New solutions for building automation with KNX

KNX via IP

KNXnet/IP

KNX IP Security

Tunneling

Routing

Medium KNX IP

WEINZIERL ENGINEERING GmbH
Achatz 3-4
84508 Burgkirchen an der Alz
GERMANY

Phone: +49 8677 / 916 36 - 0
E-Mail: info@weinzierl.de
Web: www.weinzierl.de

Table of contents

1 Introduction

While KNX has established itself as the most important standard in building automation, IP with Ethernet has also evolved into a universal communication solution for building automation. Due to the different system properties, KNX and IP can complement each other perfectly.

Figure: KNX IP LineMaster 762.1 secure

The advantages of the KNX bus over Ethernet is not only in the simple and cost-effective topology, as the bus is only connected from one device to the next. The power consumption of the individual devices is also very low. Last but not least, the devices from KNX manufacturers are specially designed for building installation.

The key advantages of Ethernet is in its high bandwidth at relatively low cost and also in its enormous spread. Ethernet is now not only used for networking computers in the office, but also for multimedia applications in the home or in industrial automation.

Despite, or even because of, the high transmission speed, LAN networks cannot replace the KNX bus; instead, the combination of KNX TP and LAN is an optimal solution for future building automation. KNX TP is primarily suitable for local control, while LAN is used for cross-system communication. Control commands can be transmitted in a LAN network together with Internet use, PC networking or multimedia. Overall, this results in a hierarchical architecture for building networking.

2 KNX IP Security

Cyber security is becoming increasingly important due to the various threats to infrastructure. This is why the KNX standard has also been expanded to include security procedures. KNX Data Security, for example, defines the encryption of telegrams on all media such as twisted pair or RF. In addition, KNX IP Security specifically protects the IP level in a KNX network.

KNX IP Security is a pragmatic approach that assumes that there is a significant point of attack at the IP level. KNX twisted pair is assumed to be relatively secure as a purely local medium located in the wall. IP communication, on the other hand, is often connected to the Internet and can therefore also be attacked remotely.

KNX IP Security secures the KNX IP communication, while the communication on KNX TP remains unencrypted. The main advantage of this approach is that the existing KNX TP devices and installations can continue to be used unchanged. Only the KNX IP devices, i.e. essentially KNX IP interfaces and KNX IP routers, need to be replaced.

3 Tunneling: PC access via a LAN connection

An important application of IP in the KNX system is the interface function to the bus. KNXnet/IP tunneling describes access, for example, from a PC to a KNX network during configuration and commissioning. The focus is always on the connection of a client (PC) to a bus line. In the first version, the tunneling procedure only used UDP, but included a security layer so that telegrams are repeated in the event of an error. Tunneling v2, which is based on TCP, was introduced with KNX IP Security.

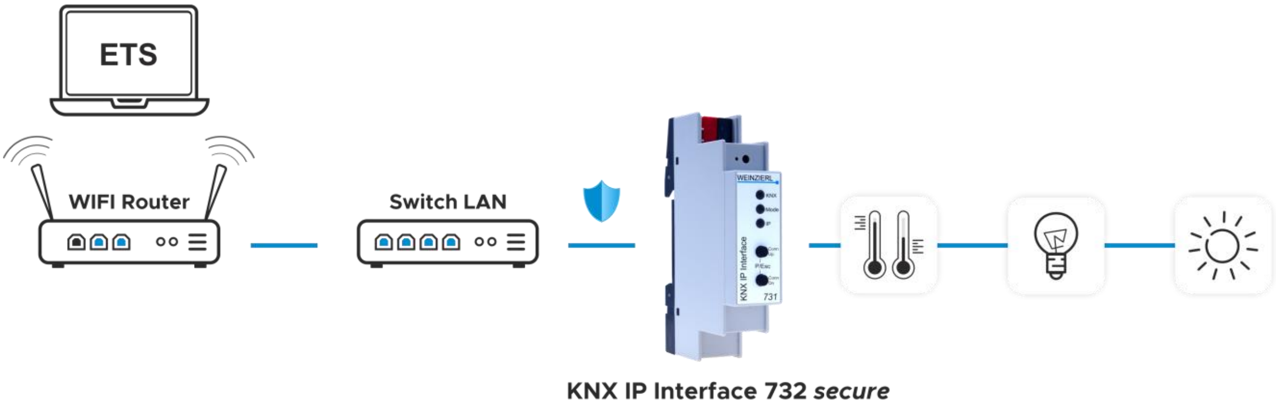


Illustration: Use of KNXnet/IP Standard Tunneling with ***KNX IP Interface 732 secure***

The tunneling protocol can be selected in the Connection Manager in the ETS and is also suitable for remote access via the Internet. For remote access, it is essential to ensure security, either via KNX IP Security or via VPN. Both security levels can also be combined.

With KNX Secure Tunneling, the ETS assigns a separate password for each tunnel, which the respective client requires to establish a connection. To do this, the client and KNX IP interface (KNXnet/IP server) first establish a secure channel using the so-called Diffie-Hellmann method. Only then are the user ID and password transmitted. A new feature of KNX Secure Tunneling is the option of establishing the connection with TCP. In addition to the possibility of accessing a bus line, tunneling also offers the possibility of programming KNX IP devices very quickly.

KNX IP interfaces can also be used to connect a visualization to a bus line. The tunneling protocol also supports the bus monitor function.

4 Routing in hierarchical architectures

A key motivation for extending the KNX system with Ethernet/IP is to increase the transmission capacity in the overall system. The transmission speed of KNX twisted pair is completely sufficient to build a bus line with up to 255 participants. However, a considerably higher bandwidth may be required across lines in the backbone. This is particularly the case if there are central devices in the system, such as visualizations, to which all telegrams are to be transmitted. In this case, selective routing is not possible.

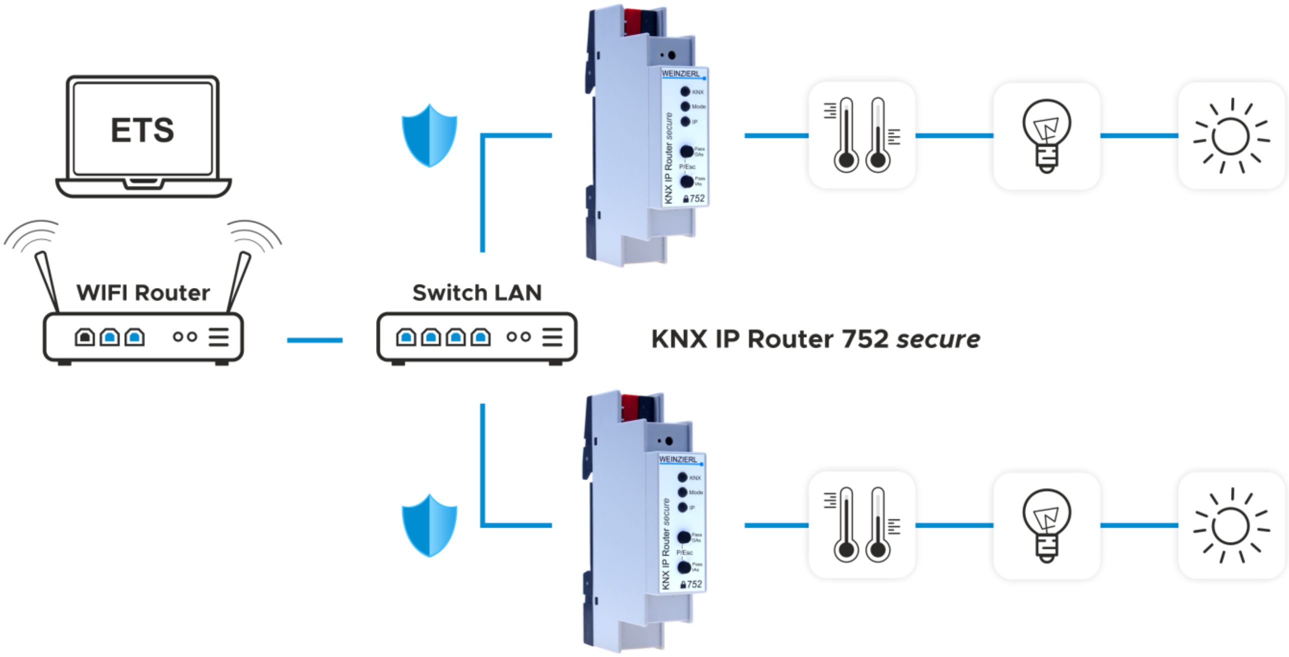


Illustration: Use of KNX net/IP Standard routing with ***KNX IP Router 752 secure***

The high bandwidth of a LAN network offers an optimum solution here. While KNX TP can only transmit a maximum of approx. 50 telegrams per second, the LAN can transmit more than 10,000 telegrams at 10 Mbit/s. In order to process this number of telegrams without losses, both high computing power and a corresponding telegram buffer from IP to KNX TP are required. Since the use of the Ethernet as a backbone for the system is very important, a corresponding protocol has been standardized in KNX. The KNXnet/IP specification describes in the Routing subsection how KNX/IP routers forward telegrams via IP. For forwarding via Ethernet, the KNX telegrams are individually packed in UDP/IP telegrams and sent as multicast telegrams via the Ethernet. All KNX/IP routers in the network can receive these telegrams simultaneously and use their routing table to decide whether to forward the telegram to the connected KNX line.

The routing protocol is suitable for connecting an unlimited number of visualizations to a KNX installation with IP backbone, but does not support the bus monitor functionality.

The routing protocol has also been extended for KNX IP Security. For this purpose, all IP routing telegrams are encrypted with the so-called backbone key. To prevent replay attacks, the telegrams carry a time stamp on a ms basis, which the recipient can use to decide whether it is a current telegram. The common system time is continuously synchronized between the devices.

5 BAOS Object Server: From telegram to data point

The exchange of control information with the building automation system is important for more and more devices, for example in the field of multimedia or security technology. For certain devices, however, it is preferable not to access the bus directly. Instead, a connection to KNX can also be implemented via Ethernet. Communication via Ethernet is particularly interesting for devices that already have a network connection. If the protocol stack for TCP/UDP/IP is already available in the operating system used, applications can communicate with other devices via Ethernet and therefore also via KNX with little effort. This is the case with many devices based on Linux or Windows CE.

It is much easier if the KNX/IP interface also takes on this task. In addition to access at telegram level, the KNX IP BAOS also provides an object server that makes the configured data points of the building available. This means that the KNX stack in the device assigns received telegrams to the corresponding communication objects and stores their values in the memory. Registered clients are informed of every change, but can also retrieve the values independently. The values of the communication objects are updated on receipt even if no client is connected. This enables a smartphone, for example, to read the process image from the BAOS interface without losing time when establishing a connection and without loading the KNX bus.

To send values to the bus, a client can have write access to the communication objects. The device can generate and send group telegrams independently. The data points are configured using the ETS® (Engineering Tool Software). In the ETS, the interface appears like a conventional bus subscriber. The data types of the communication objects are set via the parameter dialog. The group addresses can then be assigned as usual.

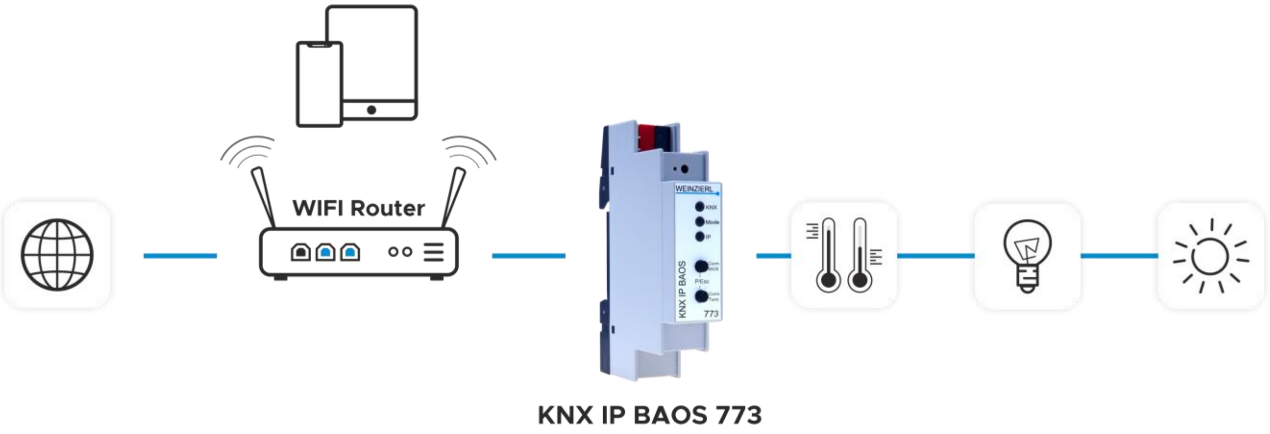


Illustration: Using the object server protocol
with ***KNX IP BAOS 773***

A client can therefore access the data points using the BAOS protocol without having to know the syntax of KNX telegrams. It addresses the data points via their number, as they are also displayed in the ETS. If group addresses are changed in the KNX network, the interface is automatically updated by an ETS download. It is not necessary to change the configuration of the client.

The KNX IP BAOS 773/774 provides two different BAOS protocols: On the one hand, the device supports the so-called KNX BAOS Binary protocol, which is also used in our BAOS modules with serial or USB interface. It is available via TCP/IP as well as via UDP/IP. The binary protocol is particularly suitable for devices that are programmed with classic programming languages such as C, C++ or C# and support IP sockets.

However, it is hardly possible to use the KNX BAOS binary protocol from a web browser. For this reason, the object server can alternatively be accessed via the new KNX BAOS Web Services, based on Java Script Object Notation (JSON). This means that the KNX IP BAOS 773/774 can be integrated directly into your own web applications.

The web services have the same range of functions as the KNX BAOS binary protocol. However, they use a text-based syntax that is sent via HTTP (TCP/IP, port 80). The Web Services do not include a graphical user interface. This must be done separately, typically in HTML and Java Script, and can be stored in the client's memory, for example. Alternatively, the protocol can also be integrated into an application based on Webkit.

With the KNX IP BAOS 774.1 *secure,* a secure variant is also available for the BAOS series. In addition to KNX Data and KNX IP Security, the device also supports BAOS IP Security with an additional password. The BAOS IP Secure protocol uses the tried and tested mechanisms of KNX IP Security.

Further information on the BAOS architecture as well as the protocol specifications and SDKs can be found in the document "World of BAOS" on weinzierl.de.

6 With BAOS up to the visu

The IP protocol naturally also enables the building to be operated via a web browser. The KNX IP BAOS 777 is a powerful multifunctional device for KNX installation. It has an integrated web server that enables access to the visualization and device settings via a standard web browser on a PC or mobile devices such as smartphones and tablets. The web interface of the visualization enables the control of the entire KNX installation divided into the individual rooms and functions.

It combines the following functionalities, among others:

- Visualization and control
- E-mail function
- Date & Time Server (NTP) synchronization
- Timer with astro timer
- KNX IP interface (KNXnet/IP)

The KNX IP BAOS 777 is an on-site solution that is very easy to integrate with the ETS. The device does not require a cloud connection or an app. No further costs are incurred during operation. KNX configuration is done exclusively with the ETS software – no additional software is needed. User-related settings such as email or timer functions can be set by the user in the web frontend.

*Illustration: Display of the visualization on a tablet with **KNX IP BAOS 777***

7 Power over Ethernet replaces the auxiliary voltage

Not all KNX IP devices can be supplied completely from the KNX bus. The KNX IP BAOS 777 must therefore be supplied via a separate power supply or via Ethernet. Not only fast information, but also energy can be transmitted via the Ethernet wire. This technology is called Power-over-Ethernet or simply PoE. It is specified as IEEE standard 802.3af.

Figure: Switch with Power-over-Ethernet (Source: Voelkner)

For PoE a network switch is required which supports this feature. Power-over Ethernet replaces not only the additional power supply but simplifies the wiring within the switchboard..

8 WLAN - the wireless alternative

With the introduction of KNXnet/IP, the ETS® and other programs also have the option of establishing bus access via IP. A major advantage of the Internet protocol is its independence from the transmission medium. In addition to the network cable, wireless transmission via WLAN (wireless LAN) is also possible.

The KNX IP Interface 740.1 *wireless* is a KNX IP interface with WLAN. The device can work as a WLAN access point with which a laptop connects directly to the ETS. Alternatively, the device also supports a client mode in which the device connects to an existing WLAN router. The WPS protocol is also supported, which enables integration at the touch of a button.

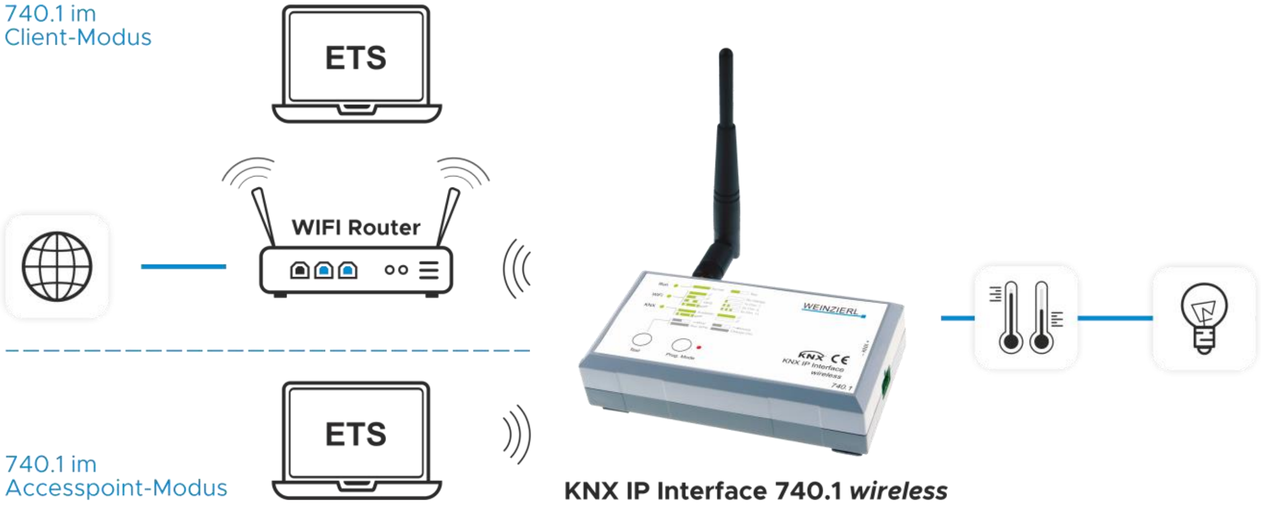
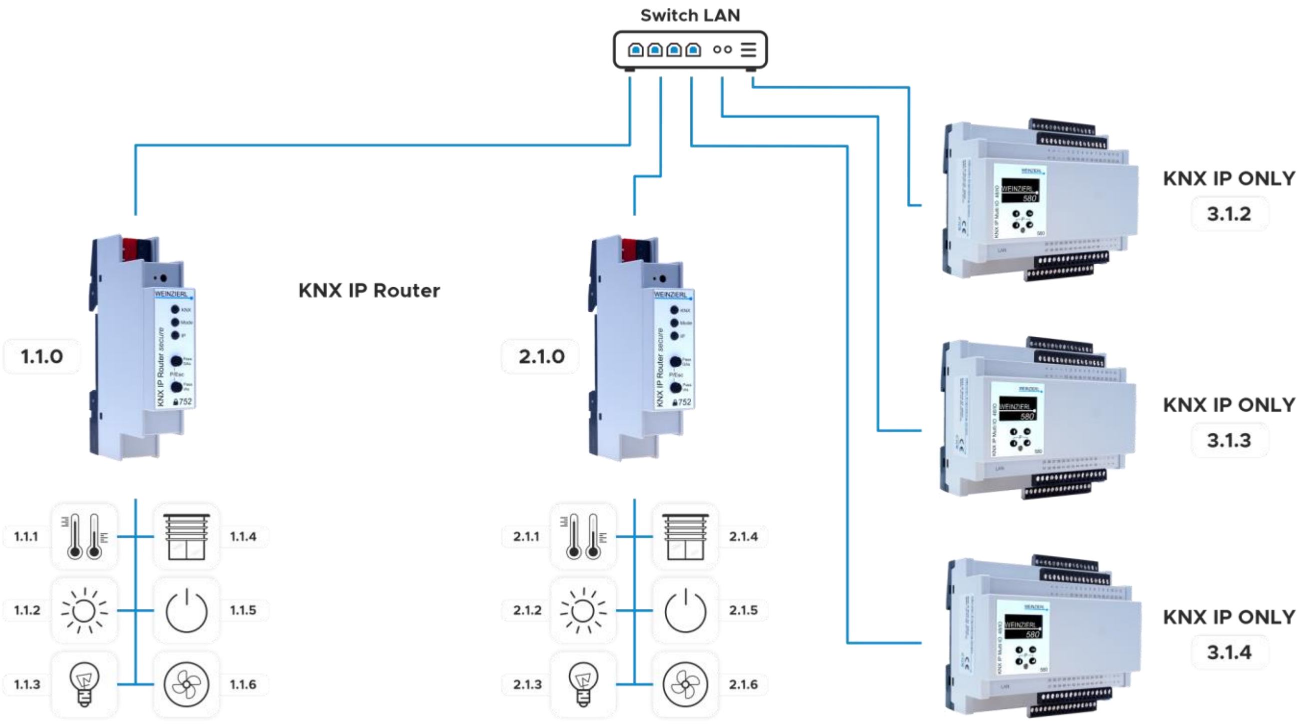


*Illustration: Use of a wireless interface
wireless interface
with **KNX IP Interface 740.1 wireless***

9 Medium KNX IP: KNX IP only Devices

The KNX IP protocol is not limited to use in interfaces and routers. KNX IP is a fully-fledged medium just like TP or RF. This means that devices can be connected directly to the KNX installation via the LAN interface. As for all KNX devices in the so-called KNX system mode, commissioning is carried out with the ETS® software. This means that the devices with medium KNX IP also have a physical address and use group telegrams for data and commands. The group telegrams are transmitted via IP as UDP multicast telegrams and can therefore also reach several devices simultaneously via IP. The download by the ETS can be carried out point-to-point via the IP address of the device. This means that even complex devices can be loaded via IP in just a few seconds. In the ETS, the devices appear as usual in the topology view with communication objects and parameters. Only the settings for the IP network (IP address, etc.) are added to the device properties.



One of the first KNX IP only devices is the KNX IP Multi IO 580: a universal input and output module for building control with 48 digital and freely configurable channels. Each channel can be used as a input, output or to control a blind. The periphery is powered by an external power supply (24 V DC). Input channels can be used to control lights or blinds via KNX, for example. However, they can also be configured as pulse counters - for example for energy meters with S0 output. Output channels can directly control signal LEDs or external relays.

10 Overview KNX IP devices

	KNXnet/IP **Tunneling** (interface e.g. for ETS)	KNXnet/IP **Routing** (line coupler via LAN)	BAOS IP ObjectServer **Binary** (access to data points)	BAOS IP ObjectServer **Web Services** (access to data points)	KNX IP Security	Supply via KNX bus	Wireless (WLAN/WiFi)	48 channel input and output device	POE (Power over Ethernet)
KNX IP Interface 731	✓					✓			
KNX IP Interface 732 *secure*	✓				✓	✓			
KNX IP Interface 740.1 *wireless*	✓					✓	✓		
KNX IP Router 751	✓	✓				✓			
KNX IP Router 752 *secure*	✓	✓			✓	✓			
KNX IP LineMaster 762.1 *secure*	✓	✓							
KNX IP BAOS 773/774	✓		✓	✓		✓			
KNX IP BAOS 774.1 *secure*	✓		✓						
KNX IP BAOS 777	✓		✓	✓					✓
KNX IP Multi IO 580								✓	

WEINZIERL ENGINEERING GmbH
Achatz 3-4
84508 Burgkirchen an der Alz
GERMANY

Phone: +49 8677 / 916 36 - 0
E-Mail: info@weinzierl.de
Web: www.weinzierl.de

2024-07-31