



HEIDELBERG, APRIL 2023

# ABB i-bus® KNX – IP Router IPR/S and IP Interface IPS/S

Building Academy Smart Buildings

Thorsten Reibel & Juergen Schilder



# Agenda

## Introduction

### ABB i-bus® KNX – IP devices

- IP Switches IS/S and ISP/S

- IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

- IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

### KNX Secure Standard “KNXnet/IP Security”

### ABB i-bus® Tool for diagnostics and commissioning

### Tips & Tricks

# ABB i-bus® KNX – IP Devices

## Motivation of ABB i-bus® KNX for IP connection

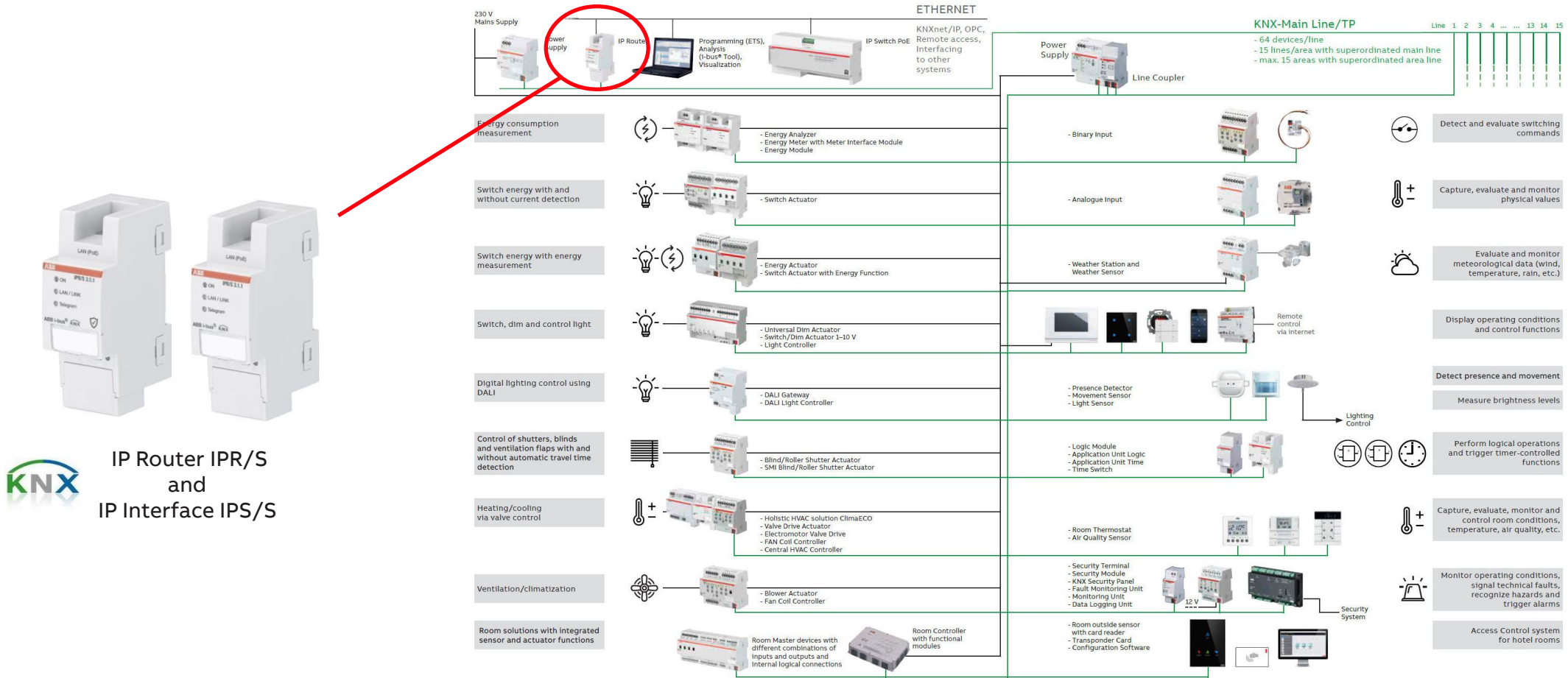
- Connection of other Building Automation protocols like BACnet
- Accessing ABB i-bus® KNX remotely e.g. via Busch-ControlTouch® App
- Connection of pure IP based KNX devices like IP touch panel
- Remote programming
- To achieve a secured backbone (KNX IP secure)
- To energize devices via PoE
- To access KNX devices like Application Controller AC/S 1.x.1 via Browser for operation
- Simplification and enhancement of KNX topology with IP Router instead of Line- and Area Couplers
- ...  
→ **ABB i-bus® KNX is not a complete solution without IP connectivity**





# ABB i-bus® KNX – IP Devices

## ABB i-bus® KNX – Product Range Overview



# ABB i-bus® KNX – IP Devices

## History of ABB i-bus® KNX IP Interfaces and IP Routers

- 2004: IP Gateway IG/S1.1
  - iETS2 Version 1.3
  - Multicast IP address 239.192.39.238
- 2008: IP Router IPR/S2.1
  - ETS 3.0f
  - KNXnet/IP protocol “Tunneling” and “Routing”
- 2009: IP Interface IPS/S2.1
  - ETS 3.0f
  - KNXnet/IP protocol “Tunneling”



IP Gateway  
IG/S 1.1



IP Router  
IPR/S 2.1



IP Interface  
IPS/S 2.1

# ABB i-bus® KNX – IP Devices

## Overview of ABB i-bus® KNX IP Interfaces and IP Routers

Devices using the KNXnet/IP protocol (standard) for the communication

- IP Interface IPS/S 3.1.1 standard (2015 to present)
- IP Router IPR/S 3.1.1 standard (2015 to present)

Devices using the KNXnet/IP **Secure** protocol for the communication

- IP Router Secure IPR/S 3.5.1 (2019 to present)
- IP Interface Secure IPS/S 3.5.1 (2021 to present)



IP Interface  
IPS/S 3.1.1



IP Router  
IPR/S 3.1.1



IP Interface  
Secure  
IPS/S 3.5.1



IP Router  
Secure  
IPR/S 3.5.1



---

# ABB i-bus® KNX – IP Devices

ABB IP Switches IS/S 8.1.1 and ISP/S 8.1.1.1

# ABB i-bus® KNX – IP Devices

ABB IP Switches IS/S 8.1.1 and ISP/S 8.1.1.1

## Introduction

- The IP infrastructure plays an important role in the reliability and availability of all building functions
- The increasing dependence on IP infrastructures for the reliability and availability of the building functionality plays a key factor in the design of the IP infrastructure
- Building Automation market is increasingly including IP connections on the field level
- Additionally, the use of PoE technology in field level devices is rising, e.g. ABB i-bus® KNX IP Router or IP Interface
- Separate technical IP infrastructures or networks are becoming more common place in buildings





# ABB i-bus® KNX – IP Devices

## ABB IP Switches IS/S 8.1.1 and ISP/S 8.1.1.1

### Overview

- The ABB IP Switches are two
  - Industrial quality standard
  - 8 Ports
  - fast Ethernet (100 Mbit/s)
  - unmanaged

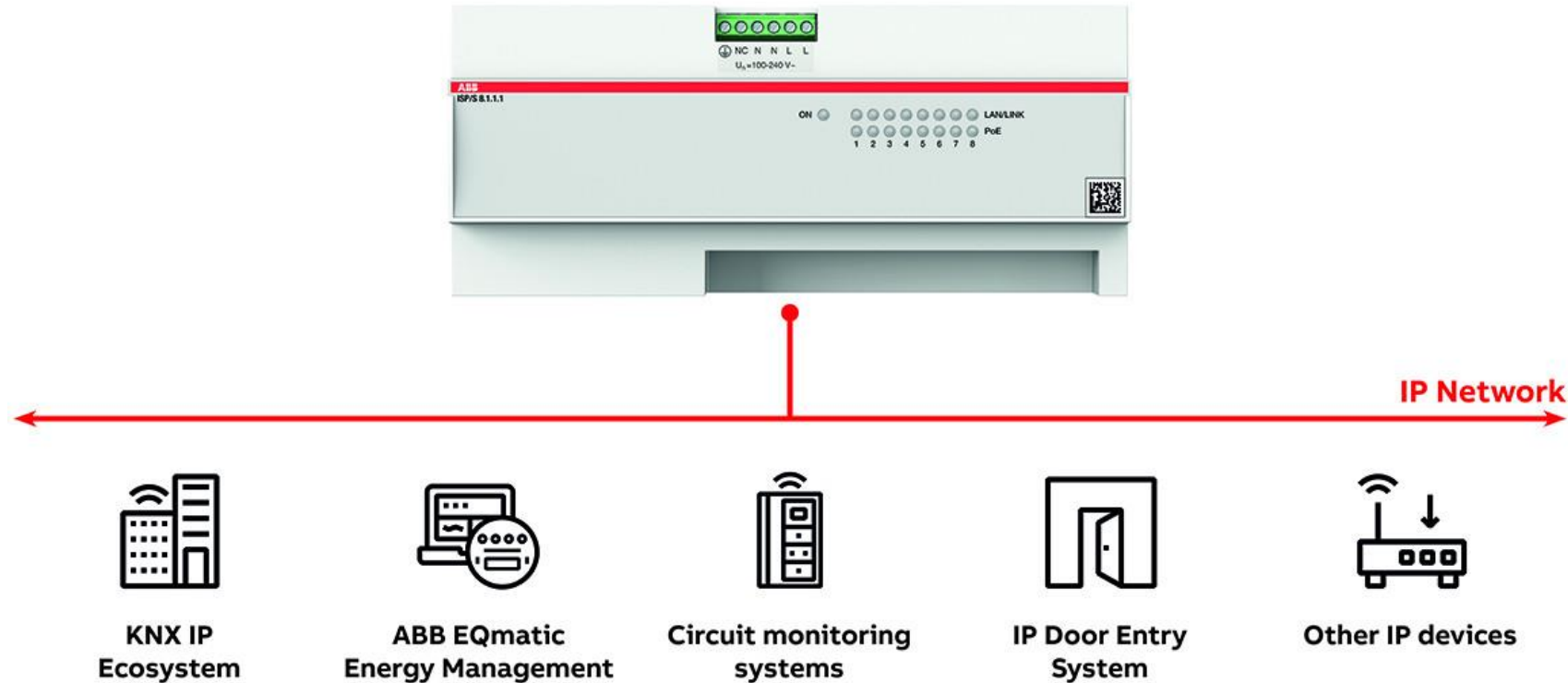
switches (with and without PoE) designed for installation in electrical distribution boards and rapid mounting on DIN-Rails



# ABB i-bus® KNX – IP Devices

ABB IP Switches IS/S 8.1.1 and ISP/S 8.1.1.1

## Overview



The ABB IP Switches are suitable for all applications, segments and markets in which distribution boards with DIN-Rail devices requiring IP connectivity

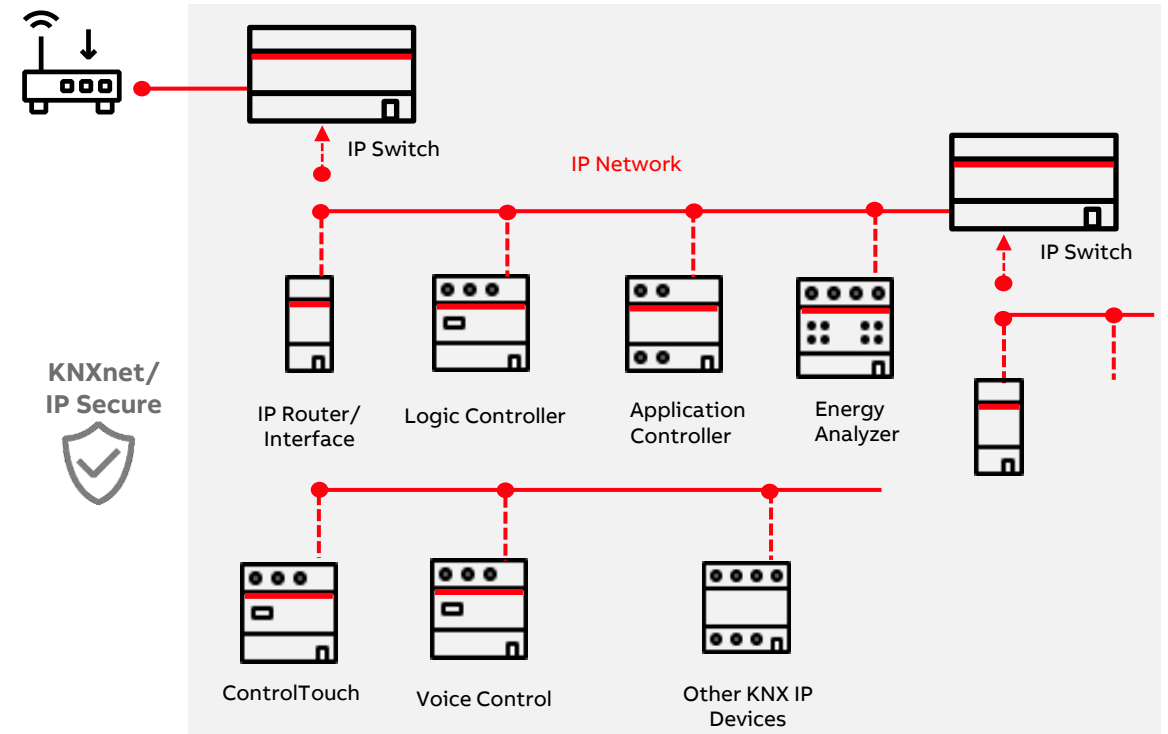
# ABB i-bus® KNX – IP Devices

ABB IP Switches IS/S 8.1.1 and ISP/S 8.1.1.1

## ABB i-bus® KNX

- IP Router IPR/S 3.1.1\* and IP Router Secure IPR/S 3.5.1\*
- IP Interface IPS/S 3.1.1\* and IP Interface Secure IPS/S 3.5.1\*
- Logic Controller ABA/S 1.2.1\*
- ABB EQmatic Energy Analyzer QA/S x.xx.1
- ClimaECO Application Controller AC/S 1.x.1
- KNX Security Panel GM/A 8.1
- Busch-ControlTouch® CT/S 2.1
- Busch-VoiceControl® VCO/S 150.2
- IP touch 7 / 10 LAN\*
- PLC AC500 with KNX communication (former BAC/S)
- ...

\* Data and PoE



Simplifying IP connectivity in your KNX installation

# ABB i-bus® KNX – IP Devices

## ABB IP Switches IS/S 8.1.1 and ISP/S 8.1.1.1

### General information

- The IP Switches
  - are designed for the special requirements of building automation
  - meets the relevant industry standards, provides very high operational reliability, even under extreme conditions and also long-term reliability and flexibility
  - are designed for installation in electrical distribution boards and small housings for rapid mounting on a 35 mm mounting rail in accordance with EN 60715

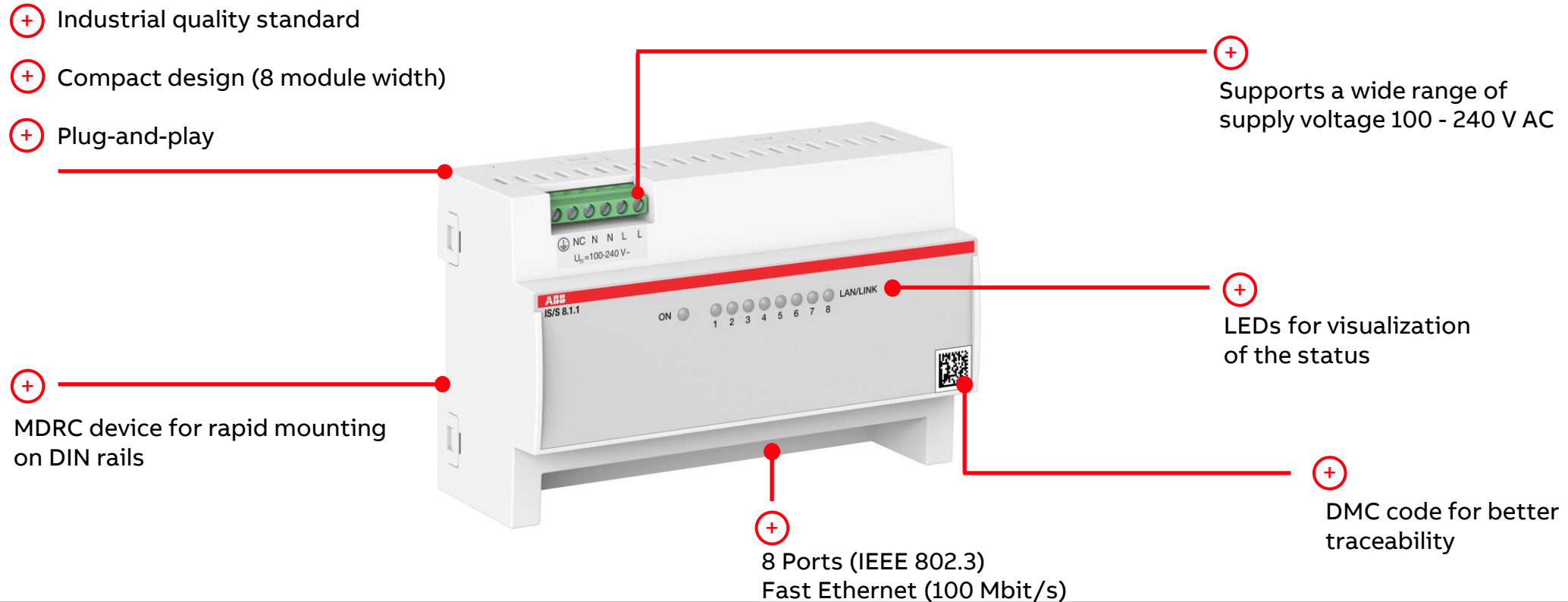
Product name	Type	Order Code
IP Switch	IS/S 8.1.1	2CDG120082R0011
IP Switch-PoE	ISP/S 8.1.1.1	2CDG120083R0011



# ABB i-bus® KNX – IP Devices

ABB IP Switches IS/S 8.1.1 and ISP/S 8.1.1.1

## Key Characteristics IP Switch IS/S 8.1.1

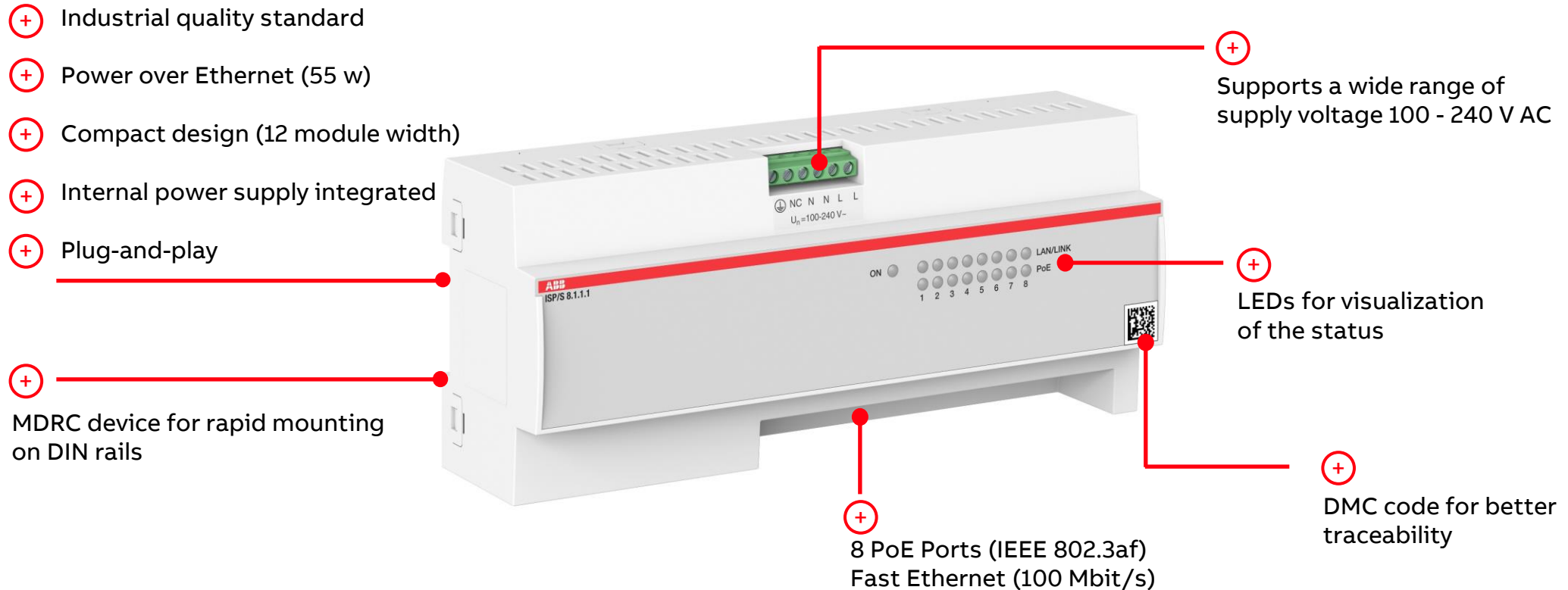




# ABB i-bus® KNX – IP Devices

## ABB IP Switches IS/S 8.1.1 and ISP/S 8.1.1.1

### Key Characteristics IP Switch ISP/S 8.1.1.1

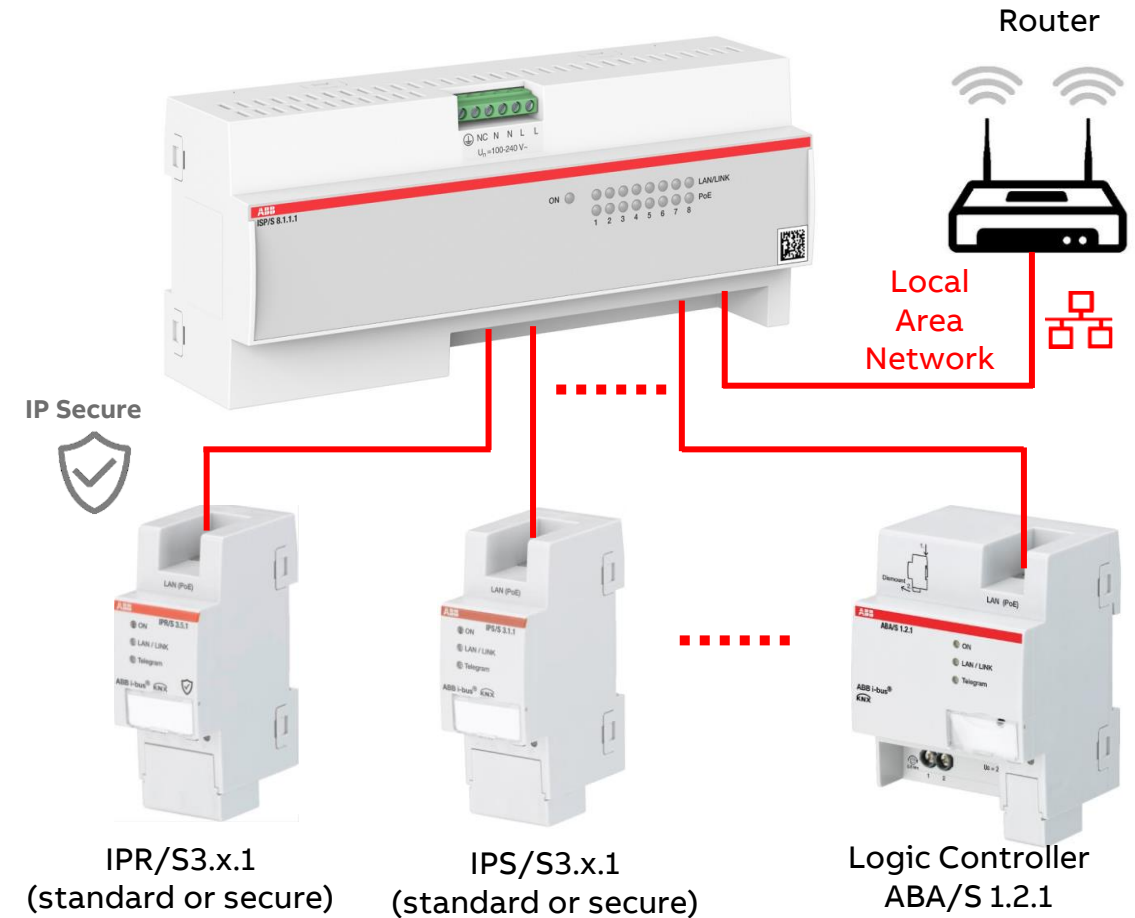


# ABB i-bus® KNX – IP Devices

## ABB IP Switches IS/S 8.1.1 and ISP/S 8.1.1.1

### IP Switch ISP/S 8.1.1.1: Support of PoE

- The device supports Power over Ethernet (PoE) in accordance with IEEE 802.3af
- The Power over Ethernet function is activated on the PoE ports on delivery
- The devices are supplied with PoE voltage via the internal voltage supply
- The PoE voltage to the twisted-pair cables is supplied via the wire pairs transmitting the signal (phantom voltage)
- The PoE voltage is decoupled from the power supply
- The individual ports are not electrically insulated from each other
- Ensure that the device does not exceed the specified maximum PoE power output → For the maximum power available to PoE end devices in total, see the technical data

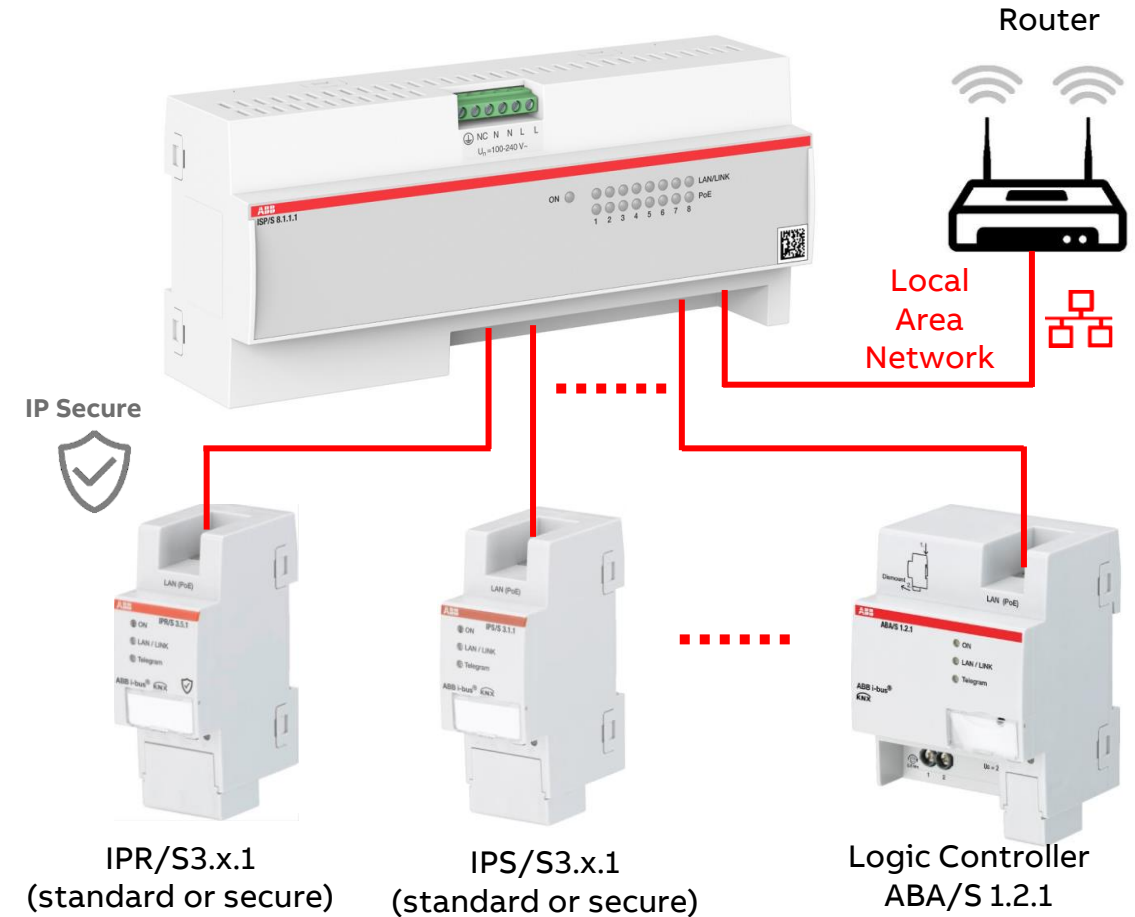


# ABB i-bus® KNX – IP Devices

## ABB IP Switches IS/S 8.1.1 and ISP/S 8.1.1.1

### IP Switch ISP/S 8.1.1.1: Support of PoE

- ABB i-bus® KNX devices that can be supplied via PoE
- PoE IEEE 802.3af class 1 (3.84 W)
  - IP Router IPR/S 3.1.1
  - IP Router Secure IPR/S 3.5.1
  - IP Interface IPS/S 3.1.1
  - IP Interface Secure IPS/S 3.5.1 → Power loss of a max. of 1.8 W
- PoE IEEE 802.3af class 2 (6.5 W)
  - Logic Controller ABA/S 1.2.1 → Power loss of a max. of 3 W
  - IP touch H8236/H8237
- Note on IP Router IPR/S and IP Interface IPS/S:  
If PoE and supply voltage are connected at the same time, PoE is used



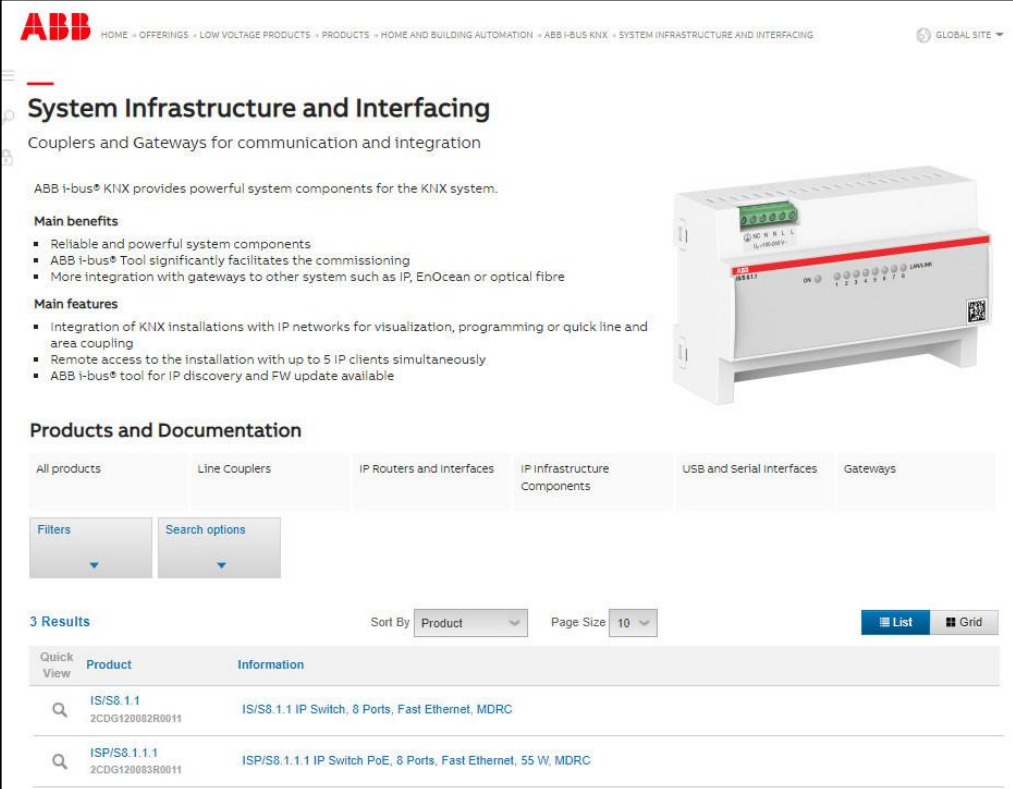
# ABB i-bus® KNX – IP Devices

ABB IP Switches IS/S 8.1.1 and ISP/S 8.1.1.1

## Homepage

[www.abb.com/KNX](http://www.abb.com/KNX)

- Products and Downloads
  - System Infrastructure and Interfacing
    - IP Infrastructure Components
- Product Manual
- Technical Data
- Operating instruction
- Engineering Guides
- Installation and Operating Instruction
- Specification Text
- ...



**ABB** HOME > OFFERINGS > LOW VOLTAGE PRODUCTS > PRODUCTS > HOME AND BUILDING AUTOMATION > ABB i-BUS KNX > SYSTEM INFRASTRUCTURE AND INTERFACING GLOBAL SITE

## System Infrastructure and Interfacing

Couplers and Gateways for communication and integration

ABB i-bus® KNX provides powerful system components for the KNX system.

**Main benefits**

- Reliable and powerful system components.
- ABB i-bus® Tool significantly facilitates the commissioning
- More integration with gateways to other system such as IP, EnOcean or optical fibre

**Main features**

- Integration of KNX installations with IP networks for visualization, programming or quick line and area coupling
- Remote access to the installation with up to 5 IP clients simultaneously
- ABB i-bus® tool for IP discovery and FW update available

**Products and Documentation**

All products Line Couplers IP Routers and interfaces IP Infrastructure Components USB and Serial interfaces Gateways

Filters Search options

3 Results Sort By Product Page Size 10 List Grid

Quick View	Product	Information
	IS/S8.1.1 2CDG120082R0011	IS/S8.1.1 IP Switch, 8 Ports, Fast Ethernet, MDRC
	ISP/S8.1.1.1 2CDG120083R0011	ISP/S8.1.1.1 IP Switch PoE, 8 Ports, Fast Ethernet, 55 W, MDRC

---

# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

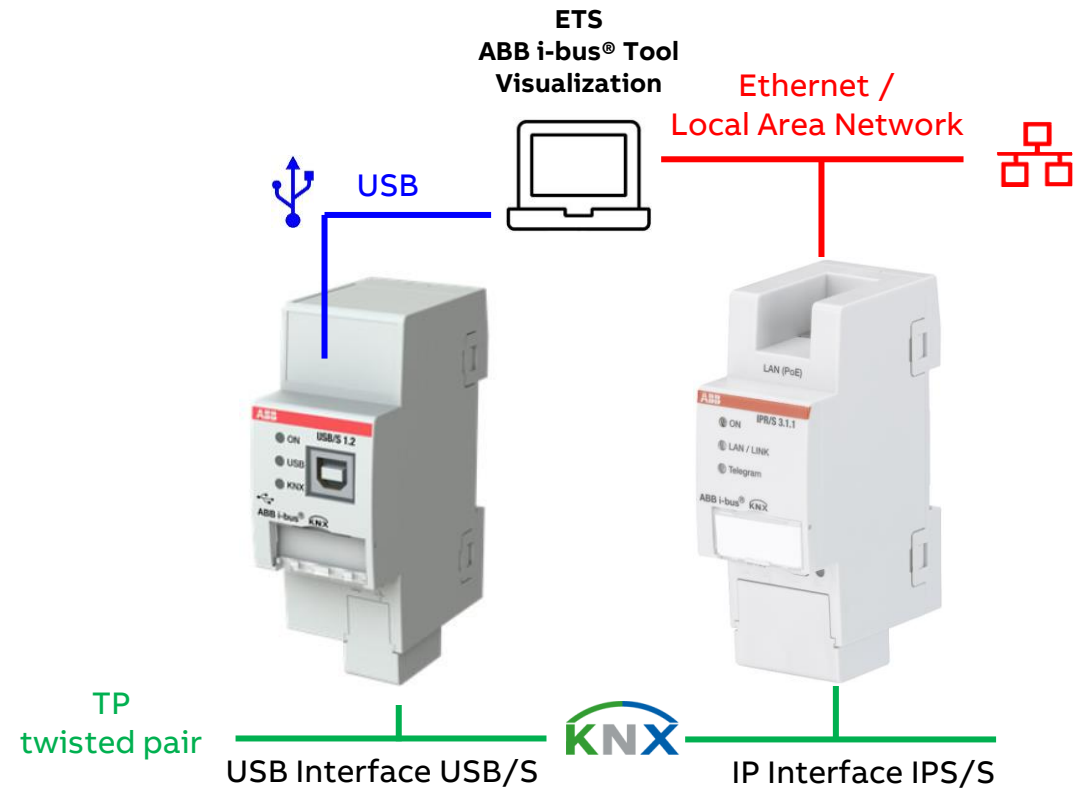


# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## Interfaces – IP and USB

- An Interface enables communication between ETS and a KNX system (programming, bus monitoring, group monitoring, diagnostic tools, ...)
- Visualization systems, ABB i-bus® Tool, or other clients, can also use the interface to access KNX
- USB Interface USB/S
  - Communication between USB and TP
- IP Interface IPS/S
  - Communication between LAN and TP
  - 5 Tunneling Server
    - Built in 5-fold “USB Interface” via LAN

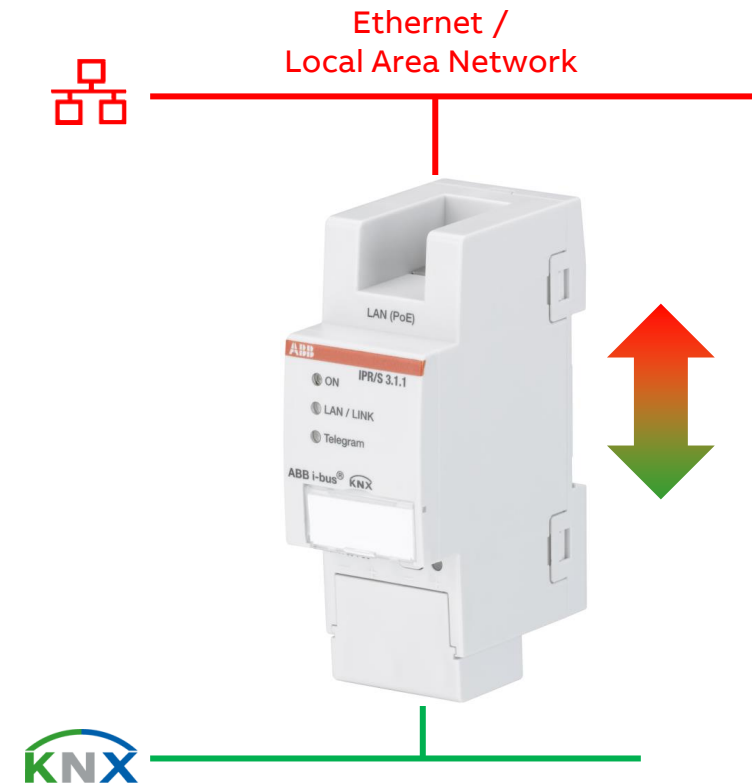


# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## KNX IP Interface – Principle

- An ABB i-bus® KNX IP Interface connects the KNX TP bus to an Ethernet network
- KNX telegrams can be sent to or received from other devices via the Ethernet network
- The IP Interface can be used as a programming interface (ETS) and clients, e.g. visualizations or tablet/smart phone with App via Wi-Fi, can access the KNX bus via the IP Interface
  - IP Interface IPS/S 3.1.1 (**standard** KNXnet/IP protocol)
  - IP Interface **Secure** IPS/S 3.5.1  
This device uses the KNXnet/IP protocol and the KNXnet/IP Security protocol from the KNX Association (tunneling) for communication
- Not for connection of KNX lines and areas over IP (no routing of KNX telegrams) → KNX IP Router IPR/S 3.x.1



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface IPS/S 3.1.1 (standard)

### KNXnet/IP Capabilities:

- Tunneling (Interface)
  - 5 Tunneling Server
  - To connect a PC to KNX via IP
    - Working with ETS (download, diagnostics,...)
    - ABB i-bus® Tool support
    - Visualisation
    - Tablet/Smart Phone with App via Wi-Fi
    - ...



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface IPS/S 3.1.1 (standard)

- Hardware
  - Network cable connection
  - Labelling field
  - DIN rail connection
  - Cover cap
  - Programming button and LED
- Power supply
  - 12 ... 30 V DC (e.g. separate Power Supply CP-D or NTU/S)
  - Power over Ethernet (PoE): IEEE 802.3af class 1
  - If PoE and supply voltage are connected at the same time, PoE is used



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface IPS/S 3.1.1 (standard)

### LED “ON”

- After the supply voltage  $U_s$  is connected, the LED initially lights up continuously
- After approx. 40 sec., the LED starts flashing until initialization is completed

### LED “LAN/LINK”

- Once initialization is completed, the LED lights up when the IP Interface is connected to an IP network
- The LED flashes when the device detects activity on the IP network, e.g. when data is exchanged

### LED “Telegram”

- The LED lights up continuously when the IP Interface is connected to KNX after the startup process is completed
- The LED flashes when the device detects activity on the KNX subline TP (twisted pair)



ON



LAN/LINK



Telegram



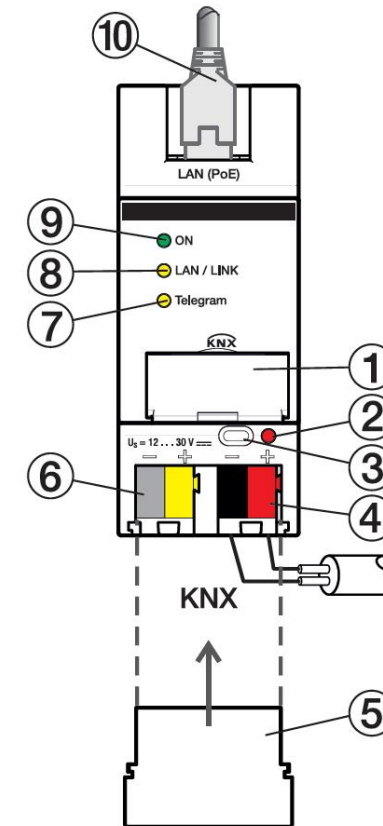


# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface IPS/S 3.1.1 (standard)

1. Label carrier
2. KNX programming LED (red)
3. KNX programming button
4. KNX bus connection terminal
5. Cover cap
6. Power supply connection  $U_s$
7. Telegram LED (yellow)
8. LAN/LINK LED (yellow)
9. ON LED (green)
10. LAN connection



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface IPS/S 3.1.1 (standard)

### Supplied state

- The device is supplied with the individual address 15.15.255
- All five tunneling connection addresses are set to 15.15.100 (only one tunnel is visible to the outside)
- In ETS, the first five free addresses in the line are assigned automatically after the IP Interface has been inserted into a line
- The IP address is set to automatic IP assignment (DHCP/AutoIP)
- The tunneling connection addresses set in the ETS will be adopted only after the first download
- The parametrized settings will be adopted after the first download

Local Interface Settings

IP Tunneling

Name  
IP Interface

Host Individual Address  
15.15.255

Individual Address  
15.15.100 Address free?

IP Address  
192.168.1.136

Port  
3671

MAC Address  
00:0C:DE:4B:81:99

Max telegram length (APDU):  
254

Serial number:  
0002:5E01B750

Close

4.1.1 IPS/S3.1.1 IP Interface,MDRC

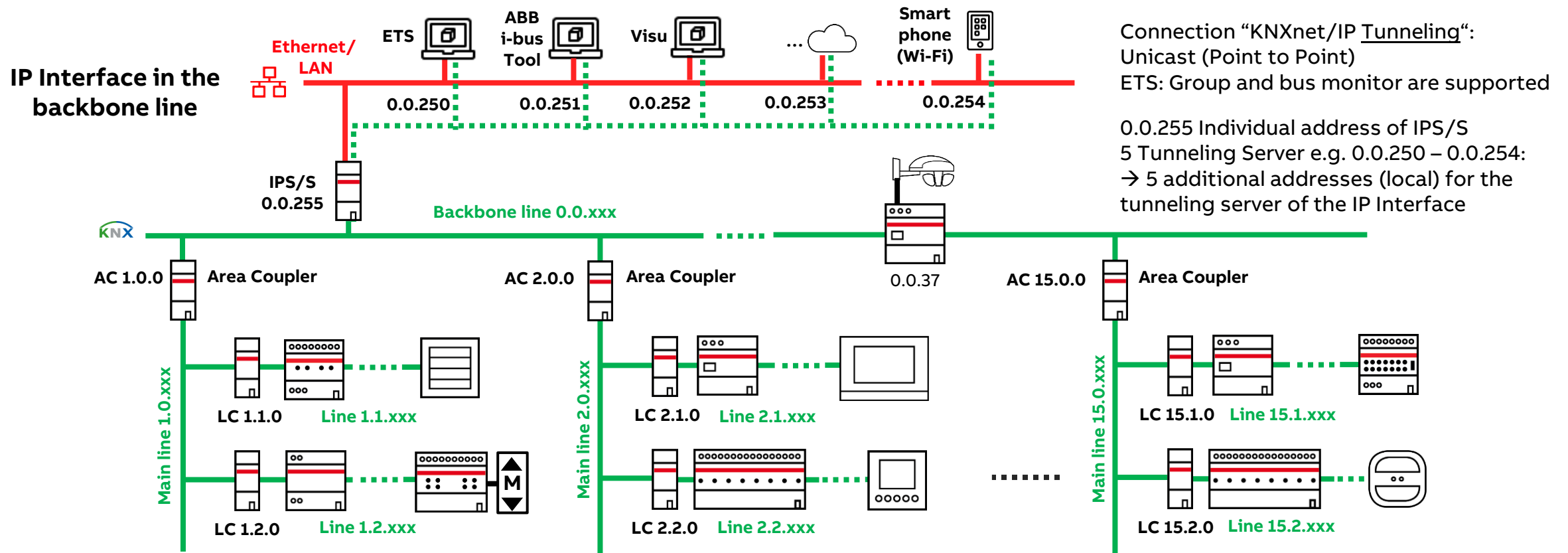
- 4.1.2 Additional individual address
- 4.1.3 Additional individual address
- 4.1.4 Additional individual address
- 4.1.5 Additional individual address
- 4.1.12 Additional individual address

4.1.255 Line 4.1.xxx IP Interface IPS/S3.1.1

- 4.1.250 Tunnel 1 - IPS/S 3.1.1
- 4.1.251 Tunnel 2 - IPS/S 3.1.1
- 4.1.252 Tunnel 3 - IPS/S 3.1.1
- 4.1.253 Tunnel 4 - IPS/S 3.1.1
- 4.1.254 Tunnel 5 - IPS/S 3.1.1

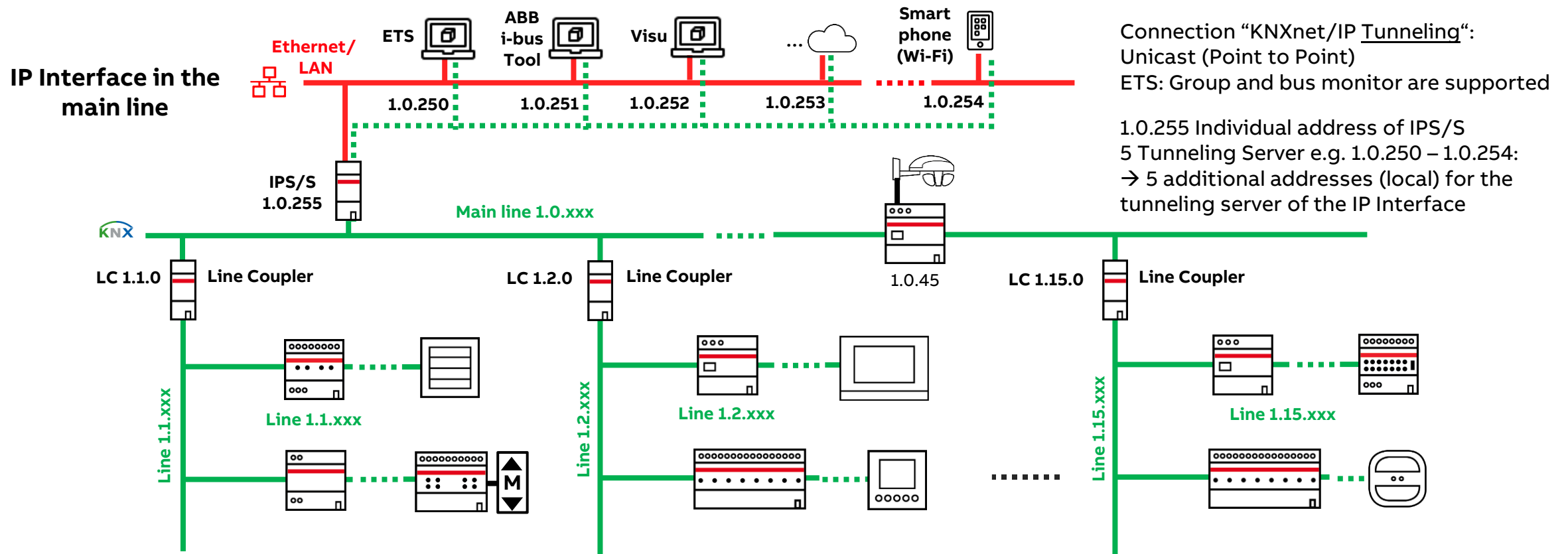
# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1



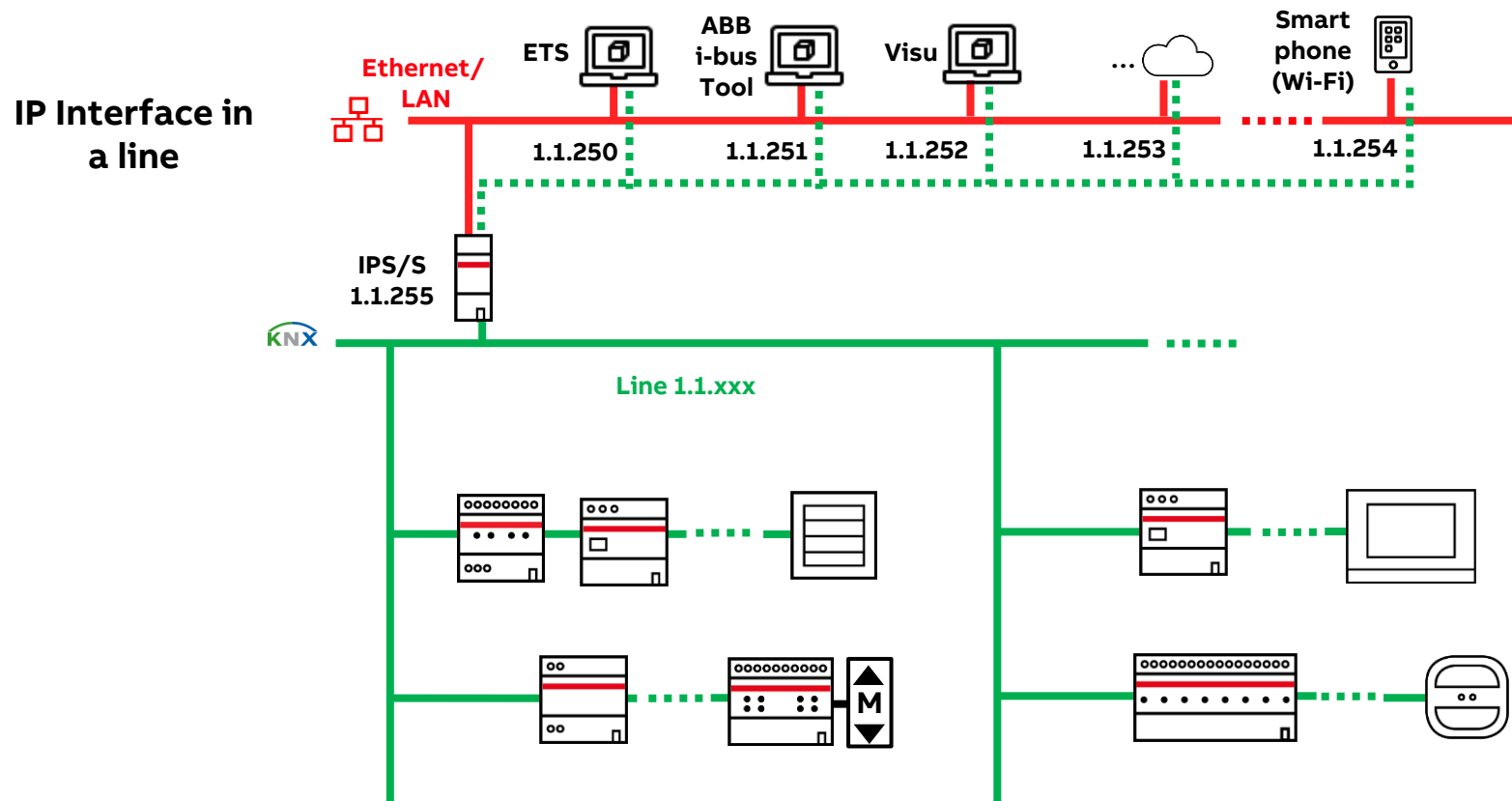
# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1



Connection “KNXnet/IP Tunneling”:

Unicast (Point to Point)

ETS: Group and bus monitor are supported

1.1.255 Individual address of IPS/S

5 Tunneling Server e.g. 1.1.250 – 1.1.254:

→ 5 additional addresses (local) for the tunneling server of the IP Interface

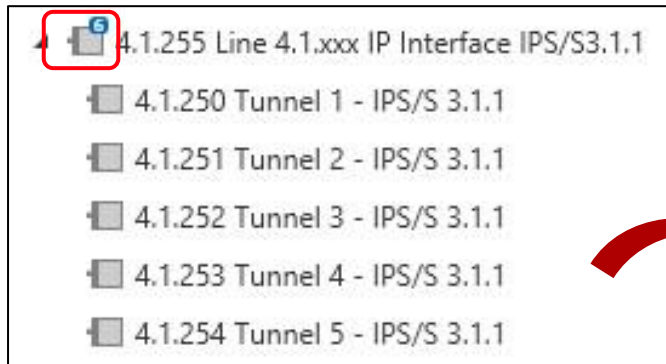


# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

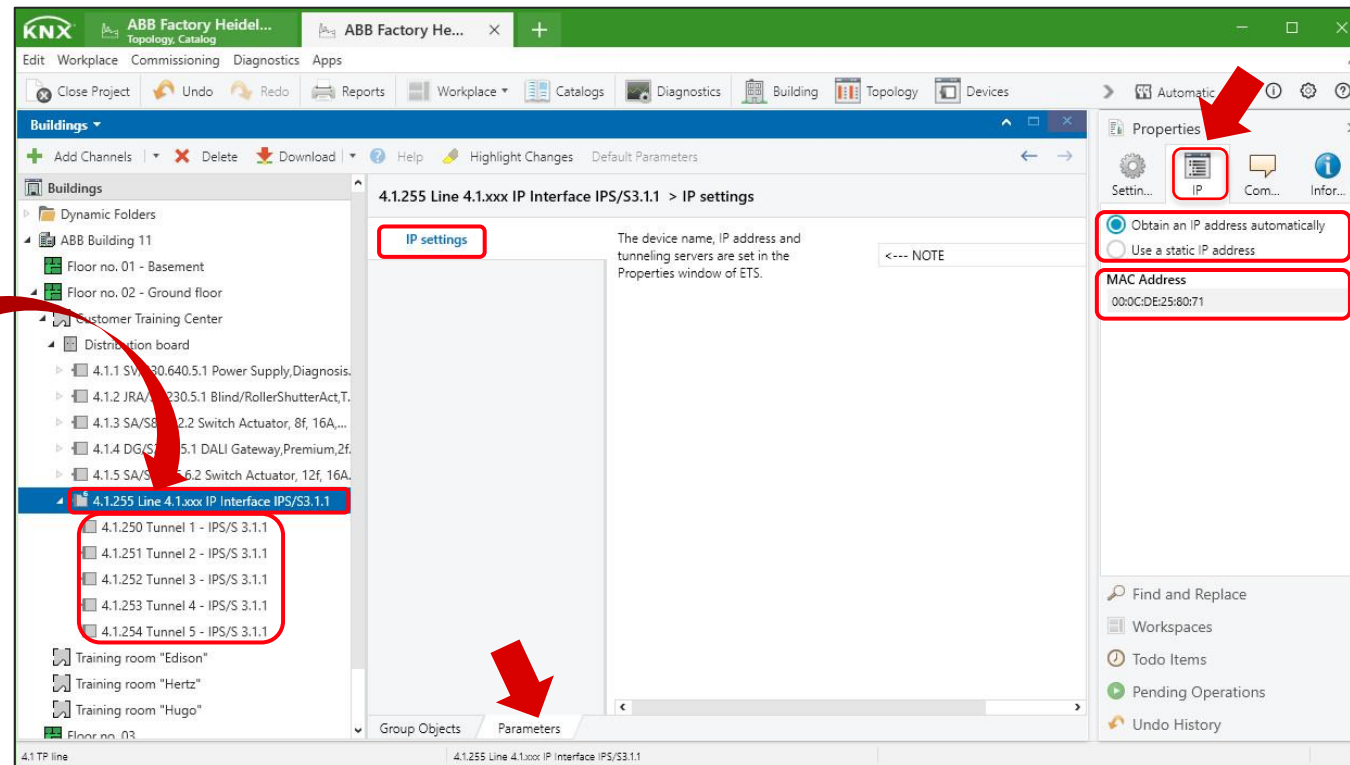
## IP Interface IPS/S 3.1.1 (standard) – Setting up a tunnel connection in the ETS

Total 6 Individual addresses



4.1.255 Individual address of IPS/S

5 Tunneling Server e.g. 4.1.250 – 4.1.254:  
→ 5 additional addresses (local) for the tunneling server



Automatic IP assignment  
(DHCP/AutoIP) or  
static/fixed IP address

MAC address  
(will be displayed after  
the first download)

# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface IPS/S 3.1.1 (standard) – Setting up a tunnel connection in the ETS

The screenshot displays the ETS (Energy Management System) interface. On the left, the 'Buildings' tree shows a project named 'ABB Factory Heidelberg'. Under 'Dynamic Folders', 'ABB Building 11' is expanded, showing various components. A red box highlights the '4.1.255 Line 4.1.xxx IP Interface IPS/S3.1.1' device. Below it, a list of tunnels is shown, with '4.1.250 Tunnel 1 - IPS/S 3.1.1' highlighted. In the center, the '4.1.255 Line 4.1.xxx IP Interface IPS/S3.1.1 > IP settings' window is open. The 'IP settings' tab is selected, showing the device name, IP address, and tunneling servers. A red box highlights the 'Line 4.1.xxx IP Interface (192.168.1.160:3671 4.1.255)' entry. On the right, the 'Local Interface Settings' dialog box is open, showing the 'IP Tunneling' section. The 'Name' field is set to 'Line 4.1.xxx IP Interface IPS/'. The 'Host Individual Address' is set to '4.1.255'. The 'Individual Address' field is set to '4.1.250', with a green message below it stating 'The individual address 4.1.250 is not used by another device.' The 'IP Address' is set to '192.168.1.160', the 'Port' is '3671', the 'MAC Address' is '00:0C:DE:25:80:71', the 'Max telegram length (APDU)' is '56', and the 'Serial number' is '0002:FC24FF51'. A red arrow points from the 'Line 4.1.xxx IP Interface' entry in the ETS to the 'Individual Address' field in the dialog box.

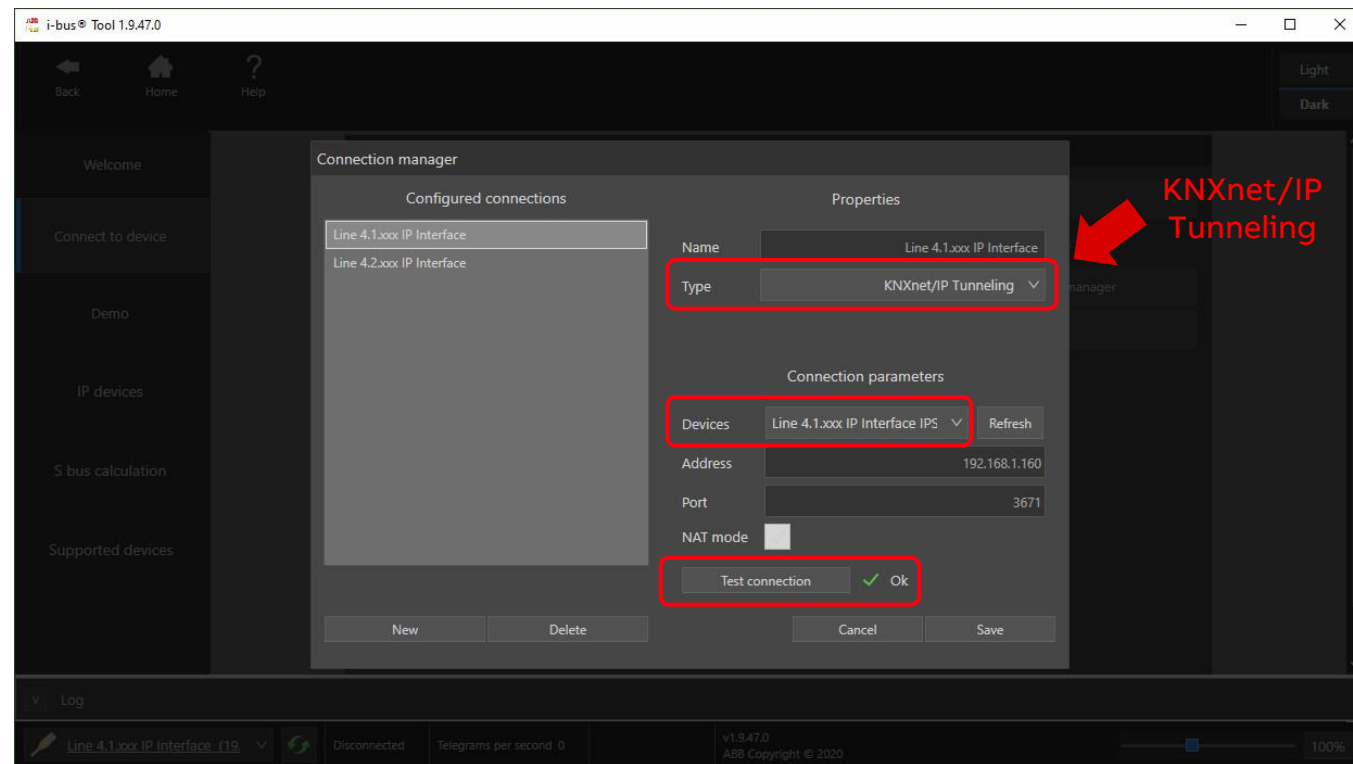
The ETS displays one of the five Tunneling Server e.g. 4.1.250



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

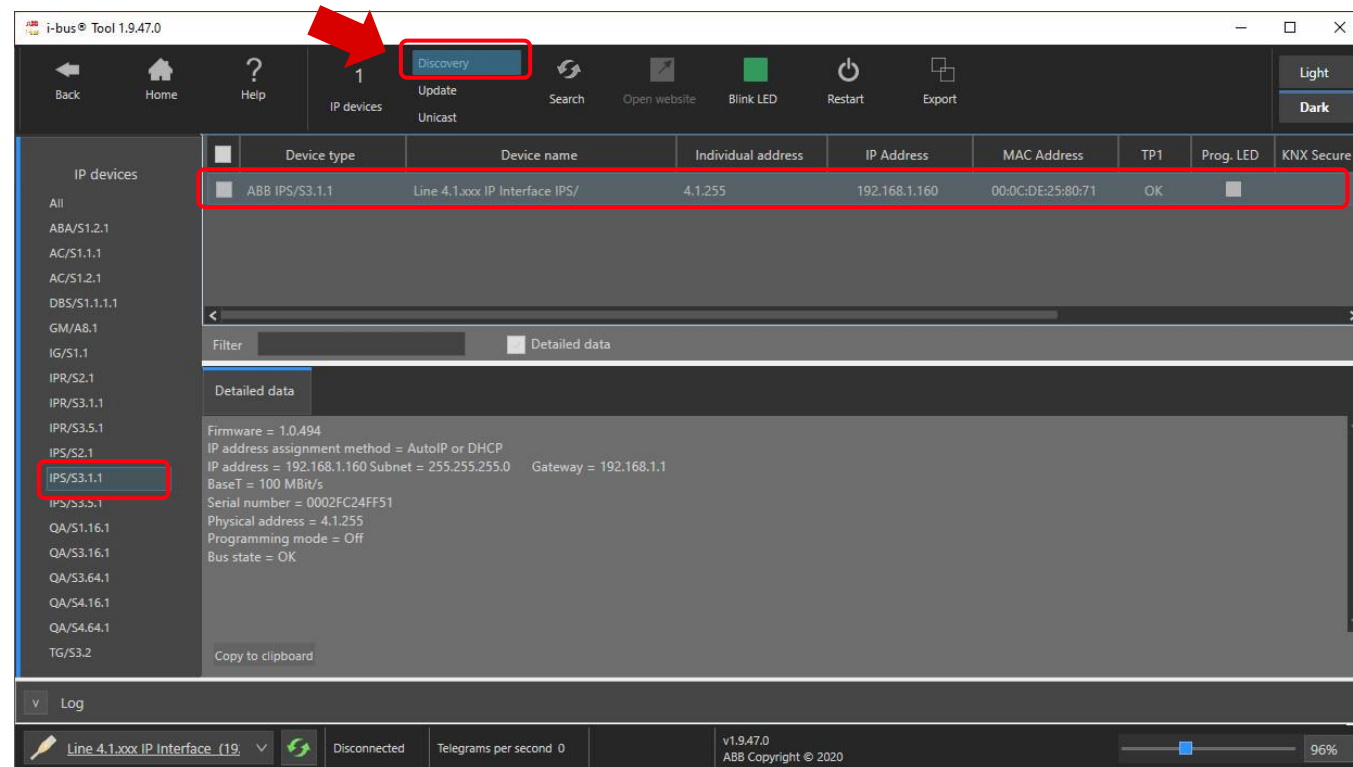
## IP Interface IPS/S 3.1.1 (standard) – Setting up a tunnel connection in the ABB i-bus® Tool



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

**IP Interface IPS/S 3.1.1 (standard) – ABB i-bus® Tool: “Discovery” (find and display ABB IP devices in the network)**



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## KNX IP Secure

### Bus safety

- Residential and functional buildings have been equipped with intelligent bus technology for 30 years
- Increasing opening towards the Internet and smart devices
- This increases comfort, safety and efficiency, but also the risk of attacks on the building infrastructure
- Buildings cannot be made absolutely secure, but the effort of an attack can be increased and the impact limited locally
- There are technical, organizational and planning aspects to be considered
- The most relevant attack scenario on a KNX installation is over the IP network



---

# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## KNX IP Secure

### General measures

Cybersecurity must be an integral part of planning and execution in a facility

Already it is possible to make access via IP (relatively) secure

- To the outside (firewall, VPN, filtering MAC addresses)
- Inside (separate technical IP network, encryption with Wi-Fi)

Prevent physical access to the KNX bus

- Lockable distribution boards
- Devices with dismantling protection
- Separate lines for sensitive areas
- No KNX cable outside the building
- ...

→ **Access-protected installation of the KNX IP Secure devices**





# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## KNX IP Secure

KNX Secure has been developed to respond to the current and future challenges regarding cyber security in building automation

- Step 1: Securing the IP communication with “KNX IP Secure”
  - Implementation of the KNX IP Secure Standard in routers, interfaces and other IP devices
  - Software clients (visualizations) are also affected
- Step 2: Implementation of “KNX Data Secure” in all field devices

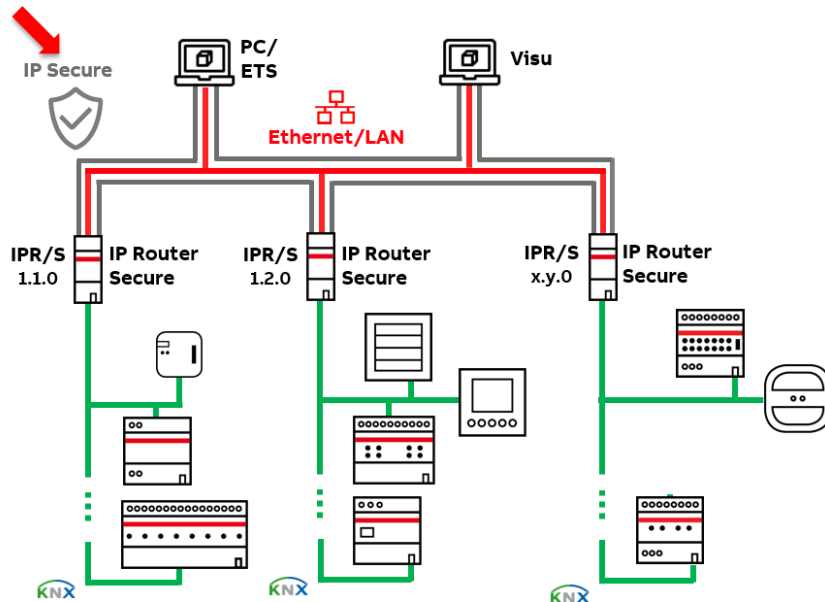


# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

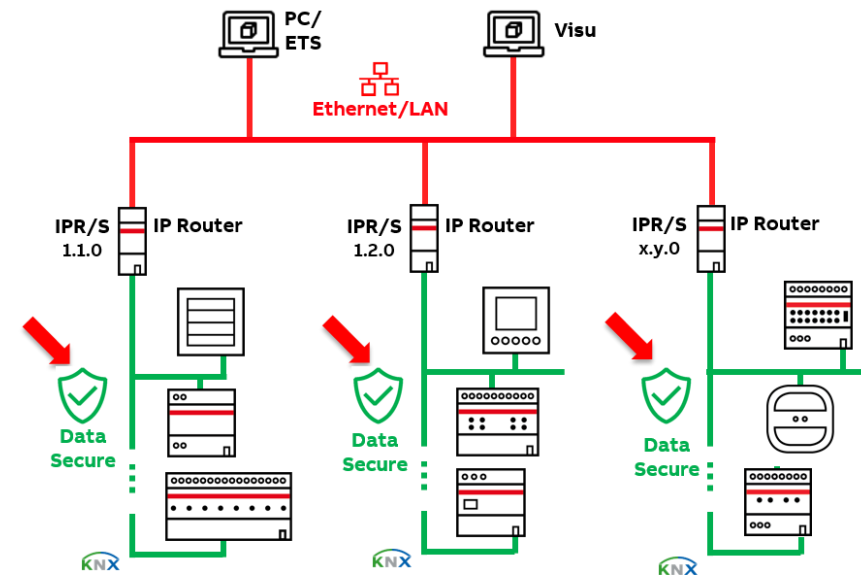
## KNX IP Secure (KNXnet/IP Secure Routing and Tunneling)

- TP Telegrams are wrapped in a secure frame on IP
- Tunneling connections are secure
- All IP devices in a project have to speak secure



## KNX Data Secure

- Each individual group telegram can be encrypted
- Communication between sensors and actuators is secure
- Data Secure is available for the medium TP and RF



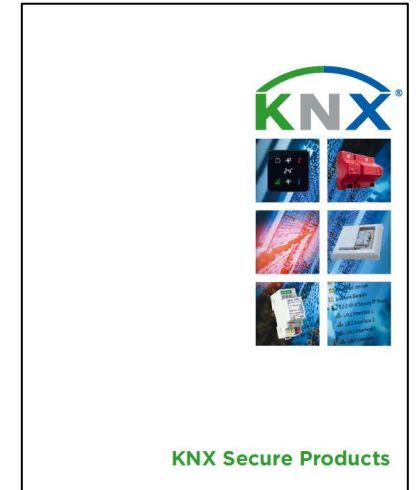
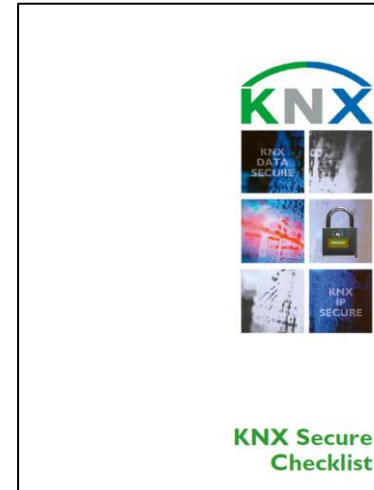


# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## KNX Secure Brochures of the KNX Association

- KNX Secure Checklist
- KNX Secure Guide
- KNX Secure Products
- <https://knxsecure.knx.org>



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1

The ABB IP Interface Secure IPS/S 3.5.1 has the same properties as the IP Interface IPS/S 3.1.1 standard

- 5 Tunneling Servers  
→ parallel access, less hardware
- Power over Ethernet (PoE)  
→ no additional power supply or 12...30 V DC
- ABB i-bus® Tool support  
→ easier commissioning and diagnostics



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1

**The ABB IP Interface Secure is a KNX device according to the KNX Secure Standard “KNXnet/IP Security”**

- The communication on the IP network is secure
  - All KNX IP Secure devices must support the KNXnet/IP security protocol
- ETS6 or ETS5 (5.7.4 or higher), the current version of the device application and firmware are required for programming
- The device should always be operated in KNX Secure mode
  - This ensures security for the tunneling servers
- The device can be safely put into operation
- All five tunnel connections can be used together encrypted or unencrypted
- Firmware update with ABB i-bus® Tool, available updates should be loaded into the device promptly



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1

### Connection “KNXnet/IP Tunneling Secure“:

Unicast (Point to Point)

ETS: Group and bus monitor are supported

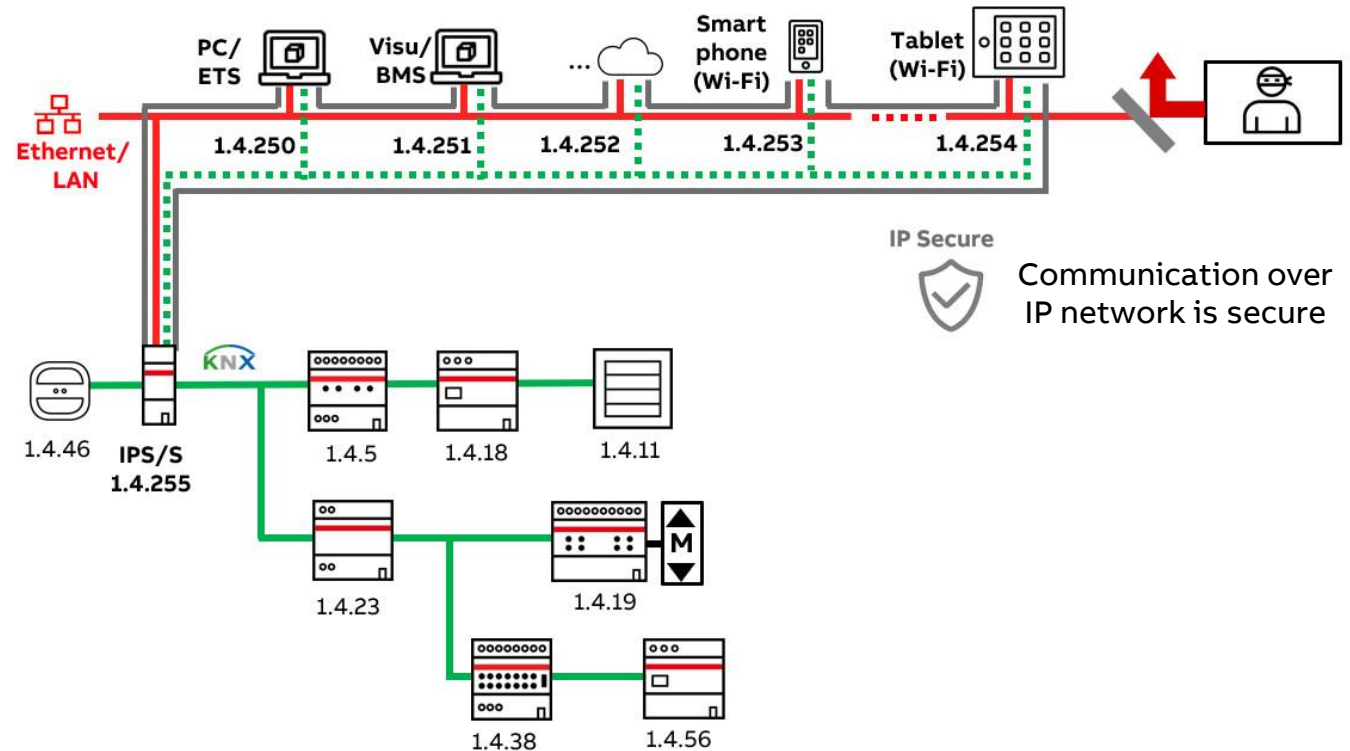
1.4.255 Individual address IP Interface

Tunneling Server e.g. 1.4.250 – 1.4.254:

→ 5 additional addresses (local) for the tunneling server of the IP Interface



IPS/S3.5.1

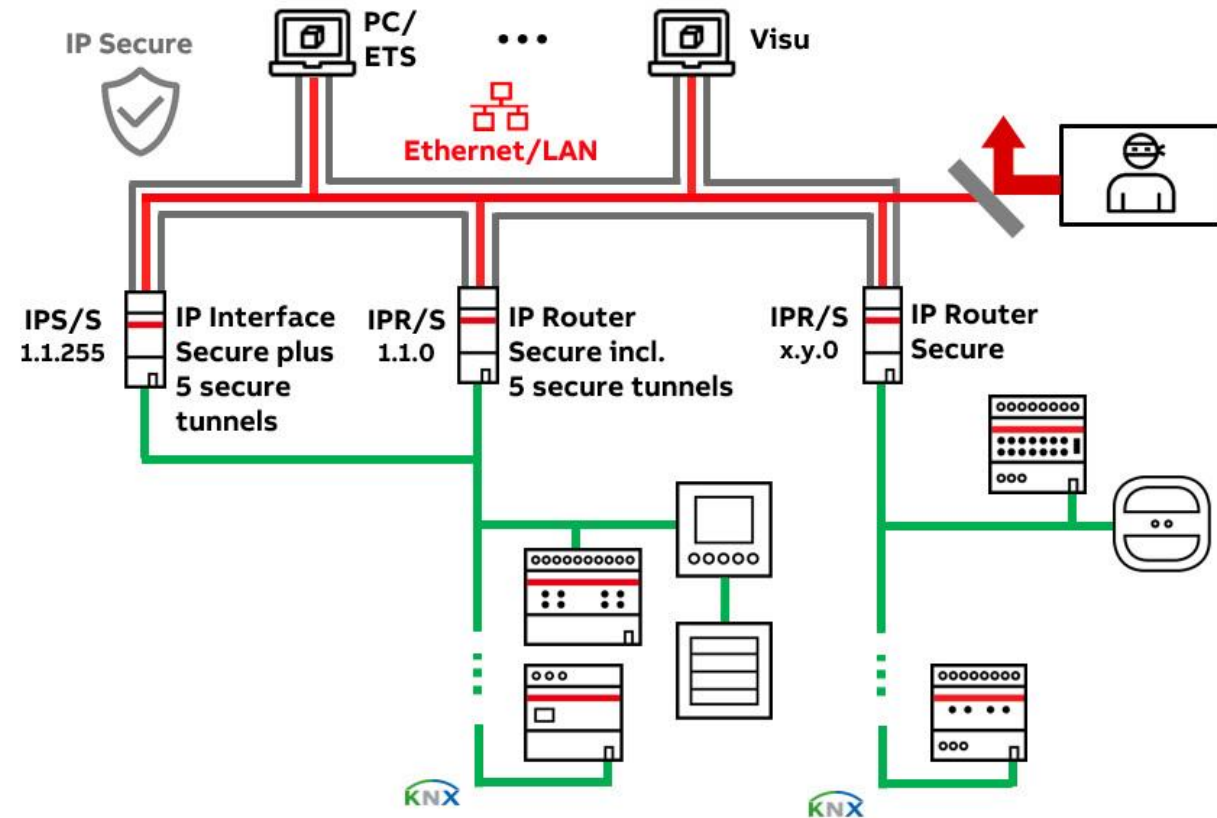


# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Areas of application

- If the existing five tunneling connections are not sufficient of an IP Router IPR/S
- Existing KNX installations with Area/Line Couplers LK/S should be connected via IP
- Connection to IP of new installations that only consist of one line, for example a residential home
- No IP Routers IPR/S are installed and a central system (BMS server, visualization system, hotel management system) establishes a connection to each individual IP Interface IPS/S via the integrated tunneling server, e.g. in a hotel
  - Secure tunneling connection from each room to central BMS
  - Security by isolated rooms
  - It covers the use case „attack” from the field level
  - No direct inter-room communication available
  - BMS can also monitor the KNX field devices



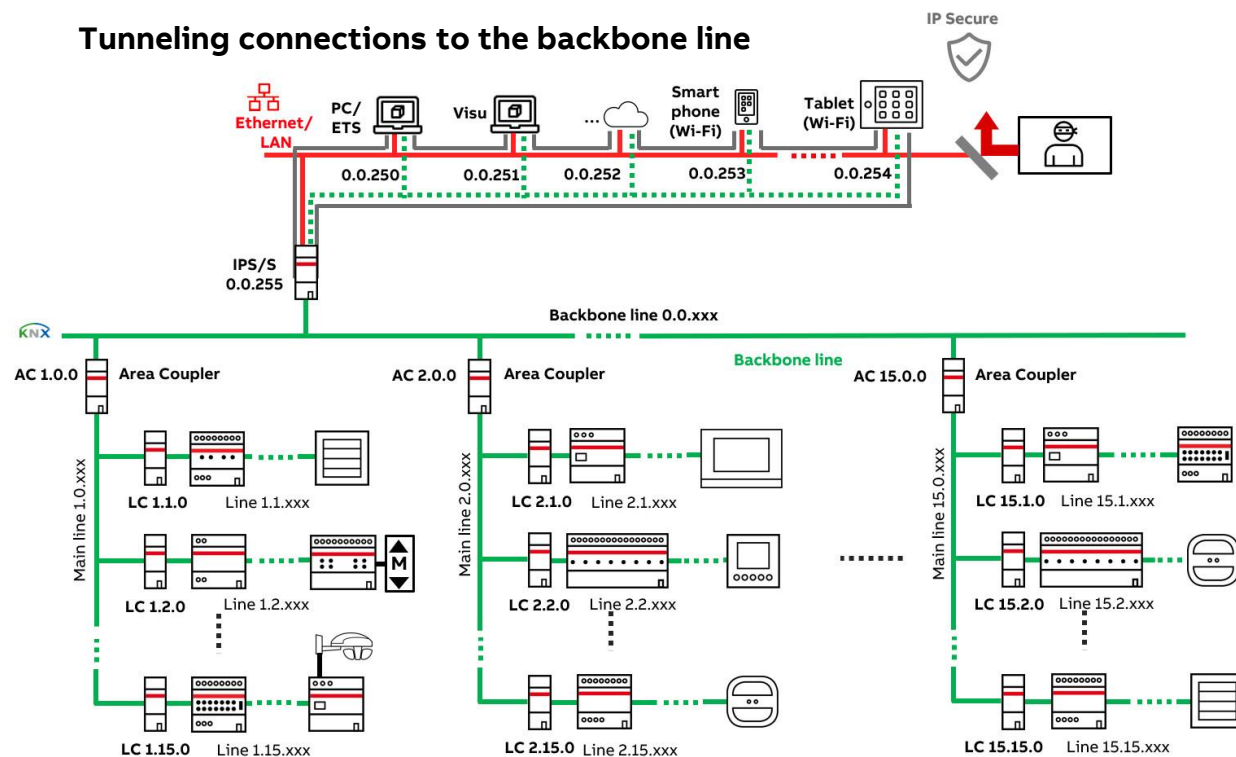
# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Areas of application

- If the existing five tunneling connections are not sufficient of an IP Router IPR/S
- Existing KNX installations with Area/Line Couplers LK/S should be connected via IP
- Connection to IP of new installations that only consist of one line, for example a residential home
- No IP Routers IPR/S are installed and a central system (BMS server, visualization system, hotel management system) establishes a connection to each individual IP Interface IPS/S via the integrated tunneling server, e.g. in a hotel
  - Secure tunneling connection from each room to central BMS
  - Security by isolated rooms
  - It covers the use case „attack” from the field level
  - No direct inter-room communication available
  - BMS can also monitor the KNX field devices

### Tunneling connections to the backbone line



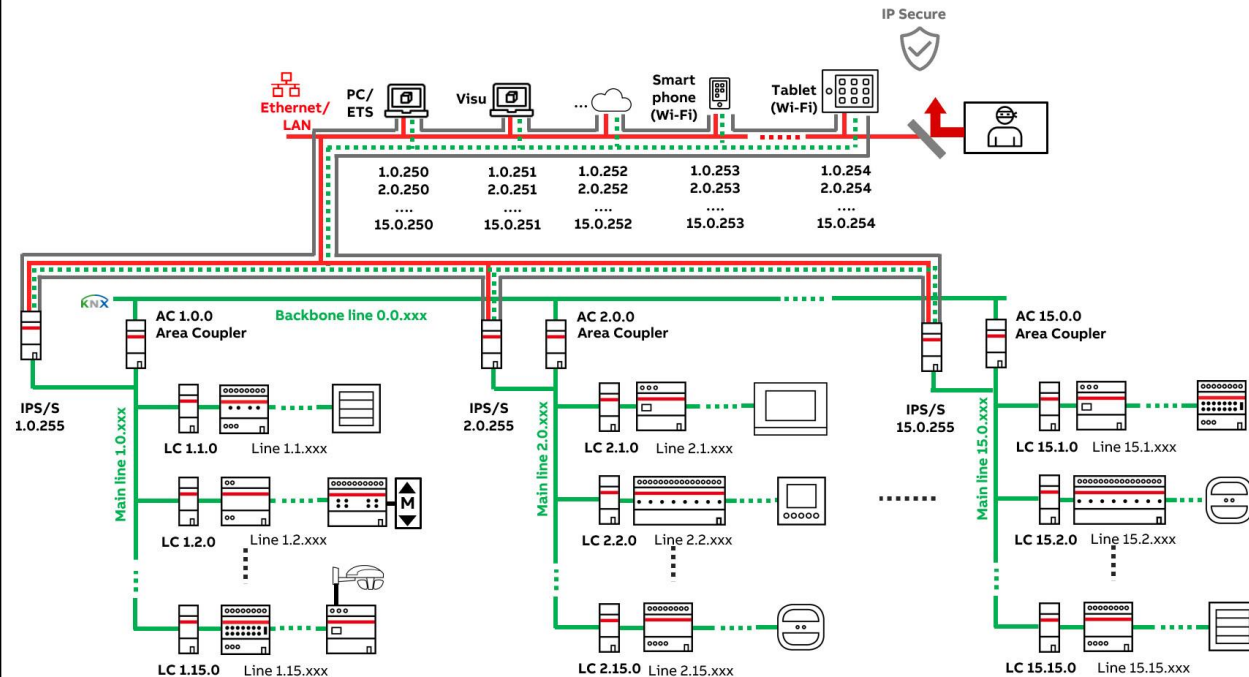
# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Areas of application

- If the existing five tunneling connections are not sufficient of an IP Router IPR/S
- Existing KNX installations with Area/Line Couplers LK/S should be connected via IP
- Connection to IP of new installations that only consist of one line, for example a residential home
- No IP Routers IPR/S are installed and a central system (BMS server, visualization system, hotel management system) establishes a connection to each individual IP Interface IPS/S via the integrated tunneling server, e.g. in a hotel
  - Secure tunneling connection from each room to central BMS
  - Security by isolated rooms
  - It covers the use case „attack” from the field level
  - No direct inter-room communication available
  - BMS can also monitor the KNX field devices

Tunneling connections to each main line → less bus traffic on backbone line



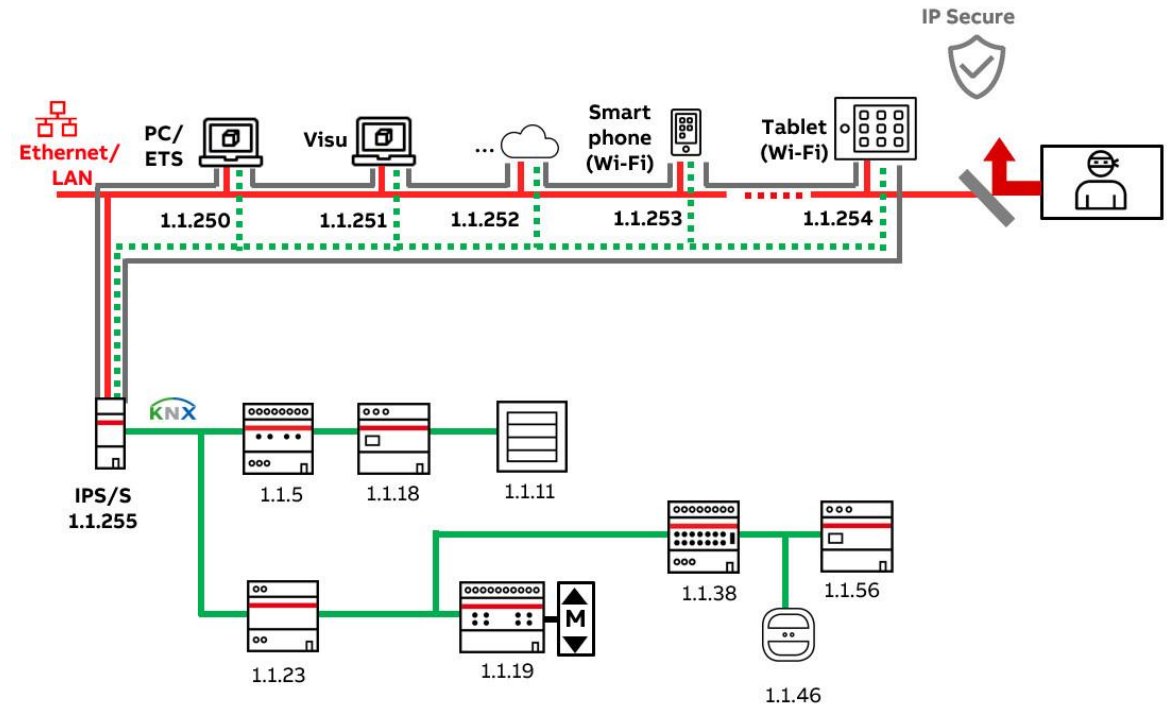


# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Areas of application

- If the existing five tunneling connections are not sufficient of an IP Router IPR/S
- Existing KNX installations with Area/Line Couplers LK/S should be connected via IP
- Connection to IP of new installations that only consist of one line, for example a residential home
- No IP Routers IPR/S are installed and a central system (BMS server, visualization system, hotel management system) establishes a connection to each individual IP Interface IPS/S via the integrated tunneling server, e.g. in a hotel
  - Secure tunneling connection from each room to central BMS
  - Security by isolated rooms
  - It covers the use case „attack” from the field level
  - No direct inter-room communication available
  - BMS can also monitor the KNX field devices



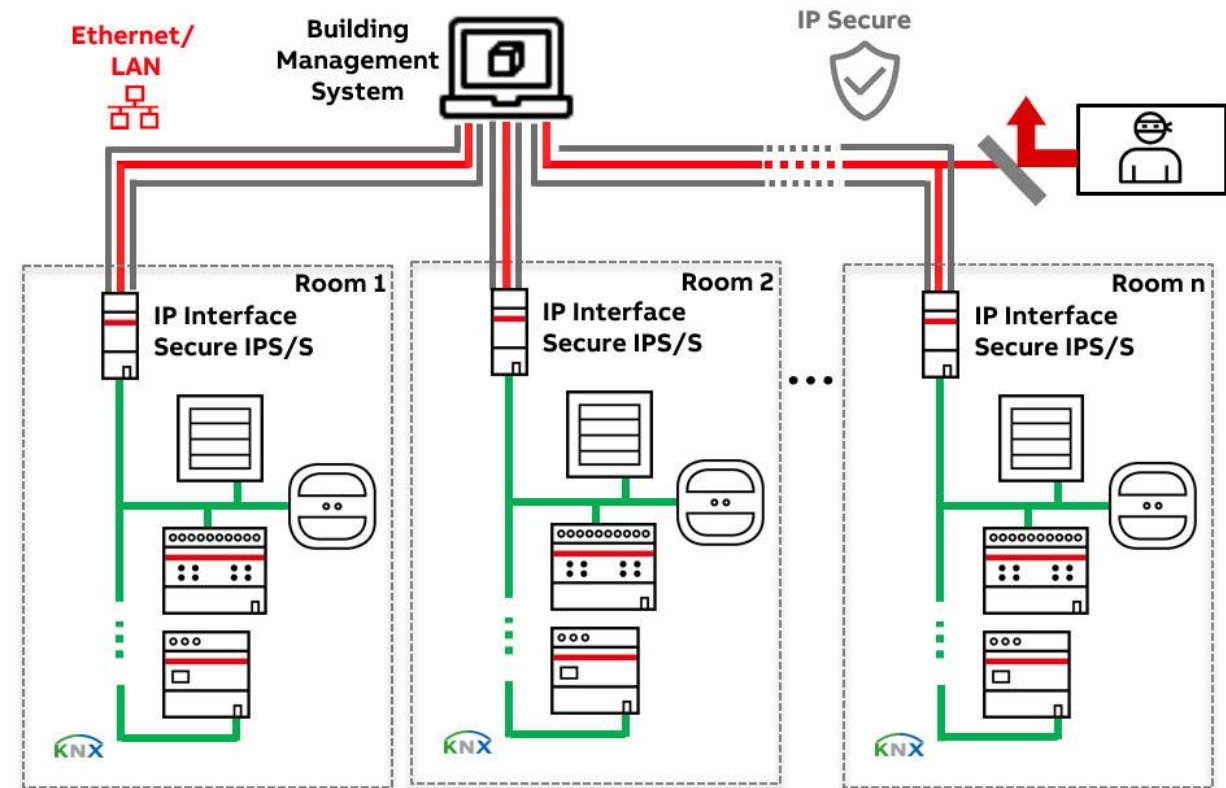


# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Areas of application

- If the existing five tunneling connections are not sufficient of an IP Router IPR/S
- Existing KNX installations with Area/Line Couplers LK/S should be connected via IP
- Connection to IP of new installations that only consist of one line, for example a residential home
- No IP Routers IPR/S are installed and a central system (BMS server, visualization system, hotel management system) establishes a connection to each individual IP Interface IPS/S via the integrated tunneling server, e.g. in a hotel
  - Secure tunneling connection from each room to central BMS
  - Security by isolated rooms
  - It covers the use case “attack” from the field level
  - No direct inter-room communication available
  - BMS can also monitor the KNX field devices



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Commissioning

- When commissioning a KNX secure device (first download) a commissioning key – “Device Certificate” – is required
- The “Device Certificate” consists of
  - FDSK = Factory Default Setup Key
  - Serial number of IP Secure device
- ABB secure devices:  
The “Device Certificate” is placed on a sticker on the left side of the device and must be imported into the ETS
- One sticker can be used for project documentation, the other can be left on the device



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Commissioning

- The FDSK is only required for initial commissioning
- After that, the ETS creates new “Tool Keys”
- The “Tool Keys” are transferred via the bus with encryption based on FDSK to the IP Interface
- Further device configuration is encrypted based on the “Tool Key”
- The FDSK is only needed again after a device reset to factory settings



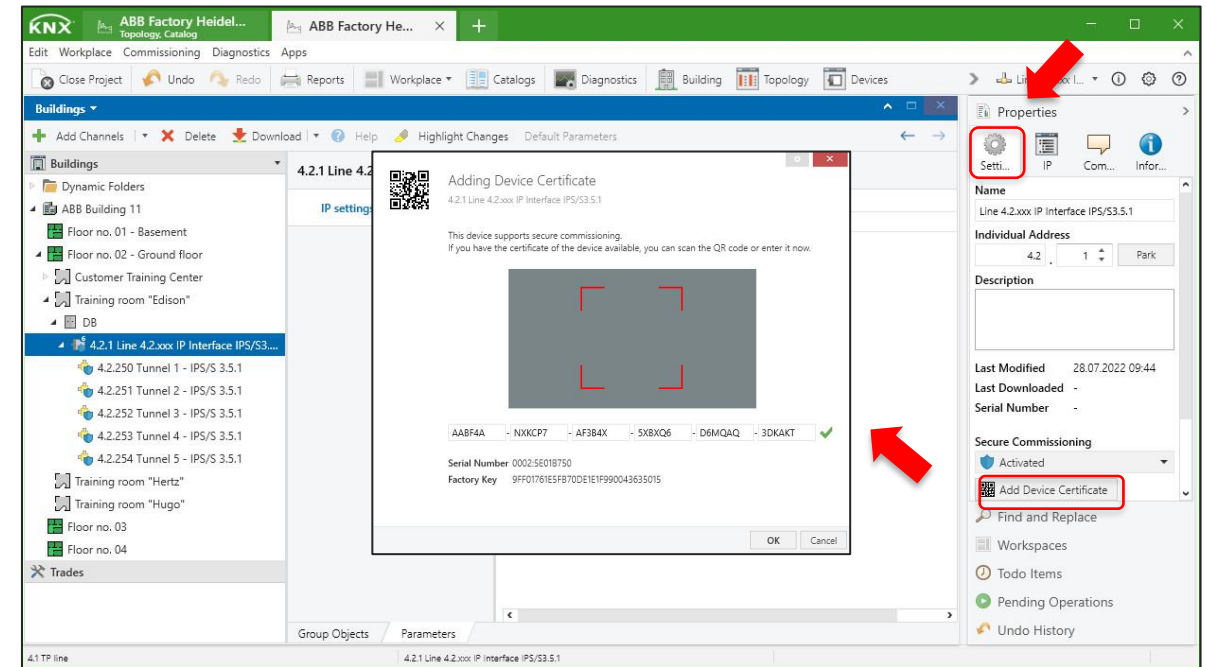
# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Commissioning

How to enter the “Device Certificate”?

- When inserting a KNX Secure device, you will be asked for it
- The ETS asks for the key when programming for the first time
- Click on “Add Device Certificate”
  - Properties → Settings → Selected device
  - ETS main menu “Security”
- The reading can be done offline
- The keys are assigned automatically to the IP Interface Secure by ETS



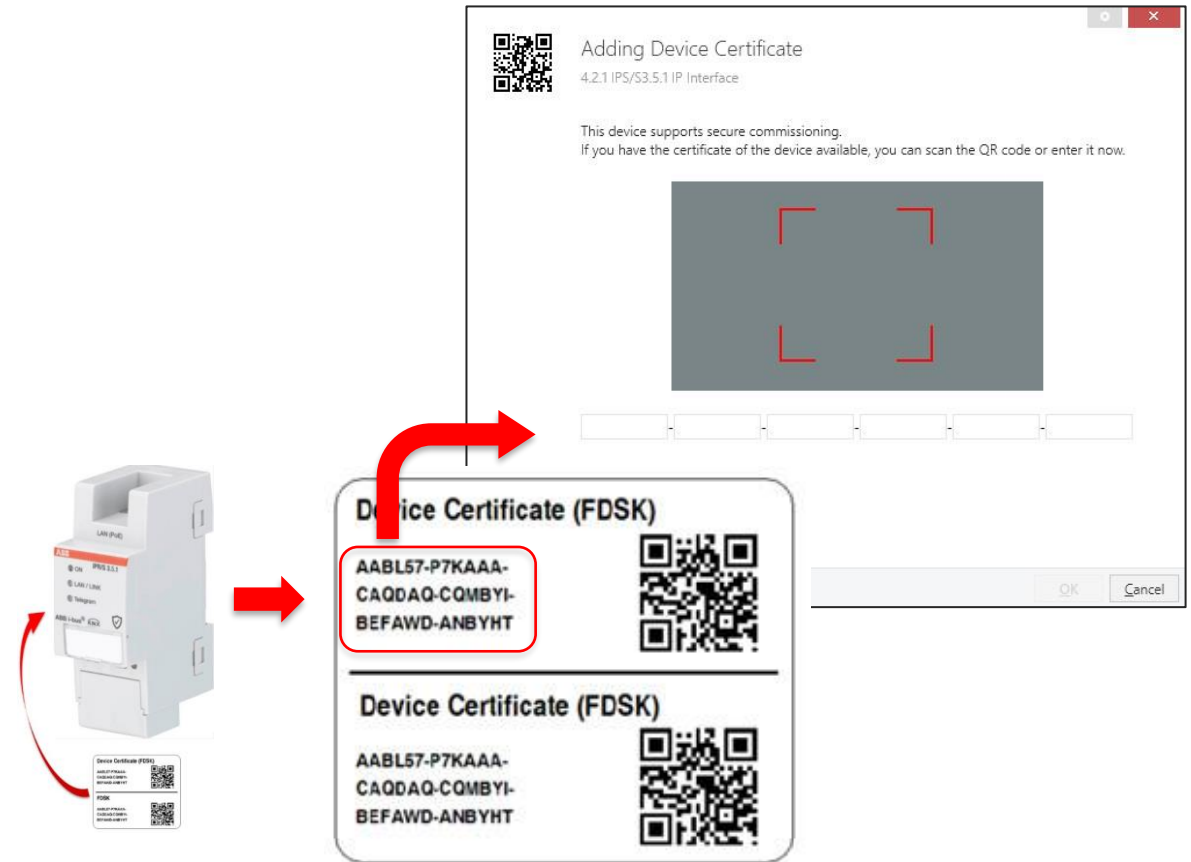
# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Commissioning

How to enter the “Device Certificate”?

- The key can be
  - Entered via the keyboard
  - Read in with a QR code scanner
  - Read with the webcam of laptop

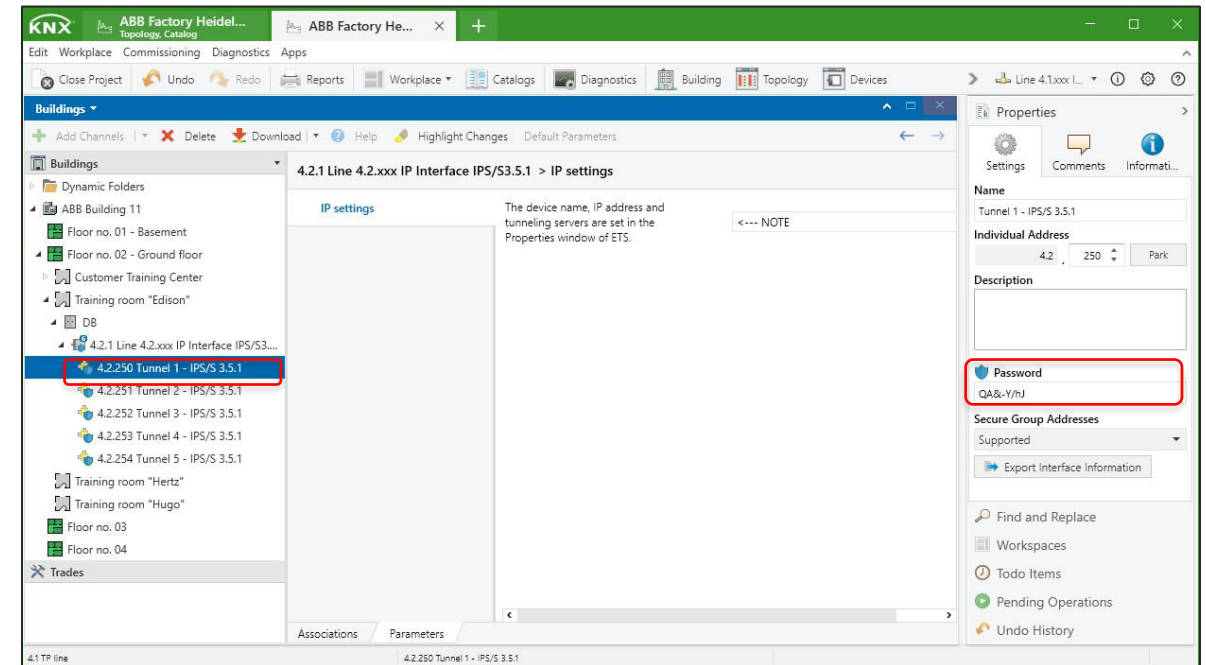


# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Commissioning

- The ETS generates separate passwords for each tunneling server
- The passwords of the tunneling server can be changed if necessary
- A tunnel address can be passed to a client (e.g. BMS or Visu) with the password
- The keys are generated and managed by the ETS
- If necessary, keys and passwords can be exported





# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Commissioning

First download of IP Interface Secure

- The IP Interface is in the delivery state (e.g. after a factory reset)
- The device is connected to KNX TP (twisted pair)
- The individual address and application program can be downloaded in different ways
  - Another programming interface which supports KNX “long frame” telegrams (APDU > 15)
    - USB Interface USB/S 1.2
    - IP Router IPR/S via KNXnet/IP Routing or KNXnet/IP Tunneling
  - Itself with one of the integrated tunneling servers



USB Interface USB/S 1.2



IP Interface IPS/S 3.5.1



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

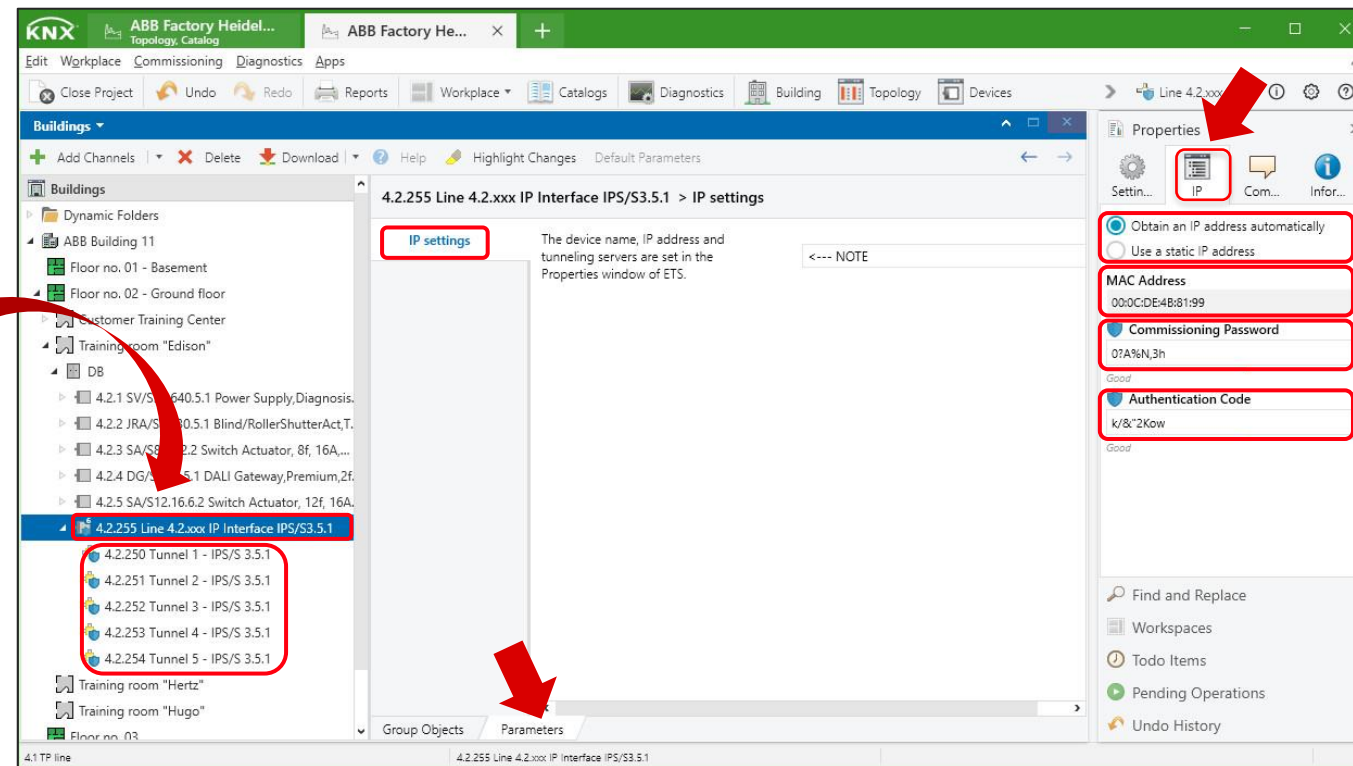
## IP Interface Secure IPS/S 3.5.1 – Setting up a tunnel connection in the ETS

Total 6 Individual addresses

- 4.2.255 Line 4.2.xxx IP Interface IPS/S3.5.1
- 4.2.250 Tunnel 1 - IPS/S 3.5.1
- 4.2.251 Tunnel 2 - IPS/S 3.5.1
- 4.2.252 Tunnel 3 - IPS/S 3.5.1
- 4.2.253 Tunnel 4 - IPS/S 3.5.1
- 4.2.254 Tunnel 5 - IPS/S 3.5.1

4.2.255 Individual address of IPS/S

5 encrypted Tunneling Server e.g.  
4.2.250 – 4.2.254:  
→ 5 additional addresses (local) for the  
tunneling server



Automatic IP assignment  
(DHCP/AutoIP) or  
static/fixed IP address

MAC address  
(will be displayed after  
the first download)

Commissioning  
password (can be  
adopted like this)

Authentication code  
(can be adopted like this)



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – Setting up a tunnel connection in the ETS

The screenshot displays the ETS (Energy Management System) software interface. On the left, the 'Buildings' tree shows a project named 'ABB Factory Heidelberg'. Under 'Dynamic Folders', the '4.2.255 Line 4.2.xxx IP Interface IPS/S3.5.1' is highlighted. Below it, a list of tunnels is shown: '4.2.250 Tunnel 1 - IPS/S 3.5.1', '4.2.251 Tunnel 2 - IPS/S 3.5.1', '4.2.252 Tunnel 3 - IPS/S 3.5.1', '4.2.253 Tunnel 4 - IPS/S 3.5.1', and '4.2.254 Tunnel 5 - IPS/S 3.5.1'. The '4.2.255 Line 4.2.xxx IP Interface IPS/S3.5.1' is selected, and its 'IP settings' are displayed in the main window. The settings include the device name, IP address, and tunneling servers. A red box highlights the 'Line 4.2.xxx IP Interface IPS/ (192.168.1.136:3671 4.2.255)' entry in the 'Devices' list. A red arrow points from this entry to the 'Local Interface Settings' dialog box on the right. The dialog box shows the 'IP Tunneling' tab selected, with fields for Name, Host Individual Address, Individual Address, IP Address, Port, MAC Address, Max telegram length (APDU), and Serial number. The 'IP Tunneling' tab is highlighted with a red box. A red arrow points from the 'Local Interface Settings' dialog box to the 'Encrypted tunneling connection' icon on the right.

Local Interface Settings

**IP Tunneling**

Name  
Line 4.2.xxx IP Interface IPS/

Host Individual Address  
4.2.255

Individual Address  
Can only be set by downloading the interface device.

IP Address  
192.168.1.136

Port  
3671

MAC Address  
00:0C:DE:4B:81:99

Max telegram length (APDU):  
254

Serial number:  
0002:5E01B750

Close



Encrypted tunneling connection

# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1 – ABB i-bus® Tool: “Discovery” (find and display ABB IP devices in the network)

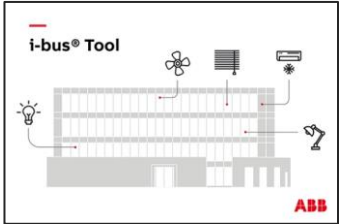


ABB i-bus® Tool 1.9.47.0

Back Home ? IP devices 1 Discovery Update Unicast Search Open website Blink LED Restart Export

Device type	Device name	Individual address	IP Address	MAC Address	TP1	Prog. LED	KNX Secure
ABB IPS/S3.5.1	Line 4.2.xxx IP Interface IPS/	4.2.255	192.168.1.136	00:0C:DE:48:81:99	OK		Active

Filter Detailed data

Detailed data

Firmware = 0.1.783  
IP address assignment method = DHCP  
IP address = 192.168.1.136 Subnet = 255.255.255.0 Gateway = 192.168.1.1  
BaseT = 100 MBit/s  
Serial number = 00025E01B750  
Physical address = 4.2.255  
Programming mode = Off  
Bus state = Ok  
Secure mode = Enabled

Copy to clipboard

Log

Line 4.1.xxx IP Interface (19) Disconnected Telegrams per second 0 v1.9.47.0 ABB Copyright © 2020 96%



KNX Secure is active

# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Interface Secure IPS/S 3.5.1

### Summary

- KNX IP Interface Secure IPS/S 3.5.1 fulfills the KNX Secure Standard “KNXnet/IP Security”
- Communication from ETS and tunneling servers are secure
- After commissioning, an IP Interface Secure behaves like a standard IP Interface
- All functions from standard IP Interface IPS/S 3.1.1 are available
- The ETS requests a password for the project
- The “Device Certificates” of all IP Interfaces Secure and other IP devices Secure must be entered
- The ETS generates and works with many keys – but there is no need to change them
- Access-protected installation of the KNX IP Secure devices



---

# ABB i-bus® KNX – IP Devices

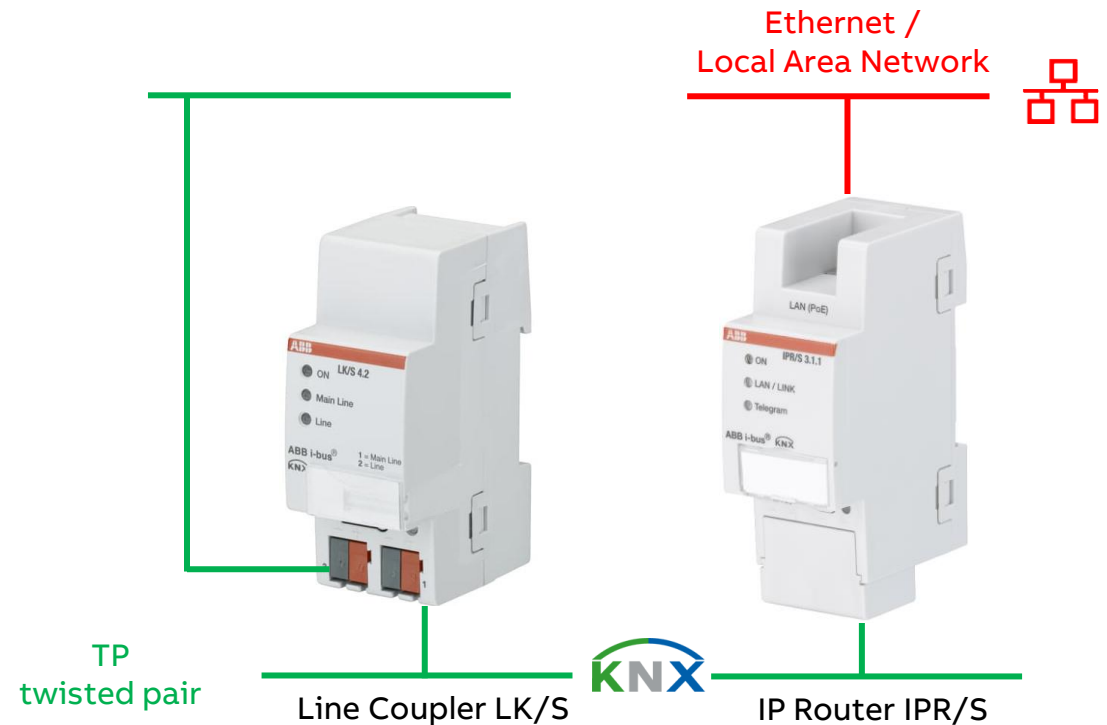
IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Coupler – IP and TP (twisted pair)

- A coupler is used in larger installations to connect KNX lines or areas
- Telegrams can be filtered to simultaneously reduce the telegram traffic between lines or areas
- Line Coupler LK/S
  - Communication between TP main/backbone line and TP subline
- IP Router IPR/S
  - Communication between LAN and TP subline
  - The KNXnet/IP protocol is used for communication
  - 5 additional Tunneling Server for programming with ETS and further clients
  - Built in 5-fold “USB Interface” via LAN

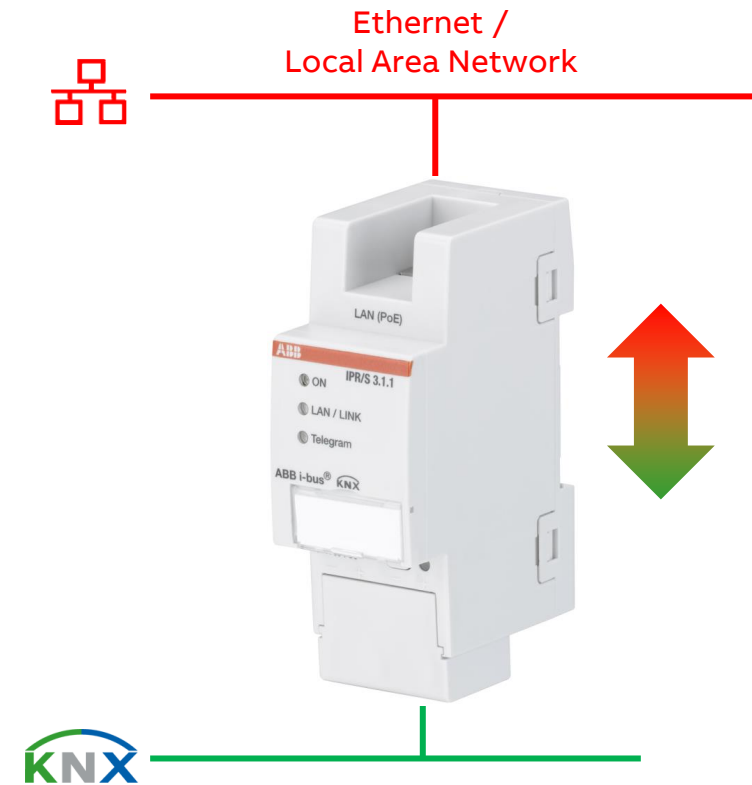


# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## KNX IP Router – Principle

- An ABB i-bus® KNX IP Router connects the KNX TP bus to an Ethernet network
- KNX telegrams can be sent to or received from other devices via the Ethernet network → routing of KNX telegrams
- This allows data exchange between KNX and IP networks
- The IP Router can be used as a Line Coupler or Area Coupler and complies with the specifications of the KNXnet/IP standard
  - IP Router IPR/S 3.1.1 (**standard** KNXnet/IP protocol)
  - IP Router **Secure** IPR/S 3.5.1  
This device uses the KNXnet/IP protocol and the KNXnet/IP Security protocol from the KNX Association (routing and tunneling) for communication
- Furthermore, the 5 tunneling server can be used in parallel for working with the ETS, access from the ABB i-bus® Tool, connection to a visualization, etc.



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router IPR/S 3.1.1 (standard)

### KNXnet/IP Capabilities:

- Routing (Coupler)
  - Connection of KNX Lines and Areas over IP network
  - Routing of KNX telegrams
- Tunneling (Interface)
  - 5 Tunneling Server
  - To connect a PC to KNX via IP
    - Working with ETS (download, diagnostics,...)
    - ABB i-bus® Tool support
    - Visualisation
    - Tablet/Smart Phone with App via Wi-Fi
    - ...



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router IPR/S 3.1.1 (standard)

- Default multicast IP address **224.0.23.12** and port **3671** for communication on IP network according to the KNXnet/IP routing protocol
- Unicast communication possible with up to 10 IPR/S 3.1.1 (not according to the KNXnet/IP standard)
- ETS parameter from KNX to LAN and LAN to KNX
  - “Filter”, “Route” or “Block” for all main groups 0...31 or group addresses 1...65,535 with free group address view
  - “Filter” or “Block” of physically addressed telegrams (e.g. download of application program, diagnostic)
  - “Route” or “Block” of broadcast telegrams (e.g. download of individual program, diagnostic)



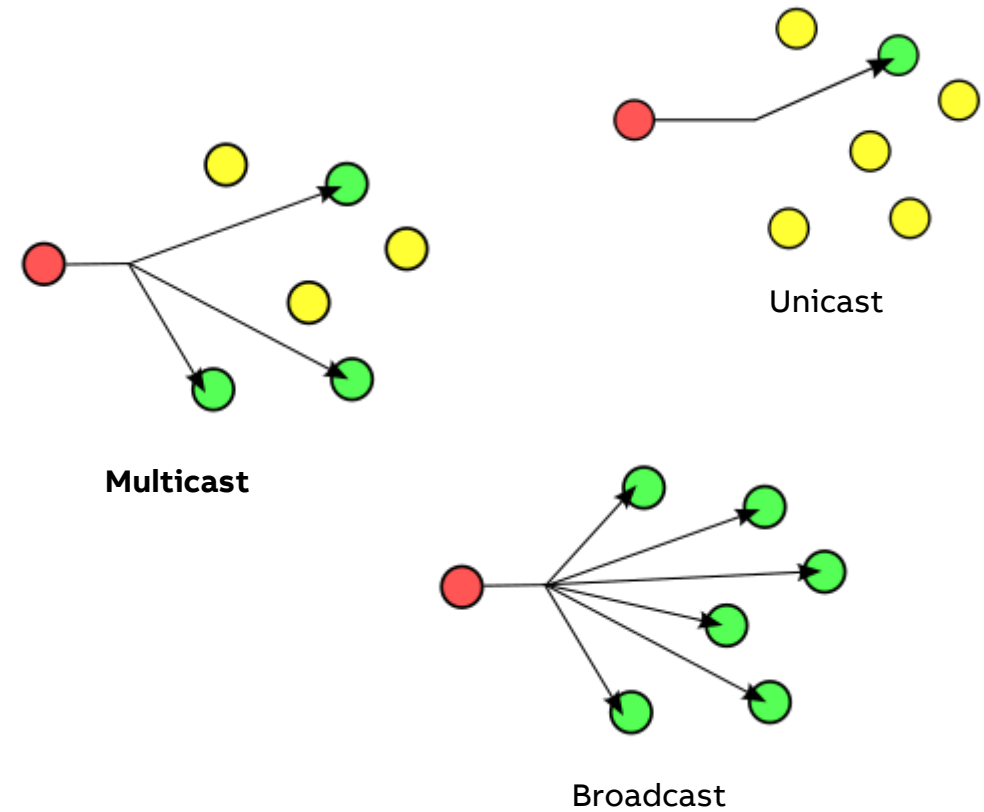


# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## KNX telegrams in the network – Multicast

- Multicast designates communication of a transmitter with a group of receivers → Point to Multipoint
- The IP Router sends the KNX telegrams packaged as UDP/IP telegrams on the IP network, and all IP Router devices parameterized with the same multicast address receive and evaluate these telegrams
- If a telegram is intended for the corresponding subline, the IP Router routes the telegram into the line – otherwise, it is rejected
- The IP Router sends telegrams from the KNX to the IP network in accordance with the KNXnet/IP protocol specification
- This multicast IP address **224.0.23.12** port **3671** is the defined address for the KNXnet/IP from the KNX Association in conjunction with IANA for KNX IP devices
- In order for several IP Router devices to communicate with one another in a network, multicast communication must be possible between the devices (e.g. routers, switches or firewalls)



# ABB i-bus® KNX – IP Devices

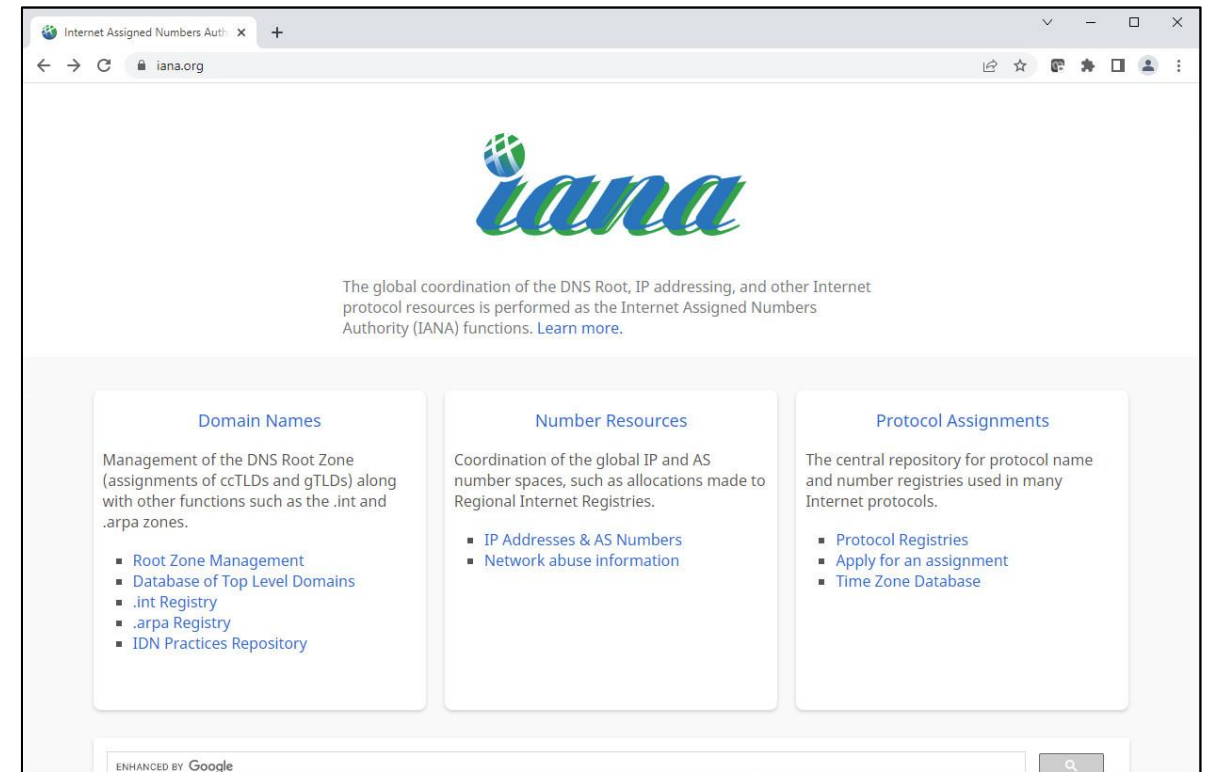
IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Internet Assigned Numbers Authority (IANA)

The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the Domain Names, IP addressing, and other Internet protocol resources

- Internet Protocol v4 Multicast Address Assignments
- AD-HOC Block (224.0.2.0 - 224.0.255.0)

Address(s)	Description References
• 224.0.23.10	Telefeed
• 224.0.23.11	SpectraTalk
• <b>224.0.23.12</b>	<b>KNXnet/IP (EIBnet/IP)</b>
• 224.0.23.13	TVE-ANNOUNCE2
• 224.0.23.14	DvbServDisc



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router IPR/S 3.1.1 (standard)

- Hardware
  - Network cable connection
  - Labelling field
  - DIN rail connection
  - Cover cap
  - Programming button and LED
- Power supply
  - 12 ... 30 V DC (e.g. separate Power Supply CP-D or NTU/S)
  - Power over Ethernet (PoE): IEEE 802.3af class 1
  - If PoE and supply voltage are connected at the same time, PoE is used



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router IPR/S 3.1.1 (standard)

### LED “ON”

- After the supply voltage  $U_s$  is connected, the LED initially lights up continuously
- After approx. 40 sec., the LED starts flashing until initialization is completed

### LED “LAN/LINK”

- Once initialization is completed, the LED lights up when the IP Interface is connected to an IP network
- The LED flashes when the device detects activity on the IP network, e.g. when data is exchanged

### LED “Telegram”

- The LED lights up continuously when the IP Interface is connected to KNX after the startup process is completed
- The LED flashes when the device detects activity on the KNX subline TP (twisted pair)



ON



LAN/LINK



Telegram

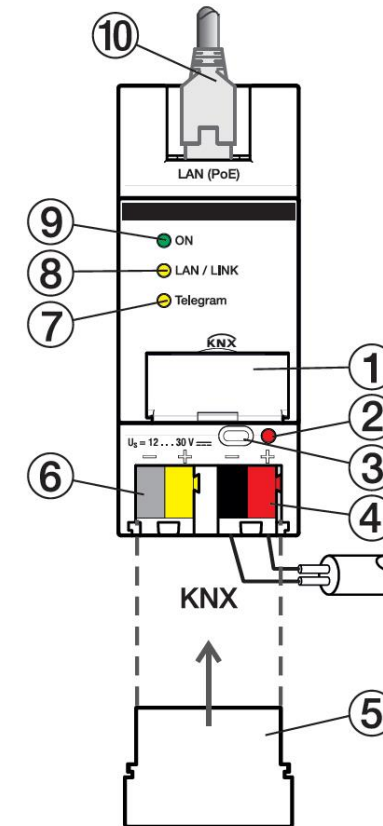


# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router IPR/S 3.1.1 (standard)

1. Label carrier
2. KNX programming LED (red)
3. KNX programming button
4. KNX bus connection terminal
5. Cover cap
6. Power supply connection  $U_s$
7. Telegram LED (yellow)
8. LAN/LINK LED (yellow)
9. ON LED (green)
10. LAN connection



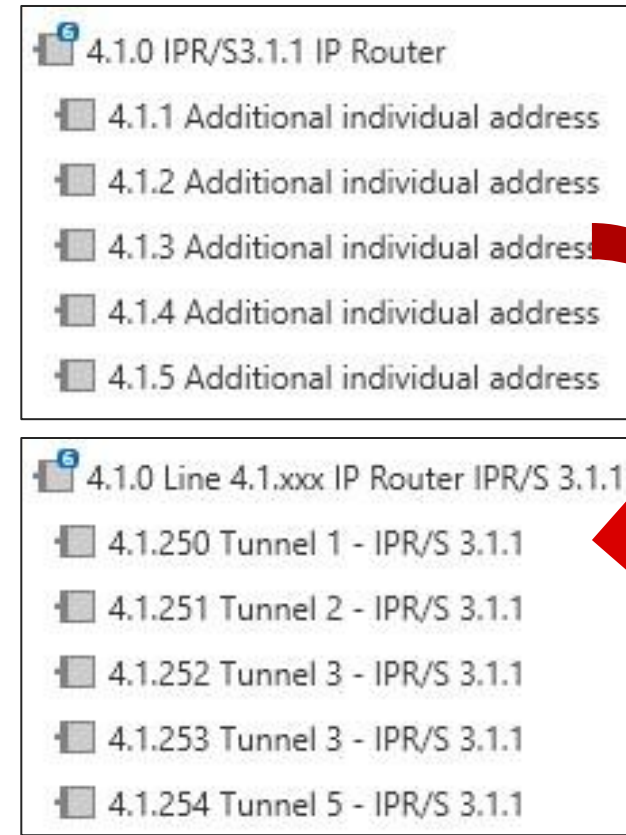
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router IPR/S 3.1.1 (standard)

### Supplied state

- The device is supplied with the individual address 15.15.0
- All tunneling connection addresses are set to 15.15.100 (only one tunnel is visible to the outside)
- The device is supplied with the option “Group telegrams - Route”  
→ This is not the default setting in the application, but it simplifies commissioning
- In ETS, the first five free addresses in the line are assigned automatically after the IP Router has been inserted into a line
- The tunneling connection addresses set in the ETS will be adopted only after the first download
- The IP address is set to automatic IP assignment (DHCP/AutoIP)
- The parametrized settings will be adopted after the first download

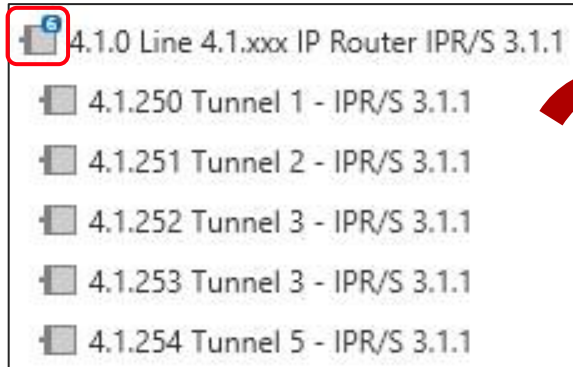


# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

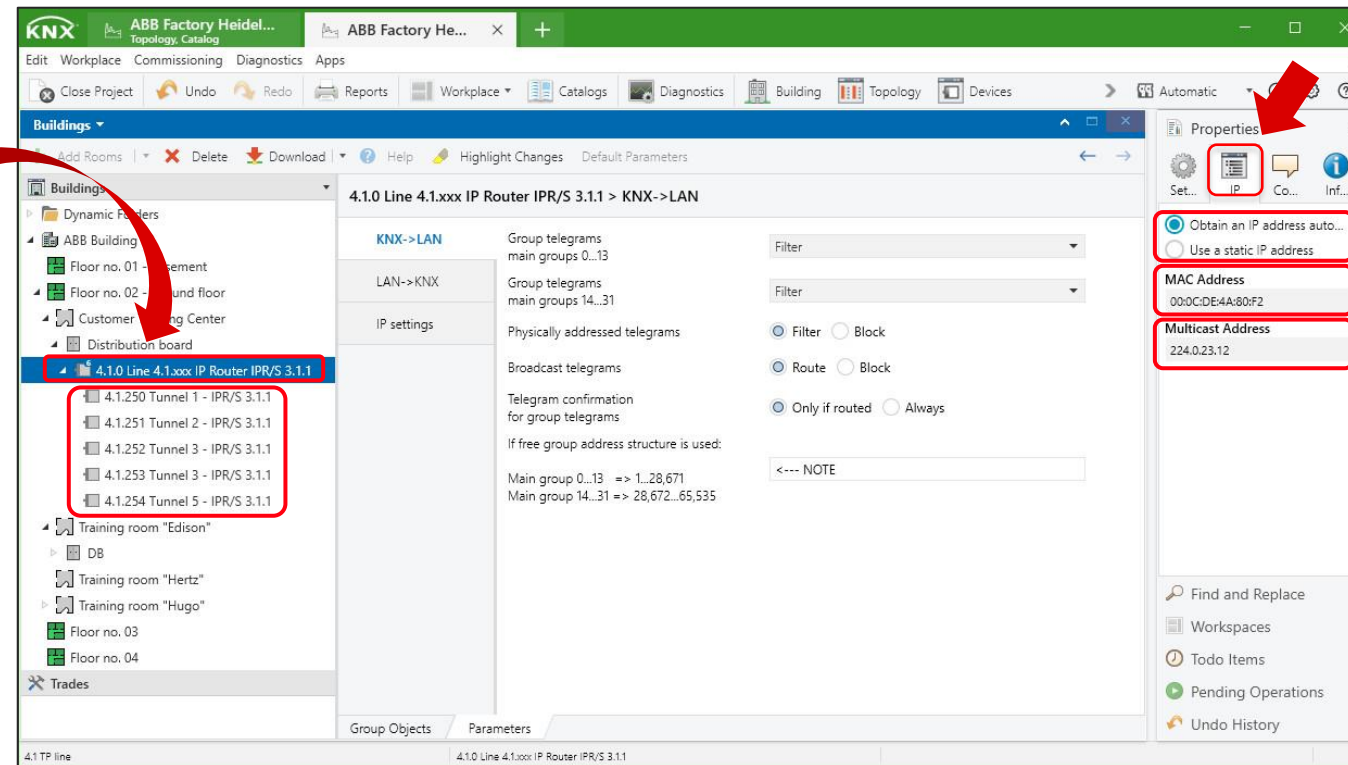
## IP Router IPR/S 3.1.1 (standard)

Total 6 Individual addresses



4.1.0 Individual address of IPR/S (Coupler)

5 Tunneling Server e.g. 4.1.250 – 4.1.254:  
→ 5 additional addresses (local) for the tunneling server (Interface)



Automatic IP assignment (DHCP/AutoIP) or static/fixed IP address

MAC address (will be displayed after the first download)

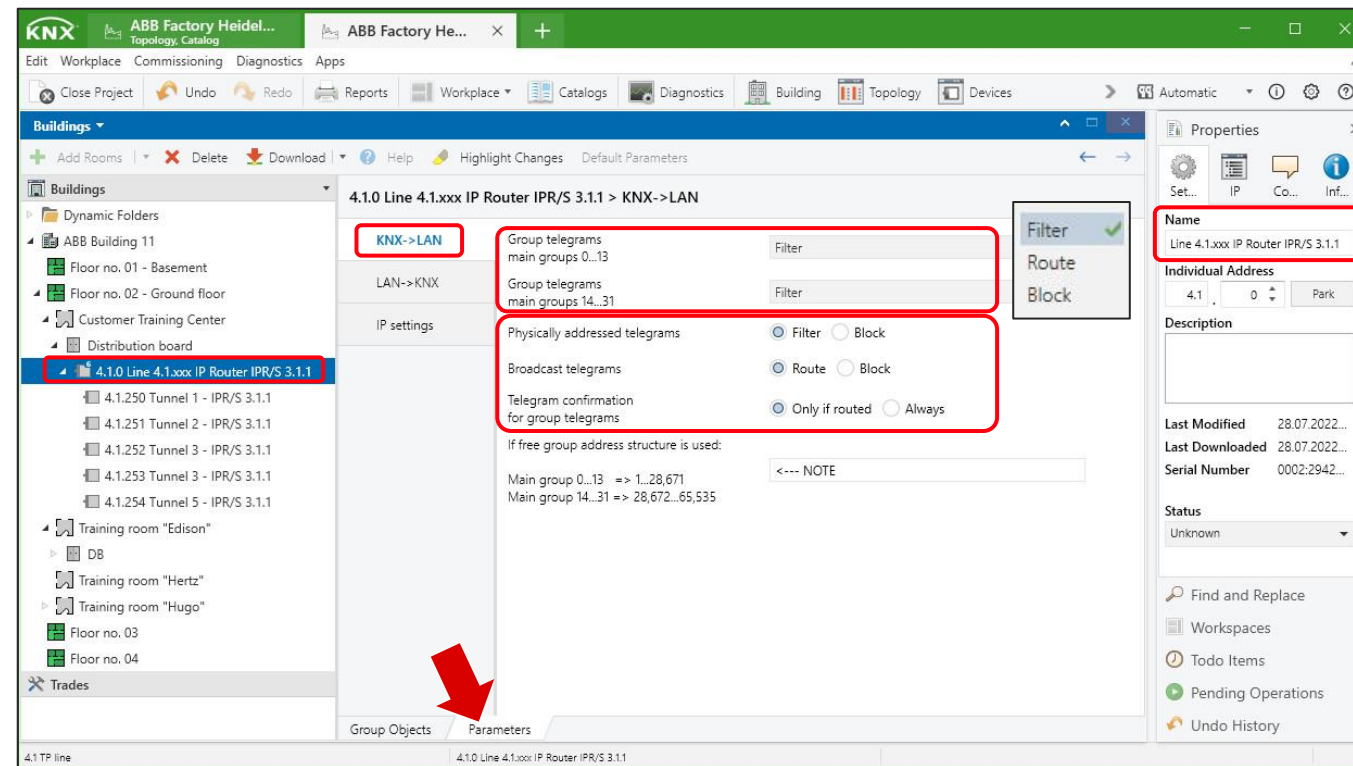
Multicast address 224.0.23.12



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router IPR/S 3.1.1 (standard) – ETS Parameter “KNX → LAN”

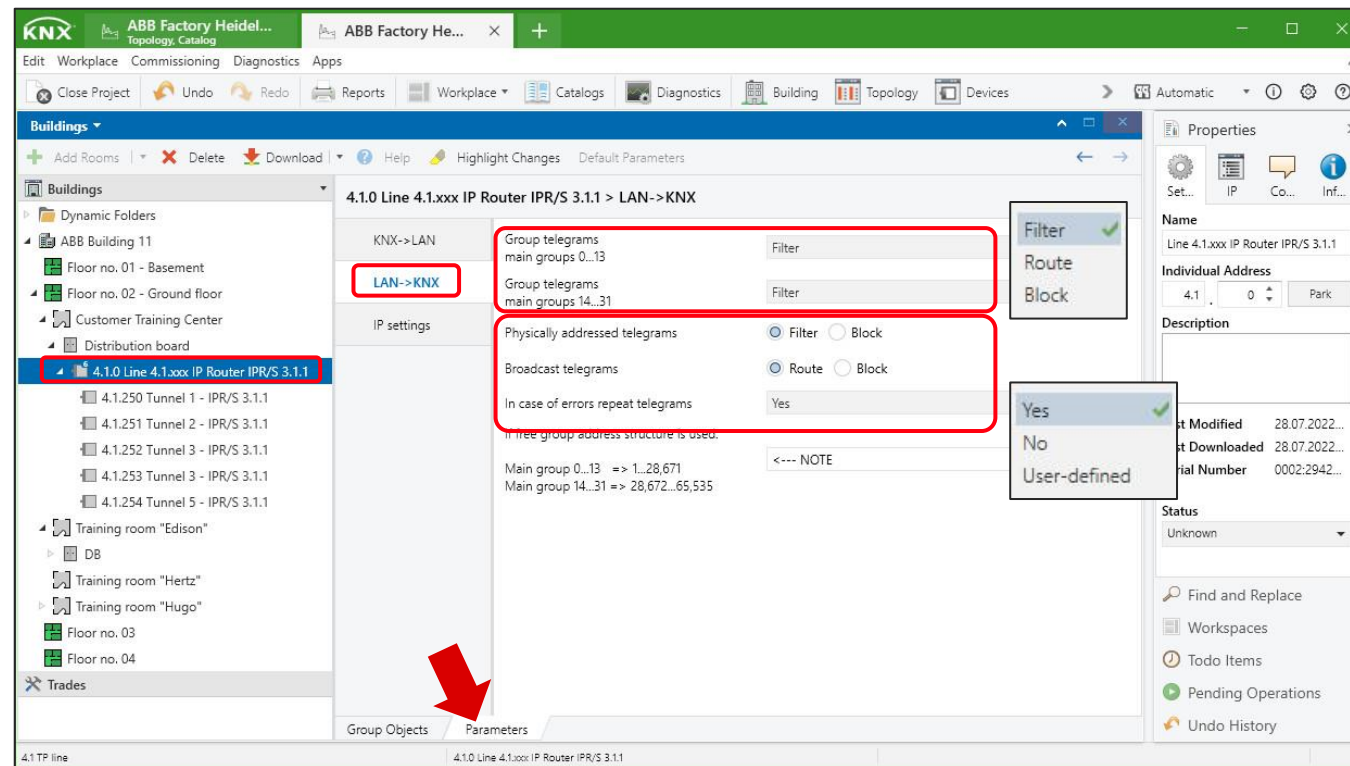


Name of the IP Router is downloaded into the device

# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

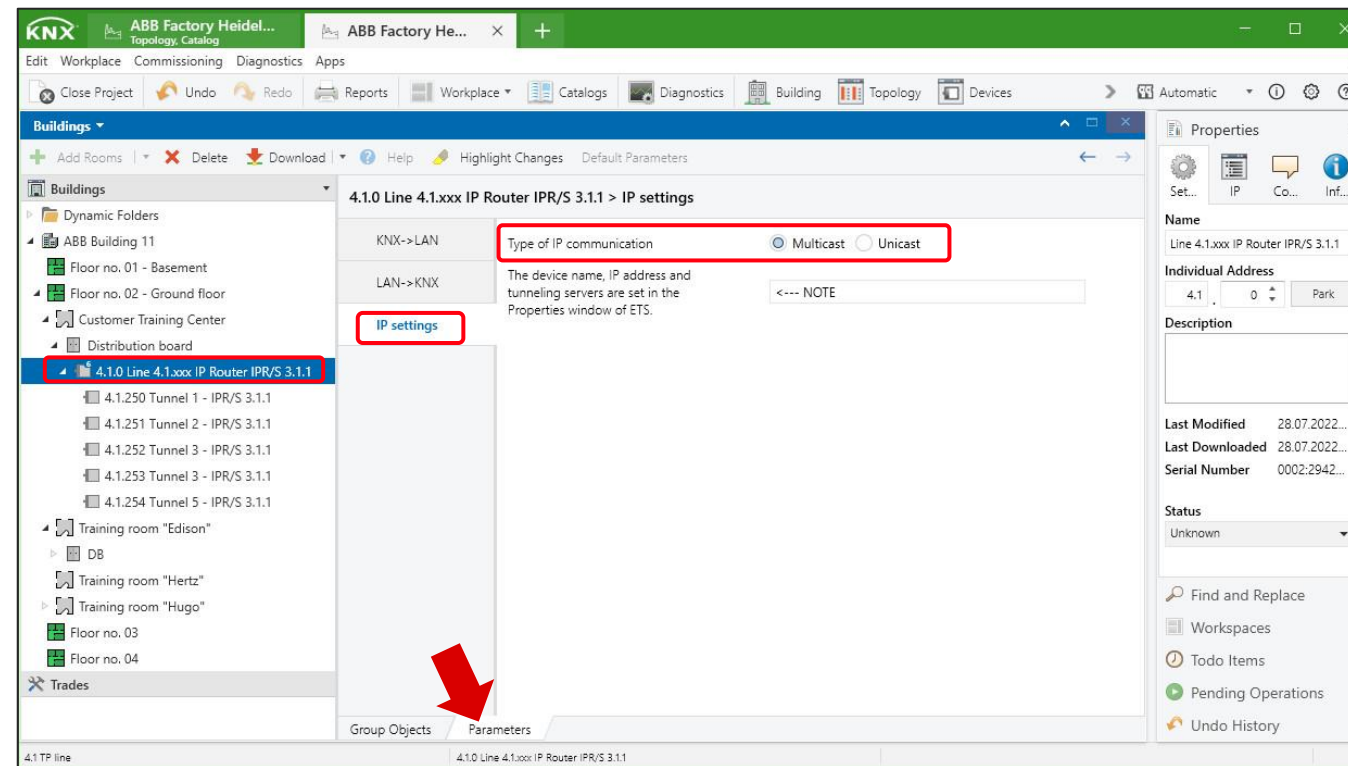
## IP Router IPR/S 3.1.1 (standard) – ETS Parameter “LAN → KNX”



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router IPR/S 3.1.1 (standard) – ETS Parameter “IP Settings”



Unicast Communication  
→ Solution if Multicast  
is not possible  
(a group of max. 10 IP  
Router)

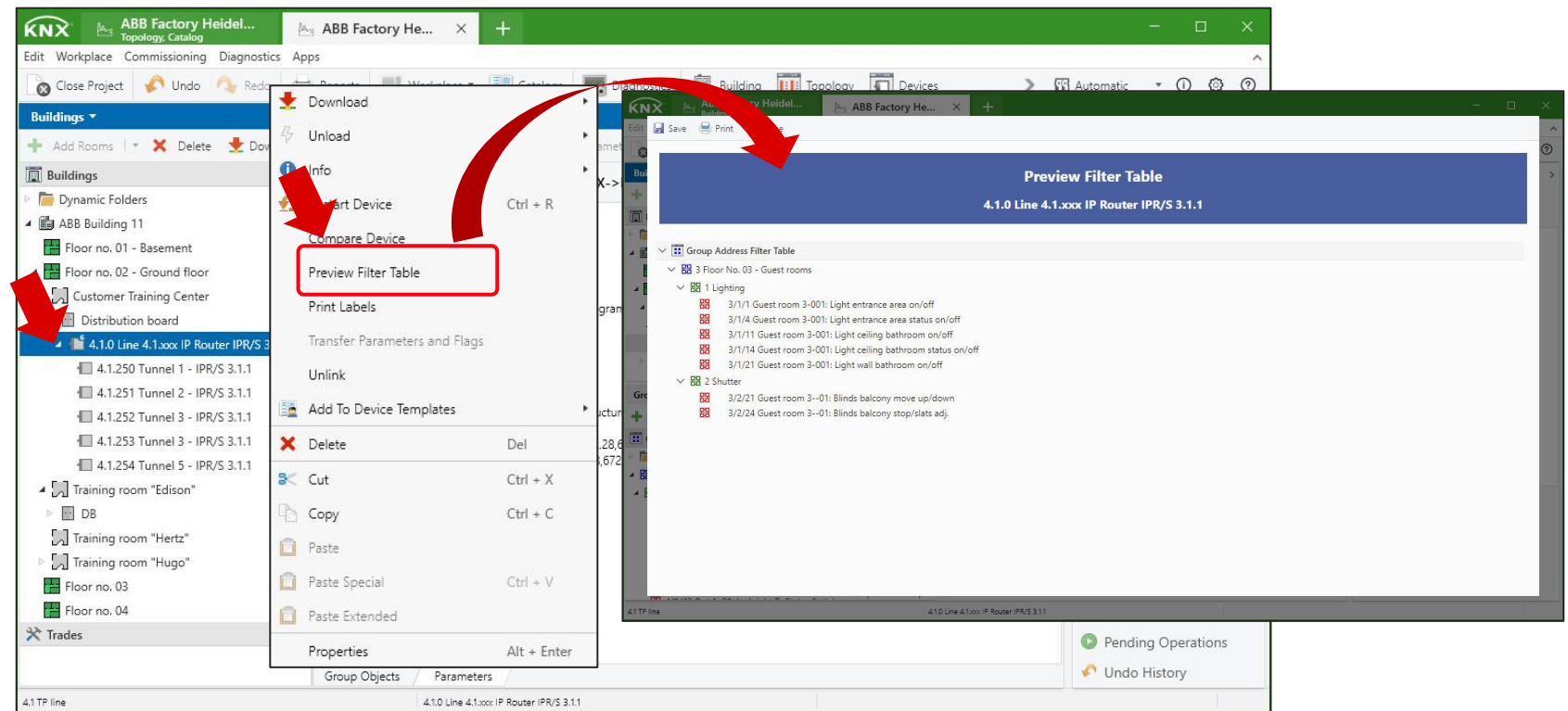
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router IPR/S 3.1.1 (standard) – ETS “Preview Filter Table”

Filter table (group addresses) is calculated automatically by the ETS

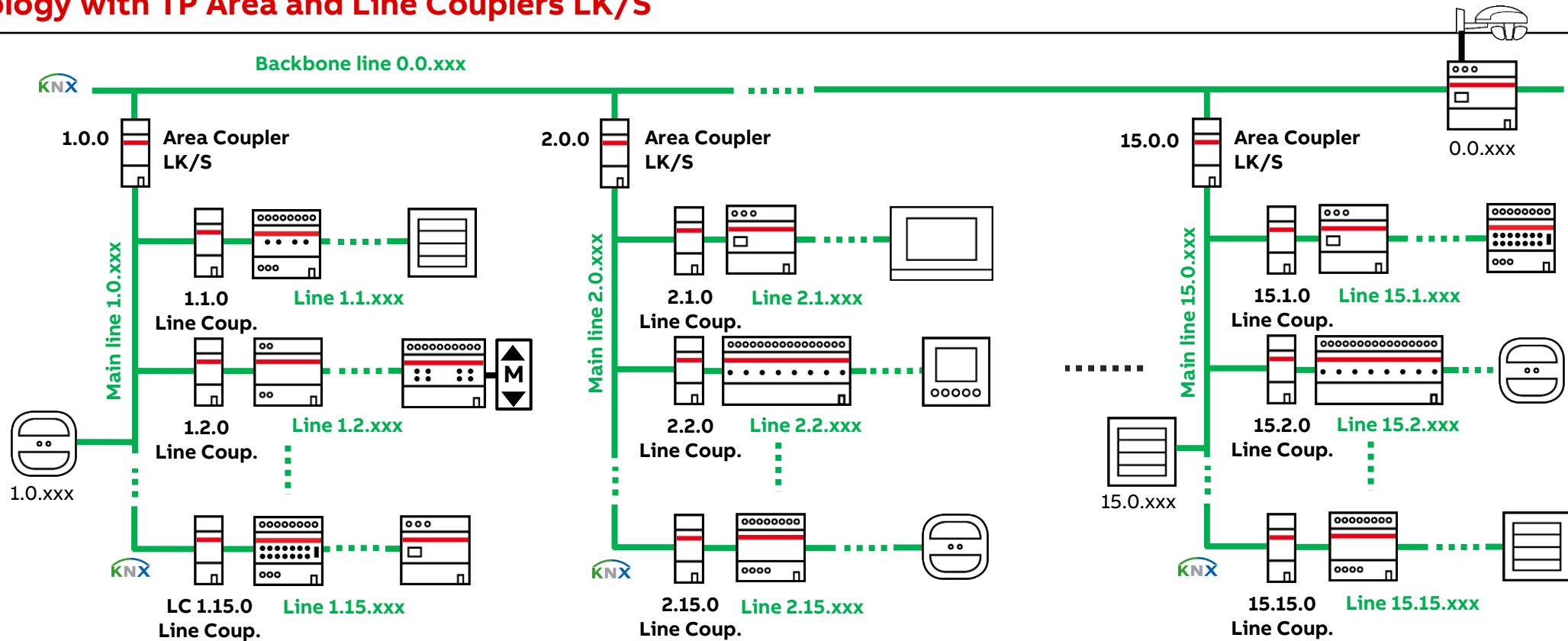
The filter table can be displayed by right-clicking on the IP Router



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

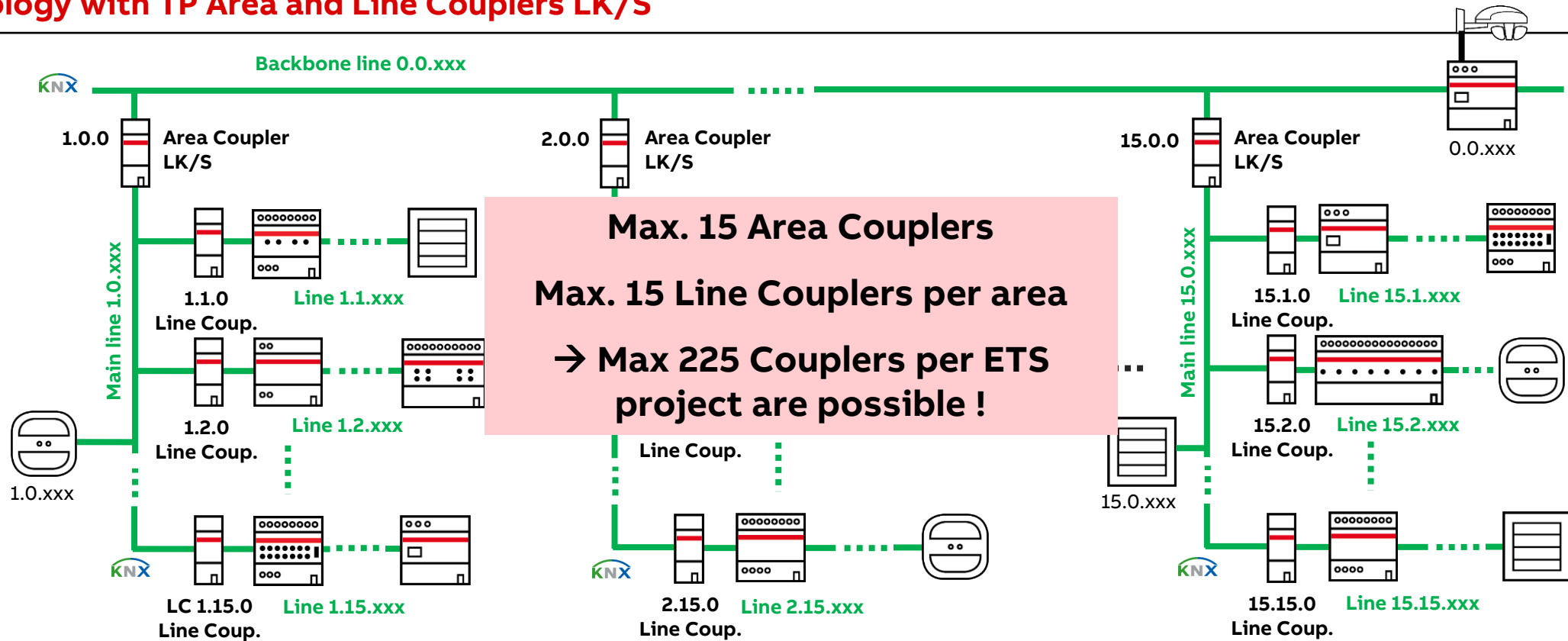
## Topology with TP Area and Line Couplers LK/S



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

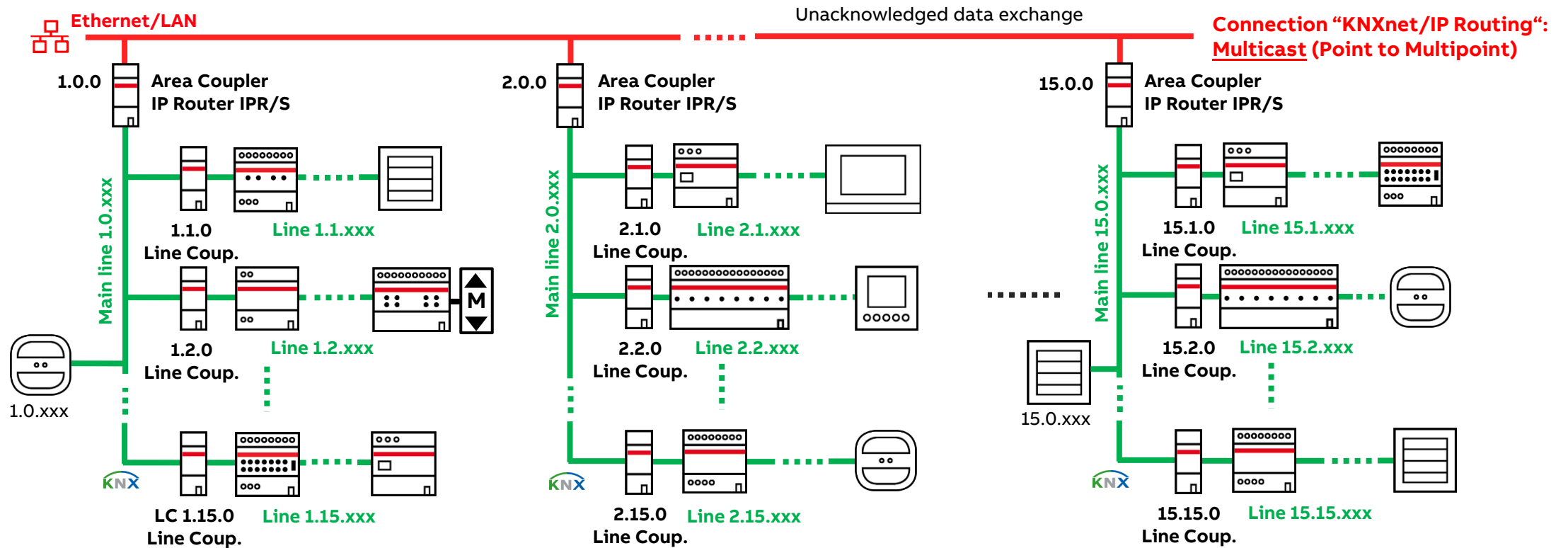
## Topology with TP Area and Line Couplers LK/S



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Topology with IP Router IPR/S as Area Coupler and TP Line Couplers LK/S

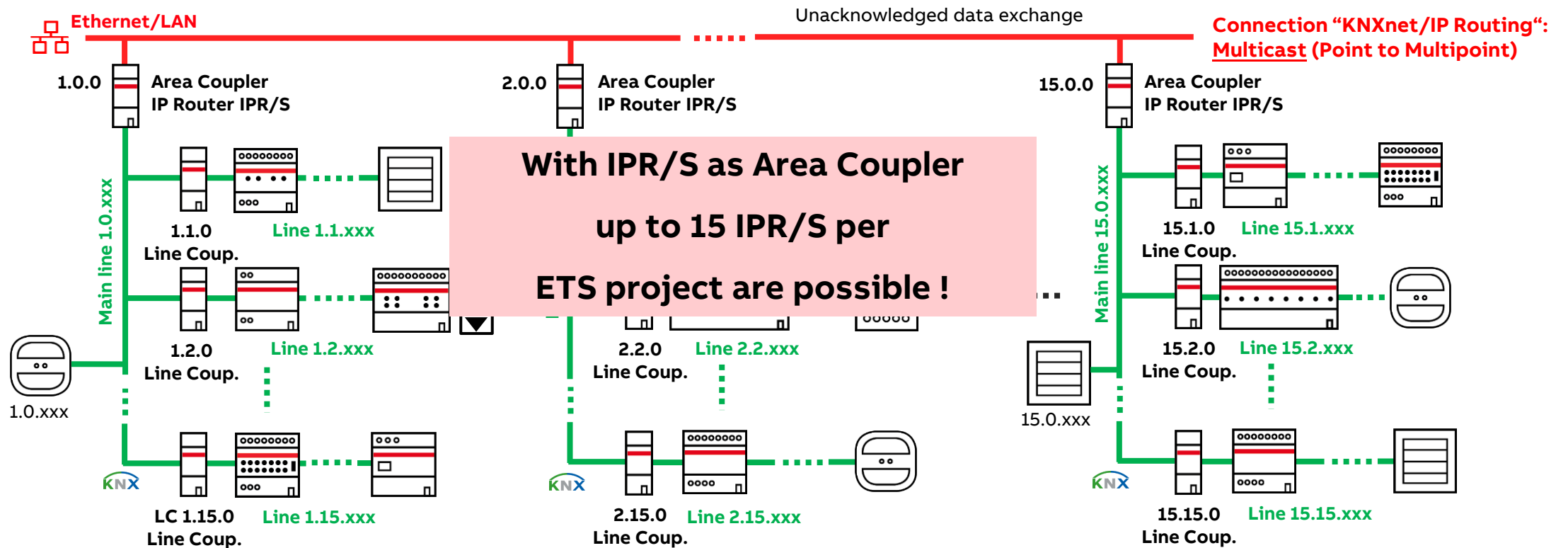




# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

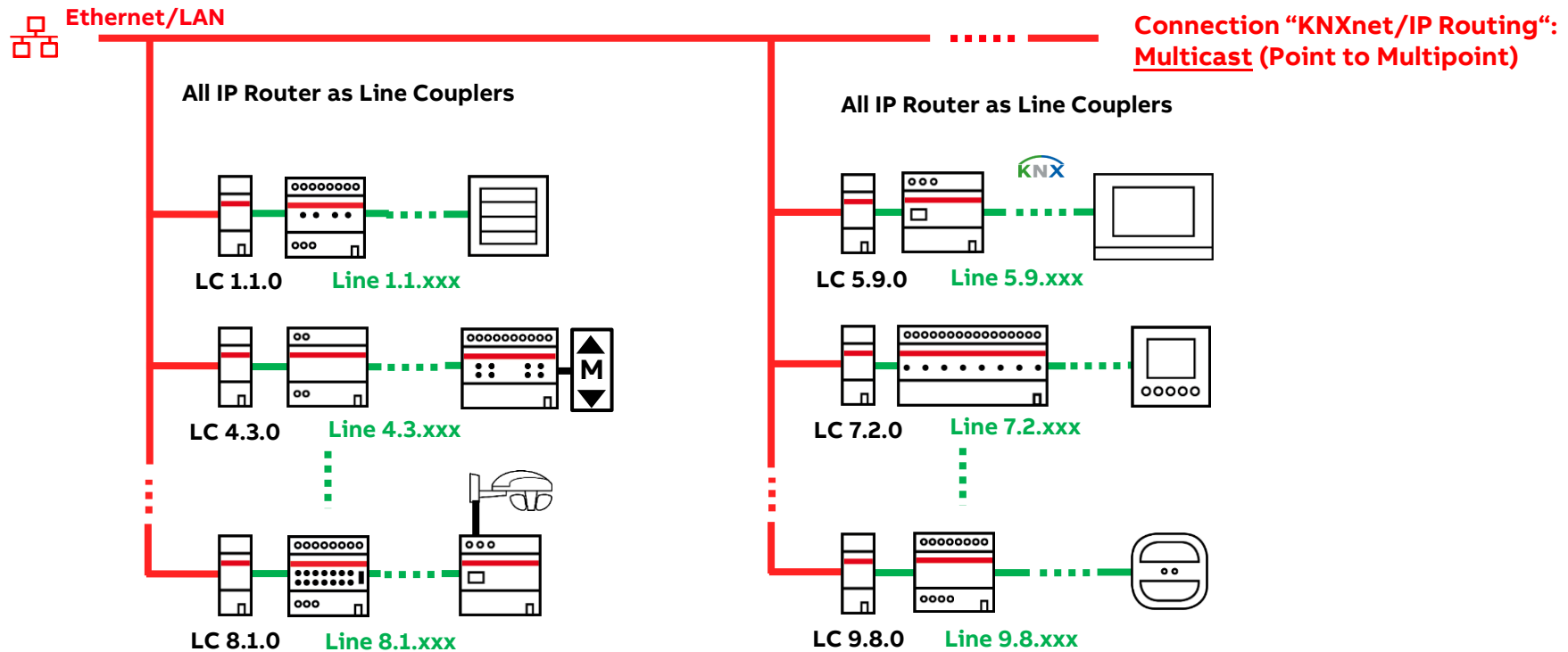
## Topology with IP Router IPR/S as Area Coupler and TP Line Couplers LK/S



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

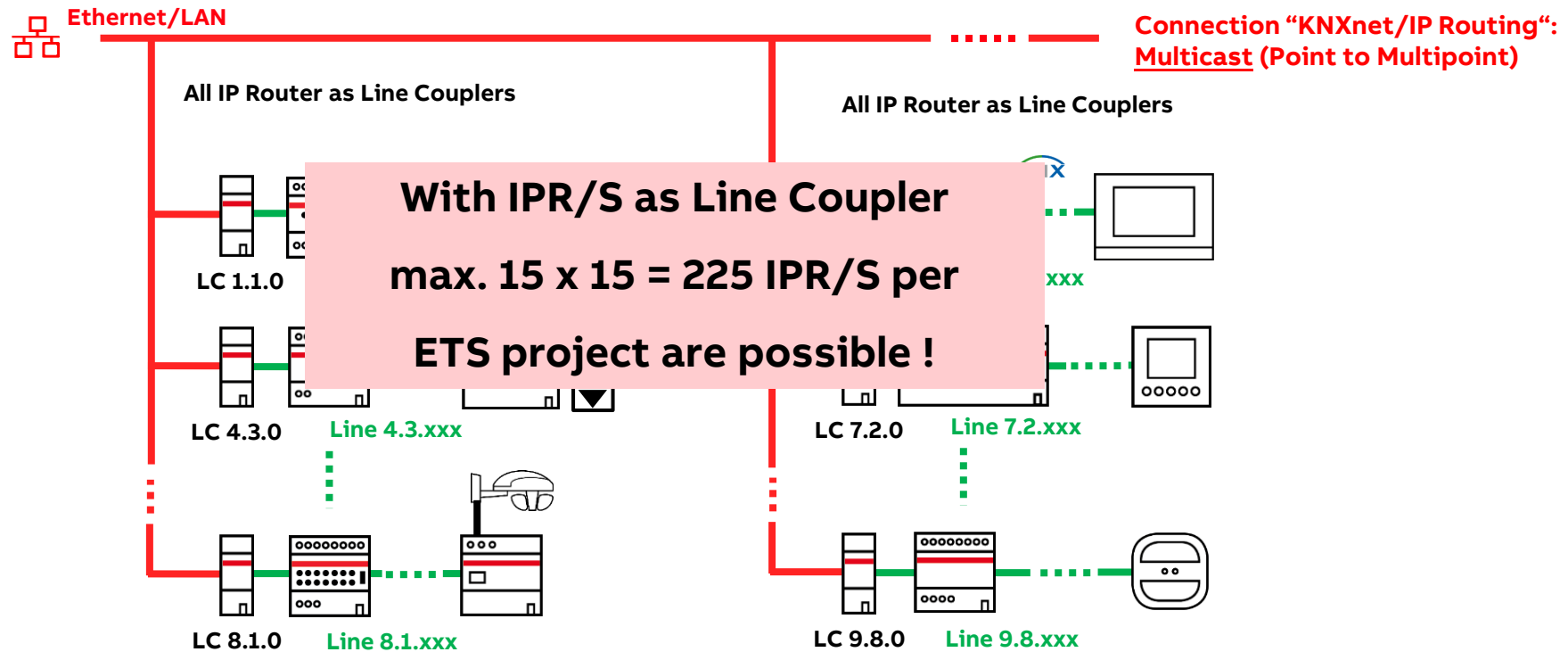
**Topology only with IP Router IPR/S as Line Coupler – no Area Couplers!**



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

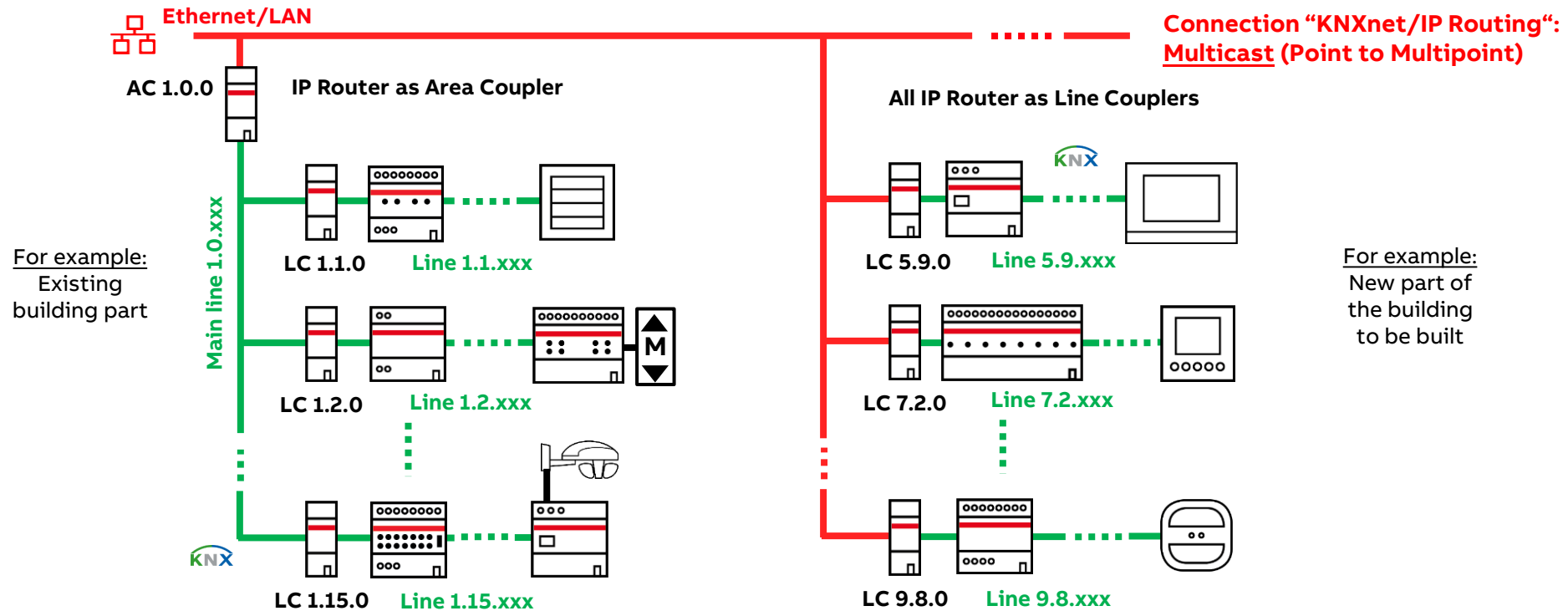
**Topology only with IP Router IPR/S as Line Coupler – no Area Couplers!**



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

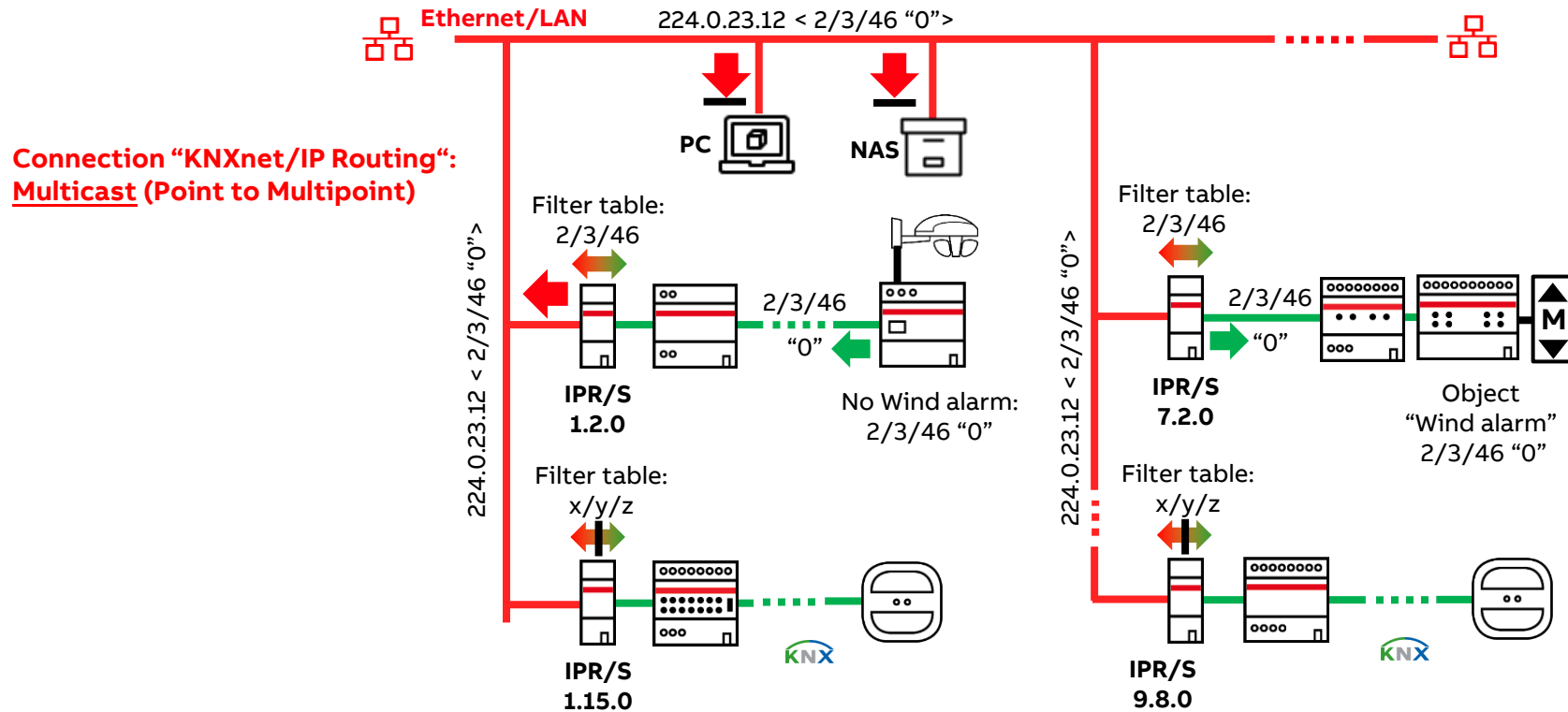
## Mixed Topology with IP Router IPR/S as Area Coupler and Line Couplers



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router: Routing → Coupler

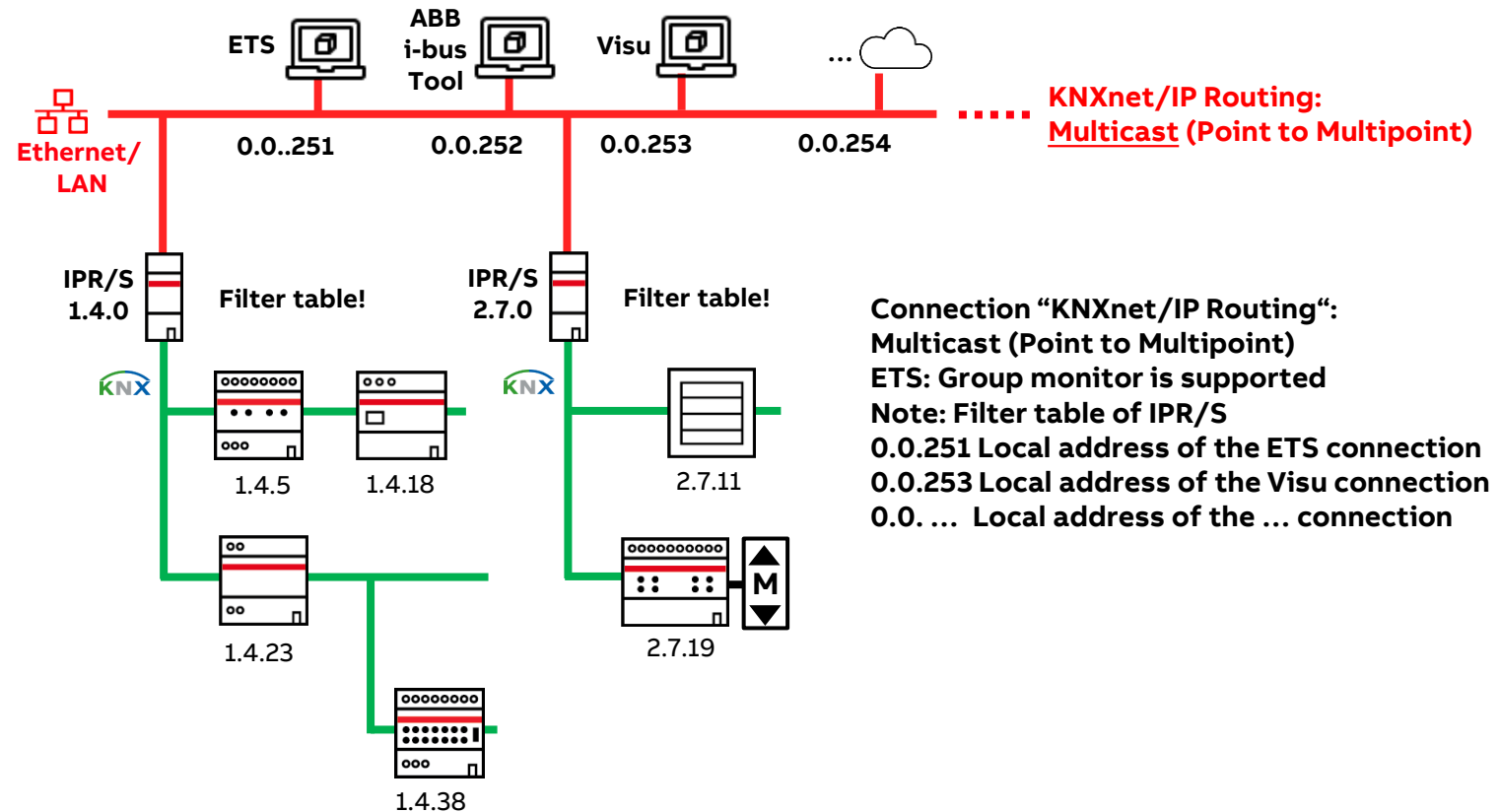


# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router: Routing → Interface

- Additional routing interface “KNXnet/IP Routing”
  - Working with ETS (download, diagnostics,...)
  - Access from the ABB i-bus® Tool
  - Connection to a visualization, etc.
- Communication via IP network!
  - Sending and receiving of KNXnet/IP multicast telegrams on the network
- Note: Filter table of IPR/S
  - Recommendation: Use of tunneling server instead of routing interface



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router: Routing → Interface – Setting up a routing connection in the ETS

The screenshot shows the ETS (Energy Management System) interface. The 'Devices' list on the left contains various IP devices. The 'Local Interface Settings' dialog box is open, showing the 'Ethernet 3' interface. The 'Individual Address' field is highlighted with a red box, and a red arrow points to it from the 'Ethernet 3' entry in the 'Devices' list. The 'Individual Address' field contains the value '0.0.255'. A green message below the field states: 'The individual address 0.0.255 is not used by another device.' The 'Multicast Address' field contains '224.0.23.12' and the 'MAC Address' field contains '3C:E1:A1:B6:CE:D0'.

IP Routing

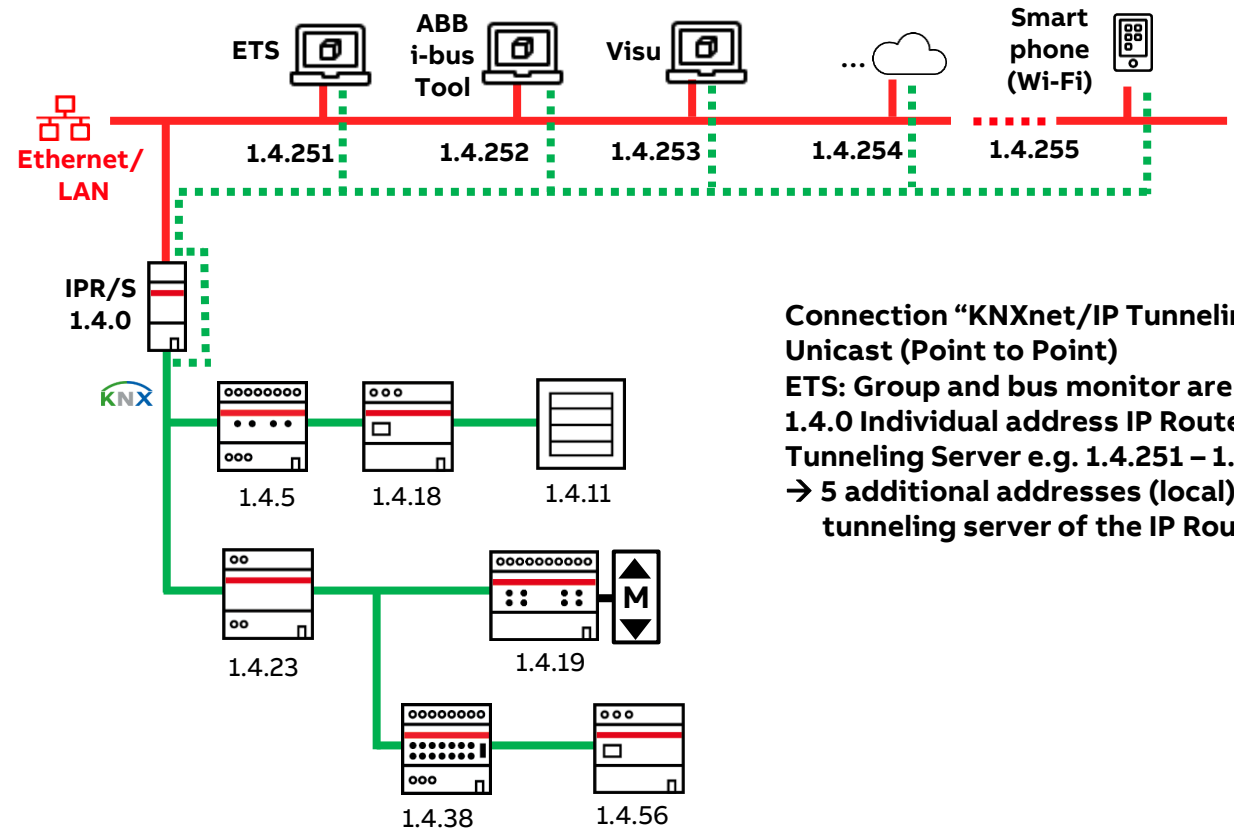


# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router: Tunneling → Interface

- Furthermore, the 5 tunneling server can be used in parallel for
  - Working with ETS (download, diagnostics, group and bus monitoring, ...)
  - Access from the ABB i-bus® Tool
  - Connection to a visualization, etc.→ Built in “IP Interface IPS/S”
- Setting up a tunnel connection in the ETS:  
See chapter “IP Interface IPS/S”



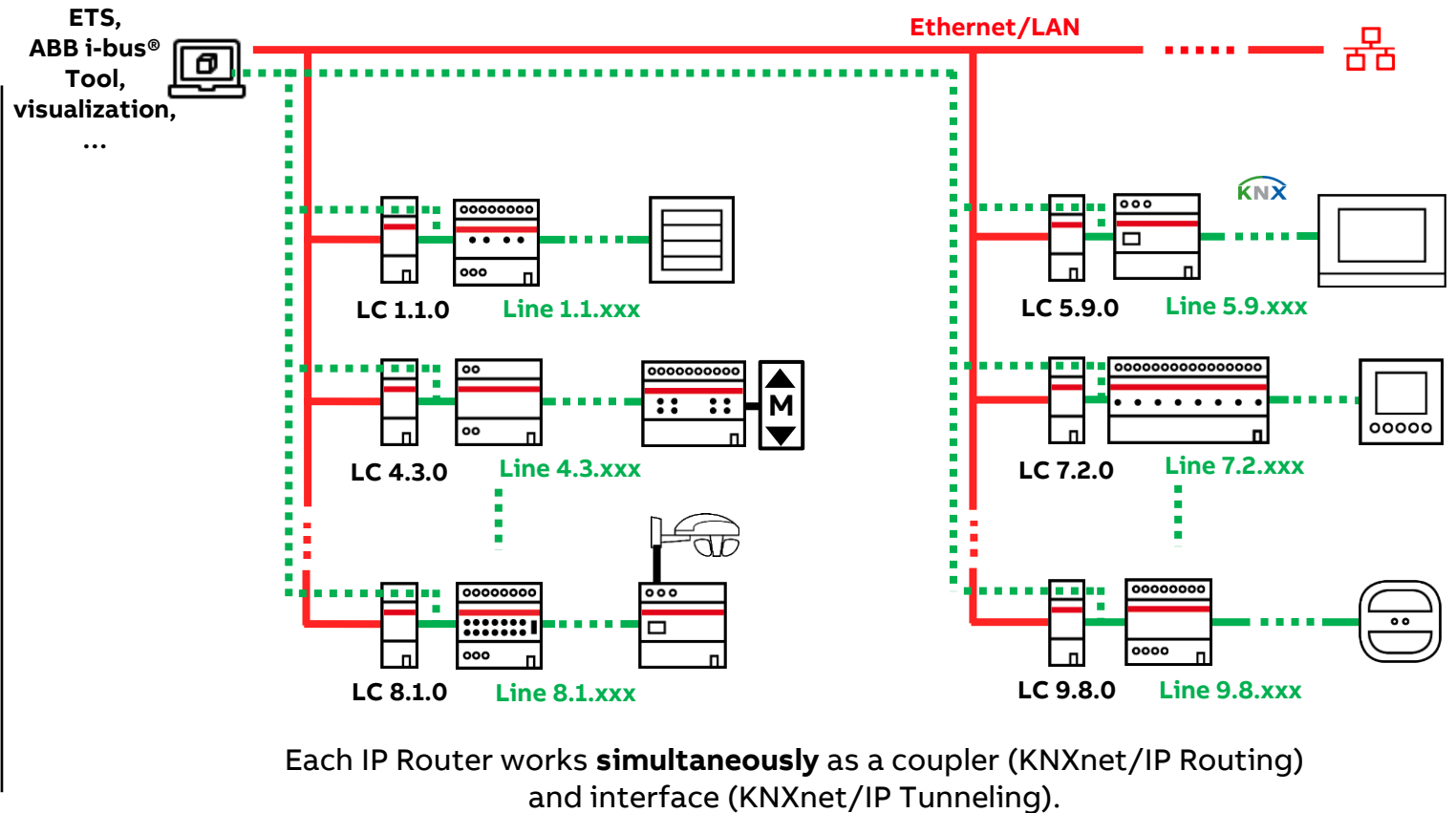
Connection “KNXnet/IP Tunneling“:  
Unicast (Point to Point)  
ETS: Group and bus monitor are supported  
1.4.0 Individual address IP Router  
Tunneling Server e.g. 1.4.251 – 1.4.255:  
→ 5 additional addresses (local) for the  
tunneling server of the IP Router

# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router: Tunneling → Interface

- Furthermore, the 5 tunneling server can be used in parallel for
  - Working with ETS (download, diagnostics, group and bus monitoring, ...)
  - Access from the ABB i-bus® Tool
  - Connection to a visualization, etc.
- A tunnel connection must be created in the ETS, ABB i-bus® Tool, visualization for each IP Router IPR/S, e.g.
  - Tunnel connection to line 1.1.xxx via tunneling server 1.1.251 of IPR/S 1.1.0
  - Tunnel connection to line 4.3.xxx via tunneling server 4.3.251 of IPR/S 4.3.0
  - Tunnel connection to line 8.1.xxx via tunneling server 8.1.251 of IPR/S 8.1.0
  - Tunnel connection to line ...



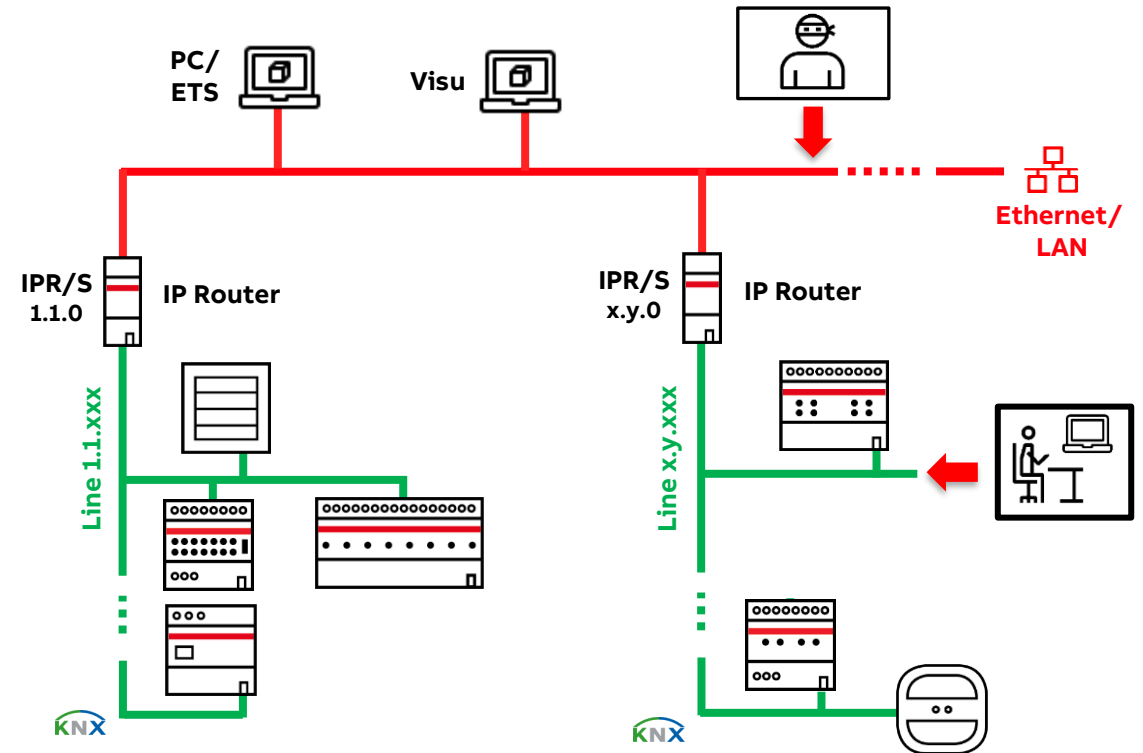
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router Secure IPR/S 3.5.1

### Situation

- The most relevant attack scenario on a KNX installation is over the IP network
- But access over TP is of course also possible and relevant for Building Automation



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router Secure IPR/S 3.5.1

### Threat scenarios

#### IP network

- Local (Wi-Fi/LAN)
  - Often no separate technical network; therefore, users have direct access to IP communication
- Remote access / Internet:
  - Network Routers are often “open” visible on the Internet
  - High number of potential attackers

#### Fieldbus

- Private housing
  - KNX cable outside the building
- Commercial buildings
  - Access to the bus via any node (especially in the hotel)



---

# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Attack types (examples)

---

Denial of Service Attack (DOS)

- Telegram flood on KNX (IP) device, as a result the device is temporarily unavailable

Doing unwanted functions

- Driving blinds, switching lights, ...

Sabotage

- Change set points, reprogram devices, short circuit bus

Espionage

- Spying on user profiles

Deceive, intrusion

- Opening a door, disabling/unset security systems

## Impacts

---

Possible impacts

- Image damage (manufacturer, system integrator, end customer)
- Data loss
- Reduction of comfort
- Security loss
- Economic damage

→ There are already ways to prevent / significantly hinder access to the system

→ Due to the current enhancements of the KNX standard ("KNX Secure"), additional security mechanisms are possible

→ KNX Secure alone does not make the system secure!

# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## The “entire chain” must be taken into account

### Manufacturer

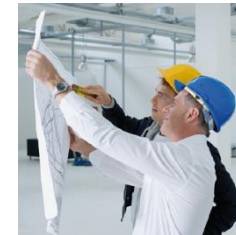
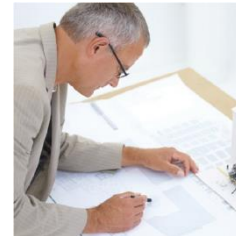
- (Product) security standards (cyber security, robustness), updates
- Specification of standards (KNX Secure)
- Provision of checklists, training, ...

### System integrator, installer

- Safety concept for planning, installation and operation
- Risk analysis

### End customer, operator of the building

- Access control, security concept
- IT security (current security settings ...)



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## General measures

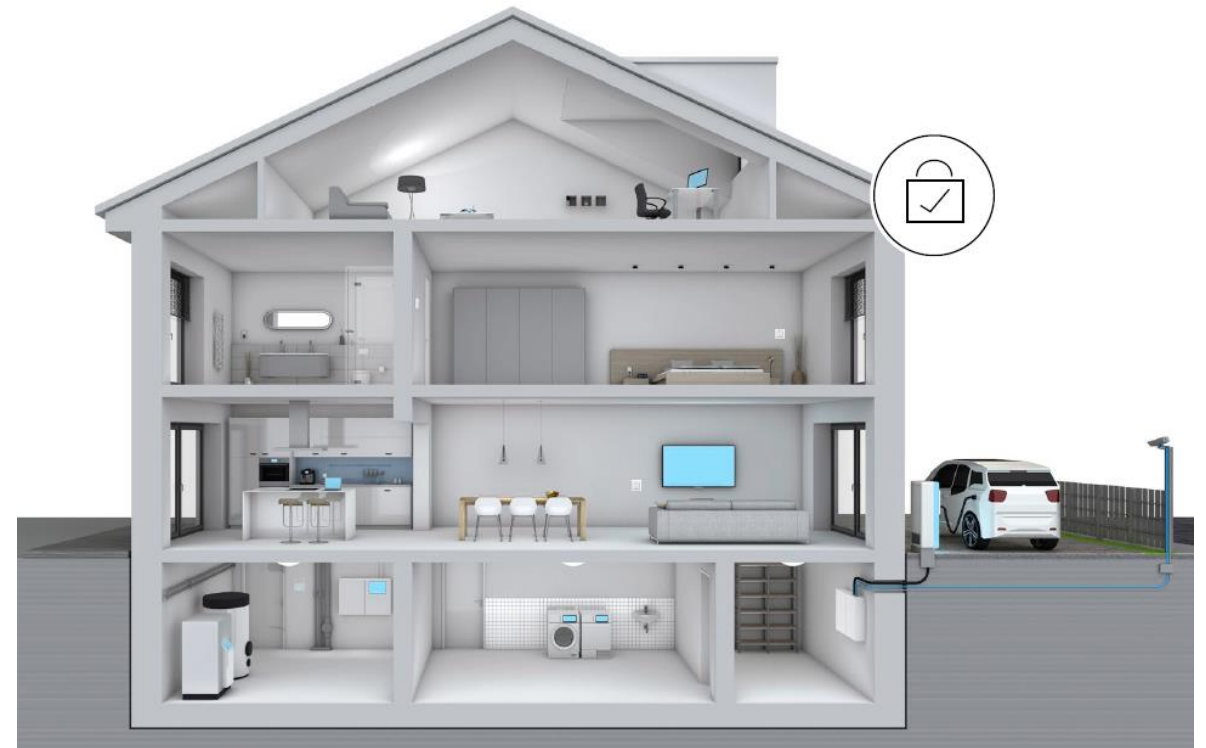
Cybersecurity must be an integral part of planning and execution a facility

Already it is possible to make access via IP (relatively) secure

- To the outside (firewall, VPN, filtering MAC addresses)
- Inside (separate technical IP network, encryption with Wi-Fi)

Prevent physical access to the bus

- Lockable distribution boards
- Devices with dismantling protection
- Separate lines for sensitive areas
- No KNX cable outside the building
- ...



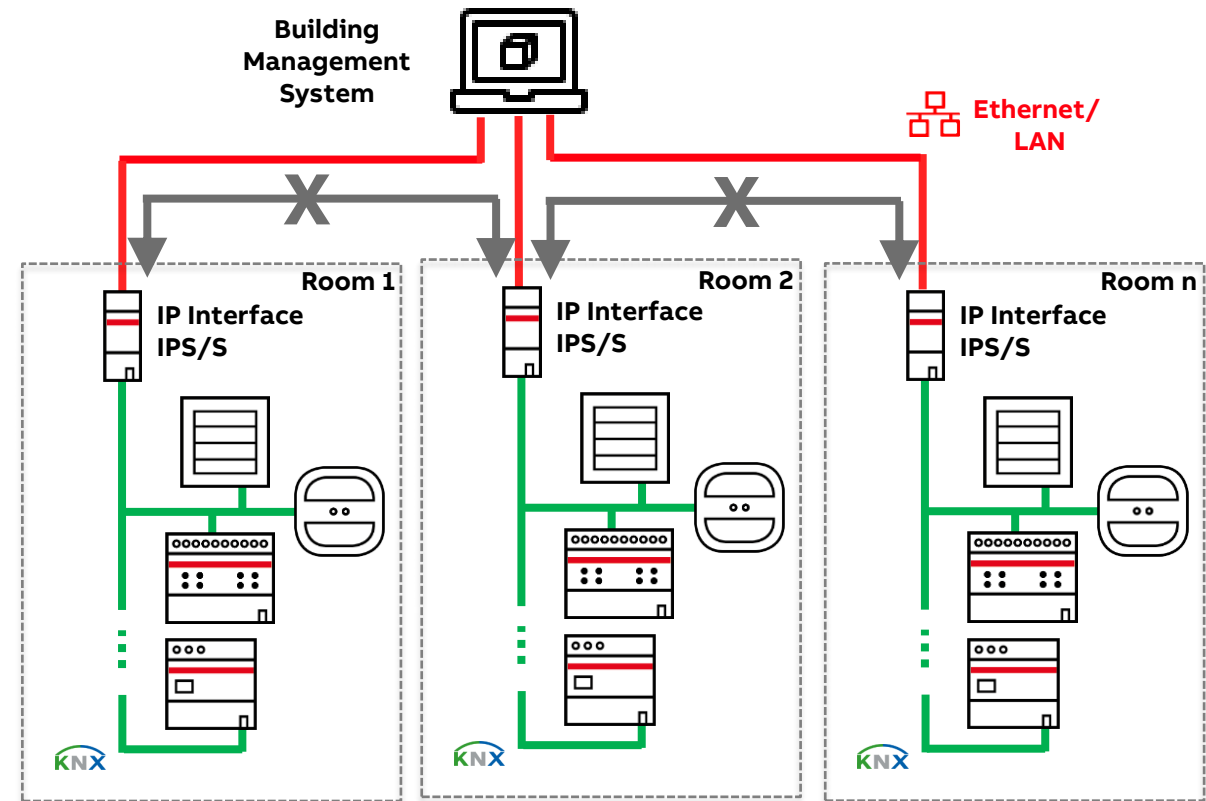


# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Special solution for the attack scenario from the field level

- Standard IP Interfaces connect hotel rooms with a central system (BMS Server)
  - Tunneling connection from each room to central BMS
  - Security by isolated rooms – no KNX Secure!
  - It covers the use case “Attack” from the field level
  - No direct inter-room communication available
  - BMS can also monitor the KNX field devices
- ABB “Hotel IP Link Bundle” HIL/S 20.1.1



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Special solution for the attack scenario from the field level

### ABB “Hotel IP Link Bundle” HIL/S 20.1.1

- The Hotel IP Link Bundle is consisting of a KNX IP Interface (IPS/S) and a KNX Power Supply (SV/S)
- The IPS/S supports the KNXnet/IP protocol (tunneling) from the KNX Association
- A central system (BMS server, visualization system, hotel management system) establishes a connection to each individual IP Interface IPS/S via the integrated tunneling server
- The SV/S generates and monitors the KNX system voltage for up to 20 KNX TP (twisted pair) devices via an integrated choke
- The additional 30 V DC voltage output is used to power the IPS/S 2.1
- Order number: 2CDG110237R0011



IP Link Bundle HIL/S 20.1.1

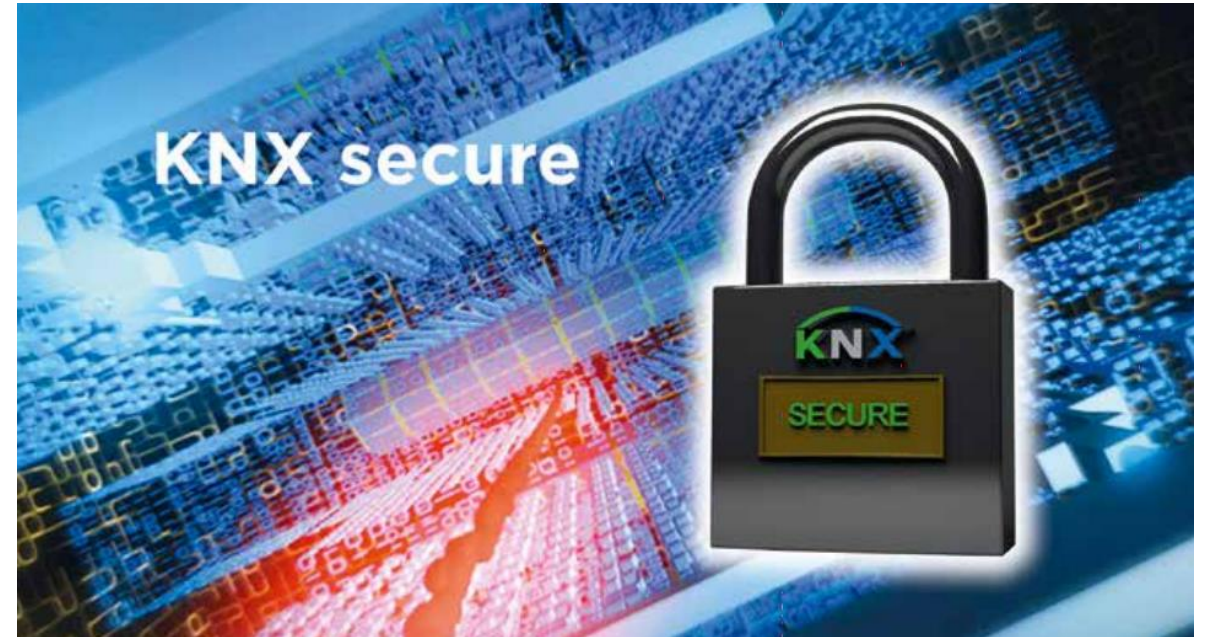
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Measure KNX Secure

KNX Secure has been developed to respond to the current and future challenges regarding cyber security in building automation

- Step 1: Securing the IP communication with “KNX IP Secure”
  - Implementation of the KNX IP Secure Standard in IP Routers, Interfaces and other IP devices
  - Software clients (visualizations) are also affected
- Step 2: Implementation of “KNX Data Secure” in all field devices



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## KNX Secure offers maximum protection

- Home and building automation with KNX is secure
- KNX Secure guarantees maximum protection
  - KNX IP Secure extends the IP protocol in such a way that all transferred telegrams and data are completely encrypted
  - KNX Data Secure effectively protects user data against unauthorized access and manipulation
- The KNX technology is standardized according to EN 50090-4-3, which means that KNX successfully blocks hacker attacks on the digital infrastructure of networked buildings
- Thus minimizing the risk of digital break-ins
- Moreover, KNX Secure meets the highest encryption standards (according to ISO 18033-3, such as AES 128 CCM encryption) in order to effectively prevent attacks on the digital infrastructure of buildings and to achieve the highest level of data protection

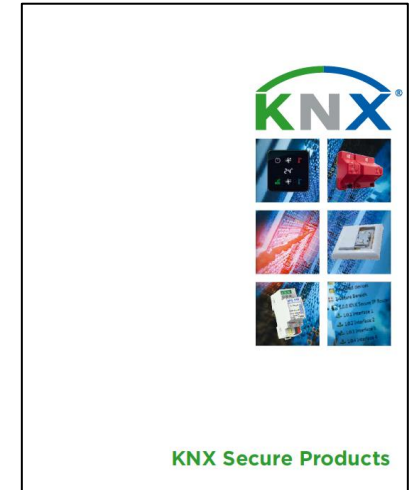


# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## KNX Secure Brochures of the KNX Association

- KNX Secure Checklist
- KNX Secure Guide
- KNX Secure Products
- <https://knxsecure.knx.org>





---

# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Conclusion

- There is no 100% security
- Manufacturers, KNX Association, associations and the system integrators are pushing the issue of safety to make the building (even) safer
- Safety, comfort and economy have to be balanced against each other
- In each project, it must be weighted how much security is necessary
- The entire lifecycle of a building must be taken into account
- Integrators with the appropriate know-how have a competitive advantage and should use it



Elbphilharmonie (Hamburg)  
Concert hall/Stadiums and recreation

# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router Secure IPR/S 3.5.1

The ABB IP Router Secure IPR/S 3.5.1 has the same properties (ETS parameter, filter table, ...) as the IP Router IPR/S 3.1.1 standard

- Routing of telegrams  
→ connection of KNX Lines and Areas over IP network
- Support of full filter table for all main groups 0...31  
→ no restrictions for usage of the extended group address range
- Power over Ethernet (PoE)  
→ no additional power supply or 12...30 V DC
- ABB i-bus® Tool support  
→ easier commissioning and diagnostics
- Unicast communication  
→ solution if Multicast is not possible
- 5 Tunneling Servers  
→ parallel access, less hardware





# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router Secure IPR/S 3.5.1

**The ABB IP Router Secure is a KNX device according to the KNX Secure Standard (KNXnet/IP Security)**

- The communication on the IP network is secure
  - All KNX IP Secure devices must support the KNXnet/IP security protocol
- ETS6 or ETS5 (5.7.4 or higher), the current version of the device application and firmware are required for programming
- The device should always be operated in KNX Secure mode
  - This ensures security for the tunneling servers
- The device can be safely put into operation
- All five tunnel connections can be used together encrypted or unencrypted
- Firmware update with ABB i-bus® Tool, available updates should be loaded into the device promptly



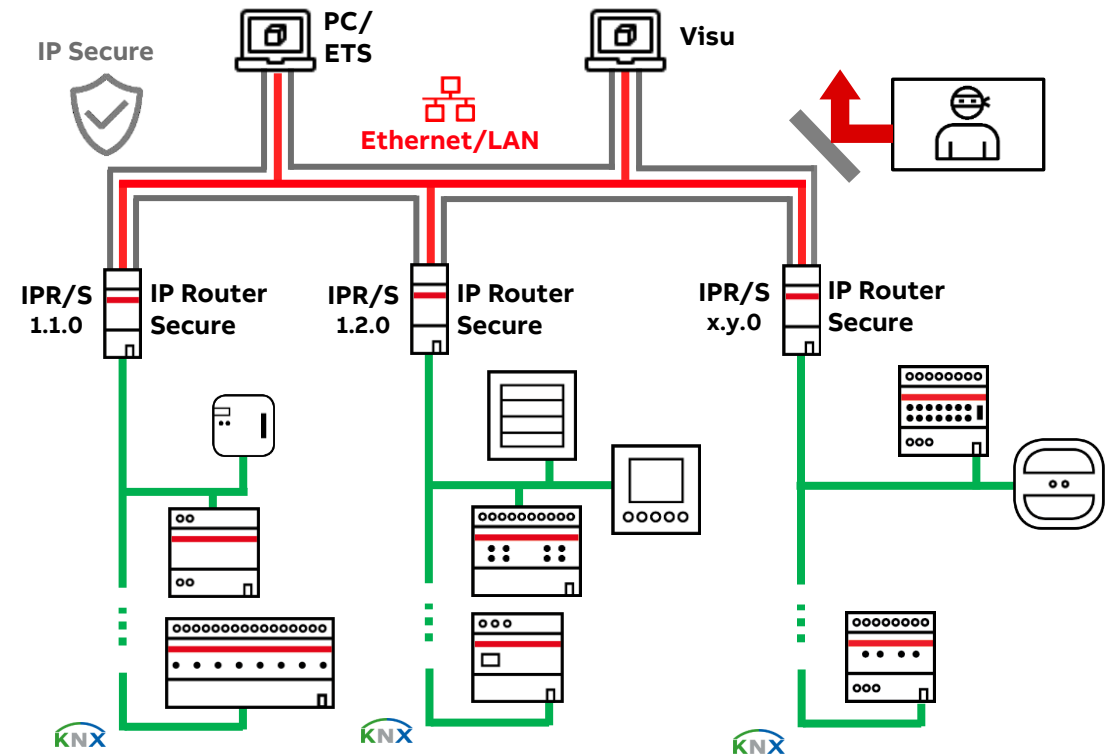
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router Secure IPR/S 3.5.1

### KNX IP Secure (KNXnet/IP Secure Routing and Tunneling)

- TP Telegrams are wrapped in a secure frame on IP
- Tunneling connections are secure
- All IP devices in a project have to speak secure



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router Secure IPR/S 3.5.1 – Commissioning

- When commissioning a KNX secure device (first download) a commissioning key – “Device Certificate” – is required
- The “Device Certificate” consists of
  - FDSK = Factory Default Setup Key
  - Serial number of IP Secure device
- ABB secure devices:  
The “Device Certificate” is placed on a sticker on the left side of the device and must be imported into the ETS
- One sticker can be used for project documentation, the other can be left on the device



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router Secure IPR/S 3.5.1 – Commissioning

- The “Device Certificate” is only required for initial commissioning
- After that, the ETS creates new “Tool Keys”
- The “Tool Keys” are transferred via the bus with encryption based on FDSK to the IP Router
- Further device configuration is encrypted based on the “Tool Key”
- The FDSK is only needed again after a device reset to factory settings



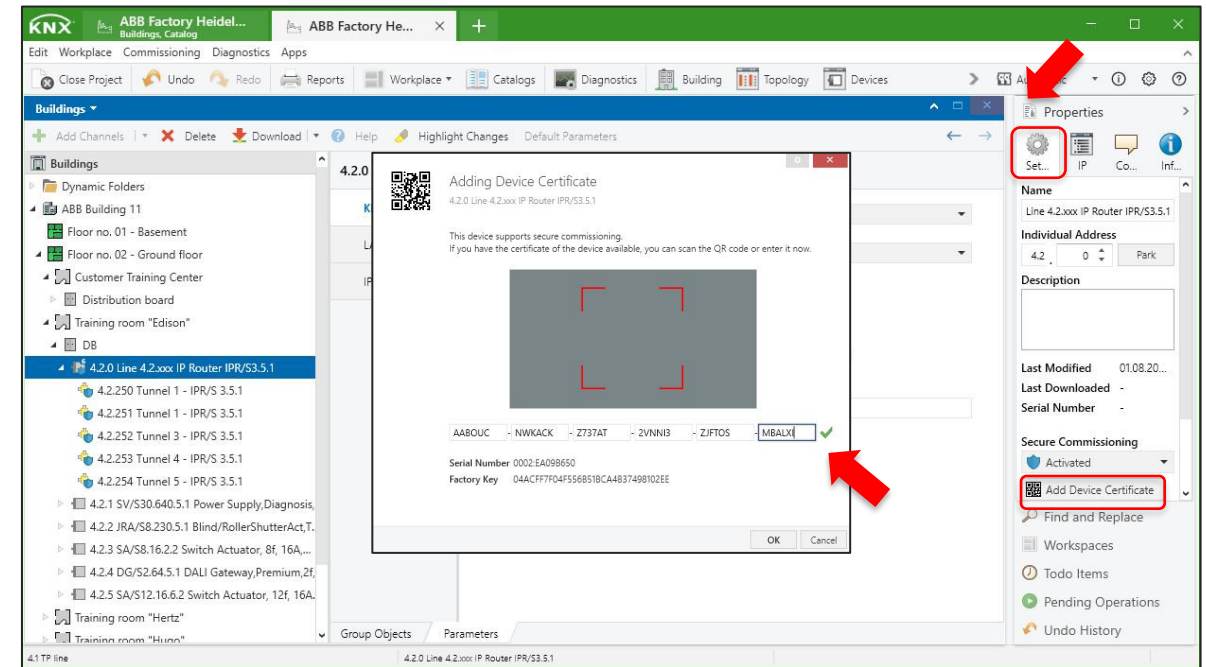
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router Secure IPR/S 3.5.1 – Commissioning

How to enter the “Device Certificate”?

- When inserting a KNX Secure device, you will be asked for it
- The ETS asks for the key when programming for the first time
- Click on “Add Device Certificate”
  - Properties → Settings → Selected device
  - ETS main menu “Security”
- The reading can be done offline
- The keys are assigned automatically to the IP Router Secure by ETS



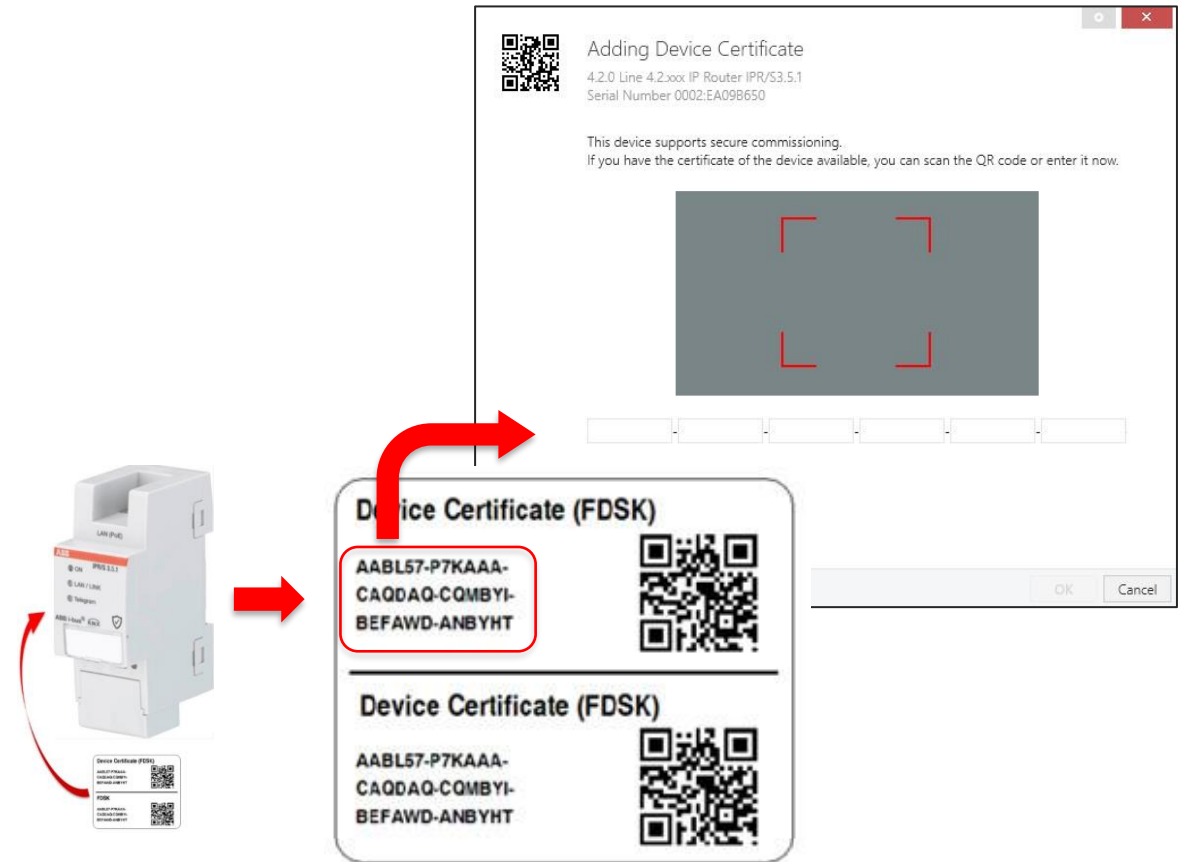
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router Secure IPR/S 3.5.1 – Commissioning

How to enter the “Device Certificate”?

- The key can be
  - Entered via the keyboard
  - Read in with a QR code scanner
  - Read with the webcam of laptop

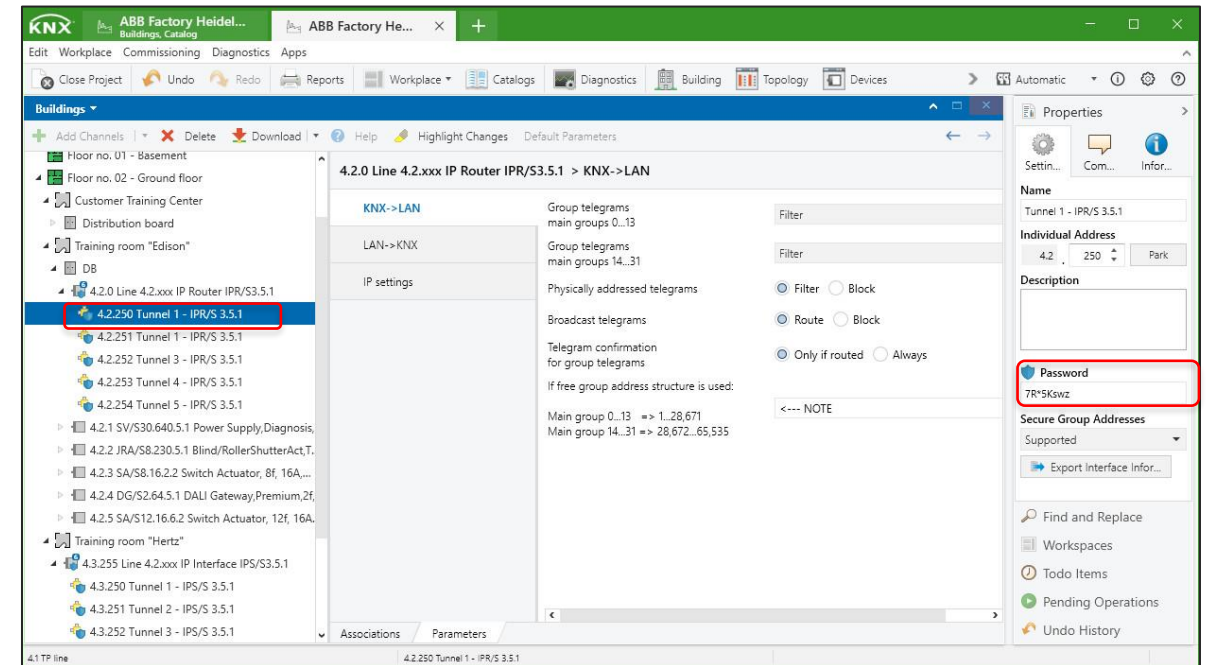


# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router Secure IPR/S 3.5.1 – Commissioning

- The ETS generates separate passwords for each tunneling server
- The passwords of the tunneling server can be changed if necessary
- A tunnel address can be passed to a client (e.g. BMS or Visu) with the password
- The keys are generated and managed by the ETS
- If necessary, keys and passwords can be exported





# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Situation 1 – Attack over the IP network

### No IP Secure

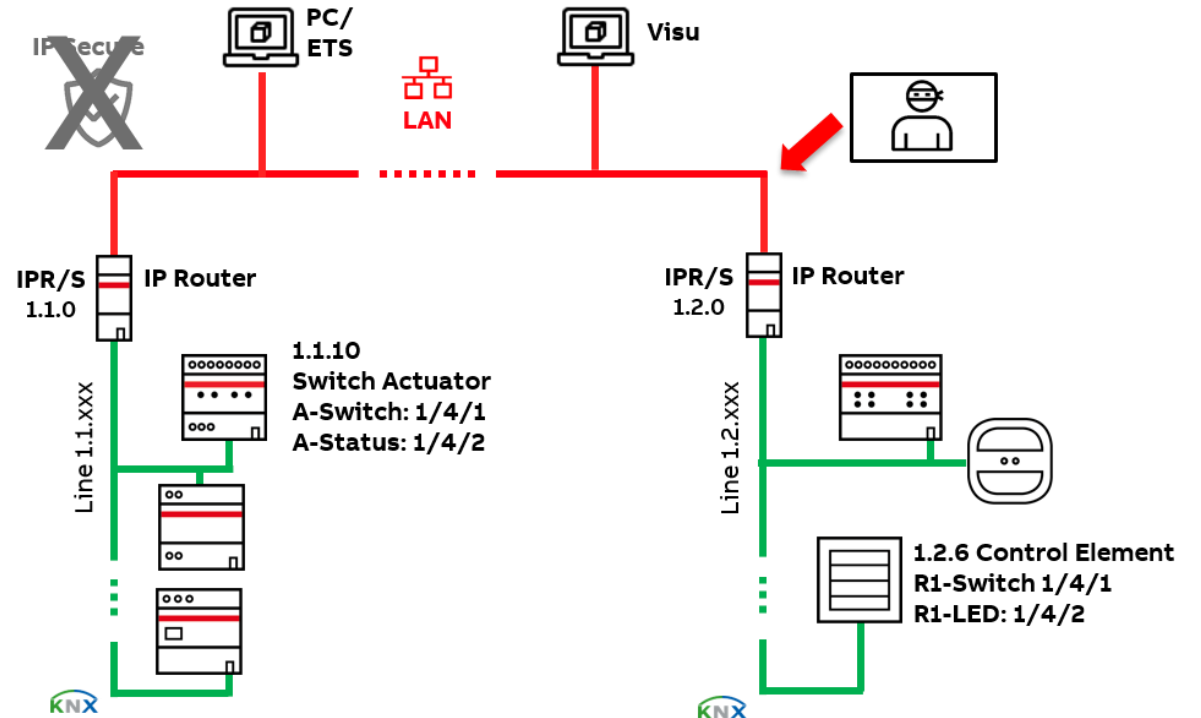
- Record and send KNX telegrams with ETS group monitor
- Record and analyze IP telegrams with special software, e.g. Wireshark

The image shows a Wireshark packet capture of traffic on an Ethernet interface. The filter is set to 'source=192.168.0.106'. The packet list shows several KNXnet/IP packets. The selected packet (No. 97) is a RoutingIndication (L\_Data.ind) with details expanded below.

No.	Time	Source	Destination	Protocol	Length	Info
92	5.488252	192.168.0.109	224.0.23.12	KNXnet/IP	60	RoutingInd L_Data.ind 1.2.6->1/4/1 GroupValueWrite \$01
93	5.539876	192.168.0.107	192.168.0.1	DNS	96	Standard query 0xb6c8 A culpehnswss01.servicebus.windows.net
94	5.568845	192.168.0.107	192.168.0.1	DNS	88	Standard query 0xfc35 A parental.rest.gti.mcafee.com
95	5.561666	192.168.0.108	224.0.23.12	KNXnet/IP	60	RoutingInd L_Data.ind 1.1.10->1/4/2 GroupValueWrite \$01
96	5.895736	192.168.0.107	192.168.0.1	DNS	86	Standard query 0x52ec A updatekeepalive.mcafee.com
97	6.281394	192.168.0.109	224.0.23.12	KNXnet/IP	60	RoutingInd L_Data.ind 1.2.6->1/4/1 GroupValueWrite \$00
98	6.361176	192.168.0.108	224.0.23.12	KNXnet/IP	60	RoutingInd L_Data.ind 1.1.10->1/4/2 GroupValueWrite \$00
99	6.368691	WistronI_d:c:1f:49	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.0.100
100	6.403460	192.168.0.107	192.168.0.1	DNS	73	Standard query 0x4013 A www.google.de
101	6.672286	192.168.0.107	192.168.0.1	DNS	87	Standard query 0x7be4 A inference.location.live.net
102	6.746145	HewlettP_5b:ec:8a	AbbStotz_4a:80:f2	ARP	42	Who has 192.168.0.108? Tell 192.168.0.107

Details of selected packet (No. 97):

- Frame 97: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: AbbStotz\_08:80:58 (00:0c:de:08:80:58), Dst: IPv4mcast\_17:0c (01:00:5e:00:17:0c)
- Internet Protocol Version 4, Src: 192.168.0.109, Dst: 224.0.23.12
- User Datagram Protocol, Src Port: 3671, Dst Port: 3671
- KNX/IP Routing Indication
- cEMI L\_Data.ind, P=Low, H=5, Src=1.2.6, Dst=1/4/1, GroupValueWrite \$00





# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Situation 1 – Attack over the IP network

**No IP Secure:** Record and analyze IP telegram with special software, e.g. Wireshark

The image shows a Wireshark packet capture of an Ethernet network. The filter is set to 'source=192.168.0.106'. The packet list shows several packets, with packet 97 highlighted. A red arrow points from packet 97 to a detailed view of the packet structure. The detailed view shows the following layers:

- Frame 97: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
- Ethernet II, Src: AbbStotz\_08:80:58 (00:0c:de:08:80:58), Dst: IPv4mcast\_01:00:5e:00:00:0c (01:00:5e:00:00:0c)
- Internet Protocol Version 4, Src: 192.168.0.109, Dst: 224.0.23.12
- User Datagram Protocol, Src Port: 3671, Dst Port: 3671
- KNX/IP Routing Indication
- cEMI L\_Data.ind, P=Low, H=5, Src=1.2.6, Dst=1/4/1, GroupValueWrite \$00

Red boxes highlight the source IP (192.168.0.109), the destination IP (224.0.23.12), and the KNX telegram details (Src=1.2.6, Dst=1/4/1, GroupValueWrite \$00). Red arrows point from the text boxes to these highlighted areas.

**IP address of IP Router: 192.168.0.109**  
**Multicast address: 224.0.23.12**

**KNX telegram:**  
**Individual address: 1.2.6**  
**Group address 1/4/1**  
**Value: "0"**

# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Situation 2 – Attack over the IP network

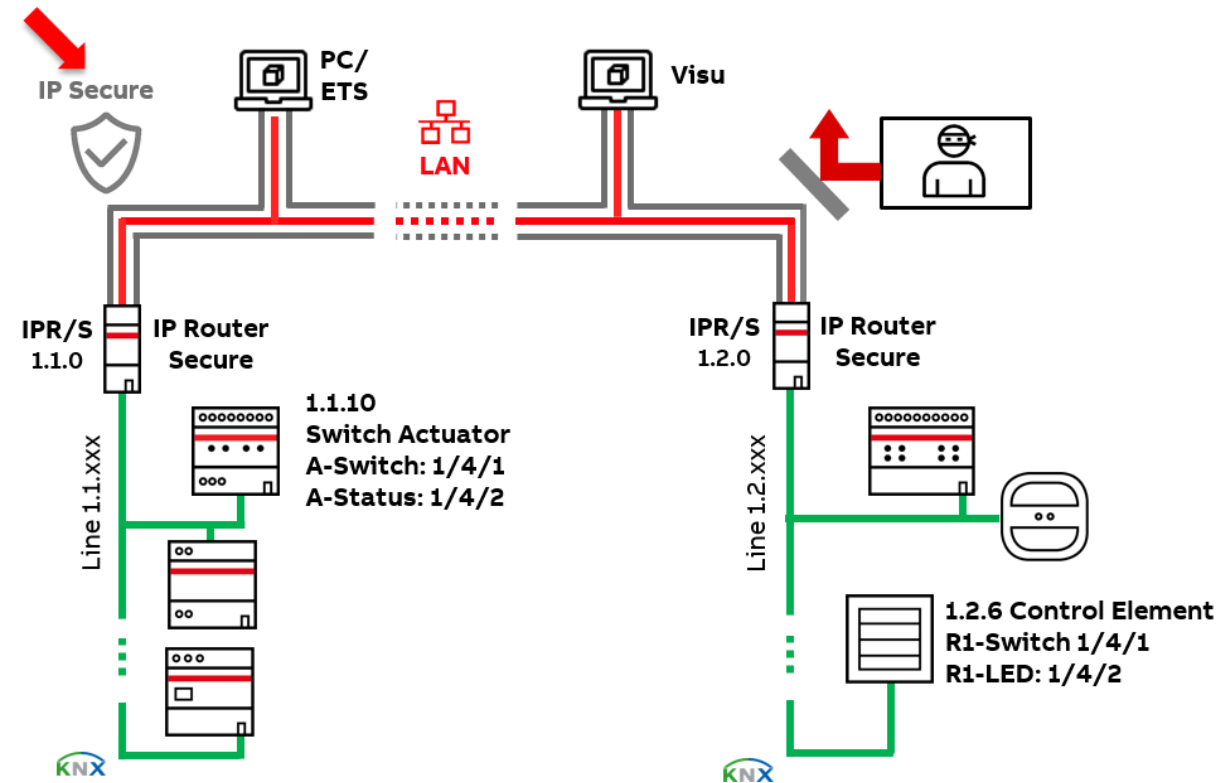
### IP Secure

- The complete KNX telegram is encrypted
- An IP telegram with the same KNX group address and the same value is different for each transmission  
→ No replay attack possible!
- The ETS has assigned a “Backbone Key” for multicast communication on IP to all KNX IP Secure devices in the project

The screenshot shows a network traffic capture in Wireshark. The selected packet is an IPsec-encapsulated KNX telegram. The details pane shows the encapsulation structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and KNX/IP Secure Wrapper. The KNX/IP Secure Wrapper section indicates that the telegram is encrypted and no key is available for decryption.

No.	Time	Source	Destination	Protocol	Length	Info
138	28.949368	192.168.0.107	192.168.1.39	SIMIP	88	get-request 1.3.6.1.4.1.236.11.5.1.1.9.15.0
139	28.988866	192.168.0.107	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.0.100
140	29.108397	192.168.0.107	192.168.0.1	DNS	84	Standard query 0x6a3c A sfs.update.microsoft.com
141	29.240720	192.168.0.105	224.0.23.12	KNXnet/IP	97	SecureWrapper \$00000006102E.00027BE4B550.0008
142	29.326881	192.168.0.106	224.0.23.12	KNXnet/IP	97	SecureWrapper \$00000006100D.00027C00B550.0069
143	29.344683	192.168.0.107	192.168.0.1	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
144	29.344703	HewlettP_5brec:8a	Avm_4c:e5:6a	ARP	42	192.168.0.107 is at a0:d3:c1:5b:ec:8a
145	29.654080	192.168.0.107	192.168.0.1	DNS	83	Standard query 0xc348 A officecdn.microsoft.com
146	29.847150	192.168.0.107	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.0.100
147	30.847166	192.168.0.107	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.0.100
148	30.948341	192.168.0.107	192.168.0.1	DNS	90	Standard query 0xb6ed A mobile.pipe.aria.microsoft.com

Frame 141: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0  
> Ethernet II, Src: AbbStotz\_B8:80:de (00:0c:de:b8:80:de), Dst: IPv4mcast\_17:0c (01:00:5e:00:17:0c)  
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 224.0.23.12  
> User Datagram Protocol, Src Port: 3671, Dst Port: 3671  
> KNX/IP Secure Wrapper, Seq Nr: \$00000006102E, Ser Nr: \$00027BE4B550, Tag: \$0008 (no key available)



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Situation 2 – Attack over the IP network

**IP Secure:** The complete KNX telegram is encrypted

The image shows a Wireshark packet capture of an Ethernet network. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
138	28.949368	192.168.0.107	192.168.1.39	SNMP	88	get-request 1.3.6.1.4.1.236.11.5.1.1.9.15.0
139	28.988866	WistronI_4c:1f:49	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.0.100
140	29.108397	192.168.0.107	192.168.0.1	DNS	84	Standard query 0x6a3c A sls.update.microsoft.com
141	29.240720	192.168.0.105	224.0.23.12	KNXnet/IP	97	SecureWrapper \$00000006102E.00027BE4B550.0008
142	29.326881	192.168.0.106	224.0.23.12	KNXnet/IP	97	SecureWrapper \$00000006108D.00027C08B550.0069
143	29.344683	Avm_4c:e5:6a	HewlettP_5b:ec:8a	ARP	60	Who has 192.168.0.107? Tell 192.168.0.1
144	29.344703	HewlettP_5b:ec:8a	Avm_4c:e5:6a	ARP	42	192.168.0.107 is at a0:d3:c1:5b:ec:8a
145	29.654080	192.168.0.107	192.168.0.1	DNS		
146	29.847150	WistronI_4c:1f:49	Broadcast	ARP		
147	30.847166	WistronI_4c:1f:49	Broadcast	ARP		
148	30.948341	192.168.0.107	192.168.0.1	DNS		

The packet details pane for packet 141 shows the following structure:

- > Frame 141: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface
- > Ethernet II, Src: AbbStotz\_88:80:de (00:0c:de:88:80:de), Dst: IPv4mcas\_17:0...
- > Internet Protocol Version 4, Src: 192.168.0.105, Dst: 224.0.23.12
- > User Datagram Protocol, Src Port: 3671, Dst Port: 3671
- > KNX/IP Secure Wrapper, Seq Nr: \$00000006102E, Ser Nr: \$00027BE4B550, Tag: \$0008 (no key available)

Red annotations highlight the following information:

- IP address of IP Router: 192.168.0.109
- Multicast address: 224.0.23.12
- Complete encrypted KNX telegram

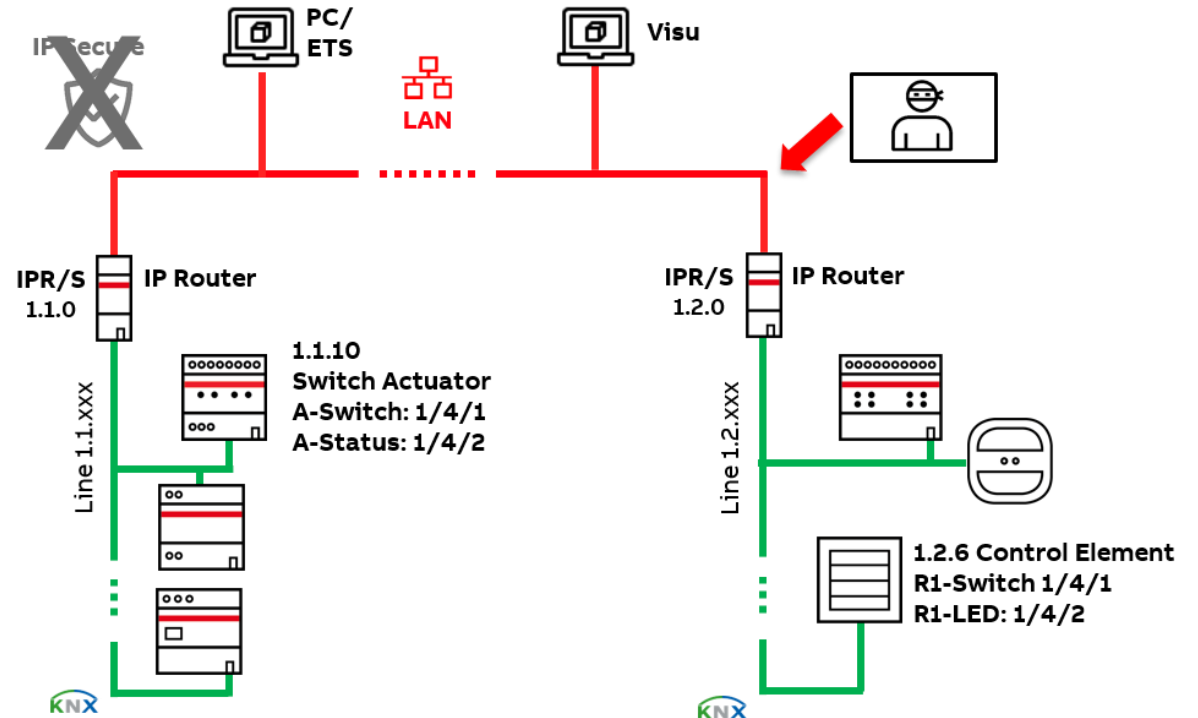
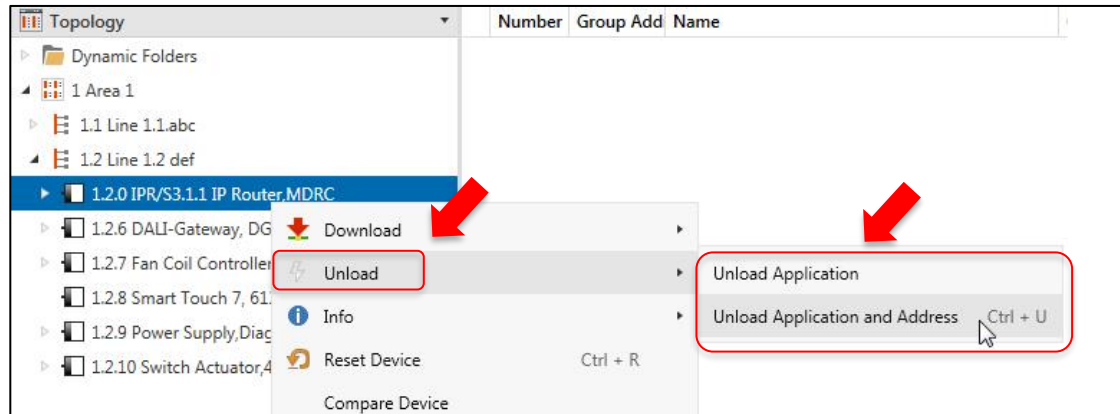
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Situation 3 – Attack over the IP network

### No IP Secure

- Unload and download an IP Router with the ETS is possible



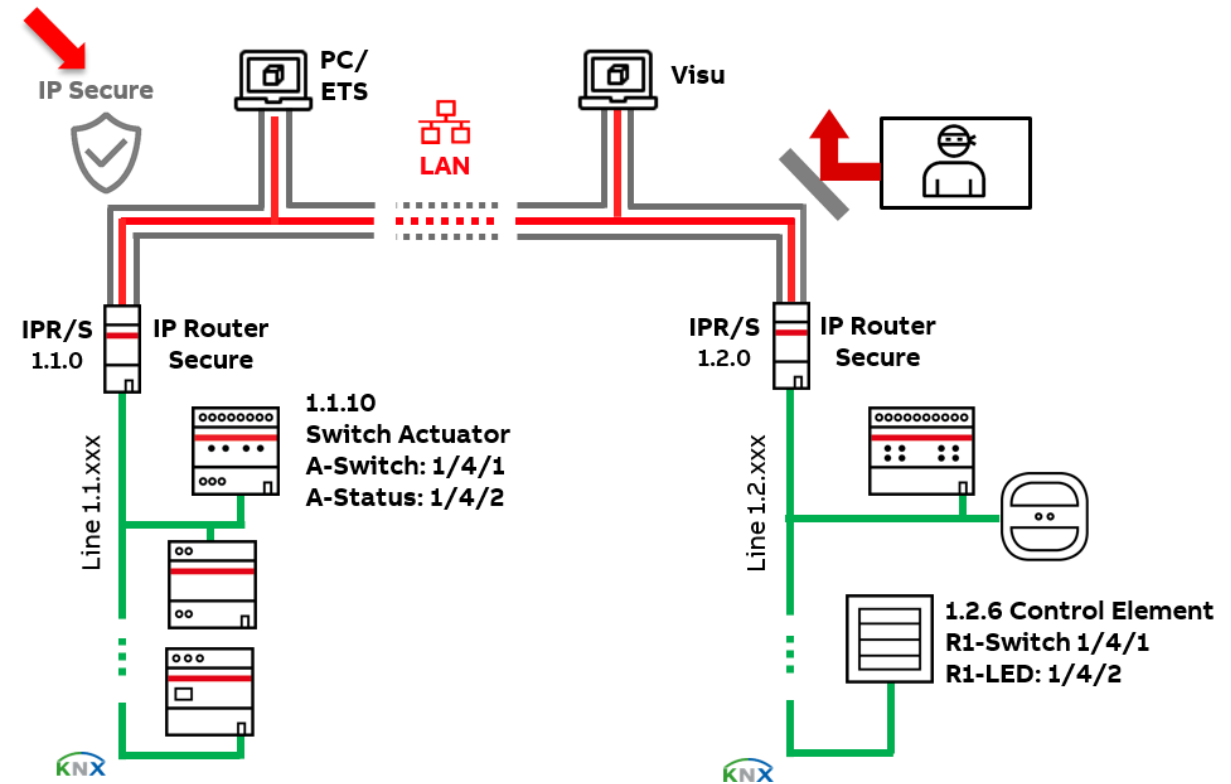
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Situation 4 – Attack over the IP network

### IP Secure

- Unload and download an IP Router with an “Attack ETS” is not possible  
→ No “Backbone Key”!



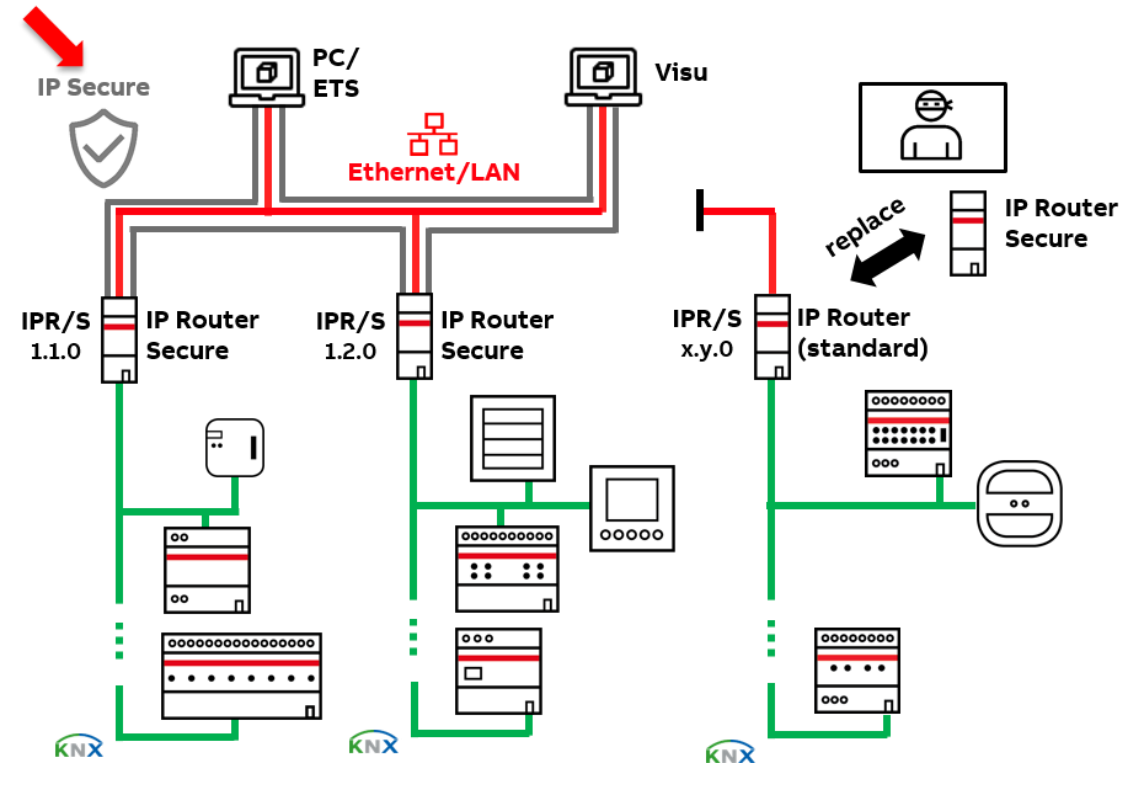
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Situation 5 – Attack over the IP network

### IP Secure

- Replacing the IP Router Secure with an IP Router standard
- This does not pose a security risk because the device is not a part of the secure system  
→ No multicast communication to other IP Router Secure possible!!!





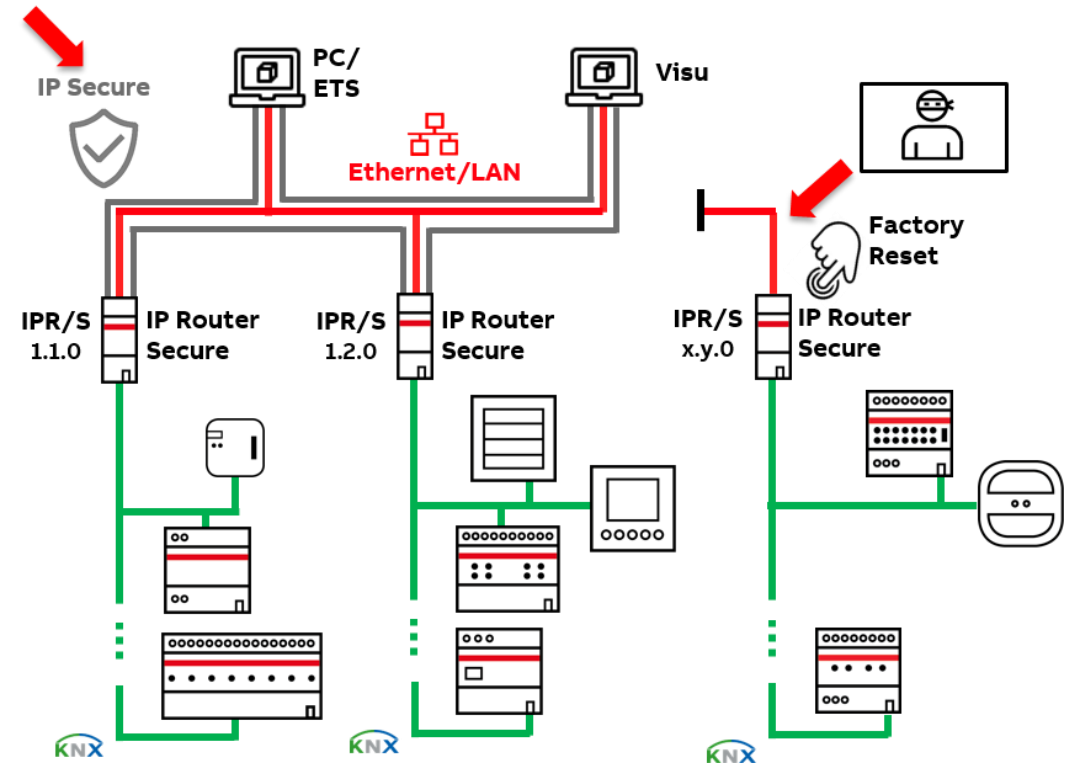
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## Situation 6 – Attack over the IP network

### IP Secure

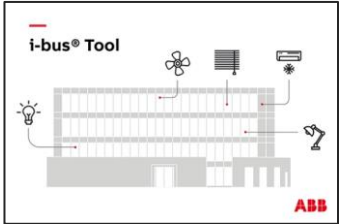
- Factory reset can be done directly on the IP Router Secure
- This does not pose a security risk because the device is no longer part of the secure system  
→ No multicast communication to other IP Router Secure possible!!!
- Despite existing FDSK there is no access to the system (e.g. the sticker with the FDSK is still on the device)
- For commissioning and operation in KNX Secure mode, the “Backbone Key” and “Tool Key” is required!



# ABB i-bus® KNX – IP Devices

IP Interface IPS/S 3.1.1 (standard) and IP Interface Secure IPS/S 3.5.1

## IP Router Router Secure IPR/S 3.5.1 – ABB i-bus® Tool: “Discovery” (find and display ABB IP devices in the network)



Discovery

Device type	Device name	Individual address	IP Address	MAC Address	TP1	Prog. LED	KNX Secure	Firmware status
<input checked="" type="checkbox"/> ABB IPR/S3.5.1	DB 3A: Line 1.1.x: ABB IP Rout	1.1.0	192.168.0.106	00:0C:DE:89:80:02	OK	<input type="checkbox"/>	Active	✓ Up to date
<input type="checkbox"/> ABB IPR/S3.5.1	DB 4C: Line 1.2.x: ABB IP Rout	1.2.0	192.168.0.105	00:0C:DE:88:80:DE	OK	<input type="checkbox"/>	Active	✓ Up to date

Filter: Detailed data

Detailed data

Unicast configuration

Firmware = 0.3.662  
IP address assignment method = DHCP  
IP address = 192.168.0.106 Subnet = 255.255.255.0 Gateway = 192.168.0.1  
BaseT = 100 MBit/s  
Serial number = 00027C08B550  
Physical address = 1.1.0  
Programming mode = Off  
Bus state = Ok  
Routing multicast = 224.0.23.12  
Secure mode = Enabled

Copy to clipboard

Log

Disconnected Telegrams per second 0 v1.9.37.10 ABB Copyright © 2018



KNX Secure is active



# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.1.1 (standard) and IP Router Secure IPR/S 3.5.1

## IP Router Secure IPR/S 3.5.1

### Summary

- KNX IP Router Secure IPR/S 3.5.1 fulfills the KNX Secure Standard “KNXnet/IP Security”
- Communication on IP network, tunneling servers and commissioning from ETS are secure
- After commissioning, an IP Router Secure behaves like a standard IP Router and has the same parameters
- All functions from standard IP Router IPR/S 3.1.1 are available
- The ETS requests a password for the project
- The “Device Certificates” (FDSK) of all IP Routers Secure and other IP devices Secure must be entered
- The ETS generates and works with many keys – but there is no need to change them



---

# ABB i-bus® KNX – IP Devices

Tips & Tricks – IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

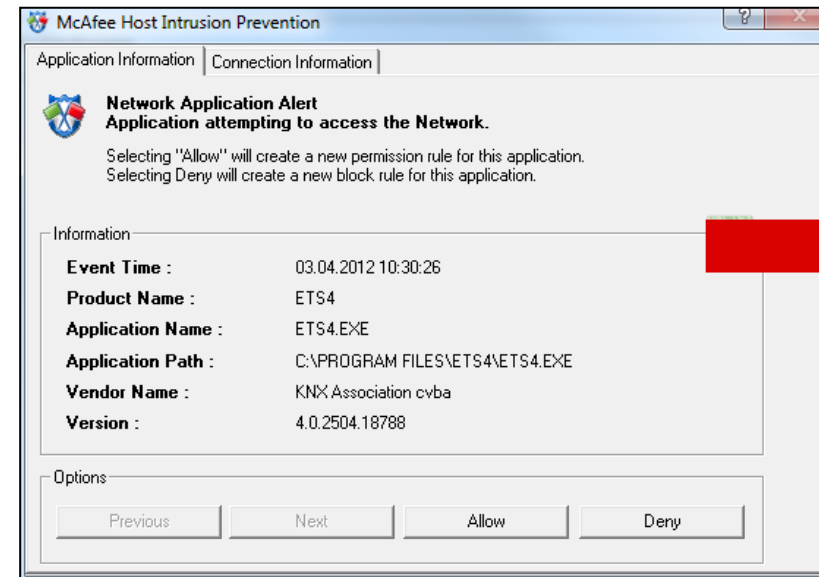
# ABB i-bus® KNX – IP Devices

## Tips & Tricks – IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

### No ETS access to the IP Network possible

ETS programming, diagnostics,... is **not always possible** with the IP Router IPR/S or IP Router Interface, e.g.

- The firewall, virus scanner, ... on the laptop is blocking a download
  - Multicast communication (Point to Multipoint) is not possible in a network (blocked by network admin)
  - External System Integrator does not have access to the company IP network
  - ...
- Always have a USB interface with you
- So you always have access to KNX



USB Interface

\_\_\_\_\_

## Tips & Tricks – IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

## Filter tables

- The filter tables of IP Router IPR/S are generated by ETS automatically in the background
- If “KNX” devices (ABB Busch-ControlTouch®, BMS, visualization, tablet apps, ...) are parameterized outside of the ETS, the ETS does not know these devices and cannot adapt the filter tables accordingly
  - Manual editing of the tables may be necessary
- When communicating via a tunnel server, there is a direct connection to the line → no editing of the filter tables required
- In the case of communication via Multicast, the connection is on the IP network and the group addresses must be added to the filter tables manually



IP Router IPR/S  
incl. filter table



BMS,  
visualization,  
...



ABB Busch-  
ControlTouch®

# ABB i-bus® KNX – IP Devices

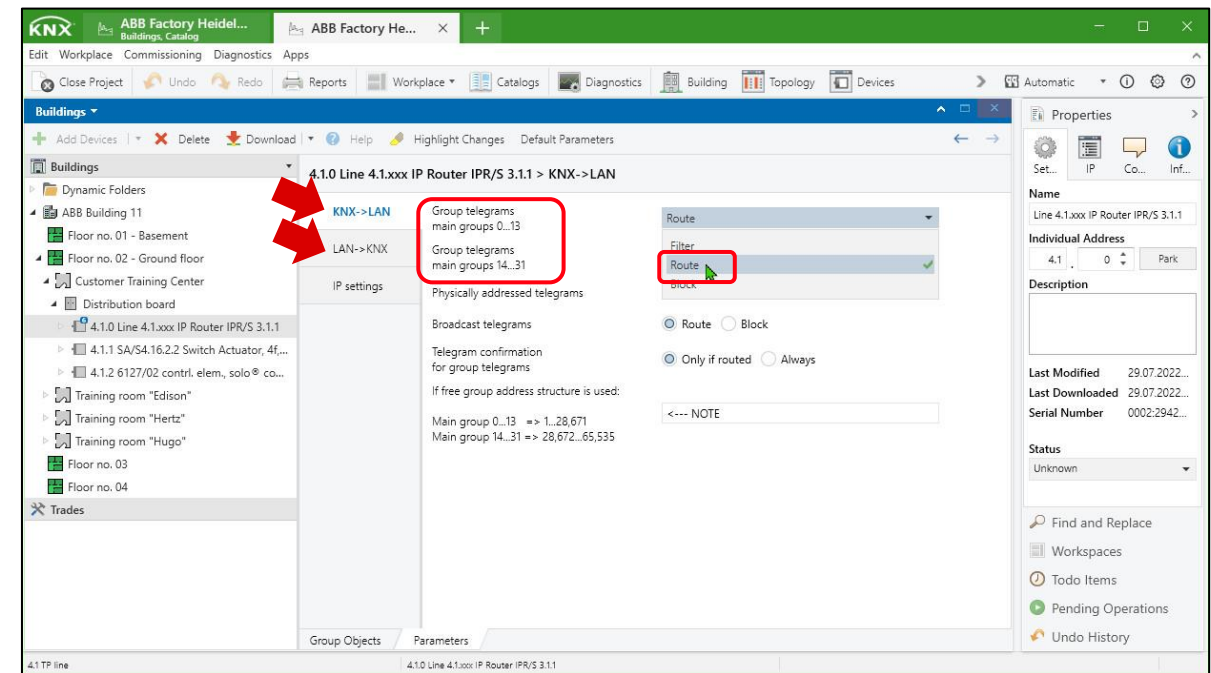
## Tips & Tricks – IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

### Filter tables – Manual editing of the filter tables (1)

#### Set the ETS parameter of IP Router IPR/S to “Route”

- All group telegrams from the main line to the line and from the line to the main line are forwarded
- The group telegrams are thus also forwarded to all other lines
- This can lead to a high bus load in all lines and possible communication problems
- Note:
  - If there is no acknowledge (ACK) of the group telegram, it will be repeated up to 3 times – in all lines!

→ Not recommended – except during initial commissioning !!!



# ABB i-bus® KNX – IP Devices

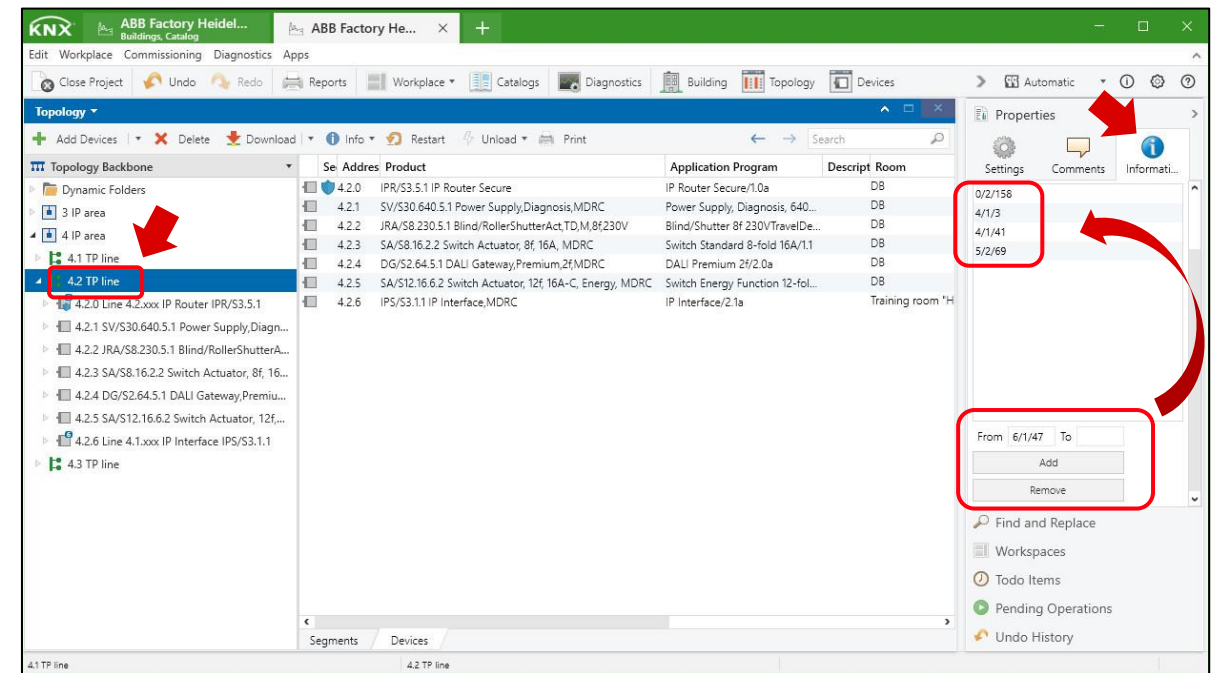
## Tips & Tricks – IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

### Filter tables – Manual editing of the filter tables (2)

#### Add group addresses to the filter tables manually

- You can manually add group addresses by clicking on a line or area (not IP Router) in the topology window
- Then select the “Information” tab in the navigation bar
- You have the option there to add and remove group addresses
- The group addresses automatically generated by the ETS and manually added are then listed in the “Manual filter table entries” dialog window (→ right mouse click on IP Router)
- Note:
  - The filter tables of all IP Routers must be edited
  - If an address of a group address is changed, this manually added group address is not updated in the filter table!

→ Not really recommended!!!



# ABB i-bus® KNX – IP Devices

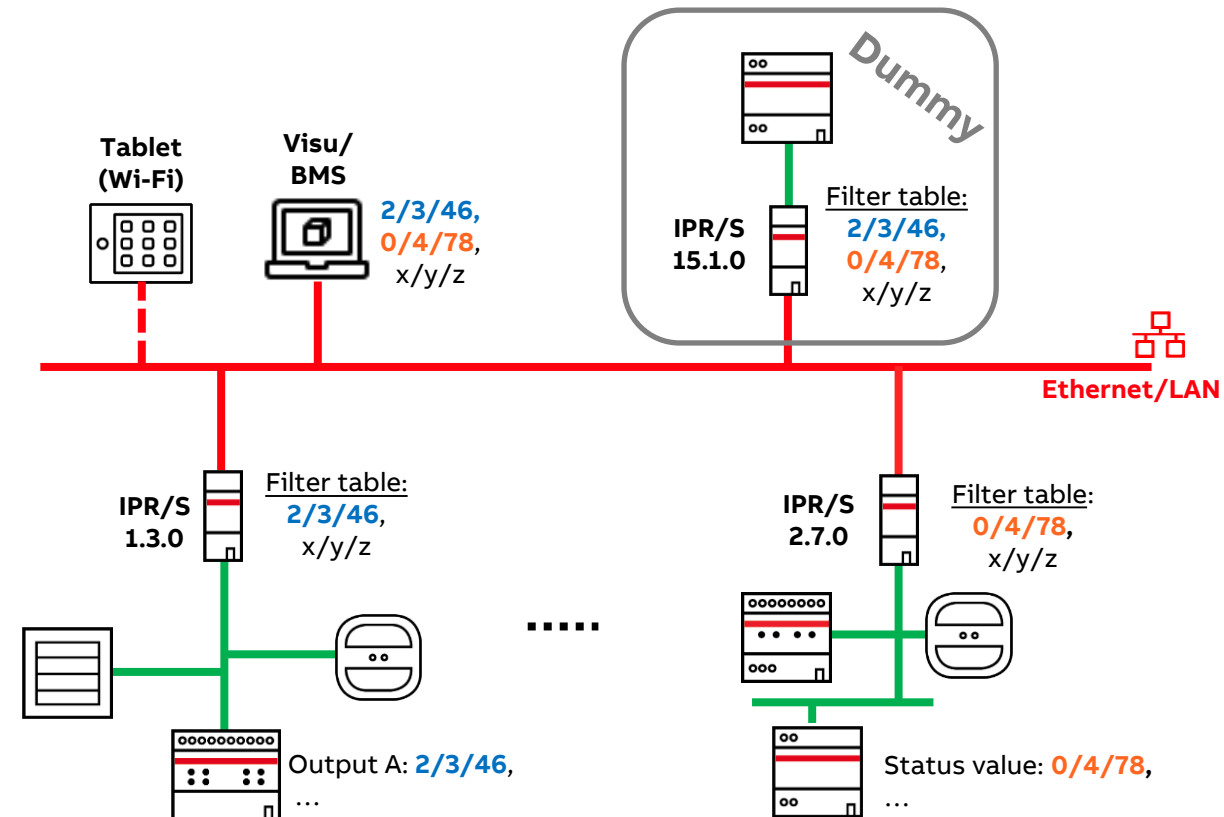
## Tips & Tricks – IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

### Filter tables – Manual editing of the filter tables (3)

#### Dummy device in ETS

- Add an additional KNX device (dummy) to the ETS and link the required group addresses
- The ETS recalculates the filter tables of all IP Routers and automatically adds these group addresses
- However, this “dummy” device only exists in the ETS

→ Recommended!!!



# ABB i-bus® KNX – IP Devices

## Tips & Tricks – IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

### Filter tables – Manual editing of the filter tables (3)

#### Dummy device in ETS

- Add an additional KNX device (dummy) to the ETS and link the required group addresses
- The ETS recalculates the filter tables of all IP Routers and automatically adds these group addresses
- However, this “dummy” device only exists in the ETS

→ Recommended!!!

The screenshot shows the ETS software interface. The 'Topology' window displays a table of dummy devices. A red box highlights the '15.1.1 Dummy device (ABA/S1.2.1 Logic Controller)' in the 'Dynamic Folders' tree. Another red box highlights the table of dummy devices in the 'Topology' window. The table has columns: Num, Group Address, Name, Length, Data Type, C, R, W, T, U, and Priority. The table lists several dummy devices with their respective group addresses and data types. The '15.1.1 Dummy device (ABA/S1.2.1 Logic Controller)' is highlighted in blue. The 'Logic Controller' window shows a filter table for the dummy device. The filter table lists various data types and their corresponding group addresses. A red arrow points from the '15.1.1 Dummy device (ABA/S1.2.1 Logic Controller)' in the 'Dynamic Folders' tree to the 'Logic Controller' window.

Num	Group Address	Name	Length	Data Type	C	R	W	T	U	Priori
1	4/1/3, 4/1/60, 4/1/81, 4/1/91	Dummy 1-bit	1 bit	switch	C	-	W	T	-	Low
2	4/1/73, 4/1/70, 4/1/95	Dummy 1-byte %	1 byte	percentage (0..100%)	C	-	W	T	-	Low
3	4/1/103, 4/1/47	Dummy Temperature	2 bytes	temperature (°C)	C	-	W	T	-	Low
4	4/1/48	Dummy Lux	2 bytes	lux (Lux)	C	-	W	T	-	Low
5	2/4/89, 3/4/14	Dummy Power	4 bytes	power (W)	C	-	W	T	-	Low
6	0/2/198, 7/4/87	Dummy Voltage	4 bytes	electric potential (V)	C	-	W	T	-	Low
502		Device clock	1 bit	trigger	C	-	T	-	-	Low
503		Device clock	3 bytes	date	C	R	W	-	-	Low
504		Device clock	3 bytes	time of day	C	R	W	-	-	Low
505		Device clock	8 bytes							

Example:

“Dummy” area 15 and line 15.1.xxx

Logic Controller ABA/S as a “Dummy device”



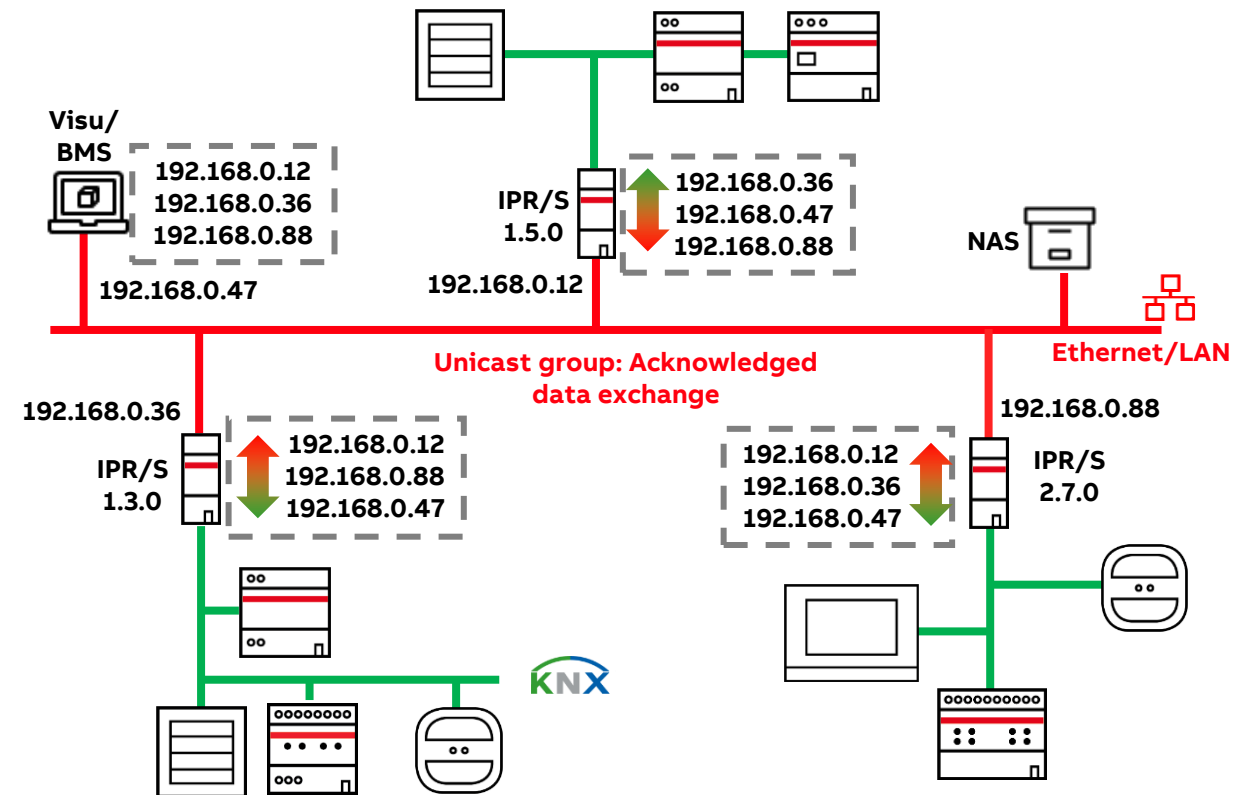
# ABB i-bus® KNX – IP Devices

## Tips & Tricks – IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

### Unicast Communication

- Solution if Multicast communication is not possible
- Up to 10 IP Routers IPR/S can be combined to form a “Unicast group”
- Each IP Router IPR/S is then assigned 9 IP addresses to which it sends its telegrams (Point to Point)
- It is also possible to link a client (e.g. a visualization or BMS) with this unicast group
- Configuration of unicast groups is simple with the ABB i-bus® Tool
- Many Unicast groups are possible at the same time, but communication is feasible only within the same group
- Network telegrams are acknowledged and repeated if necessary

**Note:** This special communication type does not comply with the KNXnet/IP specification



# ABB i-bus® KNX – IP Devices

Tips & Tricks – IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

## Unicast Communication – Configuration of unicast groups with the ABB i-bus® Tool

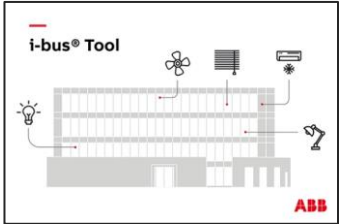


ABB i-bus® Tool 1.9.4.23

Menu: Back, Home, Help, Refresh, Discovery, Update, Unicast, Group/devices, Create unicast group, Extend group, Remove from group, IP devices (3), Statistics

Device type	Device name	Individual address	IP Address	Unicast	Unicast group
✓ ABB IPR/S 3.1.1	ABB IP Router 1.3.x - DB Floor	1.3.0	192.168.0.36	Yes	UniGroup Alpha
✓ ABB IPR/S 3.1.1	ABB IP Router 1.5.x - DB Floor	1.5.0	192.168.0.12	Yes	UniGroup Alpha
✓ ABB IPR/S 3.1.1	ABB IP Router 2.7.x - DB Floor	2.7.0	192.168.0.88	Yes	UniGroup Alpha

Detailed data: Unicast configuration

Unicast state: Unicast is active

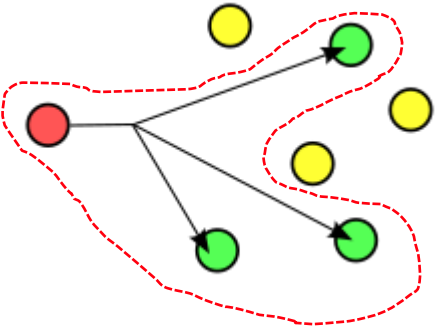
Number of supported unicast addresses: 9

Unicast group name: UniGroup Alpha

Unicast addresses table

Address	Status
1: 192.168.0.88	✓
2: 192.168.0.12	✓

Log: Disconnected, Telegrams per second 6, Refresh mode Automatic, i-bus® ABB C



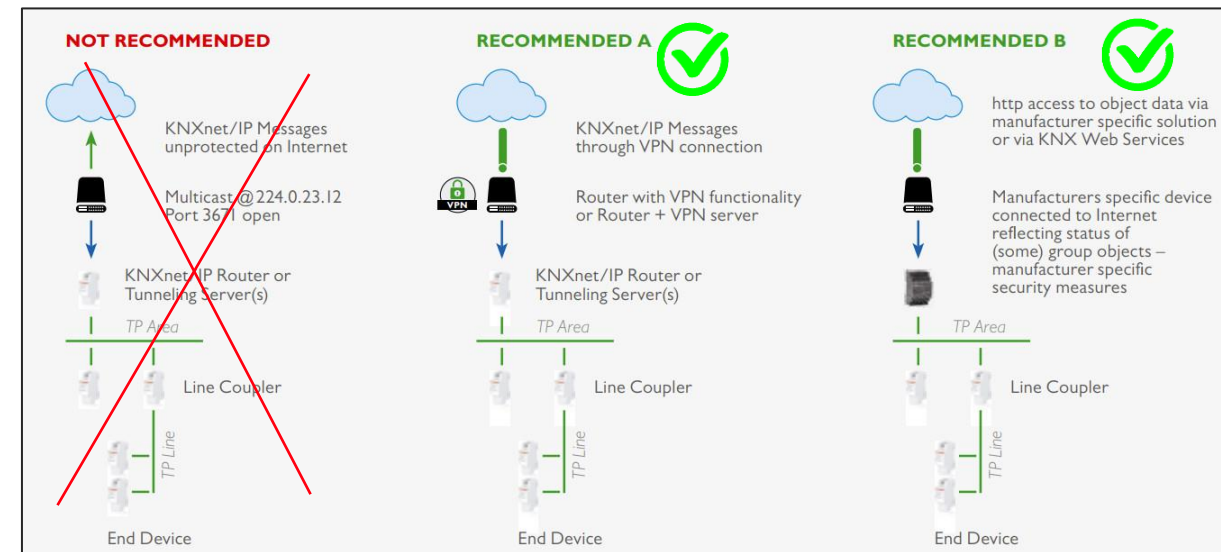
Unicast group

# ABB i-bus® KNX – IP Devices

## Tips & Tricks – IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

### Attacks from outside via the Internet

- Many KNX installations everywhere can be at risk now. It is necessary to protect this installations
    - Never open ports or using port redirection of network routers  
→ This makes the KNX communication visible via the Internet
    - Using secure access via specific devices, VPN or a portal (ABB “myBuildings” portal)
  - Current situation
    - In the past, remote access via the Internet was desired
    - Ports (e.g. 3671) were opened and they are still open!
    - KNX installations have already been “attacked” (use of open vulnerabilities) from outside and KNX devices have been reprogrammed, unloaded, ...
- Without the right security measures your KNX project could be open to attack from automated bots



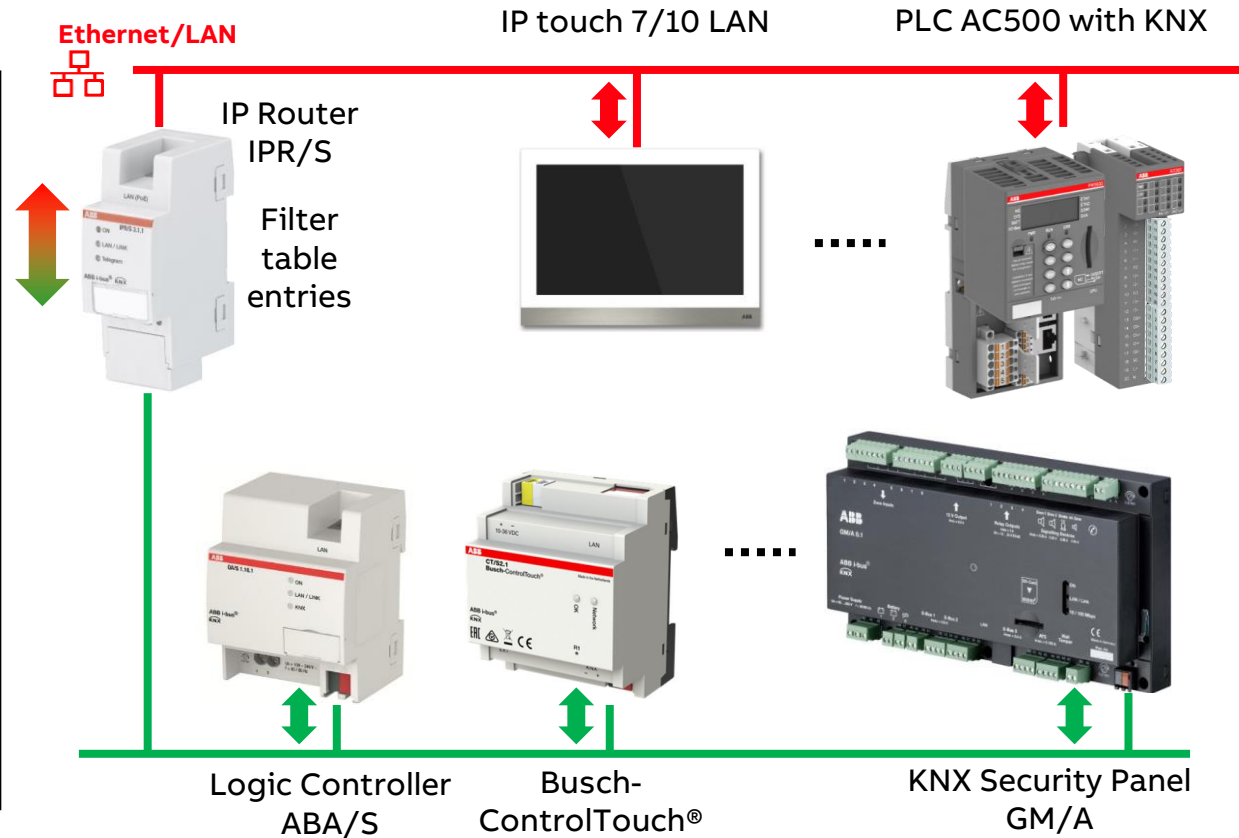
Access to KNX installations via Internet

# ABB i-bus® KNX – IP Devices

## Tips & Tricks – IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

### Communication via IP and TP of KNX devices

- There are KNX devices with an IP connection
- However, communication takes place via twisted pair TP
- The filter tables of the IP Routers IPR/S must be observed and, if necessary, edited manually
- The IP connection is e.g. only for web access with a browser
  - Logic Controller ABA/S
  - ABB EQmatic Energy Analyzer QA/S KNX
  - ClimaECO Application Controller AC/S
  - KNX Security Panel GM/A
  - ABB Busch-ControlTouch® and Busch-VoiceControl®
- KNX devices communicating via IP
  - IP touch 7 / 10 LAN
  - PLC AC500 with integrated KNX interface (former BAC/S)



---

# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

## Overview

2CDG 110 177 R0011	IP Interface	IPS/S 3.1.1
2CDG110204R0011	IP Interface Secure	IPS/S 3.5.1
2CDG 110 175 R0011	IP Router	IPR/S 3.1.1
2CDG 110 176 R0011	IP Router Secure	IPR/S 3.5.1



IP Interface  
IPS/S 3.1.1



IP Router  
IPR/S 3.1.1



IP Interface  
Secure  
IPS/S 3.5.1




IP Router  
Secure  
IPR/S 3.5.1



## IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

## Further information

- [www.abb.com/KNX](http://www.abb.com/KNX)
  - Products and Downloads
    - System Infrastructure and Interfacing
    - IP Routers and Interfaces
  - Product information (manual, software, ...)
- Training & Qualification Database
  - <https://go.abb/ba-training>
- YouTube
  - Channel “ABB Home and Building Automation”  
<https://www.youtube.com/user/ABBibusKNX>
- KNX Association
  - <https://secure.knx.org/>



HOME • OFFERINGS • LOW VOLTAGE PRODUCTS • BUILDING AND HOME AUTOMATION SOLUTIONS • ABB'S RUG KIX • SYSTEM INFRASTRUCTURE AND INTERFACING

# System Infrastructure and Interfacing

Couplers and Gateways for communication and integration


ABB I-bus® KIXIX provides powerful system components for the KIXIX system.

**Main benefits**

- Reliable and powerful system components
- ABB I-bus® Tool significantly facilitates the commissioning
- More integration with gateways to other system such as IP, EnOcean or optical fibre

**Main features**

- Integration of KIXIX installations with IP networks for visualization, programming or quick line and area coupling
- Remote access to the installation with up to 5 IP clients simultaneously
- ABB I-bus® tool for IP discovery and FW update available



## Products and Documentation

<a href="#">IPR/53.1.1</a> <a href="#">2CDD111173R0011</a>	<a href="#">IPR/53.1.1 IP Router, MDCR</a>
<a href="#">IPR/53.5.1</a> <a href="#">2CDD111173R0011</a>	<a href="#">IPR/53.5.1 IP Router Secure, MDCR</a>
<a href="#">IPR/53.5.11</a> <a href="#">2CKA00136A0204</a>	<a href="#">IPR/53.5.11 IP Router Secure, MDCR, BJE</a>
<a href="#">IPIS/53.1.1</a> <a href="#">2CDD111173R0011</a>	<a href="#">IPIS/53.1.1 IP Interface, MDCR</a>
<a href="#">IPIS/53.5.1</a> <a href="#">2CDD111173R0011</a>	<a href="#">IPIS/53.5.1 IP Interface Secure, MDCR</a>

[illegible]



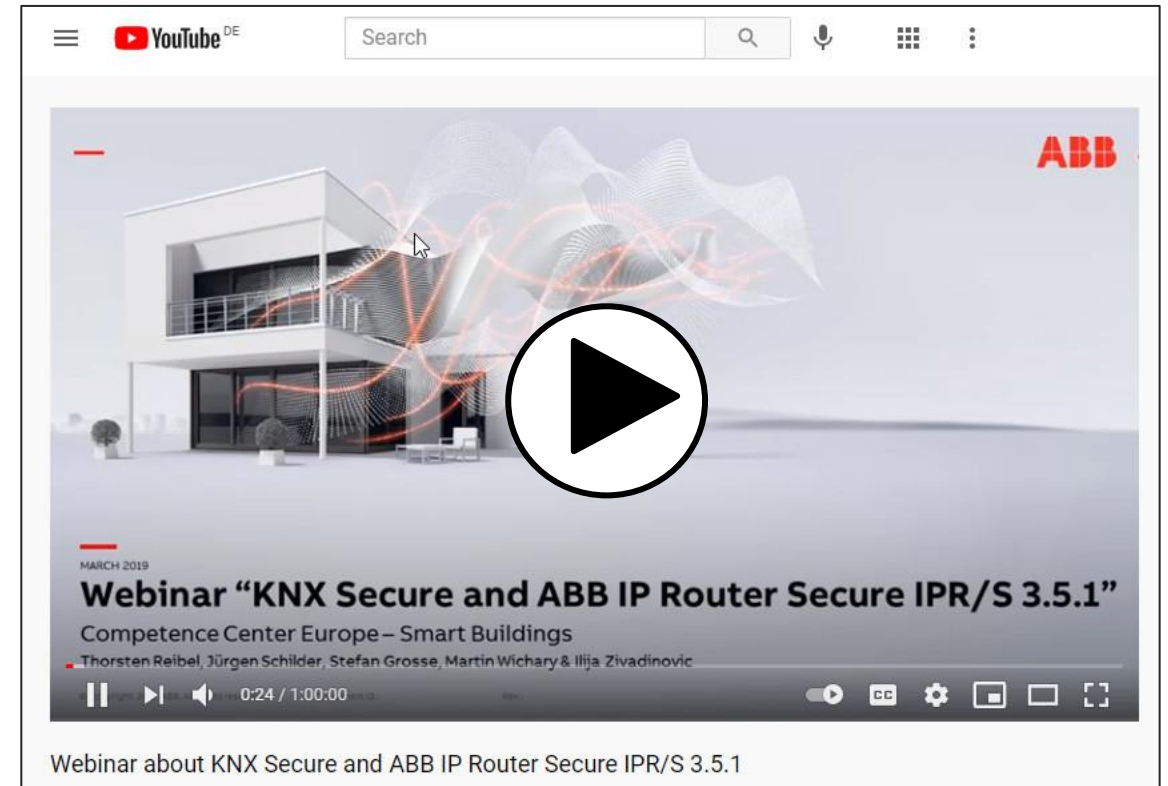
# ABB i-bus® KNX – IP Devices

IP Router IPR/S 3.x.1 and IP Router Interface IPS/S 3.x.1

## Further information

Training & Qualification Database: <https://go.abb/ba-training>

- The database contains extensive training content
  - Webinar, Learning Sessions, ... slides and videos
  - Video tutorials
  - and more ...
  - KNX Secure and ABB IP Interface Secure IPS/S 3.5.1, including detailed commissioning  
[→Link PDF](#)      [→Link Video](#)
  - KNX Secure and ABB IP Router Secure IPR/S 3.5.1; including detailed commissioning  
[→Link PDF](#)      [→Link Video](#)
  - IP Router IPR/S 3.1.1 and IP Interface IPS/S 3.1.1  
[→Link PDF](#)      [→Link Video](#)
  - Advanced features of IP devices: IP Router IPR/S 3.1.1 and IP Interface IPS/S 3.1.1  
[→Link PDF](#)      [→Link Video](#)



---

# Disclaimer

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

© Copyright [2023] ABB. All rights reserved.

**ABB**