



ROUTER KNX IP SECURE CO KNT IPR



MANUAL DE USUARIO

Aplicación

El Router KNX IP Secure permite el reenvío de telegramas entre diferentes líneas a través de una red LAN (IP) como un backbone rápido. El dispositivo también sirve como interfaz de programación entre un PC y el bus KNX (por ejemplo, para la programación de ETS).

El dispositivo es compatible con KNX Security. Esta opción se puede activar en el ETS.

Como Router Secure, el dispositivo permite acoplar la comunicación no segura en una línea KNX TP con una backbone IP segura.

KNX Security también impide el acceso no autorizado a la instalación con la función de interfaz (tunneling).

La dirección IP puede ser asignada mediante DHCP o a través de la configuración del ETS.

El dispositivo funciona según la especificación KNXnet/IP utilizando Core, Device Management, Tunneling y Routing.

El Router dispone de una tabla de filtros ampliada para el grupo principal 0... 31 y puede almacenar hasta 150 telegramas.

La alimentación se realiza a través del bus KNX.

Seguridad KNX

La Seguridad KNX ha sido añadida al estándar KNX para proteger las instalaciones KNX de accesos no autorizados. La seguridad KNX impide de forma fiable tanto la escucha de la comunicación como la manipulación de la instalación.

La especificación para KNX Security distingue entre KNX IP Security y KNX Data Security. KNX IP Security protege la comunicación a través de IP mientras que en KNX TP la comunicación permanece sin encriptar. Por lo tanto, KNX IP Security también puede utilizarse en instalaciones KNX existentes y con dispositivos KNX TP no seguros.

La Seguridad de Datos KNX describe la encriptación a nivel de telegrama. Esto significa que los telegramas del bus de par trenzado están codificados.

Seguridad IP KNX para la función de Router

El acoplamiento de líneas individuales KNX TP a través de IP se denomina enrutamiento KNX IP. La comunicación entre todos los routers IP KNX conectados tiene lugar a través de UDP multicast.

Con KNX IP Security, la comunicación de enrutamiento está encriptada. Esto significa que sólo los dispositivos IP que conocen la clave pueden descifrar la comunicación y enviar telegramas válidos. Un sello de tiempo en el telegrama de enrutamiento garantiza que no se puedan importar telegramas grabados anteriormente. Esto evita el llamado ataque de repetición.

La clave para la comunicación de enrutamiento es reasignada por el ETS para cada instalación. Si se utiliza KNX IP Security para el enrutamiento, todos los dispositivos KNX IP conectados deben soportar la seguridad y ser configurados en consecuencia.

Seguridad IP KNX para la función de Interfaz

Cuando se utiliza un Router KNX IP como interfaz al bus, el acceso a la instalación es posible sin seguridad para todos los dispositivos que tienen acceso a la red IP. Con la seguridad KNX, se requiere una contraseña. Ya se ha establecido una conexión segura para la transmisión de la contraseña. Toda la comunicación vía IP está encriptada y asegurada.

Seguridad de Datos KNX para el dispositivo

El Router también es compatible con la seguridad de datos KNX para proteger el dispositivo de accesos no autorizados desde el bus KNX. Si el Router se programa a través del bus KNX, esto se hace con telegramas encriptados.

⇒ *Nota: Los telegramas encriptados son más largos que los utilizados anteriormente sin encriptar. Por lo tanto, para una programación segura a través del bus, es necesario que la interfaz utilizada (por ejemplo, USB) y cualquier acoplador de línea intermedio soporten las llamadas tramas largas KNX.*

Seguridad de Datos KNX para telegramas de grupo

Los telegramas del bus que no se dirigen al Router como dispositivo se reenvían o bloquean según los ajustes de filtro (parámetros y tabla de filtros). No importa si los telegramas están sin cifrar o cifrados. El reenvío se realiza exclusivamente en función de la dirección de destino. Las propiedades de seguridad son comprobadas por el destinatario correspondiente.

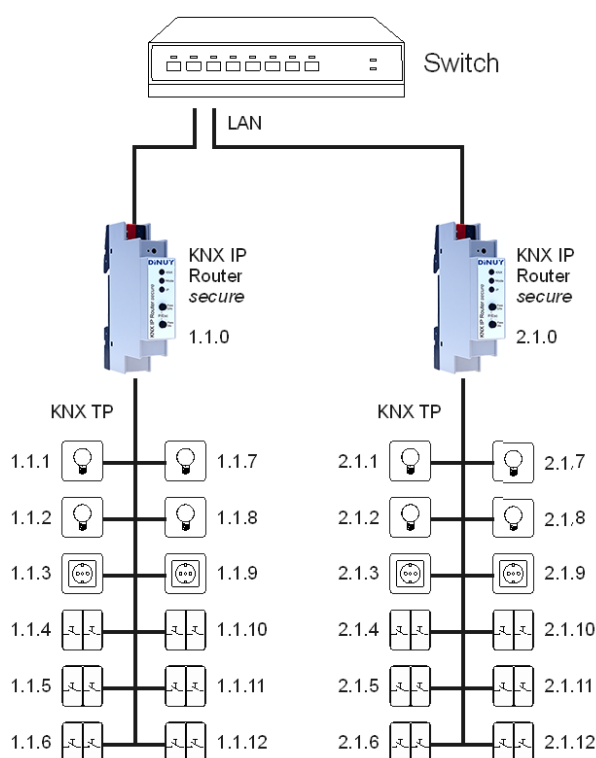
KNX Data Security y KNX IP Security pueden utilizarse en paralelo. En este caso, por ejemplo, un sensor KNX enviaría un telegrama de grupo encriptado con KNX Data Security al bus. Cuando se reenvía a través de KNX IP con KNX IP Security, el telegrama encriptado sería encriptado de nuevo de la misma manera que los telegramas no encriptados. Todos los dispositivos en el nivel KNX IP que soportan KNX IP Security pueden decodificar la encriptación IP, pero no la seguridad de los datos. Así, el telegrama de los otros routers KNX IP se transmite de nuevo con KNX Data Security a la(s) línea(s) de destino. Sólo los dispositivos que conocen la clave utilizada para la seguridad de los datos pueden interpretar el telegrama.

Función de acoplamiento (enrutamiento KNXnet/IP)

El Router KNX IP Secure puede funcionar como acoplador de línea o de área. En ambos casos, se utiliza la LAN (IP) como backbone.

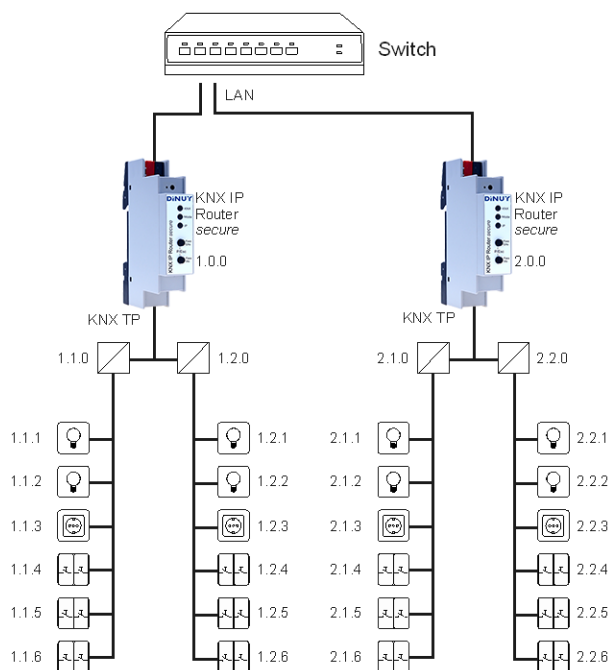
La siguiente tabla muestra los posibles usos del Router en comparación con la topología clásica:

	Topología clásica (sin IP)	Acoplamiento IP de las gamas (Rango de IPs cop.)	Acoplamiento IP de las líneas (acoplador de línea IP)
Línea de alcance (Backbone)	TP	IP	IP
Acoplamiento	Acoplador de línea KNX (máx. 15 unidades)	Router IP KNX (máx. 15 unidades)	Directamente a través del Switch LAN
Línea principal	TP	TP	IP
Acoplamiento	Acoplador de línea KNX (máx. 15x15 unidades)	Acoplador de línea KNX (máx. 15x15 unidades)	Router IP KNX (máx. 225 unidades)
Línea	TP	TP	TP



Router KNX IP como acoplador de línea

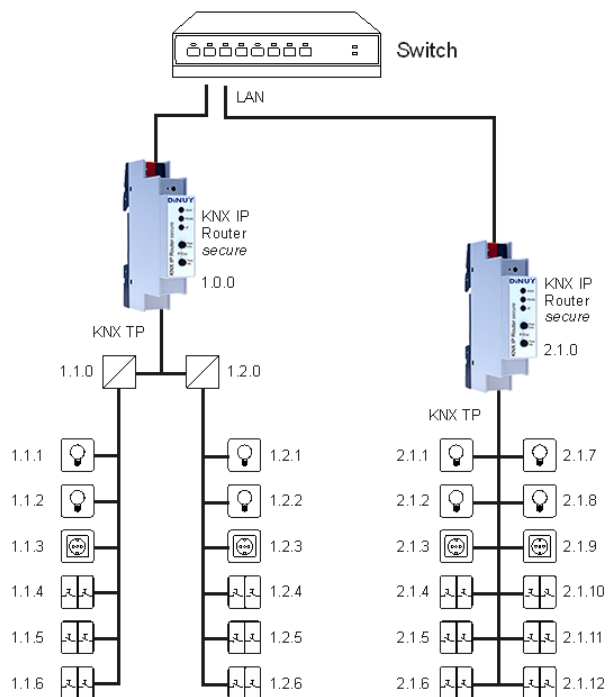
La asignación de la dirección física del Router determina si el dispositivo funciona como acoplador de línea o de área. Si la dirección física tiene la forma x.y.0 (x, y: 1..15), el Router funciona como un acoplador de línea. Si la dirección física tiene la forma x.0.0 (x: 1..15), se trata de un acoplador de área.



Router KNX IP como acoplador de área

⇒ Nota: Si el Router KNX IP se utiliza como acoplador de área (x.0.0), no puede haber ningún Router KNX IP topológicamente por debajo de él. Si, por ejemplo, un Router KNX IP tiene la dirección física 1.0.0, no debe haber ningún Router KNX IP con la dirección 1.1.0.

⇒ Nota: Si el Router KNX IP se utiliza como acoplador de línea (x.y.0), no puede haber ningún Router KNX IP topológicamente por encima de él. Si, por ejemplo, un Router KNX IP tiene la dirección física 1.1.0, no debe haber ningún Router KNX IP con la dirección 1.0.0.



Router KNX IP como acoplador de áreas y líneas

El Router KNX IP dispone de una tabla de filtros y contribuye así a reducir la carga del bus. La tabla de filtros (8kB) soporta el rango de direcciones de grupo extendido (grupos principales 0..31) y es generada automáticamente por el ETS.

Debido a la diferencia de velocidad entre Ethernet (10/100 MBit/s) y KNX TP (9,6 kBit/s), se pueden transmitir bastantes más telegramas en IP. Si se suceden rápidamente varios telegramas para una misma línea, deben almacenarse temporalmente en el Router para evitar pérdidas de telegramas. Para ello, el Router KNX IP tiene espacio de memoria para 150 telegramas (de IP a KNX).

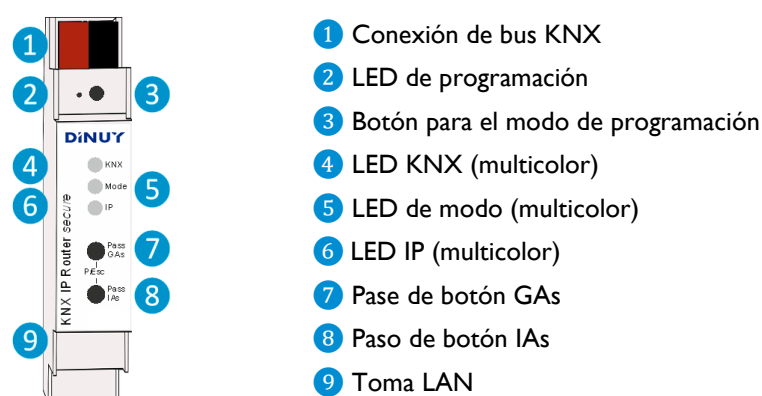
Función de acceso al bus (KNXnet/IP tunneling)

El Router KNX IP puede utilizarse como interfaz para el KNX. Se puede acceder al bus KNX desde cualquier punto de la LAN. Para ello, debe asignarse una dirección física adicional en cada caso. Esto se describe en los siguientes capítulos.

Instalación y puesta en marcha

El Router KNX IP se monta en un carril de sombrero y tiene un requisito de espacio de 1 TE (18 mm).

Dispone de los siguientes elementos de manejo y visualización:



El Interfaz se alimenta del Bus KNX. No es necesario conectar una tensión de alimentación externa.

⇒ Nota: Si no hay tensión de bus, la unidad no funciona.

Modo de programación KNX

El modo de programación KNX se activa o desactiva a través del botón de programación KNX 3 o pulsando simultáneamente los botones 7 y 8.

Funcionamiento manual e indicación de estado

El LED KNX 4 se ilumina en verde cuando hay tensión de bus KNX. Cuando este LED parpadea, el tráfico de telegramas está teniendo lugar en el bus KNX.

Los errores en la comunicación (por ejemplo, repeticiones de telegramas o fragmentos de telegramas) se indican con un breve cambio de color a rojo.

Resumen de los estados del LED KNX 4:

Comportamiento del LED	Significado
El LED se ilumina en verde	Tensión del bus KNX presente.
El LED parpadea en verde	Tráfico de telegramas en el bus KNX.
El LED se ilumina brevemente en rojo	Error en la comunicación en el bus KNX.

El LED IP 6 se enciende cuando hay un enlace Ethernet activo. Este LED es verde si la unidad tiene una configuración IP válida (dirección IP, subred y puerta de enlace). Si la configuración de la IP no es válida o no existe, este LED está en rojo. Este es también el caso, por ejemplo, si la unidad aún no ha recibido la configuración IP del servidor DHCP.

Cuando este LED parpadea, el tráfico de telegramas IP tiene lugar.

Resumen de los estados del LED IP 6:

Comportamiento LED	Significado
El LED se ilumina en verde	La unidad tiene un enlace Ethernet activo y una configuración IP válida.
El LED se ilumina en rojo	La unidad tiene un enlace Ethernet activo y una configuración IP no válida o aún no ha recibido la configuración IP del servidor DHCP .
El LED parpadea en verde	Tráfico de telegramas IP .

Para fines de prueba (por ejemplo, durante la puesta en marcha), los ajustes de enrutamiento parametrizados (filtro o bloque) pueden omitirse mediante una operación manual.

Con el botón Pasar GAs 7 se puede activar el reenvío de telegramas con dirección de grupo.

Con el botón Pasar IAs 8 se puede activar el reenvío de telegramas con dirección física.

Esto se indica con un solo parpadeo del LED de modo 5 (naranja). Si se seleccionan ambos modos al mismo tiempo, el LED de modo 5 parpadea dos veces.

Pulsando de nuevo los botones Pasar GAs 7 y Pasar IAs 8 se pueden seleccionar y deseleccionar estos ajustes según se desee.

La operación manual puede terminarse mediante la función de escape (Esc) pulsando simultáneamente los botones Pasar GAs 7 y Pasar IAs 8.

Si no están activos ni el modo de programación ni el funcionamiento manual, el LED de modo 5 puede indicar errores de configuración.

Resumen de los estados del LED de modo 5:

Comportamiento LED	Significado
El LED se ilumina en verde	La unidad funciona en modo de operación normal.
El LED se ilumina en rojo	El modo de programación está activo.
El LED parpadea 1 vez en naranja	El modo de programación no está activo. Operación manual activa: Tránsito IA o GA.
El LED parpadea 2 veces en naranja	El modo de programación no está activo. Operación manual activa: Tránsito IA y GA.
El LED parpadea en rojo	El modo de programación no está activo. El control manual no está activo. La unidad no está cargada correctamente. Por ejemplo, después de abortar una descarga.

Ajustes de fábrica

La siguiente configuración está preestablecida de fábrica:

Dirección física individual:	15.15.0
Conexión de túnel KNXnet/IP configurada:	I
Dirección física de la conexión de túnel:	15.15.240
Asignación de direcciones IP:	DHCP
Clave inicial (FDSK)	activo
Modo de seguridad	no activo

Restablecer la configuración de fábrica (Master Reset)

Es posible restablecer el Router a los ajustes de fábrica:

- Desconecte la conexión del bus KNX ① de la unidad.
- Mantenga pulsado el botón de programación KNX ③.
- Restablecer la conexión del bus KNX ① al dispositivo.
- Mantenga pulsado el botón de programación ③ durante al menos otros 6 segundos.
- Un breve parpadeo de todos los LEDs (② ④ ⑥) indica el restablecimiento exitoso de la configuración de fábrica.

Configuración del Router en el ETS

En el ETS, los interfaces se pueden seleccionar y configurar a través del menú del ETS "Bus - Interfaces".

El ETS puede acceder a los Routers KNX IP configurados incluso sin una entrada en la base de datos. Si la configuración del Router KNX IP no se corresponde con las condiciones de la instalación KNX, deberá configurarse a través del proyecto ETS. Véase la sección de la base de datos ETS.

En el estado de entrega, la dirección IP se asigna automáticamente a través de DHCP, es decir, no es necesaria ninguna otra configuración para ello. Para utilizar esta función, debe haber un servidor DHCP en la LAN (por ejemplo, muchos routers DSL tienen un servidor DHCP integrado).

Una vez que el Router KNX IP se haya conectado a la LAN y al bus KNX, debería aparecer automáticamente en el menú "Bus" bajo "Interfaces encontrados".

Al hacer clic en la interfaz encontrada, ésta se selecciona como interfaz actual. La información y las opciones específicas de la conexión aparecen entonces en la parte derecha de la ventana del ETS.

El nombre del dispositivo mostrado y la "Host Physical Address" (dirección física del dispositivo) pueden ser modificados dentro del proyecto ETS.

Como todos los dispositivos KNX programables, el Router KNX IP tiene una dirección física con la que se puede direccionar el dispositivo. Esto es utilizado, por ejemplo, por el ETS cuando se descarga el Router KNX IP a través del bus.

Para la función de interfaz, el dispositivo utiliza direcciones físicas adicionales que se pueden configurar en el ETS. Si un cliente (por ejemplo, ETS) envía telegramas al bus a través del Router KNX IP, éstos contienen una de las direcciones adicionales como dirección del emisor. Cada dirección se asigna a una conexión. De esta manera, los telegramas de respuesta pueden ser claramente reenviados al cliente correspondiente.

Las direcciones físicas adicionales deben ser del rango de direcciones de la línea de bus en la que se encuentra el Router KNX IP y no deben ser utilizadas por otro dispositivo.

Ejemplo:

Dirección del dispositivo	I.1.0 (Dirección del dispositivo en la topología)
Conexión 1	I.1.240 (1. dirección adicional)
Conexión 2	I.1.241 (2. dirección adicional)
Conexión 3	I.1.242 (3. dirección adicional)
Conexión 4	I.1.243 (4. dirección adicional)
Conexión 5	I.1.244 (5. dirección adicional)
Conexión 6	I.1.245 (6. dirección adicional)
Conexión 7	I.1.246 (7. dirección adicional)
Conexión 8	I.1.247 (8. dirección adicional)

En la sección "Dirección física" se puede seleccionar la dirección física KNX de la conexión de túnel KNXnet/IP utilizada actualmente.

The screenshot shows the DINUY software interface with the 'Bus' tab selected. The left sidebar contains a tree view with the following items: Overview, Bus, Catalogs, Settings, Connections, Interfaces, Options, Monitor, Group Monitor, Bus Monitor, Diagnostics, Unload Device, Device Info, Individual Addresses, Programming Mode, Individual Address Check, and Line Scan. The main area displays the 'Current Interface' as '1.1.0 KNX IP Router' with 'Individual Address: 1.1.240 secure'. Below this, there are sections for 'Configured Interfaces' and 'Discovered Interfaces'. The 'Discovered Interfaces' section lists three items: '1.1.0 KNX IP Router secure' (with IP 192.168.1.31:3671 and MAC 00:24:6D:01:87:BE), 'KNX-USB Interface (TP)', and another 'KNX-USB Interface (TP)'. An 'IP Tunneling' dialog box is open, showing the following fields: Name (KNX IP Router secure), Host Individual Address (1.1.0), Individual address (1.1.240), IP Address (192.168.1.31), Port (3671), and MAC Address (00:24:6D:01:87:BE).

La dirección física del dispositivo KNX, así como las direcciones físicas KNX para las conexiones de túnel adicionales, se pueden cambiar dentro del proyecto ETS después de que el dispositivo se haya añadido al proyecto

Base de datos ETS

La base de datos de ETS (a partir de ETS 5.7) puede descargarse desde la página web segura del producto Router KNX IP (www.dinuy.com) o desde el catálogo KNX Onlike de ETS.

Si el primer producto con Seguridad KNX se inserta en un proyecto, el ETS pide que se introduzca una contraseña del proyecto.

Esta contraseña protege el proyecto ETS de accesos no autorizados. Esta contraseña no es una clave utilizada para la comunicación KNX. La introducción de la contraseña puede evitarse con "Cancelar", pero no es recomendable por razones de seguridad.

El ETS requiere un certificado de cada dispositivo KNX Security que se crea en el ETS. Este certificado contiene el número de serie del dispositivo y una clave intangible (FDSK = Factory Default Setup Key).

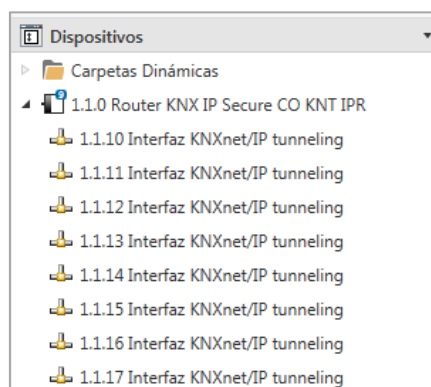
El certificado se encuentra impreso en el dispositivo. También se puede escanear cómodamente desde el código QR impreso a través de una cámara web.

La lista de todos los certificados de los dispositivos se puede gestionar en la ventana del ETS Visión General - Proyectos - Seguridad.

Esta clave inicial es necesaria para poner en funcionamiento un dispositivo de forma segura desde el principio. Aunque la descarga de ETS sea realizada por un tercero, éste no tendrá acceso a los dispositivos protegidos posteriormente. Durante la primera descarga segura, la clave inicial es sustituida por el ETS por una nueva clave que se genera individualmente para cada dispositivo. Esto evita que, personas o dispositivos que puedan conocer la clave inicial, accedan al dispositivo. La clave inicial sólo se reactiva tras un Master Reset.

El número de serie del certificado permite al ETS asignar la clave correcta a un dispositivo durante una descarga.

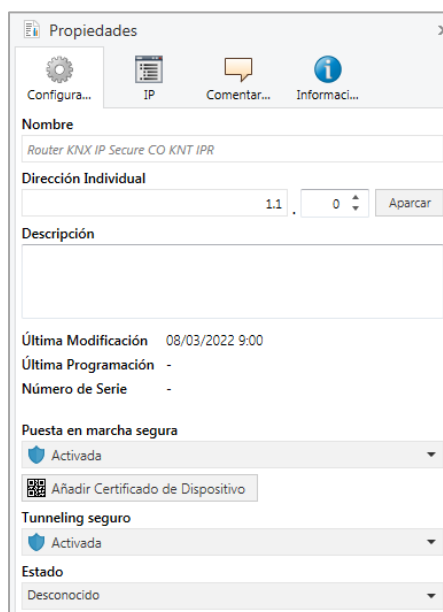
En el ETS, algunos ajustes se muestran, además de en el menú de parámetros, en el menú de propiedades (en el borde de la pantalla). La configuración IP puede realizarse ahí. Las direcciones adicionales de las conexiones del Interfaz se muestran en la vista de Topología.



Para cambiar las direcciones individuales, seleccione la entrada correspondiente en la lista e introduzca la dirección deseada en el campo de texto. Si el marco del campo de texto cambia su color a rojo después de la entrada, esto indica que la dirección introducida ya está en uso.

⇒ *Nota: Asegúrese de que ninguna de las direcciones anteriores se utiliza ya en su instalación KNX*

Al seleccionar el Router KNX IP en la estructura de árbol de la vista de topología del proyecto ETS, aparece el resumen "Propiedades" en la parte derecha de la ventana ETS. En la opción de menú "Ajustes" de Propiedades, se puede cambiar el nombre del dispositivo del Router:



Si se activa el tunnelling Secure, se creará, automáticamente, una única contraseña para cada túnel. Estas contraseñas se muestran en el menú "Configuración" cuando se selecciona uno de los túneles.

En la opción de menú "IP", de Propiedades, se pueden modificar las opciones específicas IP del Router.

Cambiando de "Obtener una dirección IP automáticamente (vía DHCP)" a "Usar una dirección IP estática", la Dirección IP, la Máscara de Subred y el Gateway por defecto, se pueden seleccionar libremente.

⇒ Nota: Los cambios realizados en los menús de propiedades sólo tienen efecto después de una descarga de la aplicación.

Dirección IP

Aquí puede introducirse la dirección IP del Router KNX IP Secure. Se utiliza para direccionar el Router a través de la red IP (LAN). El direccionamiento IP debe coordinarse con el administrador de la red.

Máscara de subred

Introduzca aquí la máscara de subred. El Router utiliza los valores introducidos en esta para determinar si un compañero de comunicación está en la red local. Si ningún interlocutor está en la red local, el Router no enviará los telegramas directamente al interlocutor, sino a la pasarela, que reenvía el telegrama.

Gateway por defecto

Introduzca aquí la dirección IP de la pasarela, por ejemplo, el router DSL de la instalación.

Dirección multidifusión

Esta dirección se utiliza para enrutar los telegramas a IP. La dirección IP multicast 224.0.23.12 ha sido reservada para este propósito (KNXnet/IP) por la IANA (Internet Assigned Numbers Authority). Si se desea otra dirección IP de multidifusión, debe ser del rango 239.0.0.0 a 239.255.255.255.

Ejemplo de asignación de direcciones IP:

Se debe acceder al Router IP con un PC:

Dirección IP del PC: 192.168.1.30
Subred del PC: 255.255.255.0

El Router KNX IP se encuentra en la misma LAN local, es decir, utiliza la misma subred. La subred restringe la asignación de la dirección IP, es decir, en este ejemplo la dirección IP de la interfaz IP debe ser 192.168.1.xx, donde "xx" puede ser un número del 1 al 254 (a excepción del 30, que ya se ha utilizado). Hay que tener cuidado de no asignar la misma dirección dos veces.

Dirección IP del Router IP: 192.168.1.31
Subred del Router IP: 255.255.255.0

Acceso remoto

Es posible el acceso remoto a través de Internet mediante el Router IP.

Diálogo de Parámetros ETS

Los siguientes parámetros se pueden ajustar con el ETS:

Ajustes generales

1.1.0 Router KNX IP Secure CO KNT IPR > Ajustes Generales	
Descripción	Nota: Para conocer el nombre del dispositivo y la configuración IP, consulte el cuadro de diálogo "Propiedades"
Ajustes Generales	Modo Prog. en el frontal del dispositivo ☐ Deshabilitado ☒ Habilitado
Reenviar (KNX -> IP)	Operación manual en el dispositivo Habilitado sin límite de tiempo
Reenviar (IP -> KNX)	

Modo Prog. en el frontal del dispositivo

Además del botón de programación ③, el Router permite activar el modo de programación en el panel frontal sin necesidad de abrir la tapa del panel. El modo de programación se puede activar y desactivar pulsando simultáneamente las teclas ⑦ y ⑧.

Esta función puede activarse y desactivarse mediante el parámetro "Modo Prog. en el frontal del dispositivo". El botón de programación empotrado ③ (junto al LED de programación ②) está siempre activado y no se ve afectado por este parámetro.

Operación manual en el dispositivo

Este parámetro establece la duración del modo de funcionamiento manual. Cuando se termina, se restablece el modo de visualización normal.

Reenviar (KNX → IP)

1.1.0 Router KNX IP Secure CO KNT IPR > Reenviar (KNX -> IP)	
Descripción	Telegramas de grupo (grupos principales 0 a 13) Filtrar
Ajustes Generales	Telegramas de grupo (grupos principales 14 a 31) Filtrar
Reenviar (KNX -> IP)	Telegramas direccionados individualmente Filtrar
Reenviar (IP -> KNX)	Telegramas Broadcast ☐ Bloquear ☒ Reenviar
	Confirmación (ACK) de telegramas de grupo ☐ Siempre ☒ Sólo si reenviado
	Confirmación (ACK) de telegramas direccionados individualmente Sólo si reenviado

Telegramas de grupo (grupos principales 0 a 13)

Bloquear: Ningún telegrama de grupo, de estos grupos principales, se reenvía a IP.

Reenviar: Todos los telegramas de grupo, de estos grupos principales, se reenvían a IP independientemente de la tabla de filtros. Esta configuración sólo debe utilizarse para fines de prueba.

Filtrar: Aquí se utiliza la tabla de filtros para comprobar si el telegrama de grupo recibido es reenviado a IP.

Telegramas de grupo (grupos principales 14 a 31)

Bloquear: Ningún telegrama de grupo, de los grupos principales 14 a 31, se reenvía a IP.

Reenviar: Todos los telegramas de grupo, de los grupos principales 14 a 31, se reenvían a IP.

Filtrar: Aquí se utiliza la tabla de filtros para comprobar si el telegrama de grupo recibido es reenviado a IP.

Telegramas direccionados individualmente (con dirección física)

Bloquear: No se reenvía ningún telegrama con dirección física a IP.

Reenviar: Todos los telegramas con dirección física se reenvían a IP.

Filtrar: La dirección física se utiliza para comprobar si el telegrama recibido con dirección física se reenvía a IP.

Telegramas Broadcast

Bloquear: Ningún telegrama de difusión recibido se reenvía a IP.

Reenviar: Todos los telegramas de difusión recibidos se reenvían a IP.

Confirmación (ACK) de telegramas de grupo

Siempre: Siempre se genera un acuse de recibo para los telegramas de grupo recibidos (desde KNX).

Sólo si reenviado: Para los telegramas de grupo recibidos (desde KNX), sólo se genera un acuse de recibo para el reenvío a IP.

Confirmación (ACK) de telegramas direccionados individualmente (con dirección física)

Siempre: Siempre se genera un acuse de recibo para los telegramas con dirección física recibidos (desde KNX).

Sólo si reenviado: Para los telegramas recibidos con dirección física (desde KNX), sólo se genera un acuse de recibo cuando se reenvía a IP.

Responder con NACK: Cada telegrama con dirección física recibido (desde KNX) es respondido con NACK (Not Acknowledge), es decir, la comunicación con telegramas con dirección física en la línea KNX correspondiente ya no es posible. La comunicación de grupo (telegramas de grupo) no se ve afectada por esto. Este ajuste puede utilizarse para evitar los intentos de manipulación.

⇒ *Nota: Si la respuesta es NACK, el acceso al dispositivo a través de KNX TP ya no es posible. La parametrización debe realizarse vía IP.*

Reenviar (IP → KNX)

1.1.0 Router KNX IP Secure CO KNT IPR > Reenviar (IP -> KNX)

Descripción	Telegramas de grupo (grupos principales 0 a 13)	Filtrar
Ajustes Generales	Telegramas de grupo (grupos principales 14 a 31)	Filtrar
Reenviar (KNX -> IP)	Telegramas direccionados individualmente	Filtrar
Reenviar (IP -> KNX)	Telegramas Broadcast	☐ Bloquear ☒ Reenviar
	Repetición de telegramas de grupo	☐ Deshabilitado ☒ Habilitado
	Repetición de telegramas direccionados individualmente	☐ Deshabilitado ☒ Habilitado
	Repetición de telegramas broadcast	☐ Deshabilitado ☒ Habilitado

Telegramas de grupo (grupos principales 0 a 13)

- Bloquear:** Ningún telegrama de grupo, de estos grupos principales, se reenvía a KNX.
- Reenviar:** Todos los telegramas de grupo, de estos grupos principales, se reenvían a KNX independientemente de la tabla de filtros. Esta configuración sólo debe utilizarse para fines de prueba.
- Filtrar:** Aquí se utiliza la tabla de filtros para comprobar si el telegrama de grupo recibido es reenviado a KNX.

Telegramas de grupo (grupos principales 14 a 31)

- Bloquear:** Ningún telegrama de grupo, de los grupos principales 14 a 31, se reenvía a KNX.
- Reenviar:** Todos los telegramas de grupo, de los grupos principales 14 a 31, se reenvían a KNX.
- Filtrar:** Aquí se utiliza la tabla de filtros para comprobar si el telegrama de grupo recibido es reenviado a KNX.

Telegramas direccionados individualmente (con dirección física)

- Bloquear:** No se reenvía ningún telegrama con dirección física a KNX.
- Reenviar:** Todos los telegramas con dirección física se reenvían a KNX.
- Filtrar:** La dirección física se utiliza para comprobar si el telegrama recibido con dirección física se reenvía a KNX.

Telegramas Broadcast

- Bloquear:** Ningún telegrama de difusión recibido se reenvía a KNX.
- Reenviar:** Todos los telegramas de difusión recibidos se reenvían a KNX.

Repetición de telegramas de grupo

- Deshabilitado:** El telegrama de grupo recibido no se envía repetidamente en el bus KNX en caso de error.
- Habilitado:** El telegrama de grupo recibido se repite hasta tres veces en caso de error.

Repetición de telegramas direccionados individualmente (con dirección física)

- Deshabilitado:** El telegrama recibido con dirección física no se envía repetidamente en el bus KNX en caso de error.
- Habilitado:** El telegrama recibido con dirección física se repite hasta tres veces en caso de error.

Repetición de telegramas broadcast

- Deshabilitado:** El telegrama de difusión recibido no se envía repetidamente en el bus KNX en caso de error.
- Habilitado:** El telegrama de emisión recibido se repite hasta tres veces en caso de error.

Programación

El Router KNX IP Secure puede ser programado a través del ETS de varias formas:

Vía Bus KNX

Para ello, sólo es necesario conectar el dispositivo al Bus. El ETS requiere un interfaz adicional (por ejemplo, USB) para tener acceso al Bus. De este modo, se puede programar tanto la dirección física como toda la aplicación, incluida la configuración IP. Se recomienda la programación a través del Bus si no se puede establecer una conexión IP.

Vía Tunnelling KNXnet/IP

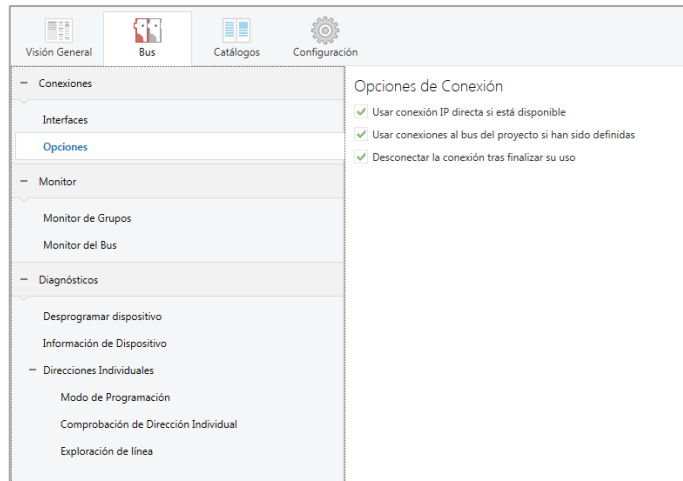
En este caso, no se requiere ningún interfaz adicional. La programación a través de KNXnet/IP tunnelling es posible si el dispositivo ya tiene una configuración IP válida (por ejemplo, a través de DHCP). En este caso, el dispositivo aparece en la configuración de los interfaces del ETS y debe ser seleccionado. La descarga se realiza desde el proyecto ETS, como con otros dispositivos.

Vía Routing KNXnet/IP

La programación a través del enrutamiento KNXnet/IP es posible si el dispositivo ya tiene una configuración IP válida (por ejemplo, a través de DHCP o Auto IP). El interfaz de enrutamiento aparece en el ETS si al menos un dispositivo, que soporta el enrutamiento, es visible en la red. El nombre del interfaz de red en el PC aparece como descripción. Si se selecciona el enrutamiento como interfaz, la programación se realiza desde el proyecto ETS como con otros dispositivos. En este caso, la LAN se utiliza como un medio KNX similar al TP. No se requiere ningún interfaz adicional.

Vía conexión IP directa

Mientras que tanto KNXnet/IP Tunneling como KNXnet/IP Routing están limitados a la velocidad de KNX TP, una conexión IP directa permite cargar el dispositivo a alta velocidad. La conexión IP directa es posible si el dispositivo ya tiene una configuración IP válida y una dirección física. Para ello, hay que seleccionar la opción "Utilizar la conexión IP directa si es posible" en el menú ETS, en "Bus - Conexiones - Opciones". La descarga tiene lugar directa-mente en el dispositivo y no es visible en el monitor del grupo ETS



⇒ Nota: Debido a los tiempos de transmisión significativamente más cortos, se recomienda realizar las descargas a través de IP.

Licencias de código abierto

El firmware utilizado en este producto se basa en el siguiente paquete de software de código abierto:

curve25519-donna: curva elíptica Curve25519, función de clave pública

Fuente: <http://code.google.com/p/curve25519-donna/>

Copyright 2008, Google Inc. Todos los derechos reservados.

Se permite la redistribución y el uso en forma de código fuente y binario, con o sin modificación, siempre que se cumplan las siguientes condiciones:

Las redistribuciones del código fuente deben conservar el aviso de copyright anterior, esta lista de condiciones y el siguiente descargo de responsabilidad.

Las redistribuciones en formato binario deben reproducir el aviso de copyright anterior, esta lista de condiciones y la siguiente exención de responsabilidad en la documentación y/o otros materiales proporcionados con la distribución.

Ni el nombre de Google Inc. ni los nombres de sus colaboradores pueden utilizarse para respaldar o promocionar productos derivados de este software sin un permiso específico previo por escrito.

ESTE SOFTWARE ES PROPORCIONADO POR LOS TITULARES DE LOS DERECHOS DE AUTOR Y LOS COLABORADORES "TAL CUAL" Y SE RECHAZA CUALQUIER GARANTÍA EXPRESA O IMPLÍCITA, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZABILIDAD E IDONEIDAD PARA UN FIN DETERMINADO. EN NINGÚN CASO EL PROPIETARIO DE LOS DERECHOS DE AUTOR O LOS COLABORADORES SERÁN RESPONSABLES DE NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR O CONSECUENTE (INCLUYENDO, PERO SIN LIMITARSE A, LA ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUTOS; LA PÉRDIDA DE USO, DATOS O BENEFICIOS; O LA INTERRUPCIÓN DE LA ACTIVIDAD COMERCIAL), SEA CUAL SEA LA CAUSA Y LA TEORÍA DE LA RESPONSABILIDAD, YA SEA POR CONTRATO, RESPONSABILIDAD ESTRUCTIVA O AGRAVIO (INCLUYENDO LA NEGLIGENCIA O DE OTRO TIPO) QUE SURJA DE CUALQUIER MANERA DEL USO DE ESTE SOFTWARE, INCLUSO SI SE AVISA DE LA POSIBILIDAD DE TALES DAÑOS.



ADVERTENCIA

- El aparato sólo puede ser instalado y puesto en marcha por un electricista autorizado.
- Deben respetarse las normas de seguridad y prevención de accidentes vigentes.
- El dispositivo no debe ser abierto.
- En la planificación e instalación de las instalaciones eléctricas deben observarse las directivas, reglamentos y disposiciones pertinentes del país correspondiente.