IPS Remote de forma que podemos tener un acceso remoto a la instalación de KNX que nos permite programar los aparatos. Sin necesidad de IP fija ni de redireccionar puertos. Se trata además de una conexión segura y encriptada. Esta misma aplicación adicional cuenta con una función de generador de fecha y hora para el bus y de un mapeador entre direcciones seguras y no seguras.

2. ESQUEMA DEL APARATO, DISPLAY Y MASTER RESET:



1: Terminales de conexión al bus KNX
2: Tecla NEXT para pasar página en el display
3: Display LCD
4: LED POWER
5: Conexión LAN
6: LED de programación
7: LED bus
8: Botón de programación

Información contenida en el display

Este aparato incorpora un display LCD que puede mostrar hasta 4 páginas de información navegables mediante la tecla NEXT:

Página 1

Muestra la versión de firmware, dirección IP, dirección física, número de serie y la cantidad de conexiones de tunnelling que se están empleando en cada momento.

Página 2

Aquí se muestra la configuración IP del aparato y el punto temporal en que se hizo reset.

Página 3

Información sobre la carga de telegramas en el bus.

Página 4

Muestra un código QR que corresponde al FDSK del aparato (Factory Default Setup Key). Solamente se muestra cuando el aparato aún se encuentra en ajustes de fábrica a nunca se le activó el modo Secure.

Indicaciones mediante LEDs

En la parte frontal del aparato existen 3 LEDs, que señalan los siguientes estados:

LED programación rojo:	Indica que el aparato está en modo de programación.
LED bus parpadea en naranja:	El bus está activo.
LED power luce en verde:	El aparato está funcionando.

Junto a la conexión LAN hay otros dos LEDs que ofrecen las siguientes indicaciones:

LED verde:	Hay conexión de red con un switch o con otro aparato.
LED amarillo:	Se están transmitiendo datos.

Master Reset

Si se desea se puede dejar el aparato en cualquier momento con sus ajustes de fábrica. Siga este procedimiento:

- Retire la conexión de bus del aparato y espere al menos 10 segundos.
- Pulse y mantenga la tecla PROG mientras le conecta el cable de bus.
- Espere hasta que el LED de programación parpadee con una frecuencia de 1 segundo. Manténgalo pulsado durante otros 10 segundos.
- Ya puede soltar el botón PROG.
- Vuelva a pulsar en corto el botón PROG dentro de los 3 segundos siguientes.
- El display se apaga y se vuelve a encender. El LED verde queda fijo y los demás apagados. El Master Reset ya está realizado.

3. CARACTERÍSTICAS TÉCNICAS:

Protección:	IP20
Homologación:	KNX
Montaje:	carril DIN, 2 M
Conexión KNX:	al bus mediante terminales de conexión
Alimentación:	a través del bus KNX
Consumo:	máx. 1 W
Corriente:	máx. 20 mA
Comunicación IP:	Ethernet 10/100 BaseT (10/100 Mbit/s)
Conexión IP:	1 x RJ 45
Display:	OLED, 128 x 64
KNXnet/IP Tunnelling:	Hasta 8 conexiones simultáneas
Servidor NTP SNTP:	Protegido con baterías
Temperatura ambiente:	-5 … +45 ºC

4. APLICACIÓN BÁSICA:

Para el IPR 300 SREG: Router IP KNX (V1.1.)
Para el IPS 300 SREG: Interfaz IP KNX (V1.1.)

4.1. Objetos de comunicación:

No tiene objetos de comunicación.

4.2. Descripción funcional de la aplicación:

General:

- Facilita la conexión con sistemas de alto nivel vía protocolo IP de internet.
- Acceso directo a la instalación KNX desde cualquier punto de acceso de la red IP, mediante el KNXnet/IP Tunnelling.
- Comunicación rápida entre líneas KNX, áreas y sistemas (EIBnet/IP Routing) (solamente IPR)
- Filtrado y enrutamiento de telegramas dependiendo de las direcciones físicas y de grupo (solamente IPR)
- Transmisión de fallos en el sistema KNX a distintas aplicaciones vía KNXnet/IP
- Conexión sencilla a programas de visualización.
- Acepta hasta 8 conexiones simultáneas
- A partir de ETS 5.7 se puede utilizar en modo KNX Data Secure
- A partir de ETS 5.7 se puede utilizar en modo IP Secure
- Transmisión de hasta 48 telegramas por segundo en modo IP Secure
- Configuración completa mediante ETS

Funcionamiento como acoplador de área o de línea (solamente IPR …):

En este modo de funcionamiento, su misión es interconectar dos líneas KNX, asegurando un correcto flujo de telegramas entre ellas y una separación eléctrica. Puede transmitir telegramas de dirección física para la puesta en marcha de los componentes, como telegramas de grupo para el normal funcionamiento del sistema.

Para transmitir telegramas de dirección física es muy importante que el router conozca su propia dirección física, puesto que siempre la compara con la dirección física del destinatario, cuando estamos en proceso de programación. Dependiendo de la parametrización, el acoplador transmite telegramas cuando la dirección de

destino corresponde a su línea, bloquea el paso de todos ellos o permite el paso de todos, para finalidades de puesta en marcha.

Con respecto a los telegramas de grupo, el comportamiento del router se puede también parametrizar. Se puede hacer también que impida el paso de todos los telegramas, que los deje pasar a todos, o transmita de forma selectiva en función de una tabla de filtros recibida desde el ETS: El aparato dejará pasar solamente aquellos telegramas cuya dirección de grupo esté contenida en la tabla de filtros, con la excepción de las direcciones que pertenezcan a los grupos principales 14 y 15. Estas direcciones no caben en la tabla de filtros, y por eso el router dispone de un parámetro específico para establecer el comportamiento del aparato respecto de las mismas. La tabla de filtros se genera en el ETS de forma automática, y se transmite al aparato durante el volcado de la aplicación.

4.3. Programación y puesta en marcha:

Este aparato dispone de un botón y un LED de programación, como todos los aparatos de KNX. Pero tiene la particularidad de que se le pueden cargar dos programas de aplicación distintos. Eso significa que ocupa 2 direcciones físicas en el bus, que habrá que asignar por separado.

- **Asignación de la primera dirección física**

La primera dirección física va siempre relacionada con la aplicación básica de interface IP KNX. Se asigna por el método tradicional de pulsar corto sobre el botón de programación para que el LED de programación quede fijo.

- **Asignación de la segunda dirección física**

La segunda dirección física va siempre relacionada con la aplicación adicional que permite el servidor de fecha y hora además del control remoto. Para ponerlo en modo de programación recibiendo la dirección física que corresponde a esta aplicación hay que seguir estos pasos:

- Pulse corto sobre el botón de programación. El LED de programación queda fijo.
- Pulse nuevamente corto sobre el botón de programación. El LED de programación parpadea lentamente. Ya está preparado para recibir la dirección física correspondiente a la aplicación adicional.

- **Retornar el aparato a los ajustes de fábrica**

Si se requiere volver el aparato a los ajustes de fábrica, siga los estos pasos:

- Retire el cable de KNX del aparato.
- Pulse y mantenga el botón de programación.
- Sin soltar el botón de programación, vuelva a conectar el cable de bus KNX.
- Mantenga el botón pulsado hasta que los LEDs rojo y amarillo parpadeen lentamente.
- Suéltelo y vuelva a pulsarlo hasta que el LED rojo haga centelleos rápidos.
- Ya puede soltar el aparato. Los LEDs se encienden un instante y se vuelven a apagar. El proceso de ajuste a los valores de fábrica ha concluido.

4.4. Asignación de las 8 conexiones simultáneas:

Este aparato necesita una dirección física, como cualquier otro componente de KNX. Además de eso ocupará una dirección física local para cada una de las 8 conexiones IP Tunnelling que pueda establecer. Estas direcciones físicas locales deberán ser siempre coherentes con el lugar topológico que el aparato dentro de la instalación KNX. Es decir, si el aparato está físicamente colocado en la línea 1.3 del bus, entonces su dirección física local será del tipo: 1.3.xxx. De lo contrario, en caso de haber acopladores de línea o amplificadores en la instalación, nunca podremos conectar con aparatos ubicados en otras líneas para poder programarlos.

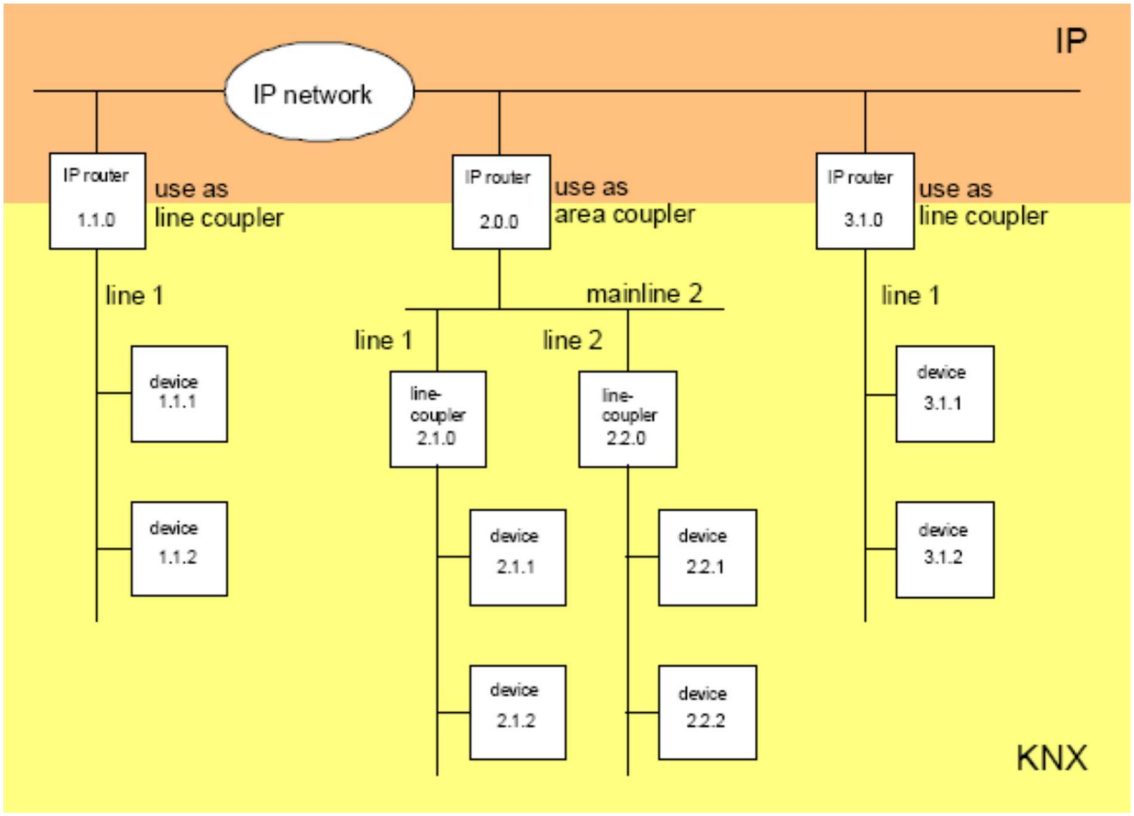
4.5. Topología:

En su funcionamiento como acoplador de área o de línea, el router transmite telegramas entre el bus KNX y la red IP. La función exacta del dispositivo se determina por su dirección física según estos criterios:

Acoplador de área: A.0.0 ($1 \leq A \leq 15$)

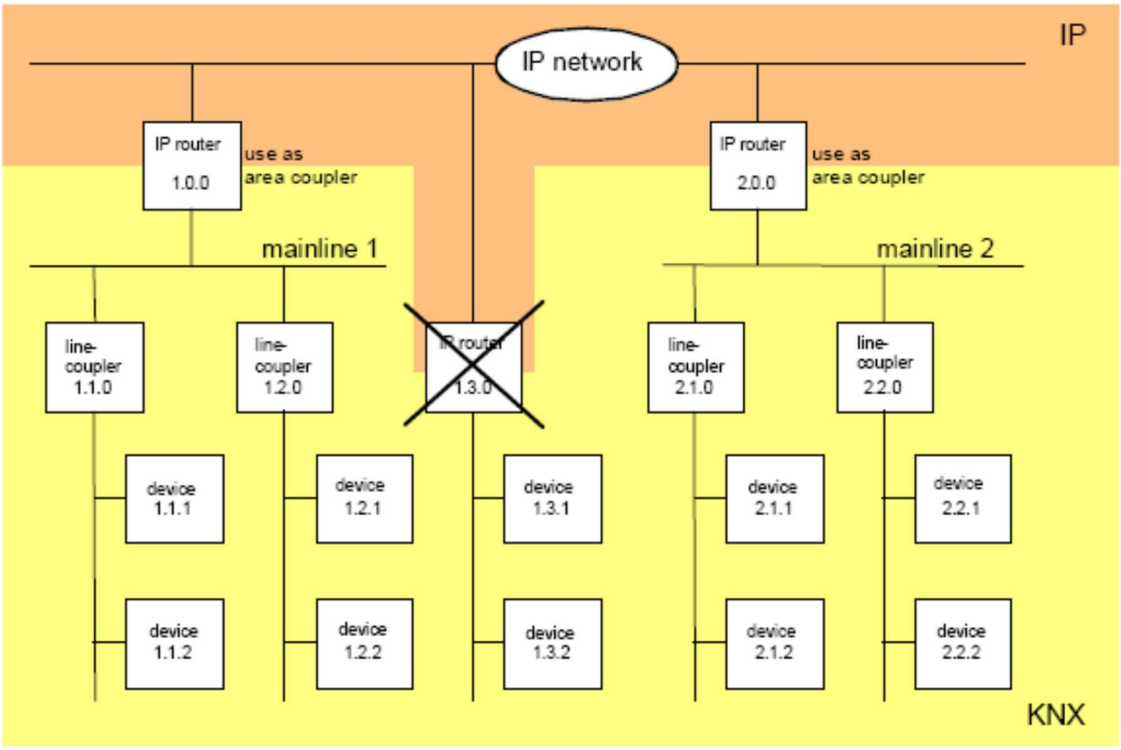
Acoplador de línea: A.L.0 ($1 \leq A \leq 15$, $1 \leq L \leq 15$)

El Router IP puede ser en principio utilizado como acoplador de área o de línea:



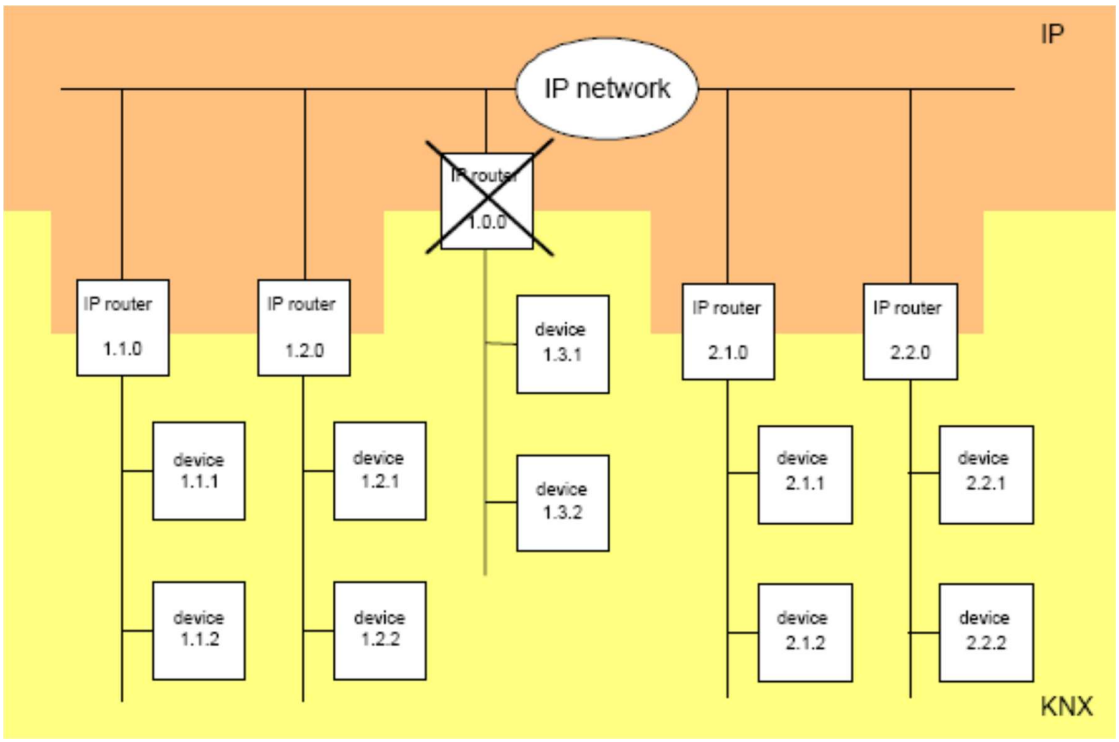
Router IP como acoplador de línea/área

Si el Router IP es usado como acoplador de área con la dirección física x.0.0 (x = 1…15), entonces ningún otro router en la misma red configurado como acoplador de línea x.y.0 (y=1…15 – misma área) puede estar topológicamente por debajo del anterior:



Router IP como acoplador de área

Si un Router IP se usa como acoplador de línea con la dirección física x.y.0 (x = 1…15, y = 1…15), entonces no puede haber ningún otro con la misma dirección de área que esté por encima de éste topológicamente hablando.



Nota: El perfecto funcionamiento del Router IP como acoplador de área o de línea (KNXnet/IP Routing) depende de que los componentes de esa red soporten el IP multicasting. Los routers de la red deben permitir deben estar configurados de forma que transmitan los **datagramas multicasting.** Para el KNXnet/IP Routing, la dirección IP multicast reservada es la 224.0.23.12.

Funcionamiento como interface IP

El Router IP también puede servir simultáneamente de módulo de comunicación, para conectarse al sistema KNX con un PC mediante la conexión de red. Por ejemplo, para programar los componentes, o para una visualización. Se necesita el ETS 3.0 c o superior para poder programar los componentes desde la red, o monitorizar los telegramas como si se tratase de una conexión RS 232 o USB.

Para conseguir una comunicación estable mediante el KNXnet/IP Tunnelling se necesita una segunda dirección física (similar a la dirección física local en una conexión USB o RS 232). Desde el punto de vista topológico, el router se proyecta dentro de una línea del KNX como un componente más.

4.6. Parámetros:

4.6.1. Parámetros “Configuración IP”:

La configuración IP del aparato no se hace dentro del capítulo de parámetros sino en el apartado de “Propiedades” que aparece a la derecha de la pantalla.

- Activar la configuración avanzada: Si activamos esta opción aparece un grupo de parámetros llamado “Configuración avanzada”.

4.6.2. Parámetros “Configuración avanzada”:

Este grupo de parámetros solamente está disponible si se ha activado la configuración avanzada en el grupo de parámetros de configuración IP.

4.6.2.1. Parámetros “Propiedades de la línea inferior”:

Este grupo de telegramas hace referencia al comportamiento del aparato respecto de los telegramas que pasan desde el mundo IP a KNX, y solamente está disponible en el IP Router.

- Confirmar cada uno de los telegramas (ACK): Si se activa esta opción el IP Router confirmará cada telegrama recibido desde el par trenzado, tanto si lo ha dejado pasar como si no al mundo IP. En caso de contestar negativamente aparecen los dos parámetros siguientes.

- Confirmar solamente telegramas enrutados (ACK): En este caso enviará confirmación al par trenzado solamente si el telegrama ha pasado a través del IP Router.

- Repetir telegramas si no se confirman: Cuando el aparato transmita al par trenzado un telegrama que viene del mundo IP, deberá recibir un ACK cuando llegue a su destinatario. En este parámetro se establece si en caso de no recibir ese telegrama deberá repetir o no su envío.

- Bloqueo de programación lado TP: En caso de que el cable de bus esté expuesto o no del todo protegido, mediante este parámetro podemos evitar que este aparato se pueda reprogramar por el lado del par trenzado. Su programación por el lado IP siempre será posible.

- Tasa máxima de telegramas (solo KNX TP): Este parámetro también está disponible en el IPS 300 SREG, y define la máxima cantidad de telegramas por

segundo que se pueden enviar al par trenzado, evitando así la posibilidad de saturación en el bus.

4.6.2.2. Parámetros “Túnel estándar”:

Este grupo de telegramas hace referencia al comportamiento del aparato en modo tunnelling y por tanto está disponible tanto en el IPR como en el IPS.

- Conexión lenta (solo conexiones UDP): Las conexiones de Tunnelling por UDP trabajan normalmente con un “time out” de conexión de 1 segundo. Ese tiempo puede ser muy poco para las conexiones a través de Internet. Habilitando este parámetro podemos llegar a establecer un “time out” de hasta 8 segundos.

- Conexión IP preferida para túnel x: Este aparato puede establecer hasta 8 conexiones simultáneas de tunnelling, que por defecto asigna de forma aleatoria a cada uno de los aparatos que tenga conectados por la red IP. Habilitando este parámetro nos aparece un campo donde podemos fijar la dirección IP a la que deseamos que se asigne cada una de las direcciones de tunnelling. Esto nos permitirá en todo momento saber mediante el display qué aparatos están conectados por IP haciendo uso de su conexión de tunnelling, y cuáles no.

4.6.2.3. Parámetros “Enrutamiento”:

- Comprobación de la topología: Si activamos este parámetro el router reconocerá los posibles errores que pueda haber en el direccionamiento de los componentes de KNX que tenga por debajo. Aquellos telegramas que vengan defectuosos no serán retransmitidos y su dirección de procedencia se podrá leer en el display del aparato.

- Activación del algoritmo de enrutamiento: Solamente será necesario activar este parámetro si el router se inserta en una instalación KNX existente desde antes de 2018. En esa fecha se cambió el algoritmo de enrutamiento, y si no se hace la adaptación pueden surgir problemas de transmisión.

4.6.3. Parámetros “Filtro”:

Este grupo de parámetros solamente está disponible en el IP Router.

4.6.3.1. Parámetros “Dirección física de filtrado”:

- Telegramas direccionados físicamente: Define si los telegramas con destino a dirección física pasarán o no de la red IP a la línea de bus KNX, y viceversa. Se trata básicamente de los telegramas implicados en el volcado de la programación a los componentes. Lo normal – opción por defecto -, es que pasen o no en función de que sean coherentes con la dirección física del Router IP (filtrar). Otras opciones es dejar pasar (redireccionar), solamente recomendado durante la fase de puesta en marcha de la instalación, o no dejar pasar ninguno (bloquear).

- Bloqueo de telegramas broadcast: Permite dejar siempre pasar o bloquear los telegramas de grupo, independientemente de a qué grupo principal pertenezcan.

4.6.3.2. Parámetros “Filtro de telegrama de grupos”:

Este grupo de telegramas hace referencia al comportamiento del aparato respecto de los telegramas que pasan **desde el mundo IP a KNX**:

- Telegramas de grupo de los grupos principales 0 a 13: Define si los telegramas de los grupos principales de 0 a 13 pasarán o no de la red IP a la línea de bus KNX. Lo normal – opción por defecto -, es que pasen o no en función de que se encuentren en la tabla de filtros (filtrar). Otras opciones es dejar pasar todos (transmitir), solamente recomendado durante la fase de puesta en marcha de la instalación, o no dejar pasar ninguno (bloquear). Los grupos 0 a 13 forman un bloque.

- Telegramas de grupo de los grupos principales 14 a 15: Define si los telegramas de los grupos principales de 14 a 15 pasarán o no de la red IP a la línea de bus KNX. Lo normal – opción por defecto -, es que pasen o no en función de que se encuentren en la tabla de filtros (filtrar). Otras opciones es dejar pasar todos (transmitir), solamente recomendado durante la fase de puesta en marcha de la instalación, o no dejar pasar ninguno (bloquear). Los grupos 14 y 15 forman un bloque.

- Telegramas de grupo de los grupos principales 16 a 31: Define si los telegramas de los grupos principales de 16 a 31 pasarán o no de la red IP a la línea de bus KNX. Lo normal – opción por defecto -, es que pasen o no en función de que se encuentren en la tabla de filtros (filtrar). Otras opciones es dejar pasar todos (transmitir), solamente recomendado durante la fase de puesta en marcha de la instalación, o no dejar pasar ninguno (bloquear). Los grupos 16 y 31 forman un bloque.

- Filtro ampliado telegrama de grupo: Además del filtrado de direcciones de grupo orientado a bloques, cada uno de los grupos puede ser o no filtrado por separado. Con este parámetro se habilita esa posibilidad.

Este otro grupo de telegramas hace referencia al comportamiento del aparato respecto de los telegramas que pasan **desde el mundo KNX a IP**:

- Telegramas de grupo de los grupos principales 0 a 13: Define si los telegramas de los grupos principales de 0 a 13 pasarán o no de la línea de bus KNX a la red IP. Lo normal – opción por defecto -, es que pasen o no en función de que se encuentren en la tabla de filtros (filtrar). Otras opciones es dejar pasar todos (transmitir), solamente recomendado durante la fase de puesta en marcha de la instalación, o no dejar pasar ninguno (bloquear). Los grupos 0 a 13 forman un bloque.

- Telegramas de grupo de los grupos principales 14 a 15: Define si los telegramas de los grupos principales de 14 a 15 pasarán o no de la línea de bus KNX a la red IP. Lo normal – opción por defecto -, es que pasen o no en función de que se encuentren en la tabla de filtros (filtrar). Otras opciones es dejar pasar todos (transmitir), solamente recomendado durante la fase de puesta en marcha de la instalación, o no dejar pasar ninguno (bloquear). Los grupos 14 y 15 forman un bloque.

- Telegramas de grupo de los grupos principales 16 a 31: Define si los telegramas de los grupos principales de 16 a 31 pasarán o no de la línea de bus KNX a la red IP. Lo normal – opción por defecto -, es que pasen o no en función de que se encuentren en la tabla de filtros (filtrar). Otras opciones es dejar pasar todos (transmitir), solamente recomendado durante la fase de puesta en marcha de la instalación, o no dejar pasar ninguno (bloquear). Los grupos 16 y 31 forman un bloque.

- Filtro ampliado telegrama de grupo: Además del filtrado de direcciones de grupo orientado a bloques, cada uno de los grupos puede ser o no filtrado por separado. Con este parámetro se habilita esa posibilidad.

4.6.3.3. Parámetros “Enrutamiento”:

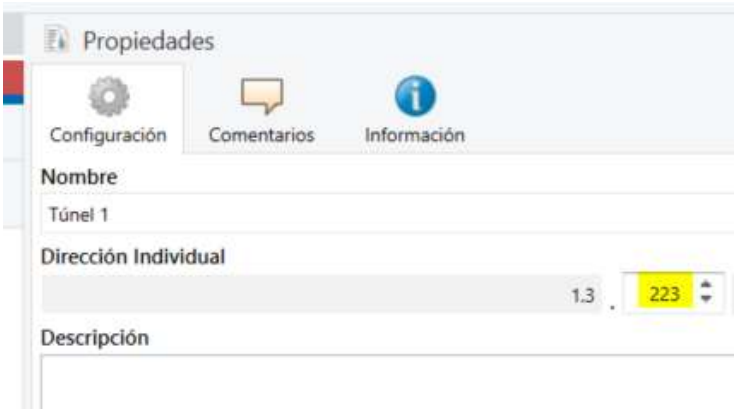
No hay parámetros que ajustar en este grupo.

4.6.3.4. Parámetros “Túnel”:

No hay parámetros que ajustar en este grupo, pero la aplicación permite asignar una dirección física virtual (local) a cada una de las 8 conexiones tunnelling. Esas direcciones quedarán reservadas para las conexiones y no estarán ya disponibles para ningún otro aparato de KNX de la instalación. Así evitaremos conflictos que provoquen la reducción de conexiones disponibles.

Para asignar esas direcciones físicas virtuales seleccionaremos cada una de las conexiones de túnel que aparecen bajo el aparato en el ETS, como si fuesen objetos de comunicación:

Seleccionando cada uno de ellos tendremos sus propiedades a la derecha de la ventana del ETS:



En el campo “Dirección individual” podremos introducir la dirección física virtual de cada conexión de túnel.

4.7. Configuración IP:

La configuración IP del aparato no se hace dentro del capítulo de parámetros sino en el apartado “Propiedades” que aparece a la derecha de la pantalla del ETS cuando se selecciona este aparato:

Si la red dispone de servicio DHCP se podrá seleccionar la opción “Obtener una dirección IP automáticamente”. Seleccionando “Usar una dirección IP estática” aparecerán los parámetros para entrar la dirección IP, la máscara de subred y la puerta de enlace (Gateway por defecto).

- Dirección multidifusión (multicast): Se utiliza para enrutar telegramas de bus KNX de un Router IP a todos los otros routers. En este caso, solamente los Routers IP que usan la misma dirección mulitcast se podrán comunicar entre ellos. La dirección IP predefinida de fábrica es la 224.0.23.12. Esta dirección se asigna al enrutamiento KNXnet/IP y se reserva para esta aplicación especial. Para uso general en una red, todas las direcciones desde la 239.0.0.0 hasta la 239.255.255.255 están disponibles. Cada byte de la IP se escribe por separado, dando lugar al conocido formato IP : byte 1 . byte 2 . byte 3 . byte 4.

4.8. El modo “Secure”:

Este aparato puede trabajar tanto en IP Secure como en Data Secure. Si deseamos habilitar estas posibilidades dentro del apartado de configuración, en la parte derecha del ETS:

Podemos habilitar por separado la puesta en marcha segura y el túnel seguro. En ambos casos necesitamos añadir el certificado del dispositivo (FDSK), que lo haremos escaneando el código QR del aparato o bien mediante la App “JUNG KNX Secure Scanner”. **Tenga en cuenta que la inclusión de un solo aparato KNX Secure supone proteger el proyecto de ETS con un password, y que si no lo recuerda la única posibilidad de volver a usar el aparato será hacerle un master reset.**

5. CONFIGURACION DEL IPS REMOTE:

5.1. ¿Qué es el IPS Remote y para qué sirve?

El IPS Remote es una aplicación compatible con el IPS 300 SREG que está pensada para poder acceder de forma remota y segura a la instalación de KNX y así poder realizar tareas de mantenimiento y programación sin necesidad de desplazarse físicamente a la instalación.

Requisitos para hacer funcionar el IPS Remote:

- Se necesita un módulo IP del modelo IPS 300 SREG o posterior.
- El aparato debe tener la versión de firmware 1.055 o superior.
- Es necesario obtener un código en el entorno MyJUNG que se introducirá en los parámetros del aparato. Con eso queda habilitado para realizar esta función.
- En el ETS hay que instalar la App “IPS Remote”.
- En la instalación de destino hay que dejar previsto un botón físico o virtual desde el cual se pueda enviar en algún momento un telegrama de activación para que el aparato acepte conexiones remotas.
- Todo el funcionamiento ser realiza bajo las premisas de KNX Secure.

5.2. Proceso de configuración:

A continuación se describen los pasos necesarios para configurar la función IPS Remote sobre un interface IP:

5.2.1. Actualización de dispositivos existentes:

Para que sea posible esta configuración el aparato debe tener cargada la versión de **firmware 1.055 o superior**. Si no es así, esa nueva versión se puede descargar desde el catálogo-online dentro de la web www.jung.de/es.

¡**ATENCIÓN!** Para realizar esta actualización de firmware hay que desactivar el KNX Secure del aparato dentro del ETS y volcarle la aplicación en este modo. De lo contrario no se podrá volcar el nuevo firmware.

Dentro del apartado “Otros idiomas” tenemos acceso a la actualización del firmware:

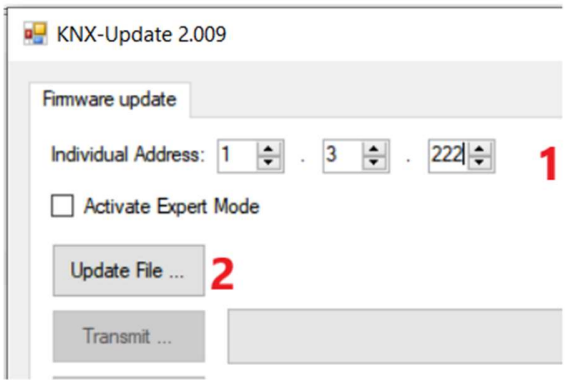
Descargas internacionales

	ES	DE	EN	
Instrucciones de servicio	406.6 kB	403.4 kB	395.1 kB	38
Guía de programación	1.0 MB	6.8 MB	5.9 MB	
Software		5.4 MB	5.4 MB	
Texto de licitación		1.7 kB	1.7 kB	
Declaración de conformidad CE	48.8 kB	48.8 kB	48.8 kB	4
Base de datos para ETS5	167.2 kB	167.2 kB	167.2 kB	16
CAD (dwg)	104.1 kB	104.1 kB	104.1 kB	10
Release notes		581.1 kB	581.1 kB	
Update		2.6 MB	2.6 MB	
Use cases		31.0 MB	17.1 MB	
Hojas de caracteristicas	ES	DE	EN	

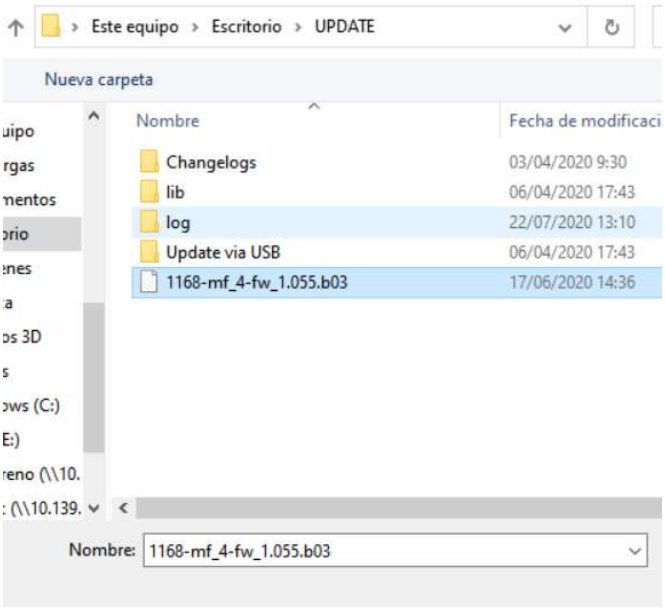
La actualización se descarga en forma de archivo .zip. Descomprímalo en una carpeta y ejecute el archivo:

“KNX-Update-V2.009.exe”

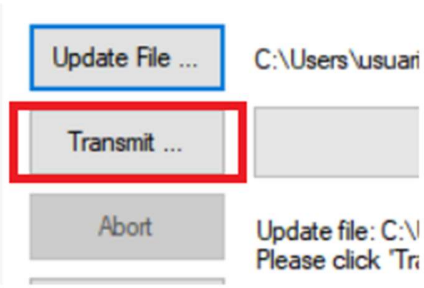
Inserte la dirección física del aparato en el campo “Individual address” y pulse sobre el botón “Update File”



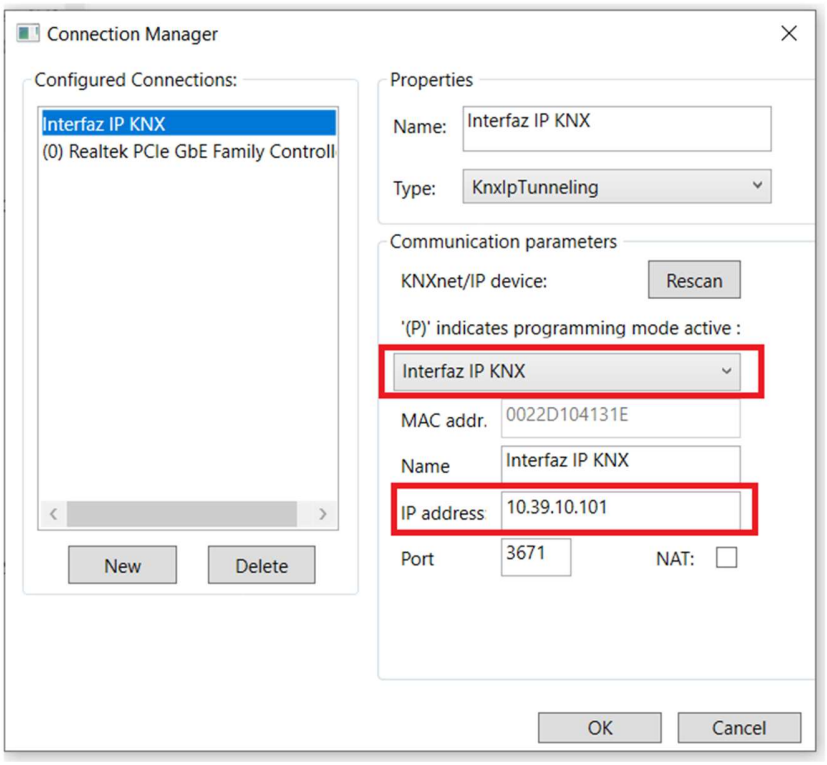
Seleccione ahora el archivo de firmware, que tendrá extensión .b03:



Pulse ahora sobre el botón “Transmit”:



Acepte la ventana que aparece y entonces accederá a esta otra:

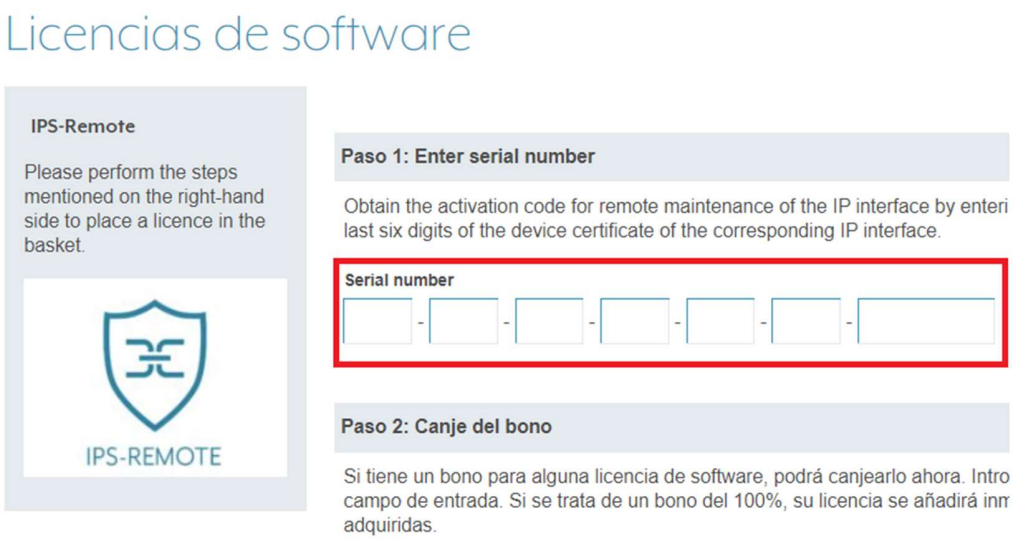


En el menú desplegable busque el interface sobre el cual quiere volcar el firmware. Lo reconocerá porque al seleccionarlo aparecerá su IP en el campo “IP address”. La puede contrastar con la que aparece en el display del aparato. Pulsando sobre el “OK” comienza la descarga, que dura un par de minutos. Lógicamente el **IPS deberá estar conectado a la misma red que el ordenador** para llevar a cabo este proceso.

Una vez termine, el aparato se reinicia. Compruebe en el display que efectivamente ya está en la versión 1.055.

5.2.2. Obtención del código de licencia:

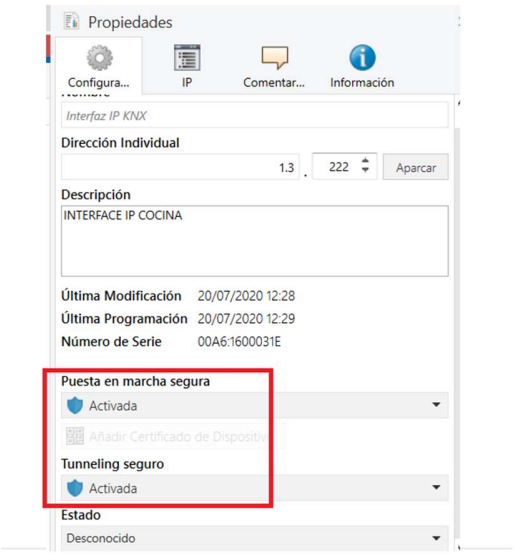
El código de licencia se obtiene exclusivamente en el portal MyJUNG, dentro de la web www.jung.de/es. Entre en el menú “SOFTWARE LICENSE ACTIVATION” y dentro de eso en pulse para obtener licencia del IPS Remote:



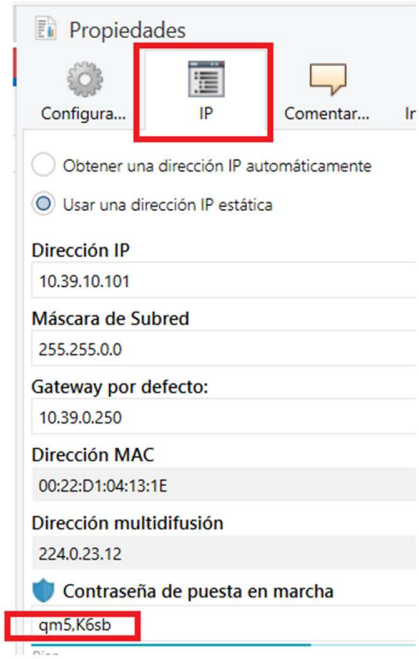
El “Serial number” del aparato es el código que aparece junto al QR que va en la etiqueta. Es el mismo que se utiliza para el KNX Secure. Una vez finalizado el proceso de compra obtendrá el código que se necesita para introducir en los parámetros del IPS 300 SREG.

5.2.3. Preparación del módulo IPS 300 SREG:

Para que sea posible el acceso remoto es necesario activar tanto la **Puesta en marcha segura** como el **Tunnelling seguro.**



Estos dos parámetros se encuentran en la pestaña “**Configuración**” de la ventana de propiedades del aparato, que aparece de forma contextual a la derecha de la pantalla del ETS. En la pestaña “IP” encontramos la **Contraseña de puesta en marcha segura**. Cópiela en el portapapeles de su ordenador porque la necesitará más tarde cuando tenga que volcar la aplicación sobre el aparato



Por último, vuelque la dirección física y el programa de aplicación sobre el aparato, y ya estará listo para recibir la App del IPS Remote. Recuerde que solamente podrá establecer comunicación remota con el aparato si abre la App de IPS Remote desde **el mismo proyecto de ETS** con el que se ha hecho el volcado al aparato.

En este momento será cuando se le pida la contraseña de la puesta en marcha segura.

¡ATENCIÓN!

- Para que todo esto sea posible es necesario que el aparato tenga activado el KNX Secure, lo cual implica leer los QR e introducir el código secure correspondiente tanto para la aplicación básica de módulo de comunicación IP como para la función adicional del interfaz IP.

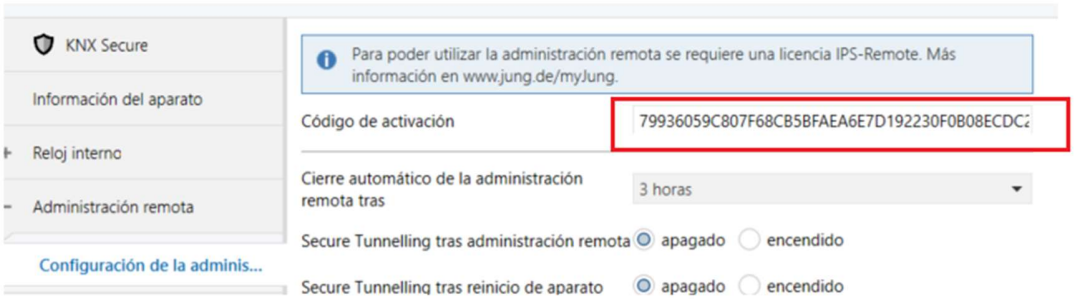
- El proyecto de ETS al completo queda afectado por el KNX Secure, lo que implica que en adelante será siempre necesaria una contraseña para poder abrirlo.

- La única comunicación que se realiza de forma encriptada es la del ETS con el propio módulo IPS. El resto de conexiones de túnel pueden ser utilizadas para otras aplicaciones y no requieren encriptación, con lo cual este módulo puede interactuar con aparatos no seguros.

5.2.4. Activación del acceso remoto:

El acceso remoto se consigue mediante un nuevo programa de aplicación adicional al ya existente del IPS 300 SREG. Descargue por tanto la base de datos *.knxprod* actualizada para este aparato e inserte en su proyecto de ETS el programa de aplicación “Interfaz IP – función adicional”.

Esta aplicación tiene varias funciones que veremos más adelante. De momento nos centramos en lo que es relevante para el acceso remoto. Básicamente se trata de introducir en el correspondiente parámetro el código de activación obtenido en el entorno MyJUNG:



El siguiente paso es preparar una dirección de grupo de 1 bit que relacionaremos con el objeto 9 de este programa de aplicación:

Número	Nombre	Función del Objeto	Descripción	Dirección de
9	Habilitar administración remota - entrada	Conmutación	ACTIVACION	7/6/1
10	Código de activación válido - salida	Estado	CODIGO VALIDO	7/6/2
11	Modo seguro activo - salida	Estado		
12	Conexión con el servidor - salida	Estado		
13	Secure Tunnelling activo - salida	Estado	SECURE TUNNELLING	7/6/3
14	Programación mediante administración...	Estado		

Para poder establecer el control remoto con el aparato será necesario que ese objeto 9 tenga valor “1”. Habrá que tener por lo tanto algún aparato local capaz de enviarle esa dirección cuando sea requerido el acceso remoto. Ese estado de activación no es permanente. Se puede parametrizar entre 15 minutos y 24 horas. Por defecto son 3 horas.

Finalmente vuelque este otro programa de aplicación sobre el aparato. Es adicional al que ya tiene como módulo de comunicación IP. Eso quiere decir que este módulo ocupará dos direcciones físicas en el bus KNX, y además tendremos que habilitar el modo de programación para esta segunda aplicación de ETS.

Activación del modo de programación para la aplicación “Interfaz IP – función adicional”

1) Pulsación corta sobre el botón de programación. El LED de programación queda permanentemente encendido. El aparato estaría preparado para recibir la primera dirección física, que es la que corresponde al módulo de comunicación IP.

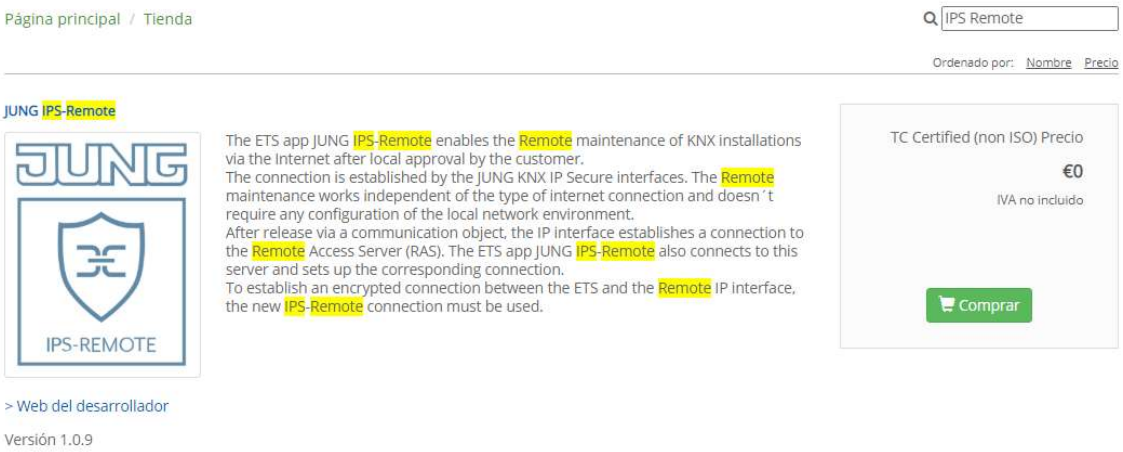
2) Una nueva pulsación corta hace que el LED de programación comience a parpadear. Así está preparado para recibir la dirección física correspondiente a esta función adicional.

5.2.5. Instalación y configuración de la App IPS-Remote:

En la práctica este acceso remoto se habilita a través de la App llamada “IPS-Remote”. Si no la tiene instalada, debe Vd. acceder a su cuenta MyKNX para descargarla e instalarla sobre su ETS.

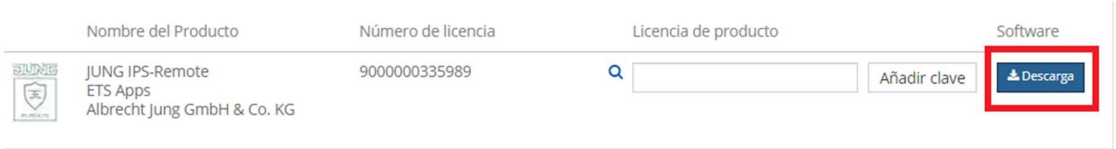
Acceda a su entorno privado en www.myknx.org y entre en la tienda on-line:

Ahí podrá seleccionar el apartado de ETS App y encontrarla entrando “IPS Remote” en el campo del buscador:

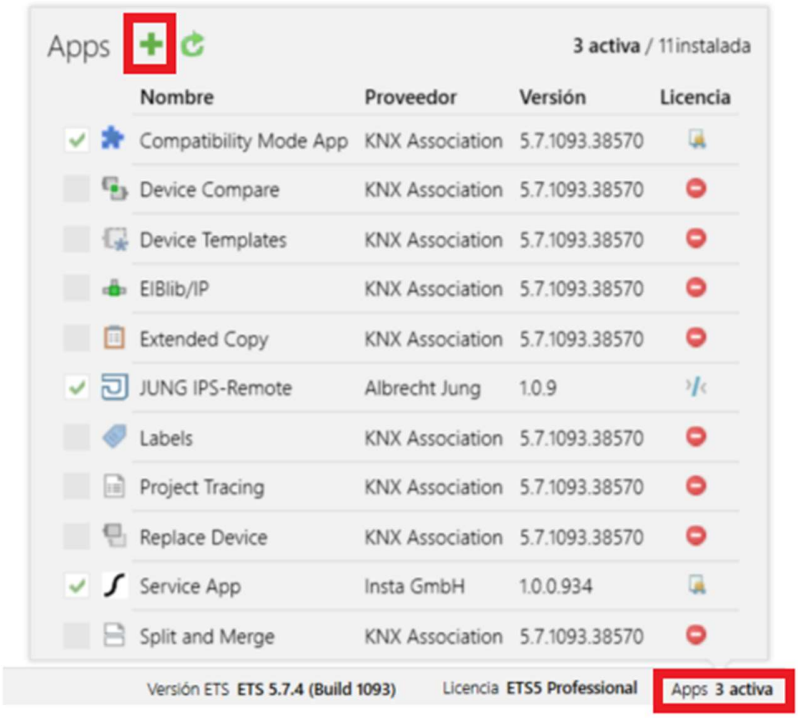


Una vez la tenga ya en su cuenta, necesitará descargarse el archivo de instalación para su ETS:

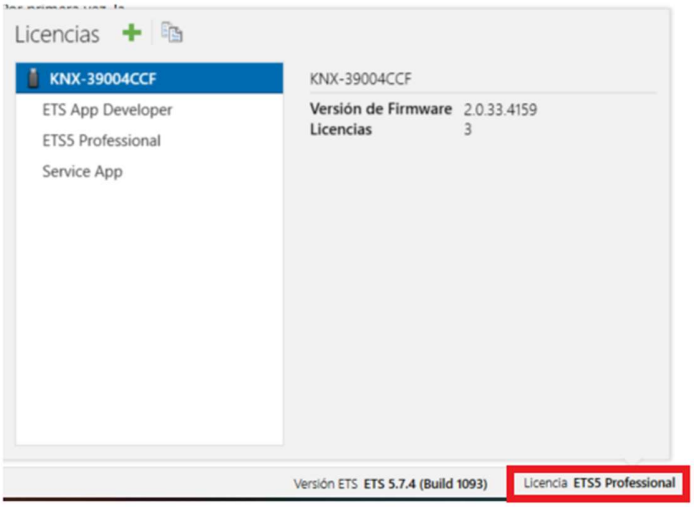
jung-ips-remote-1-0-9.etsapp



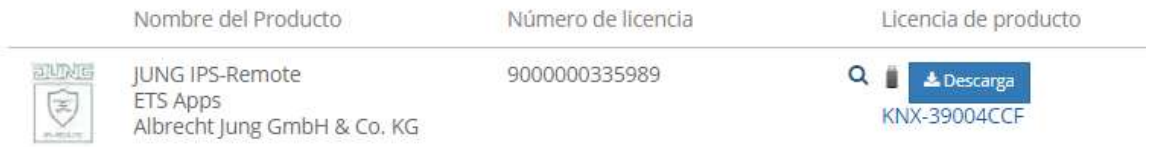
Abra el ETS y pulse sobre el botón de Apps que hay en la esquina inferior derecha. Aparece una ventana donde pulsando sobre el signo “+” podremos buscar e instalar el archivo: *jung-ips-remote-1-0-9.etsapp*



Así le aparece ya la App en la lista de aplicaciones instaladas. Ahora tendrá que obtener la licencia. Para ello regrese a su entorno de MyKNX, concretamente al punto donde descargó el archivo de instalación de la App. En el campo vacío de clave de producto introduzca el número de dongle de su ETS. Lo podrá obtener pulsando sobre el apartado de licencia del ETS, en la parte inferior derecha de la ventana principal. En este caso del ejemplo sería el KNX-39004CCF:



Copie y pegue ese código alfanumérico en el campo de clave de producto dentro del apartado de la App en el MyKNX, y pulse sobre obtener la clave.

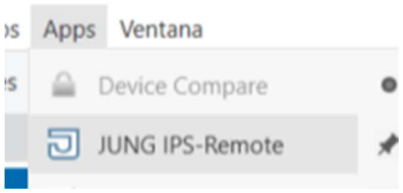


Aparece entonces un botón de descarga con el que podrá obtener el archivo *.license* de licencia de esta App gratuita. Añada ese archivo en el apartado de licencias del ETS y la App ya quedará totalmente operativa.

5.2.6. Establecimiento de la conexión remota:

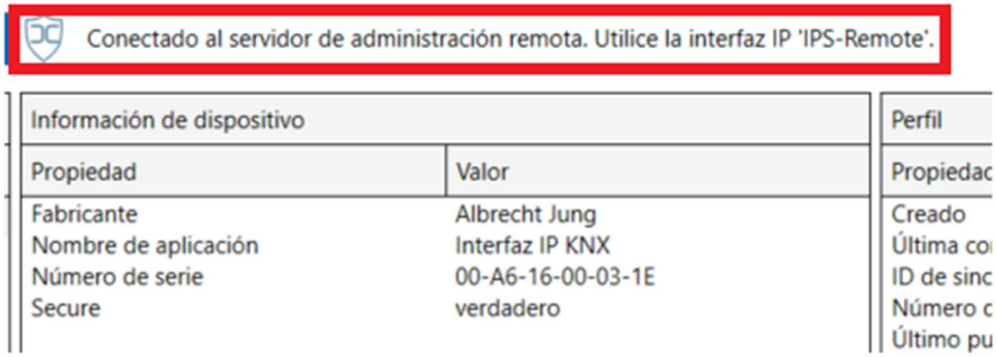
Una vez está todo configurado, la conexión remota se puede establecer ya desde cualquier red que tenga acceso a Internet, sin necesidad de que sea la red local de la instalación donde está el módulo IPS. La premisa necesaria es que al aparato se le haya mandado en local un telegrama con valor “1” a través del objeto de comunicación 9, tal como se especifica en el punto 5.2.4. De esta forma aseguramos una privacidad de la instalación, y que no podrá haber una conexión remota sin “permiso” de quien haya en la instalación.

Abra el proyecto de ETS donde se encuentra este módulo IPS y ejecute la App del IPS Remote:

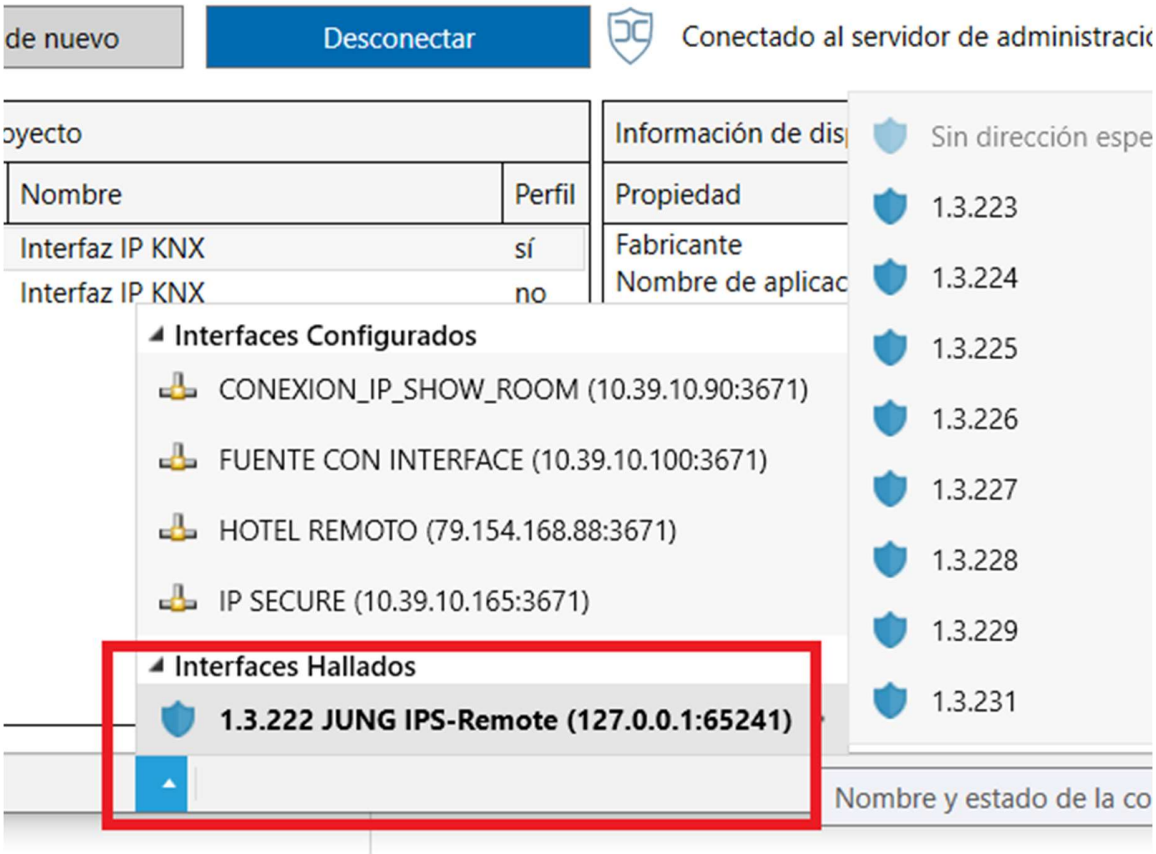


La propia App encontrará dentro del proyecto los interfaces IP que puedan ser accedidos remotamente. En el caso de este ejemplo es el 1.3.222:

Selecciónelo y pulse primero sobre sincronizar y después sobre conectar. Si todo es correcto, obtendremos el siguiente mensaje de confirmación:



En la parte de “Interfaces hallados” del ETS ya tendremos disponible la conexión Remote con sus 8 túneles disponibles. Podremos seleccionar cualquiera de ellos para realizar una conexión. Recuerde que le pedirá después la contraseña de puesta en marcha segura. Véase al final del capítulo 5.2.3.


de nuevo
Desconectar
Conectado al servidor de administraci
oyecto
Información de dis
Nombre
Perfil
Propiedad
Interfaz IP KNX
sí
Fabricante
Interfaz IP KNX
no
Nombre de aplicac
Sin dirección espe
1.3.223
1.3.224
1.3.225
1.3.226
1.3.227
1.3.228
1.3.229
1.3.231
Interfaces Configurados
CONEXION_IP_SHOW_ROOM (10.39.10.90:3671)
FUENTE CON INTERFACE (10.39.10.100:3671)
HOTEL REMOTO (79.154.168.88:3671)
IP SECURE (10.39.10.165:3671)
Interfaces Hallados
1.3.222 JUNG IPS-Remote (127.0.0.1:65241)
Nombre y estado de la co

6. APLICACIÓN ADICIONAL IPS REMOTE:

Solamente disponible para el IPS 300 SREG: Interfaz IP – Función adicional

6.1. Objetos de comunicación:

Obj	Función	Nombre	Tipo	DPT-ID
1	Estado	Servidor reloj ext – salida	1 bit	1.002
2	Estado	Reloj interno vál – salida	1 bit	1.002
3	Salida de hora	Hora – salida	3 bytes	10.001
4	Salida de fecha	Fecha – salida	3 bytes	11.001
5	Salida hora fecha	Fecha/Hora – salida	8 bytes	19.001
6	Petición	Fecha/Hora – entrada	1 bit	1.017
7	Petición	Sinc. Servidor NTP - entr	1 bit	1.017
8	Hora verano/inv	Hora verano/inv – sal	1 bit	1.002
9	Conmutación	Habil. Admin remota – en	1 bit	1.003
10	Estado	Código activac. válid entr	1 bit	1.002
11	Estado	Modo seguro activ – salid	1 bit	1.002
12	Estado	Conexión com el servidor	1 bit	1.003
13	Estado	Secure Tunnelling act	1 bit	1.002
14	Estado	Program. mediante admin	1 bit	1.002
15	Entrada/Salida	Mapeador objeto 1A	------	-------
16	Entrada/Salida	Mapeador objeto 1B	------	-------
17	Entrada/Salida	Mapeador objeto 2A	------	-------
18	Entrada/Salida	Mapeador objeto 2B	------	-------
19	Entrada/Salida	Mapeador objeto 3A	------	-------
20	Entrada/Salida	Mapeador objeto 3B	------	-------
21	Entrada/Salida	Mapeador objeto 4A	------	-------
22	Entrada/Salida	Mapeador objeto 4B	------	-------
23	Entrada/Salida	Mapeador objeto 5A	------	-------
24	Entrada/Salida	Mapeador objeto 5B	------	-------
25	Entrada/Salida	Mapeador objeto 6A	------	-------
26	Entrada/Salida	Mapeador objeto 6B	------	-------
27	Entrada/Salida	Mapeador objeto 7A	------	-------
28	Entrada/Salida	Mapeador objeto 7B	------	-------
29	Entrada/Salida	Mapeador objeto 8A	------	-------
30	Entrada/Salida	Mapeador objeto 8B	------	-------
31	Entrada/Salida	Mapeador objeto 9A	------	-------
32	Entrada/Salida	Mapeador objeto 9B	------	-------
33	Entrada/Salida	Mapeador objeto 10A	------	-------
34	Entrada/Salida	Mapeador objeto 10B	------	-------

Descripción de los objetos:

- 1: Este aparato es capaz de captar la hora y fecha desde un servidor NTP externo y transmitir esa información al bus KNX. Tras la puesta en marcha o reinicio del aparato, se conectará cada 48 horas para sincronizarse. Si en los parámetros de configuración del reloj interno habilitamos el estado del servidor de tiempos, nos aparece este objeto de comunicación de 1 bit mediante el cual podremos saber si el servidor NTP está disponible, y así sabremos si la sincronización se está llevando a cabo correctamente. Aunque no se pueda sincronizar, el aparato seguirá manteniendo la hora y fecha gracias a su reloj interno pero no podremos garantizar que la hora es exacta.

- 2: Antes de la puesta en marcha del aparato, y si no se ha sincronizado con el servidor NTP, la hora no será válida y por tanto este objeto de comunicación estará con valor “0”. Cuando el aparato se conecte con el servidor y reciba la hora correctamente, este objeto de comunicación tomará valor “1”. El aparato lleva integrada una batería que le permite mantener la fecha y hora durante 36 horas. Si tiene un corte de alimentación que supera ese tiempo entonces se pierde y cuando lo reiniciemos este objeto quedará de nuevo a “0”, indicando que la fecha y hora no son válidos.

- 3: Objeto de 3 bytes mediante el cual envía la hora al bus KNX.

- 4: Objeto de 3 bytes mediante el cual envía la fecha al bus KNX.

- 5: Objeto de 8 bytes que permite enviar la fecha y hora conjuntamente al bus.

- 6: Recibiendo un telegrama con valor “1” mediante este objeto de comunicación provocamos el envío de la fecha y hora al bus.

- 7: Con un telegrama valor “1” haremos que el aparato se sincronice en ese momento con el servidor NTP.

- 8: Mediante un valor “1” el aparato indicará que se encuentra en horario de verano. Esta polaridad se puede cambiar mediante parámetros.

- 9: Este objeto de entrada se utiliza para habilitar la conexión remota, mediante recepción de un telegrama con valor “1”. Esta habilitación es temporal, con un máximo de 24 horas, según se parametrice. Pasado este tiempo se vuelve a deshabilitar la conexión remota.

- 10: Si el código de activación de la función IPS Remote que entramos en parámetros no es válido, tendremos un valor “0” en este objeto de comunicación.

- 11: Indica si el modo seguro está activado.

- 12: Indica si hay alguna conexión remota activa con el servidor.

- 13: Mediante este objeto de comunicación nos indica si está activado el túnel seguro, enviando un valor “1”. En caso contrario no se puede establecer la conexión remota.

- 14: Este otro objeto indica si en este momento se está realizando el volcado de alguna programación de forma remota.

- 15 … 54: Este aparato permite mapear direcciones seguras a no seguras y viceversa. Un total de 20 canales que se pueden habilitar por parámetros en grupos de 10. En el apartado de parámetros se explica el funcionamiento de este mapeo.

6.2. Descripción funcional de la aplicación:

General:

- El módulo IPS puede interaccionar con la App del IPS Remote permitiendo así la programación remota de instalaciones KNX de una forma encriptada y sin necesidad de abrir puertos ni de tener IP fija.
- El módulo IPS también puede tener función de generador de fecha y hora para el bus, sincronizadas con un servidor NTP.
- Dispone de un total de 20 canales de mapeo bidireccional para direcciones de grupo. De esta forma se pueden vincular direcciones seguras y no seguras.

6.3. Parámetros:

6.3.1. Parámetros “Configuración del reloj interno”:

Este aparato cuenta con un reloj interno que permite enviar al bus la fecha y la hora. Este reloj se puede sincronizar con un patrón externo para garantizar siempre una exactitud de los datos que transmite. La sincronización se produce de forma automática cada 48 horas. Si el aparato pierde la alimentación cuenta con una reserva de batería de 36 horas durante las cuales mantiene la fecha y hora.

- Utilizar servidor NTP estándar (pool.ntp.org): Activando esta opción trabajaremos con el servidor NTP que trae por defecto. En caso contrario nos aparecerá otro parámetro donde podemos fijar la IP de cualquier otro servidor de fecha y hora.

- Estado servidor de tiempo externo válido: Este parámetro solamente es visible si trabajamos con el servidor NTP estándar. Habilita el objeto de comunicación 1

mediante el cual nos indicará si el servidor NTP externo está o no disponible, y si por tanto se ha podido sincronizar.

- Notificar estado hora interno tras reinicio: Habilita el objeto 2, a través del cual nos indicará si la hora que tiene es o no correcta. Si por ejemplo ha estado más de 36 horas sin alimentación habrá perdido la hora, y cuando arranque nos indicará por aquí que la hora que tiene no es correcta.

- Franja horaria (0=UTC): La del lugar donde se encuentre instalado el aparato. En España es + 1 h, y ese valor se pone en este parámetro. En horario de verano nos encontramos en + 2 h, pero esa otra hora ya se añade automáticamente por el hecho de estar en horario de verano.

- Cambio automático horario de verano / invierno: Autoexplicativo.

- Enviar hora tras reinicio: Se refiere tras reprogramar el aparato o reiniciarlo.

- Enviar hora cíclicamente: Si se habilita este parámetro aparece otro mediante el cual podemos establecer el ciclo con el cual se mandará de forma automática la fecha y la hora al bus.

- Invertir el objeto de tiempo de verano/invierno: Este parámetro sirve para invertir la polaridad del objeto 8, de forma que un “1” signifique invierno.

6.3.2. Parámetros “Configuración de la administración remota”:

El IPS Remote es una aplicación compatible con el IPS 300 SREG que está pensada para poder acceder de forma remota y segura a la instalación de KNX y así poder realizar tareas de mantenimiento y programación sin necesidad de desplazarse físicamente a la instalación. En el capítulo 5 se explica su funcionamiento y configuración.

- Código de activación: Se trata del código que obtenemos en MyJUNG para habilitar en este aparato el IPS Remote. El objeto de comunicación 10 nos indicará si es o no válido.

- Cierre automático de la administración remota tras: Cada vez que se desea establecer la conexión remota con el aparato hay que habilitarla enviando un telegrama al objeto 9. Esa habilitación no es perpetua, y decaerá una vez transcurrido el tiempo aquí parametrizado.

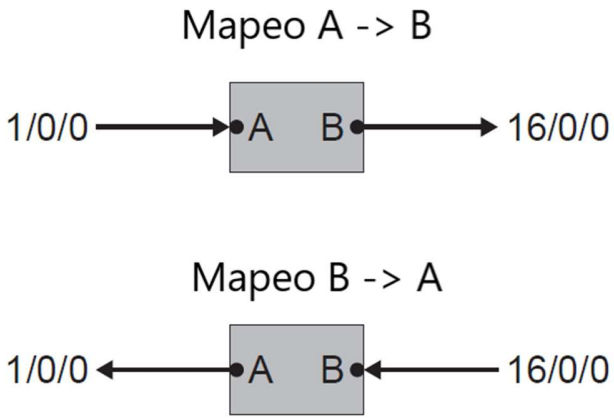
- Secure tunnelling tras administración remota: Durante la conexión remota el túnel debe ser seguro. Aquí se establece si tras la conexión remota quedará activo el

túnel seguro. Lo normal es dejarlo que no quede en modo seguro para así poder utilizar esas conexiones para comunicar con aparatos que no son seguros.

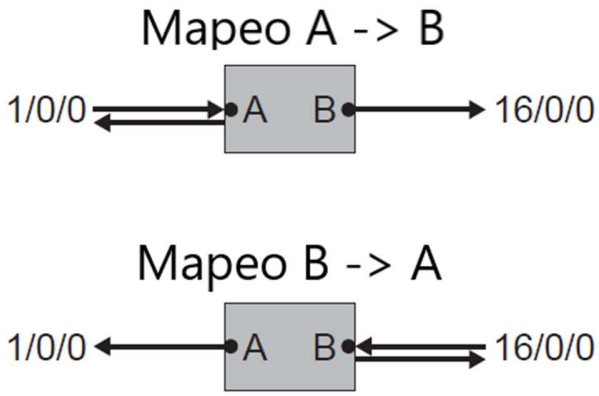
- Secure tunnelling tras administración remota: Aquí se establece si tras la conexión remota quedará activo el túnel seguro.

6.3.3. Parámetros “Mapeador Secure <-> plain”:

La función de mapeado permite establecer hasta 20 canales de conversión, cada uno de los cuales con 2 objetos de comunicación, para redireccionar direcciones de grupo seguras a direcciones no seguras, y viceversa. Para cada uno de estos canales se puede seleccionar la longitud de datos.



Cada canal de comunicación establecido tiene un objeto A y otro objeto B. En el caso del esquema anterior, cualquier valor escrito sobre la dirección 1/0/0/ pasará a la dirección 16/0/0 sin importar cuál de ellas es la segura y cuál no lo es. Y lo mismo en sentido contrario. De esa forma podremos unir una dirección no segura, por ejemplo la 1/0/0 con otra que sí lo sea, por ejemplo la 16/0/0.



En el esquema anterior se representa el comportamiento cuando hay peticiones de estado. Una petición de lectura sobre la dirección 1/0/0 provoca una petición de lectura sobre la dirección 16/0/0. Si el flag de lectura está activado en el objeto A entonces responderá enviando al bus el valor que tenga en ese momento. Lo mismo aplica para el objeto B. Ambos son bidireccionales.