# User Manual

## K-BUS IP Router with Secure_V1.2

## BNIPR-00/00.S


## KNX/EIB Home and Building Control System

# Attentions

1. **Please keep devices away from strong magnetic field, high temperature, wet environment;**


2. **Do not fall the device to the ground or make them get hard impact;**


3. **Do not use wet cloth or volatile reagent to wipe the device;**


4. **Do not disassemble the devices.**

# Contents


Chapter 1 Summary ---- 1

1.1 Function overview ---- 2

1.2 Tunneling ---- 3

1.3 Routing ---- 3

1.4 KNX IP Routers ---- 3

Chapter 2 Technical Data ---- 4

Chapter 3 Dimension and Connection diagram ---- 5

3.1 Dimension diagram ---- 5

3.2 Connection diagram ---- 5

Chapter 4 Planning and Application ---- 2

4.1 KNX Telegrams in the IP Network ---- 2

4.2 The IP Router in a Network Installation ---- 2

4.3 The IP Router as an Area Coupler ---- 2

4.4 The IP Router in a Mixed System ---- 3

4.5 The IP Router as a Line Coupler ---- 4

Chapter 5 Parameter setting description in the ETS ---- 5

5.1 Parameter window “General” ---- 5

5.2 Parameter window “Routing (KNX->LAN)” ---- 8

5.3 Parameter window “Routing (LAN->KNX)” ---- 10

5.4 Use of the integrated tunneling servers ---- 13

5.5 KNX Secure ---- 15

5.6 ETS bus configuration interface ---- 18

Chapter 6 Factory setting ---- 21

# Chapter 1 Summary

The IP Router can be used as line or backbone coupler. It provides a data connection between the upper KNXnet/IP line (main line or backbone) and the lower TP KNX bus line (sub line). The basic functionality of the IP Router is to couple the Ethernet with one or more KNX-TP lines. The IP Router features a galvanic isolation between the Ethernet and the KNX-TP line(s). Due to its flexibility the IP Router can be used as a line coupler e.g. to connect several KNX TP lines via Ethernet. And it can be used as a backbone coupler to connect several TP areas or different TP installation systems via Ethernet.

The device supports the KNX Secure protocol (KNXnet/IP Security).

The main task of the IP Router is filtering the traffic according to the installation hierarchy. For group oriented communication the traffic is filtered according to the built-in filter tables.

With the ETS or any other KNX compatible commissioning tool the IP Router can be used as the programming interface. For this purpose the device provides up to 5 additional physical addresses that can be used for IP tunneling. The IP Router has no KNX communication objects for itself.

The IP Router is a Tunneling and Routing device. These features are described in the following sections in detail. It is able to use the Engineering Tool Software ETS (ETS5 or later) with a .knxprod file to allocate the physical address and set the parameter.

The IP Router is a modular installation device. It can be installed in the distribution board on 35mm mounting rails according to EN 60715.

This manual provides the technical information about the IP Router as well as assembly and programming in detail for users, and explains how to use the interface device by the application examples.

**The device also does not support bus monitoring.**

## 1.1 Function overview

The IP Router has the follow functions:

- **The IP Router supports long messages up to 55 bytes.**
- **The IP Router favorably replaces a line coupler or an area coupler. Using LAN as a fast medium to exchange telegrams between lines and/or areas is the great advantage.**
- **The IP Router works with no external power supply.**
- **Providing tunneling protocols and a connection point for the ETS (or any other tool to enable commissioning and monitoring) . Five parallel connections are possible, one separate address for each and every connection.**
- **ACK sending on sent out messages is ETS configurable**
- **After no ACK response on a sent message the IP Router can repeat it up to three times. For physically addressed or for group addressed telegrams this can be configured via ETS independently. In case of an ACK response there will be no repetition.**
- **The IP Router is featuring a high internal amount of communication buffers being capable of smoothing peeks in the communication load course.**
- **The IP Router supports KNXnet/IP, ARP, ICMP, IGMP, HTTP, UDP/IP, TCP/IP and DHCP.**

## 1.2 Tunneling

The presence of the Internet Protocol (IP) has led to the definition of KNXnet/IP. KNXnet/IP provides the means for point-to-point connections like “KNXnet/IP Tunneling” for ETS and/or between a supervisory system and a KNX installation.

The KNXnet/IP Device Management provides configuring KNXnet/IP devices via the KNX network effectively. Additionally, with this the time required for network configurations is reduced.

## 1.3 Routing

Routing is the way of interconnecting KNX lines or areas via IP network(s) using KNXnet/IP. In IP networks the KNXnet/IP Routing defines how KNXnet/IP routers communicate with each other.

## 1.4 KNX IP Routers

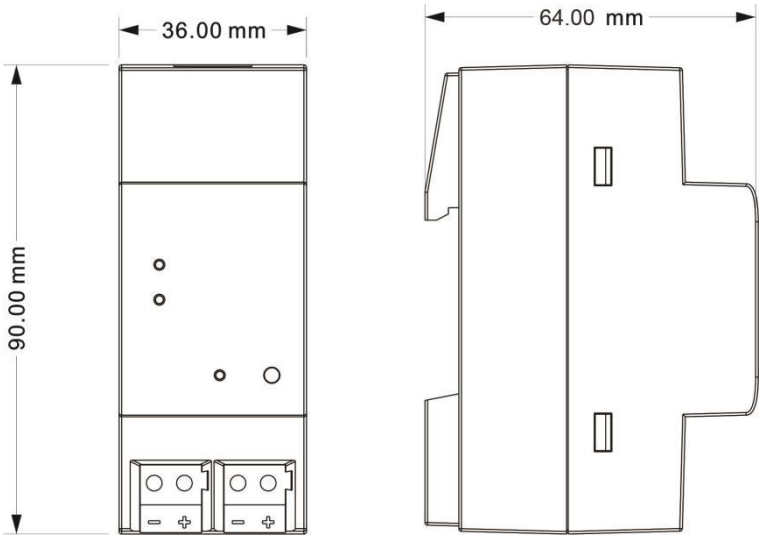
The IP Router is a KNX IP router. KNX IP routers are highly similar to TP line couplers. The only exception is that they use the communication medium Ethernet as their main line. However, it is also possible to integrate KNX end devices via IP directly. This makes the Ethernet a KNX medium.

# Chapter 2 Technical Data

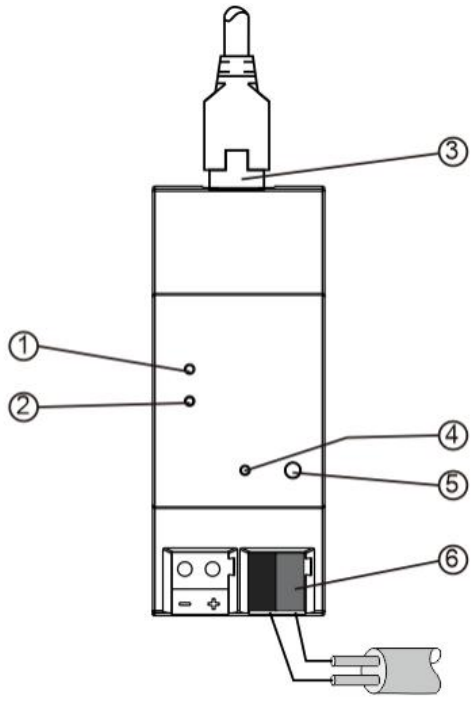
| | | |
|---|---|---|
| **Power supply** | Bus voltage | 21-30V DC, via the KNX bus |
| | Bus current | <19.5mA, 24V; <15.5mA, 30V |
| | Bus consumption | <470mW |
| **Connections** | KNX | Via bus connection terminal (Red/Black) |
| | LAN | RJ45 socket for 100/10 Base-T |
| **Operating and display** | LAN LED | On: The network connect normally<br>Flashing: The telegram traffic between device and network |
| | KNX LED | On: The KNX bus connect normally<br>Flashing: The telegram traffic between KNX bus and device |
| | Programming LED and button | For assigning the physical address |
| **Temperature** | Operation | –5 °C ... + 45 °C |
| | Storage | –25 °C ... + 55 °C |
| | Transport | – 25 °C ... + 70 °C |
| **Ambient** | Humidity | <93%, except dewing |
| **Dimensions** | 36 mm×90 mm×64mm | |
| **Weight** | 0.1KG | |
| **Housing, colour** | Plastic housing, beige | |
| **Design** | Modular installation device, on 35mm mounting rail | |

# Chapter 3 Dimension and Connection diagram

## 3.1 Dimension diagram




## 3.2 Connection diagram




① LAN LED ON, indicate that network connect normally

LAN LED flashing, indicate that telegram traffic between device and network

② KNX LED ON, indicate that KNX bus connect normally

KNX LED flashing, indicate that telegram traffic between KNX bus and device

③ LAN connection

④ Programming LED, red LED ON for assignment of physical address

⑤ Programming button, to enter or exit the physical address programming mode

**Reset the device to the factory configuration: press the programming button and hold for 4 seconds then release, repeat the operation for 4 times, and the interval between each operation is less than 3 seconds, after this operation, It will reset and restart.**

⑥ KNX bus connection terminal

# Chapter 4 Planning and Application

## 4.1 KNX Telegrams in the IP Network

The IP Router sends telegrams from/to the KNX to/from the IP network in accordance with the KNXnet/IP protocol specification. According to the default setting these telegrams are sent as multicast telegrams to the multicast IP address 224.0.23.12 port 3671. The multicast IP address 224.0.23.12 is the defined address for the KNXnet/IP from the KNX Association in conjunction with the IANA. This address of the device can not be changed. During commissioning, it is important to note:

- **All KNX IP devices that are intended to communicate with each other via IP network must have the same IP multicast address**
- **IGMP (Internet Group Management Protocol) is used for the IP configuration to establish multicast group memberships**
- **If the IP address is changed from the IP side, it may sometimes happen that the ETS does not recognize the device anymore and the connection can no longer be established (tunneling uses IP address). As a precaution, always run a restart or change the address from the TP side**
- **Please ask your administrator if problems occur for the IP Address assignment**
- **According to the topology, the additional physical addresses (for tunnelling) always have to be assigned in the range of sub line addresses. For more information about the IP tunneling addresses please refer to Chapter 6.**
- **If a KNX/USB or KNX/IP interface is used to program a device of another line connected to a KNX IP Router, you should pay close attention to have the correct topology!**

## 4.2 The IP Router in a Network Installation

In a network installation the IP Router can either be used as a KNX area coupler or as a KNX line coupler.

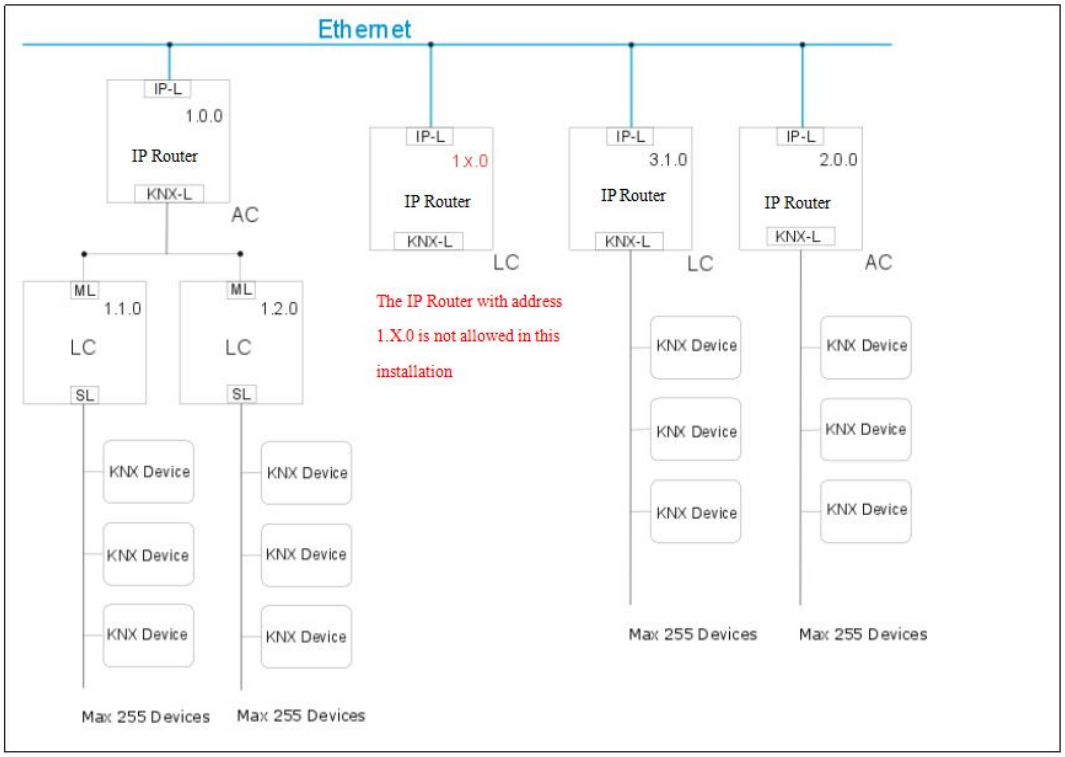
## 4.3 The IP Router as an Area Coupler

The IP Router can replace an area coupler in a KNX network. For this purpose it must receive the physical address of an area coupler (X.0.0, 1≤X≤15). In the ETS up to 15 areas can be defined with area couplers.

## 4.4 The IP Router in a Mixed System

If it is necessary in a KNX system to use the IP Router at one point as an area coupler, e.g. office or home complex, and at another point as a line coupler, e.g. a remote underground garage or a pool; this is possible. It is only necessary to ensure that the IP Router used as a line coupler uses a line coupler address from a free addressing area. The following picture best illustrates the topology with IP Router routers as area and/or line couplers. Special attention needs to be paid that if a IP Router area coupler with address “1.0.0” already exists in the installation, no other IP Router line coupler (or any other KNX IP router) with address “1.X.0, 1≤X≤15” is allowed to be used in that network, and of course vice versa, if a IP Router line coupler with address “1.1.0” already exists in the installation, no other IP Router area coupler (or any other KNX IP router) with address “1.0.0” is allowed to be used in that network.

A direct connection between two IP Routers is possible as well. In this case, the auto IP will assign each IP Router an IP address and the two IP Routers will communicate over either a normal or a crossed network cable.




Mixed system

## 4.5 The IP Router as a Line Coupler

The IP Router of a KNX network can assume the functionality of a line coupler. For this purpose it must have the physical address of a line coupler (X.Y.0, 1≤X & Y ≤15). In the ETS up to 225 lines can be defined (from 1.1.0 to 15.15.0).

When the coupler receives telegrams (for example during commissioning) that use physical addresses as destination addresses, it compares the physical addresses of the receiver with its own physical address and then decides whether it has to route the telegrams or not.

Due to telegrams with group addresses the coupler reacts in accordance with its parameter settings. During normal operation (default setting), the coupler only routes those telegrams whose group addresses have been entered in its filter table.

If the coupler routes a telegram and does not receive an acknowledgement, or if a bus device discovers a transmission error, the coupler repeats the telegram up to three times (depending on the corresponding parameter that is set to the device through the last ETS download). With the parameters "Repetitions if ...telegram“, this repeat behaviour can be set. These parameters should stay with the default setting.

# Chapter 5 Parameter setting description in the ETS

## 5.1 Parameter window “General”

Parameter window “General” is shown in fig. 5.1.1. The device information,including company name, project name,DNS server can be set here.

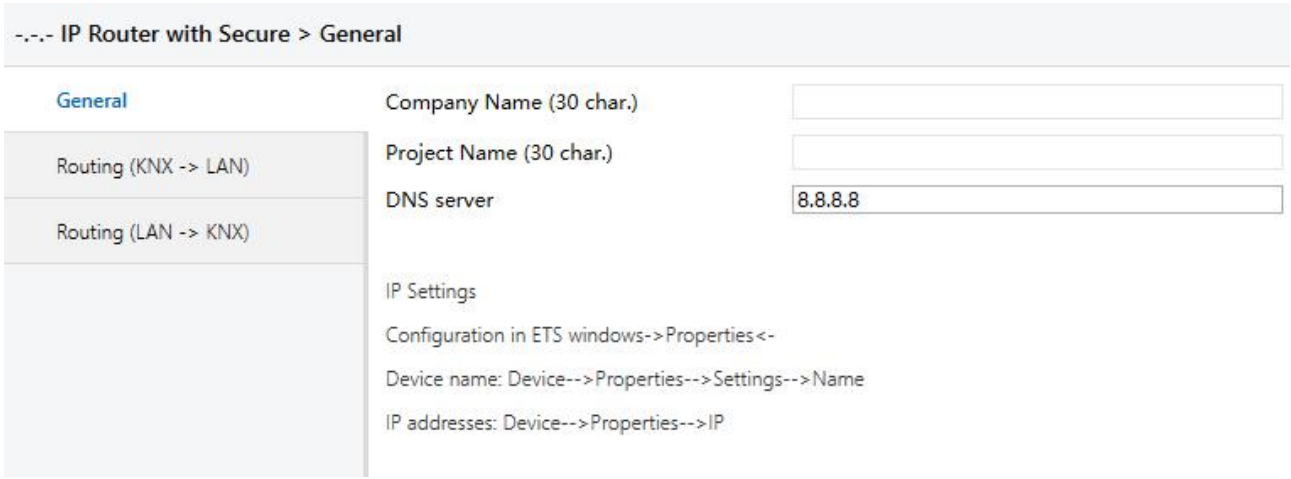



Fig 5.1.1 “General” parameter window

**Parameter "Company Name (30 char.)"**

This parameter is used to set the company name the device belongs to. Maximum 30 characters can be input.

**Parameter "Project Name (30 char.)"**

This parameter is used to set the project name the device belongs to. Maximum 30 characters can be input.

**Parameter "DNS server"**

This parameter is used to set the DNS server address.

**IP settings**

**Configuration in ETS windows-->Properties**

Configure the IP parameters of the IP device in the properties window of ETS.

**Device name: Device-->Properties-->Settings-->Name**

The device name can be entered in the Settings Properties window. The device name loaded into the device can be changed in the Name field, as shown in Figure5.1.2 below.

The device name is used for identification of the device on the LAN. For example, the installation location can be identified by the names assigned to the devices, e.g. IP Router, hall, etc

**Note: Only the first 30 characters of the device name are loaded into the device; the rest is truncated.**

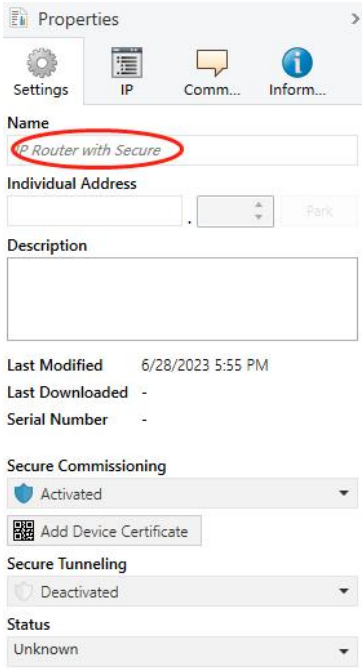



Fig. 5.1.2 Settings

**IP addresses: Device-->Properties-->IP**

The IP address can be defined in the IP Properties window, as shown in Figure 5.1.3 below.

The following options are available for setting the IP address:

Options:

**Obtain an IP address automatically**

**Use a static IP address**

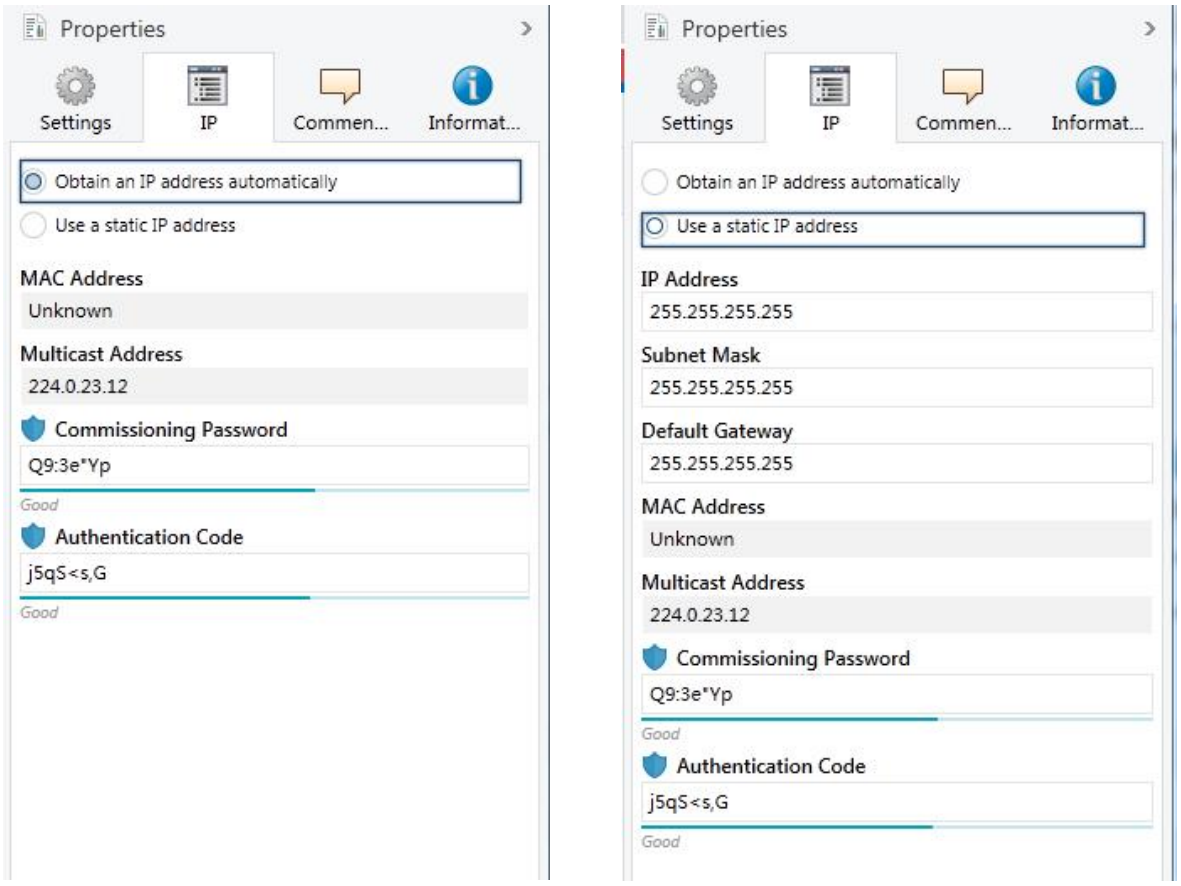



Fig. 5.1.3 IP

**Obtain an IP address automatically**：In the default setting the IP Router with Secure expects the assignment of an IP address by a DHCP (dynamic host configuration protocol) server. This server responds to a request by assigning a free IP address to the device. If a DHCP server is not available in the network, the device will be inaccessible.

**Use a static IP address**：If no DHCP server is installed on the network or if the IP address should remain the same, it can be assigned as static. When assigning static IP addresses, ensure that each device receives a different IP address, and also configure the matching subnet mask and default gateway.

The MAC address is read from the device after a download

The multicast address is only displayed here, 224.0.23.12, it can not be changed.

The commissioning password and the authentication code are only visible when KNX Secure is activated, and are required for IP tunneling connections.

## 5.2 Parameter window “Routing (KNX->LAN)”

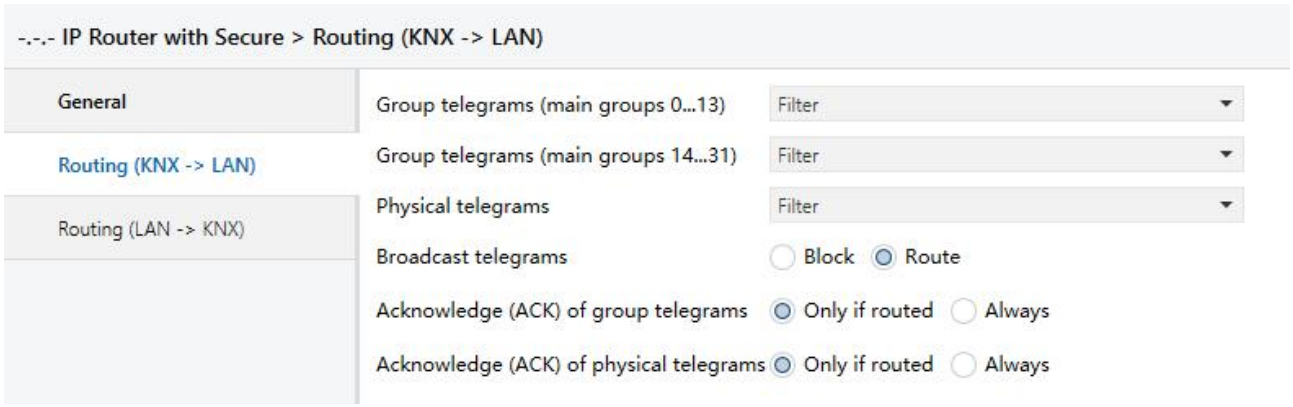



Fig. 5.2 Parameter window “Routing(KNX->LAN)”

**Parameter "Group telegrams (main groups 0...13)"**

This parameter defines whether the telegrams with group addresses of the main groups 0 to 13 are filtered, routed or blocked. Options:

**Block**

**Route**

**Filter**

Block: No Group telegrams (main group 0…13) are routed to LAN.

Route: All Group telegrams (main group 0…13) are routed to LAN.

Filter: Group telegrams (main group 0…13) are routed to LAN if entered in the filter table.

**Parameter "Group telegrams (main groups 14...31)"**

This parameter defines whether the telegrams with group addresses of the main groups 14 to 31 are filtered, routed or blocked. Options:

**Block**

**Route**

**Filter**

Block: No Group telegrams (main group 14…31) are routed to LAN.

Route: All Group telegrams (main group 14…31) are routed to LAN.

Filter: Group telegrams (main group 14…31) are routed to LAN if entered in the filter table.

## Parameter "Physical telegrams "

This parameter defines whether physically addressed telegrams are filtered, routed or blocked.

Options:

**Block**

**Route**

**Filter**

Block: No physical telegram is routed to LAN.

Route: All physical telegrams are routed to LAN.

Filter: Only physical telegrams are routed to LAN based on the physical address.

**Note: The parameter "Route" for Group telegrams and Physical telegrams is intended only for testing purposes and should not be set for normal operation.**

## Parameter "Broadcast telegrams "

This parameter defines whether Broadcast telegrams are routed or blocked. Options:

**Block**

**Route**

Block: No received broadcast telegrams are routed to LAN. With this setting it is not possible to send broadcast telegrams from a line of a lower level than the IP Router to another line, e.g. during programming.

Route: All received broadcast telegrams are routed to LAN.

## Parameter "Acknowledge(ACK) of group telegrams "

This parameter defines whether the IP Router is to acknowledge group telegrams with a telegram.

Options:

**Only if routed**

**Always**

Only if routed: A acknowledge is only generated for received group telegrams (from KNX) if they are routed to LAN.

Always: A acknowledge is generated for every received group telegram (from KNX).

**Parameter "Acknowledge(ACK) of physical telegrams "**

This parameter defines whether the IP Router is to acknowledge physical telegrams with a telegram. Options:

**Only if routed**

**Always**

Only if routed: A acknowledge is only generated for received physical telegrams (from KNX) if they are routed to LAN.

Always: A acknowledge is generated for every received physical telegram (from KNX).

## 5.3 Parameter window "Routing (LAN->KNX)"

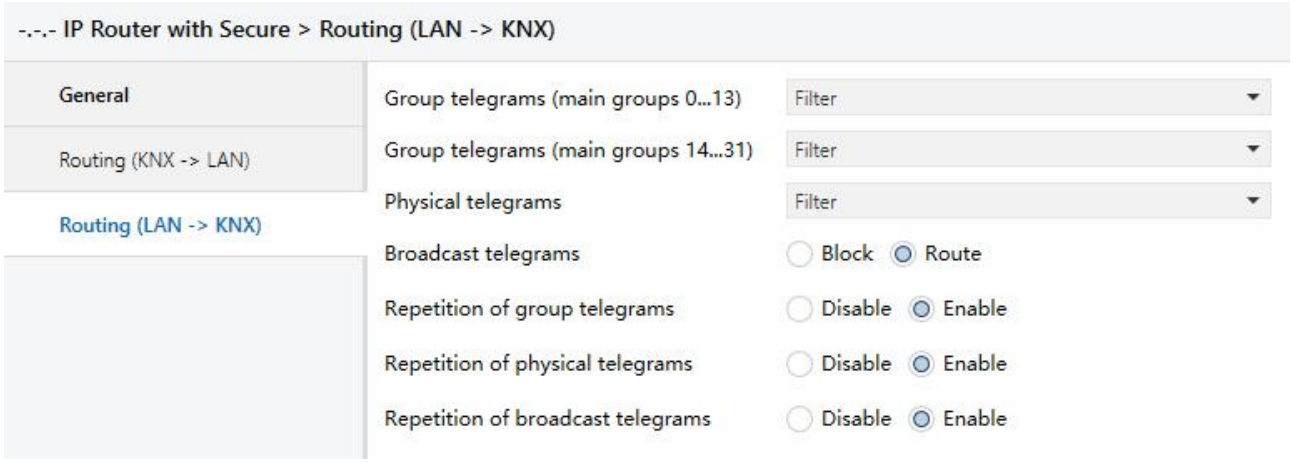



Fig. 5.3 Parameter window "Routing(LAN->KNX)"

**Parameter "Group telegrams (main groups 0...13)"**

This parameter defines whether the telegrams with group addresses of the main groups 0 to 13 are filtered, routed or blocked. Options:

**Block**

**Route**

**Filter**

Block: No Group telegrams (main group 0…13) are routed to KNX.

Route: All Group telegrams (main group 0…13) are routed to KNX.

Filter: Group telegrams (main group 0…13) are routed to KNX if entered in the filter table.

### Parameter "Group telegrams (main groups 14...31)"

This parameter defines whether the telegrams with group addresses of the main groups 14 to 31 are filtered, routed or blocked. Options:

**Block**

**Route**

**Filter**

Block: No Group telegrams (main group 14…31) are routed to KNX.

Route: All Group telegrams (main group 14…31) are routed to KNX.

Filter: Group telegrams (main group 14…31) are routed to KNX if entered in the filter table.

### Parameter "Physical telegrams "

This parameter defines whether physically addressed telegrams are filtered, routed or blocked. Options:

**Block**

**Route**

**Filter**

Block: No physical telegram is routed to KNX.

Route: All physical telegrams are routed to KNX.

Filter: Only physical telegrams are routed to KNX based on the physical address.

**Note: The parameter "Route" for Group telegrams and Physical telegrams is intended only for testing purposes and should not be set for normal operation.**

### Parameter "Broadcast telegrams "

This parameter defines whether Broadcast telegrams are routed or blocked. Options:

**Block**

**Route**

Block: No received broadcast telegrams are routed to KNX. With this setting it is not possible to send broadcast telegrams from a line of a lower level than the IP Router to another line, e.g. during programming.

Route: All received broadcast telegrams are routed to KNX.

### Parameter "Repetition of group telegrams "

This parameter defines whether the received group telegrams are re-sent in case of a fault (e.g. due to missing receiver). Options:

**Disable**

**Enable**

Disable: The received group telegram is not re-sent to KNX in case of a fault.

Enable: The received group telegram is re-sent up to three times in case of a fault.

### Parameter "Repetition of physical telegrams "

This parameter defines whether the received physical telegrams are re-sent in case of a fault (e.g. due to missing receiver). Options:

**Disable**

**Enable**

Disable: The received physical telegram is not re-sent to KNX in case of a fault.

Enable: The received physical telegram is re-sent up to three times in case of a fault.

### Parameter "Repetition of broadcast telegrams "

This parameter defines whether the received broadcast telegrams are re-sent in case of a fault (e.g. due to missing receiver). Options:

**Disable**

**Enable**

Disable: The received broadcast telegram is not re-sent to KNX in case of a fault.

Enable: The received broadcast telegram is re-sent up to three times in case of a fault.

## 5.4 Use of the integrated tunneling servers

The IP Router with Secure offers 5 additional physical addresses, which can be used for a tunneling connection, shown in fig. 5.4.1. These so-called tunneling servers can be used with the ETS as a programming interface or with another visual display client, with smartphone, with tablet, with bus tool etc.

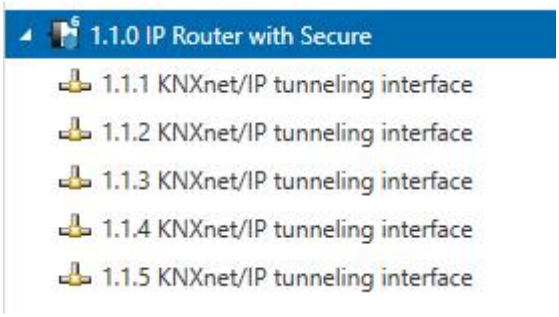



Fig.5.4.1 Tunneling

The physical address of each tunneling connection can be changed in the setting property window, and their physical addresses must fit the topology.

In ETS, the first five free addresses in the line are assigned automatically after the device has been inserted into a line. This is a property of the ETS and cannot be changed.

The addresses will be available in the device after the first download.

If this is not desired, the setting can be changed manually in the Properties window via activated the Park, shown in fig. 5.4.2. This tunnel will receive the address 15.15.255 after download. If the option Park is selected for all tunneling servers, all tunneling servers will be assigned the address 15.15.255. ( 15.15.255 is the default address for devices with no physical address assigned)

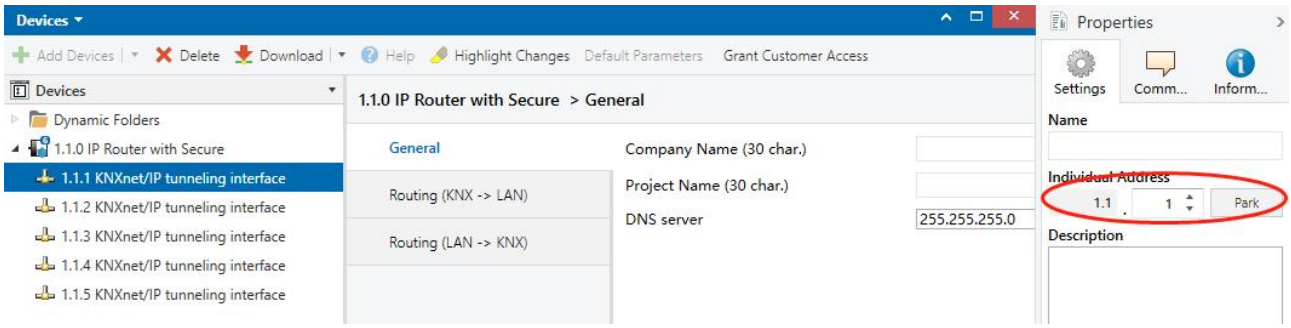



Fig.5.4.2 Setting - Park

In addition, the tunneling servers can also be encrypted with KNX Secure. First activate Secure Commissioning, and then activate Secure Tunneling, as shown in Figure 5.4.3. After activating Secure

Tunneling, the password for each Tunneling connection can be set in ETS, as shown in Figure 5.4.4, and users can change this password as needed.

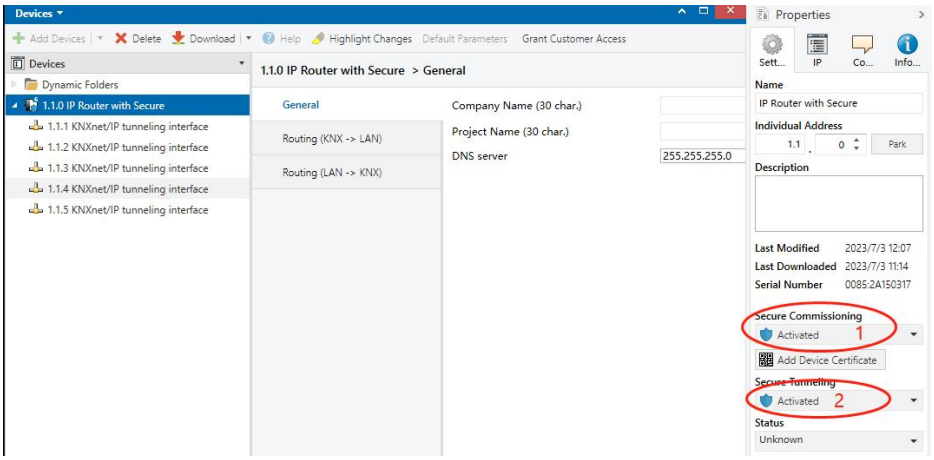



Fig.5.4.3 Setting - Secure activated

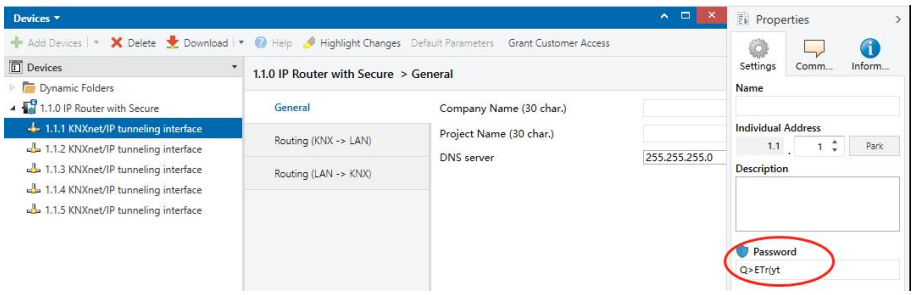



Fig.5.4.4 Setting - tunneling password

If a project password is not assigned to the project, ETS will prompt to assign a project password when activate Secure Commissioning , as shown in Figure 5.4.5 below. In other words, you must set a project password for the project, otherwise the Secure Commissioning cannot be activated.


Fig.5.4.5 Set project password

## 5.5 KNX Secure

The IP Router with Secure is a KNX device according to the KNX Secure standard. In other words, the device can run in secure mode, and the tunneling connection are encrypted.

Therefore, the following information must be taken into account during device commissioning:

❖ It is essential to assign a project password as soon as a KNX Secure device is imported into a project. This will protect the project against unauthorized access.

**The password must be kept in a safe place – access to the project is not possible without it (not even the KNX Association or device manufacturer will be able to access it)!**

**Without the project password, the commissioning key will not be able to be imported.**

❖ A commissioning key is required when commissioning a KNX Secure device (first download). This key (FDSK = Factory Default Setup Key) is included on a sticker on the side of the device, and it must be imported into the ETS prior to the first download.

✧ On the first download of the device, a window pops up in the ETS to prompt the user to enter the key, as shown in Figure 5.5.1 below. The certificate can also be read from the device using a QR scanner (recommended).

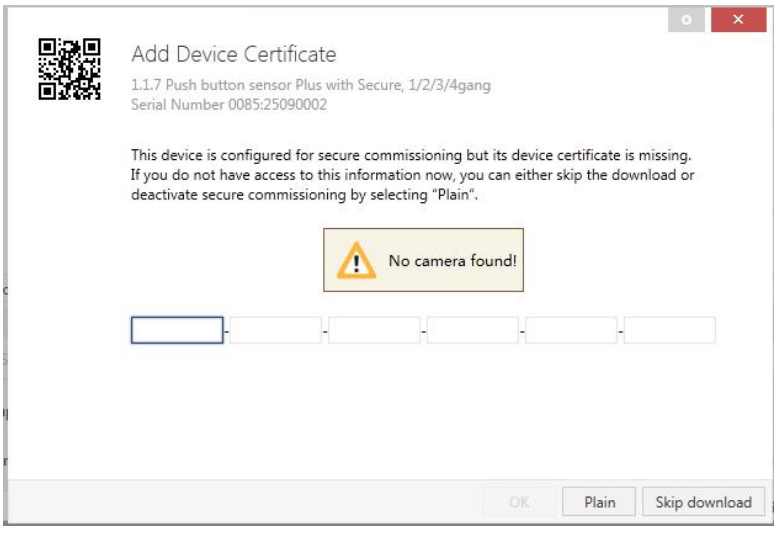



Fig.5.5.1 Add Device Certificate window

✧ Alternatively, the certificates of all Secure devices can be entered in the ETS beforehand. This is done on the “Security” tab on the project overview page, as shown in Figure 5.5.2 below.

The certificates can be also added to the selected device in the project, as shown in Figure 5.5.3.

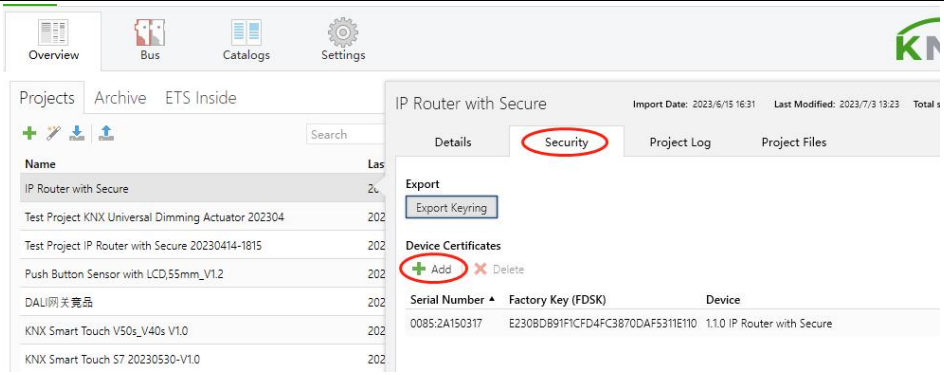



Fig. 5.5.2 Add Device Certificate in overview

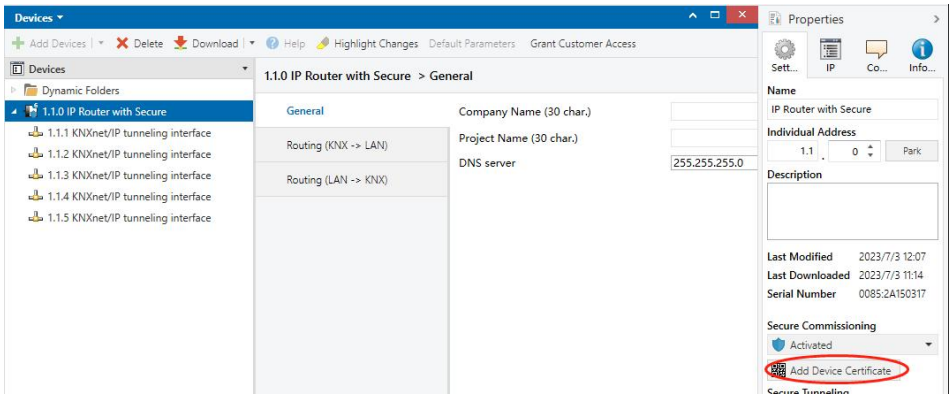



Fig. 5.5.3 Add Device Certificate in project

✧ FDSK sticker is applied on the device.

**Without the FDSK, it will no longer be possible to operate the device in KNX Secure mode after a reset.**

The FDSK is required only for initial commissioning. After entering the initial FDSK, the ETS will assign a new key, as shown in Figure 5.5.4 below.

The FDSK will be required again only if the device was reset to its factory settings (e.g. If the device is to be used in a different ETS project).


Fig. 5.5.4 Adding Device Certificate window

**Example:**

If this application in the project needs to be tried with another device, it is no longer the original device. When the application is downloaded to a new device, the following prompt will appear on the left of figure 5.5.5, click yes, the Add Device Certificate window will appear, then enter the initial FDSK of the new device, and you need to reset the device to the factory settings (it is not required if the device is still factory default; If it has been used, it will be required to reset, otherwise the following error message will appear on the right of figure 5.5.5), and then the device can be successfully downloaded again.

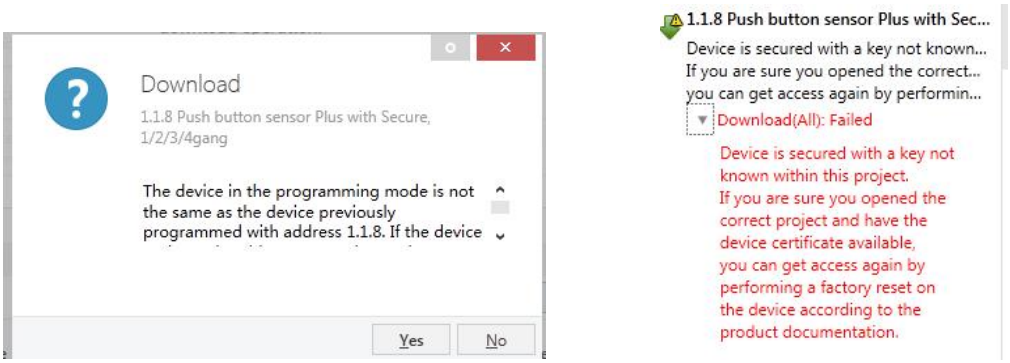



Fig. 5.5.5 Example

Whether the device is replaced in the same project, or the device is replaced in a different project, the processing is similar: **Reset the device to the factory settings, then reassign the FDSK.**

After the device is downloaded successfully, the label Add Device Certificate turns gray, indicating that the key for this device has been assigned successfully, as shown in Figure 5.5.6 below.

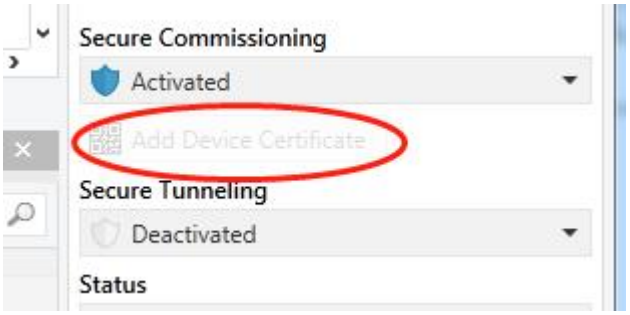



Fig. 5.5.6

**ETS generates and manages keys:**

Keys and passwords can be exported as needed to the use of security keys outside of the associated ETS projects, e.g. if a client would like to access one of the tunnels. As shown in Figure 5.5.7 below, the file extension is .knxkeys.

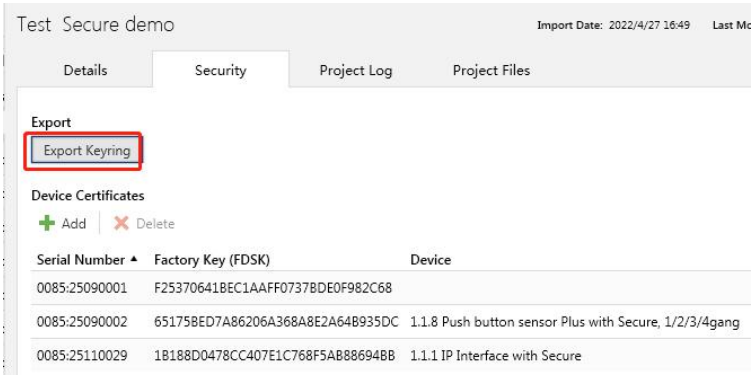



Fig. 5.5.7

## 5.6 ETS bus configuration interface

Generally, after obtaining the device,to make the device work normally, we first need to configure the device with reasonable parameters and physical addresses in the ETS. The configuration of IP parameters should be defined according to the network environment, and the physical address of the device is defined according to the topology of the KNX system. After completing the configuration, download it to the device.

When IP router work normally, it can view the IP address, physical address, port number and other information of the device, as shown in Fig.5.6.1 below.

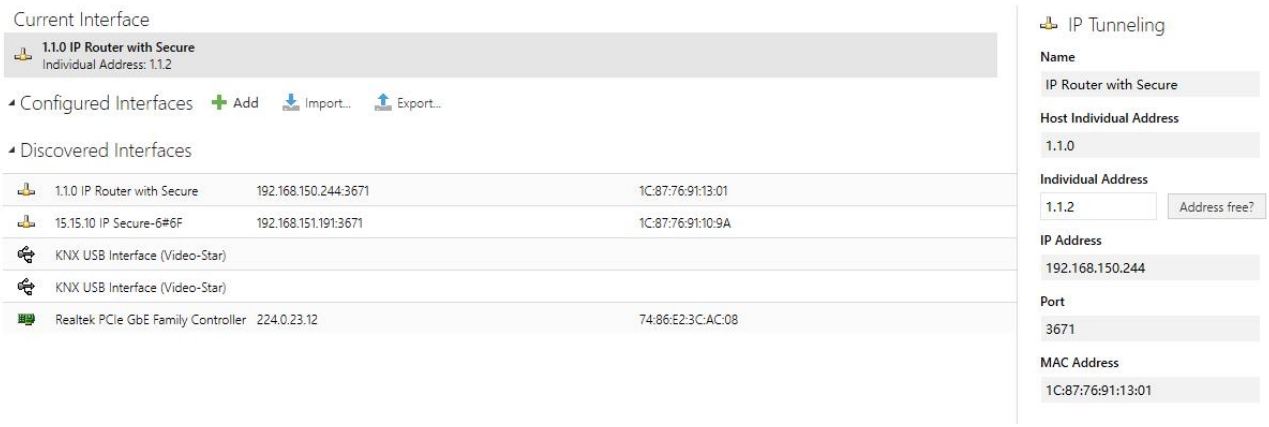
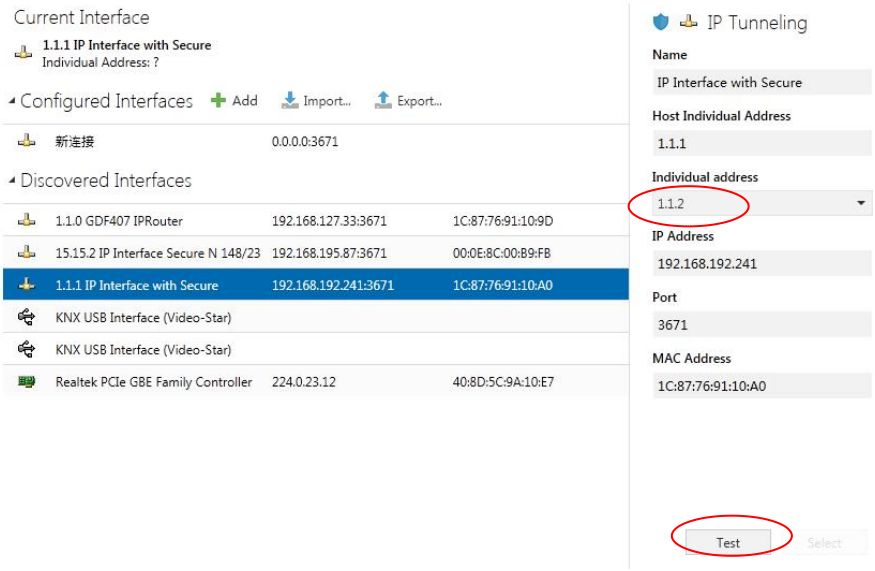



Fig.5.6.1 ETS bus configuration interface

**ETS with IP connection example( the IP router is similar with IP interface):**

The whole process is shown in Figure 5.6.2 below. Select the IP device, select one of the Tunneling (such as physical address 1.1.2), click “Test”, the commissioning password and authentication code input window will pop up (the password and authentication code can be viewed in the device property window in the project), enter the password and authentication code. After click “OK”, the word Ok will appear next to the “Test” button, and then click “Select” to connect.



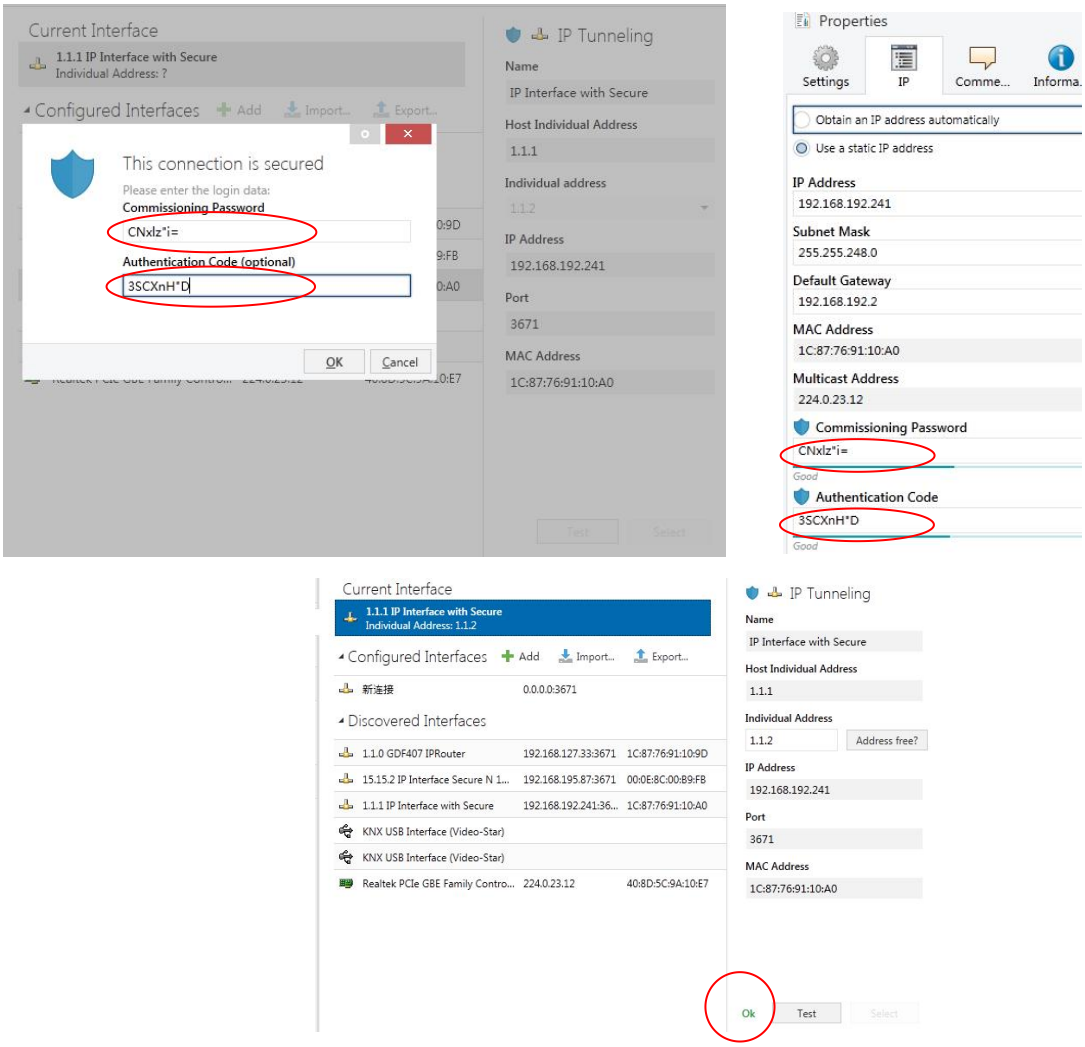



Fig. 5.6.2 IP tunneling connection

In Figure 5.6.2, if Secure Tunneling is not activated, , the commissioning password and authentication code are not required when the device is connected as an interface; if Secure Tunneling is activated, ETS will prompt you to enter the commissioning password and authentication code when connecting.

The IP Router can be reset to its factory settings if necessary, see chapter 6, Factory setting

**Note: Any USB interface used for programming a KNX Secure device must support “long frames”. Otherwise ETS will report a download failure information.**

# Chapter 6 Factory setting

The IP Router is delivered with the following default factory settings:

| | |
|---|---|
| **Physical address** | 15.15.0 |
| **Physical address for IP tunneling connections** | 15.15.241<br>15.15.242<br>15.15.243<br>15.15.244<br>15.15.245 |
| **IP configuration** | |
| **IP address assignment** | Fixed for 192.168.2.200 |
| **IP routing multicast address** | 224.0.23.12 |
| **Routing (KNX->LAN)** | |
| **Group telegrams (main group 0...13)** | Filter (Filter table is empty) |
| **Group telegrams (main group 14...31)** | Filter |
| **Physical telegrams** | Filter |
| **Broadcast telegrams** | Route |
| **Acknowledge(ACK) of group telegrams** | Only if routed |
| **Acknowledge(ACK) of physical telegrams** | Only if routed |
| **Routing (LAN->KNX)** | |
| **Group telegrams (main group 0...13)** | Filter (Filter table is empty) |
| **Group telegrams (main group 14...31)** | Filter |
| **Physical telegrams** | Filter |
| **Broadcast telegrams** | Route |
| **Repetition if group telegrams** | Enabled |
| **Repetition if physical telegrams** | Enabled |
| **Repetition if broadcast telegrams** | Enabled |

**Please note that the factory state of the IP router: It does block all telegrams because the filter table is not defined.**