



Security

Weinzierl Engineering GmbH

© 2023

Agenda

- **KNX Security general**
- **KNX Data Security**
- **KNX IP Security**
- **Secure Devices**
- **Security in ETS5**



KNX Security

Based on AES

- Advanced Encryption Standard

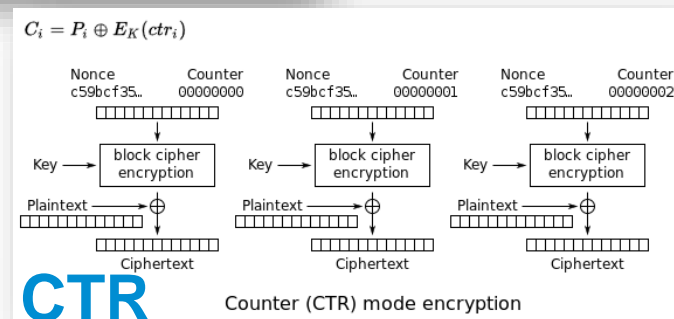
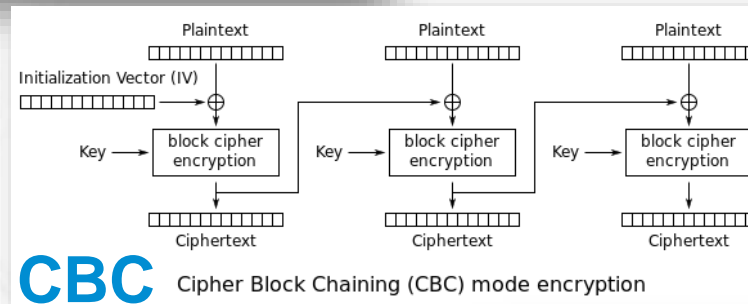
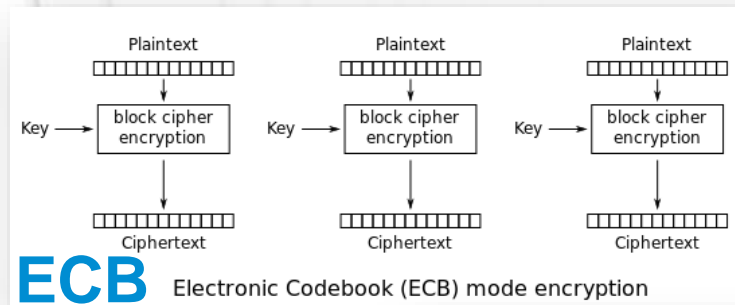
Subset of Rijndael (Rijmen + Daemen) chipher

Since 2000 “de facto” standard for symmetric encryption

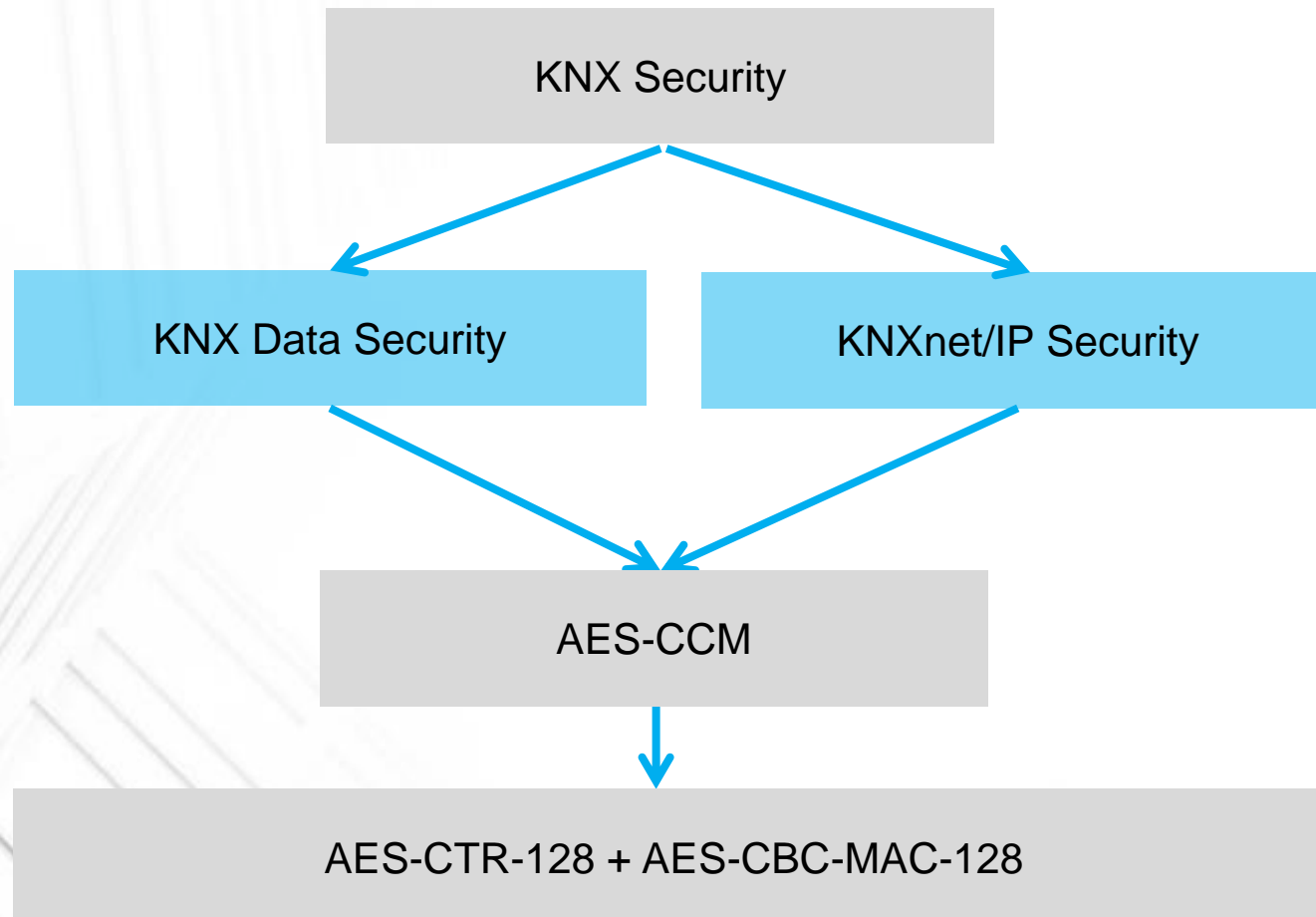


- Block length: 128 bits
- Key length: 128, 192, 256 bits
- Operational modes: ECB, CBC, CFB, OFB, CTR

KNX Security: AES modes



KNX Security



KNX Security Properties

Data Integrity

- Prevents an attacker from manipulating the data. (MAC)



Freshness

- Prevents data from being recorded and replayed. (SeqNo)

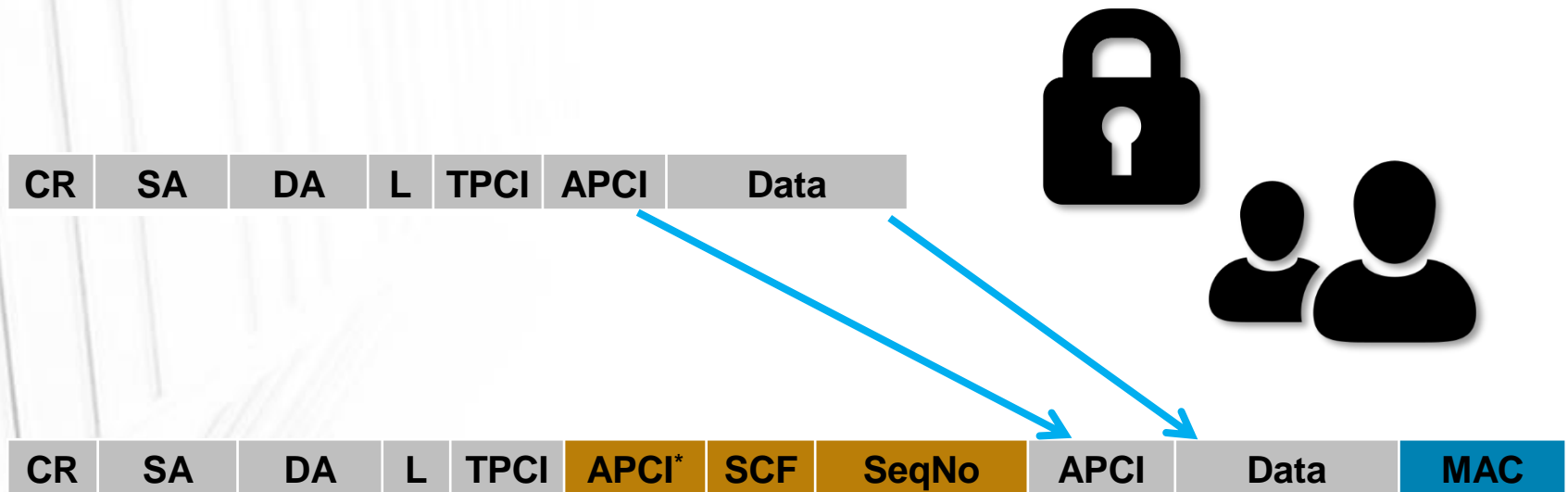


Confidentiality

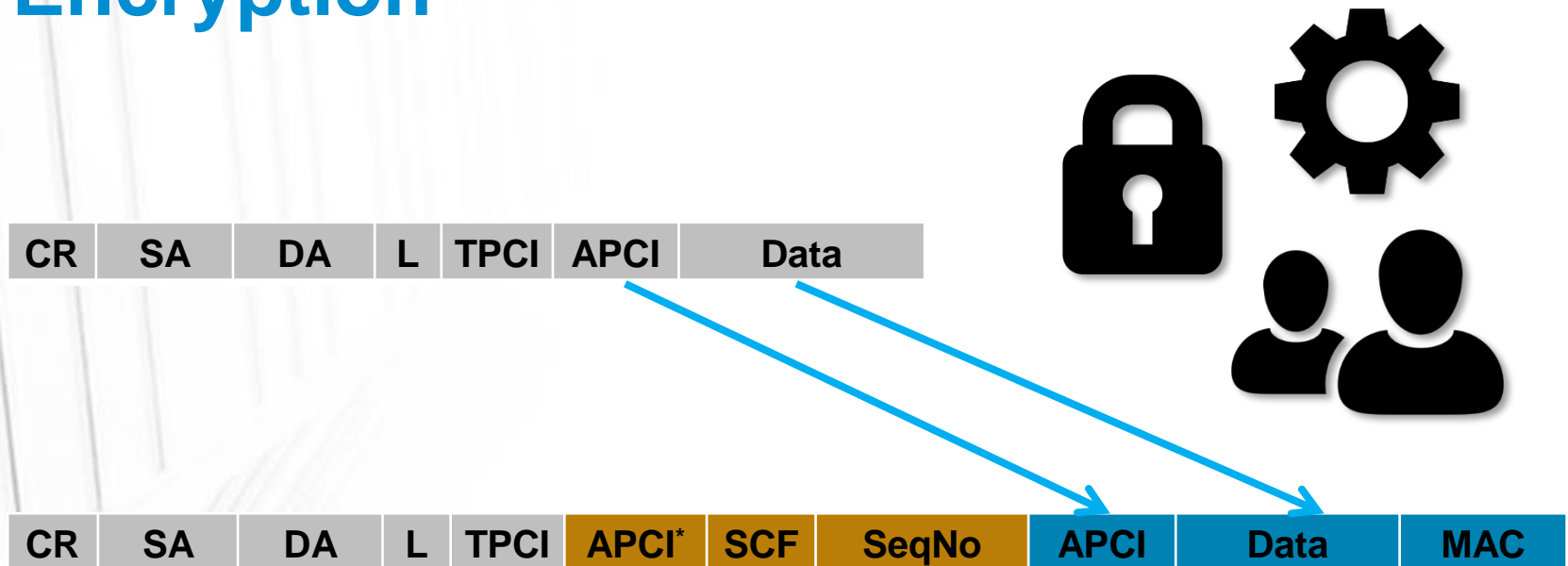
- Data is encrypted. (AES)



KNX Data Security: Authentication



KNX Data Security: Authentication and Encryption



KNX Data Security: Keys



FDSK (Factory default setup key)

- Active on commissioning
- Reactivated after master reset
- Non-readable/non-writable

Tool key

- Replace FDSK
- Writable only

P2P keys

- Point-to-point communication
- Readable/writable

Group keys

- Runtime communication
- Readable/writable

KNX Data Security: Sequence counter

1
2
3

48-bits long

Sending

- One per device
- Continuously incremented on sent message
- PID_SEQUENCE_NUMBER_SENDING

Receiving

- One per communication partner (device)
- Accept only higher values
- PID_SECURITY_INDIVIDUAL_ADDRESS_TABLE

Tool access

- Accept only higher values
- Non-readable/non-writable

Storage!

KNX Data Security: Sync procedure

Request



Secure APCI	SCF	SeqNr _{local}	KNX Serial Number	Challenge	MAC
10 bit	1 octet	6 octets	6 octets	6 octets	4 octets
3F1h	9Ah			N ₁	

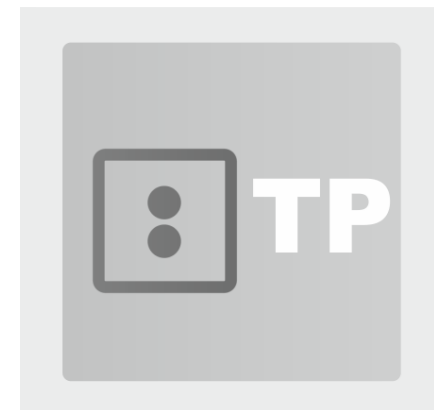
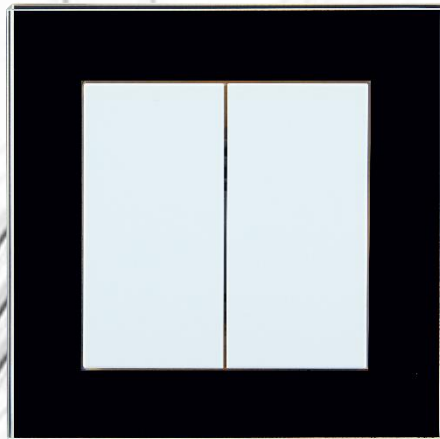
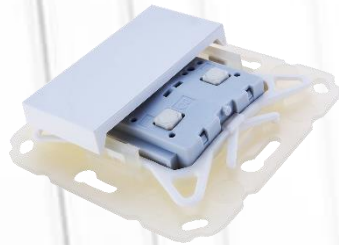
Response

Secure APCI	SCF	Challenge XOR Random	SeqNr _{remote}	SeqNr _{local}	MAC
10 bit	1 octet	6 octets	6 octets	6 octets	4 octets
3F1h	9Bh			N ₁	

KNX TP Push Button 420 *secure*

KNX TP Push Button

- Series MATCH 55
- For standard frame 55 mm
- Single rocker or double rocker
- With KNX Security



KNX RF / ENO Push Button 440 *secure*

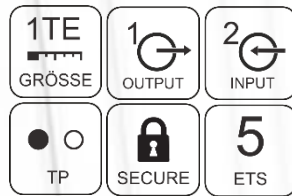


KNX RF / ENO Push Button 440 secure

- Series MATCH 55
- For standard frame 55 mm
- Single rocker or double rocker
- Integrated interface USB to KNX RF
- Power supply via battery CR2032
- with KNX Security
- KNX RF/TP media coupler 673.1 secure



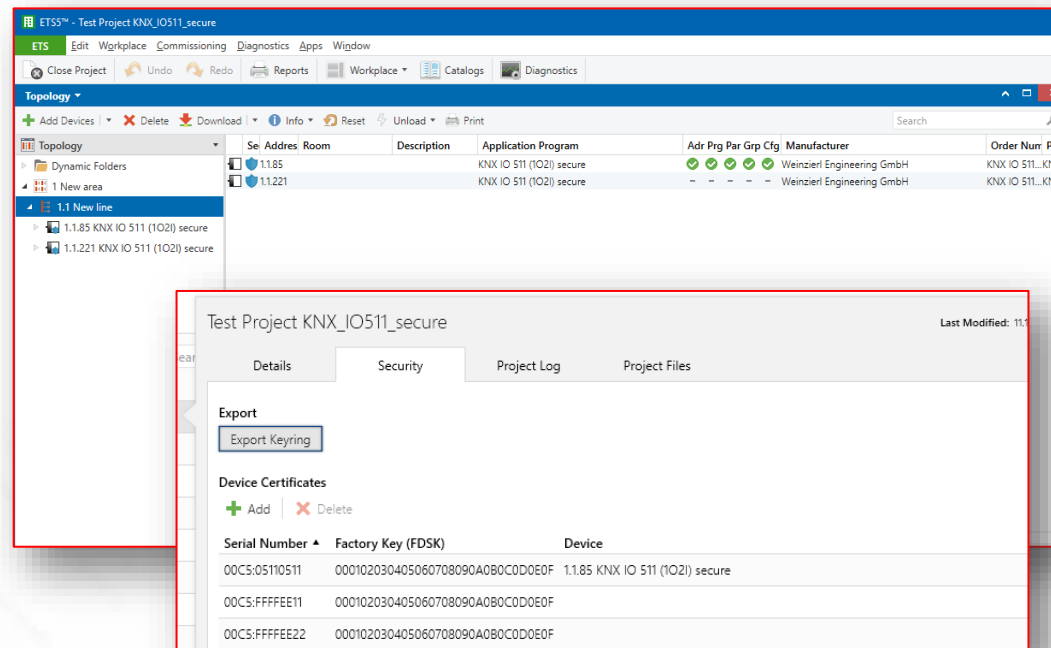
KNX IO 511.1 secure



Input and Output

For getting started with KNX data security

First secure device of KNX IO compact series

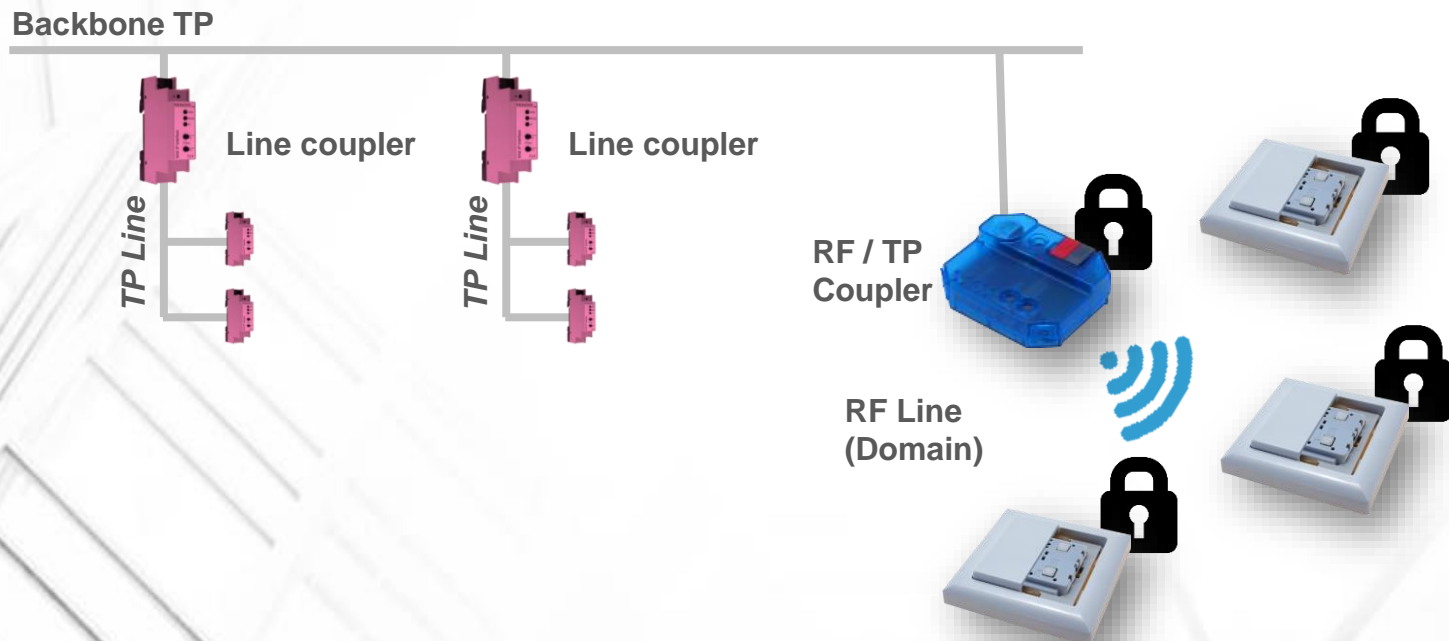


Mixing secure and non-secure

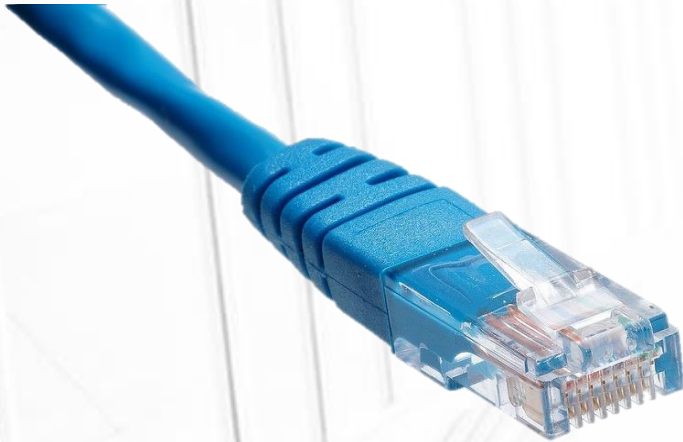
Security per link

Security in sub-systems

- KNX Secure Proxy
- In preparation for ETS



KNX IP Security



Goal

- Be secure in IP
- Stay compatible on TP

KNX IP Secure Devices

- KNX IP Security
- KNX Data Security

KNX IP Interface *secure*

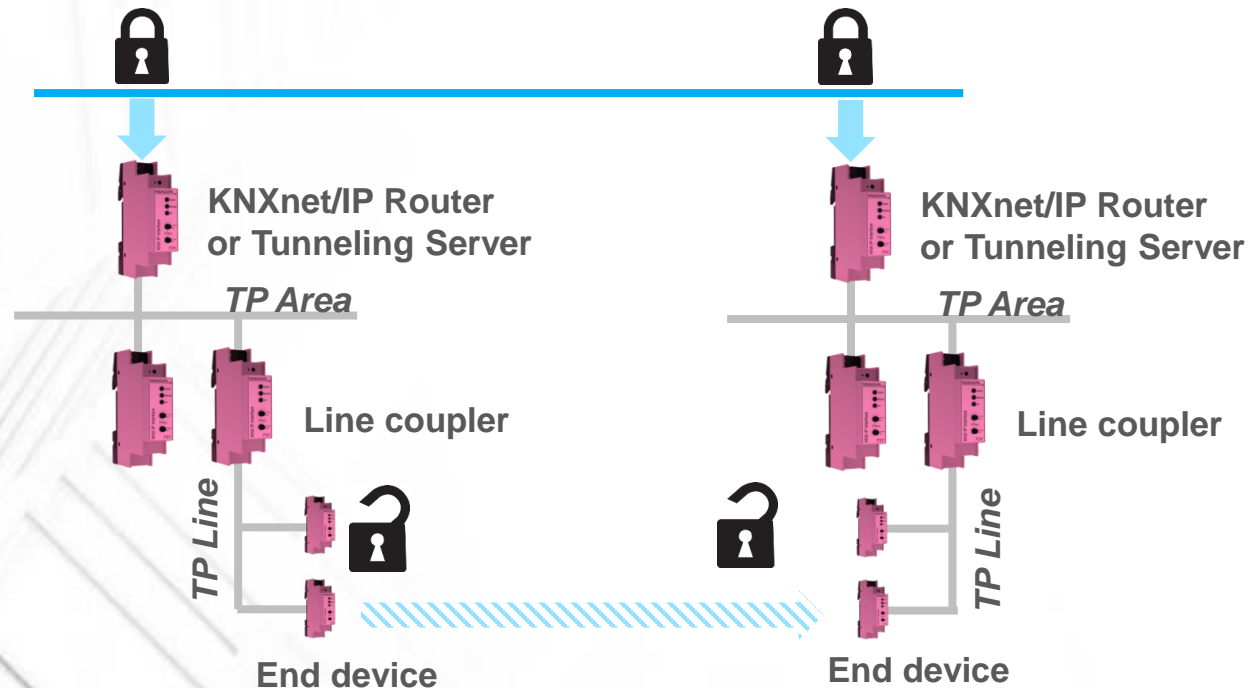
KNX IP Router *secure*

Medium KNX IP *secure*

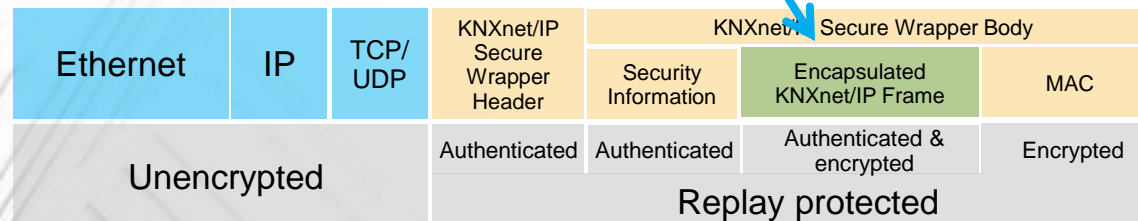
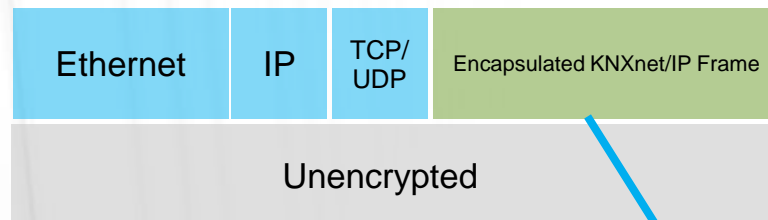


KNXnet/IP Security

- Protects data within IP network (Routing)
- Protects access to KNX network (Tunneling)



KNXnet/IP Security: Frame



KNXnet/IP Security: Features



Multicast communication (routing)

- Fix key
- Sequence counter → timer based
- Sync mechanism

Unicast communication (sessions)

- Individual key negotiated using ECDH (Curve25519)
- Device authentication code
- User password

KNX IP Security: Keys



FDSK (Factory Default Setup Key)


- Active on commissioning
- Reactivated after master reset
- Non-readable/non-writable
- Via QR Code

Tool key

- Replace FDSK by ETS
- Not visible to customers

Scanning FDSK in ETS






Adding Device Certificates

KNX IP Interface 732 secure

This device supports secure configuration. To do so, ETS must know the factory key of that device, that you can find printed on the device or in the packaging. If you do not have access to this information now, you can enter the key later in the dashboard or before downloading the device.



ADC777 - 674ZZ5 - OIC5HU - OV2JAZ - VDBYEE - **IA3DGS** ✓

Serial Number 00C5:FFFFDFE6
Factory Key 73D7205D3D1D5D2419A8C3821100D8CD

Cancel

Device Certificates

ETS5™ - KNX IP Interface 732 secure

ETS Edit Workplace Commissioning Diagnostics Apps Window

Overview Bus Catalogs Settings

Projects Archive ETS Inside

Search

Name	Last Modified	Status
KNX IP Interface 732 secure	02.11.2018 09:46	Unknown
KNX IP Router 752 secure	02.11.2018 08:25	Unknown
2018-10-25-001 Misc. devices	02.11.2018 08:19	Unknown
KNX Stack Demo	17.10.2018 14:54	Unknown
KNX Stack Demo (Secure)	17.10.2018 14:54	Unknown
KNX BAOS 83x Demo	17.10.2018 14:54	Unknown
KNX BAOS 840 Demo	17.10.2018 14:53	Unknown

KNX IP Interface 732 secure

Last Modified: 02.11.2018 09:46 Total size: 15.9 KB

Details Security Project Log Project Files

Export

Export Keyring

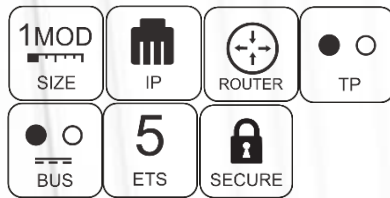
Device Certificates

+ Add - Delete

Serial Number	Factory Key (FDSK)	Device
00C5:FFFFDFE8	15CE43CF0C1C41FF9B39466CF1077836	1.1.65 KNX IP Interface 732 secure

ETS Version ETS 5.6.6 (Build 1190) License Demo Apps 0 active

KNX IP Interface 732 *secure*



First KNX IP Interface with 18mm width (1 Unit)

- KNXnet/IP Tunneling
- Up to 8 simultaneous connections

User Interface

- Display of tunneling connections on the device
- Display of communication errors



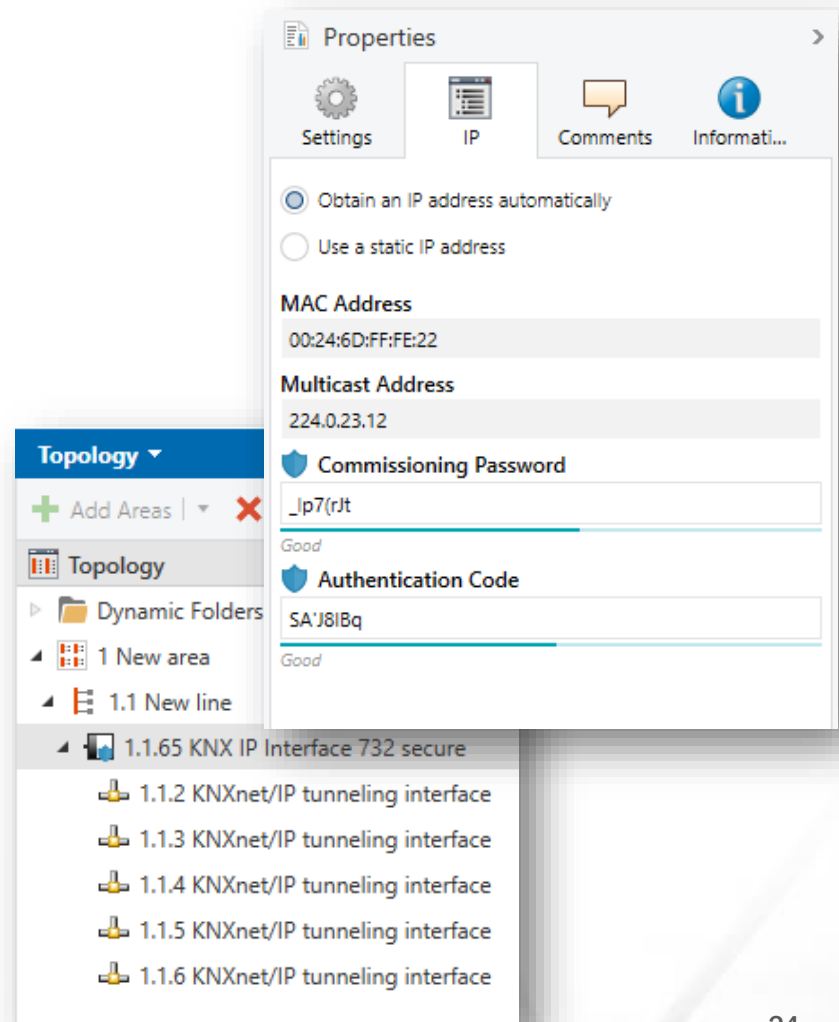
KNX IP: Individual addresses

Device address

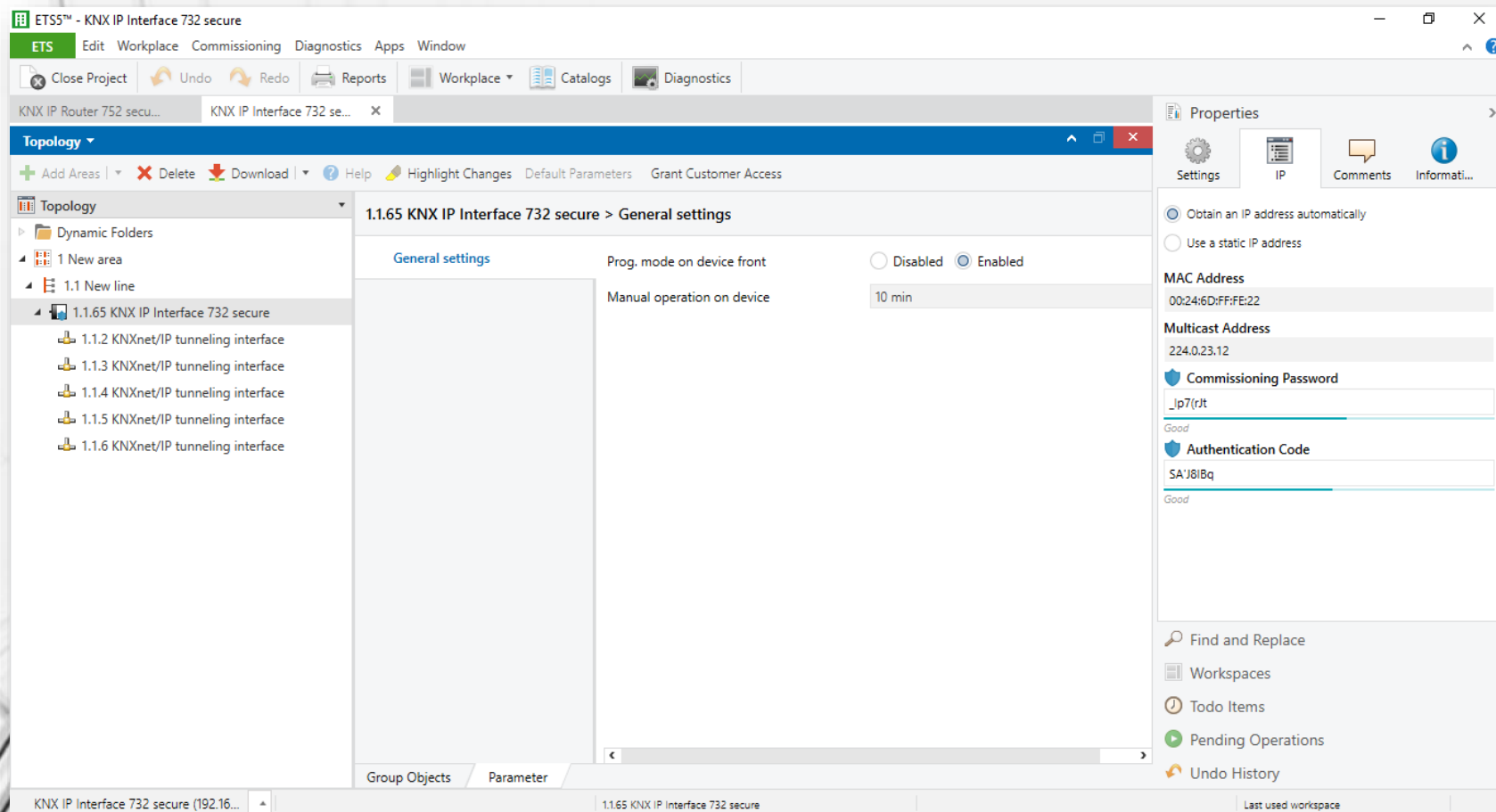
- As with all devices

Additional physical addresses

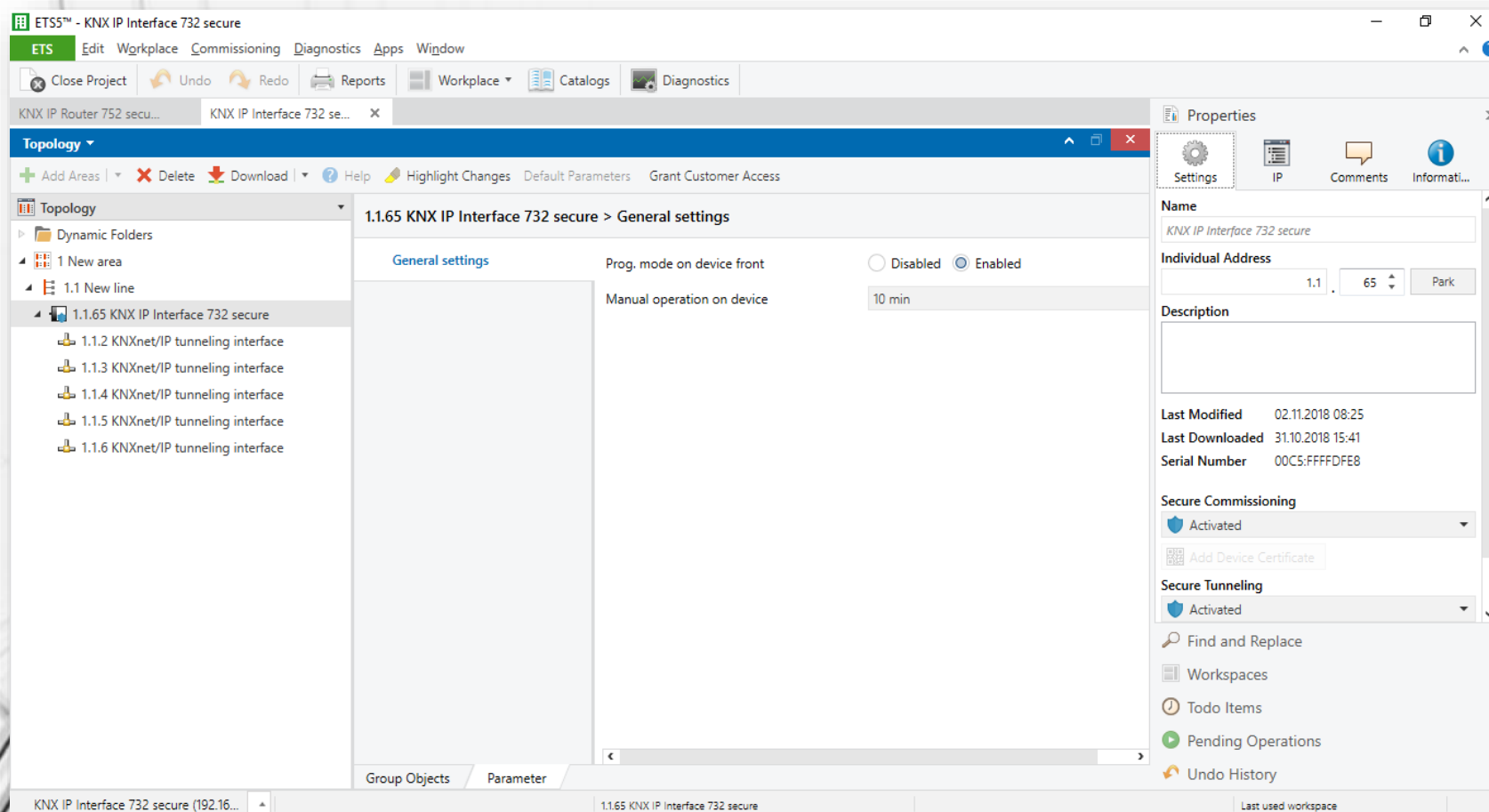
- One for each connection
- Must not be the same as your own device address
- Must not be used by other devices
- Since ETS5:
Visible in the topology view



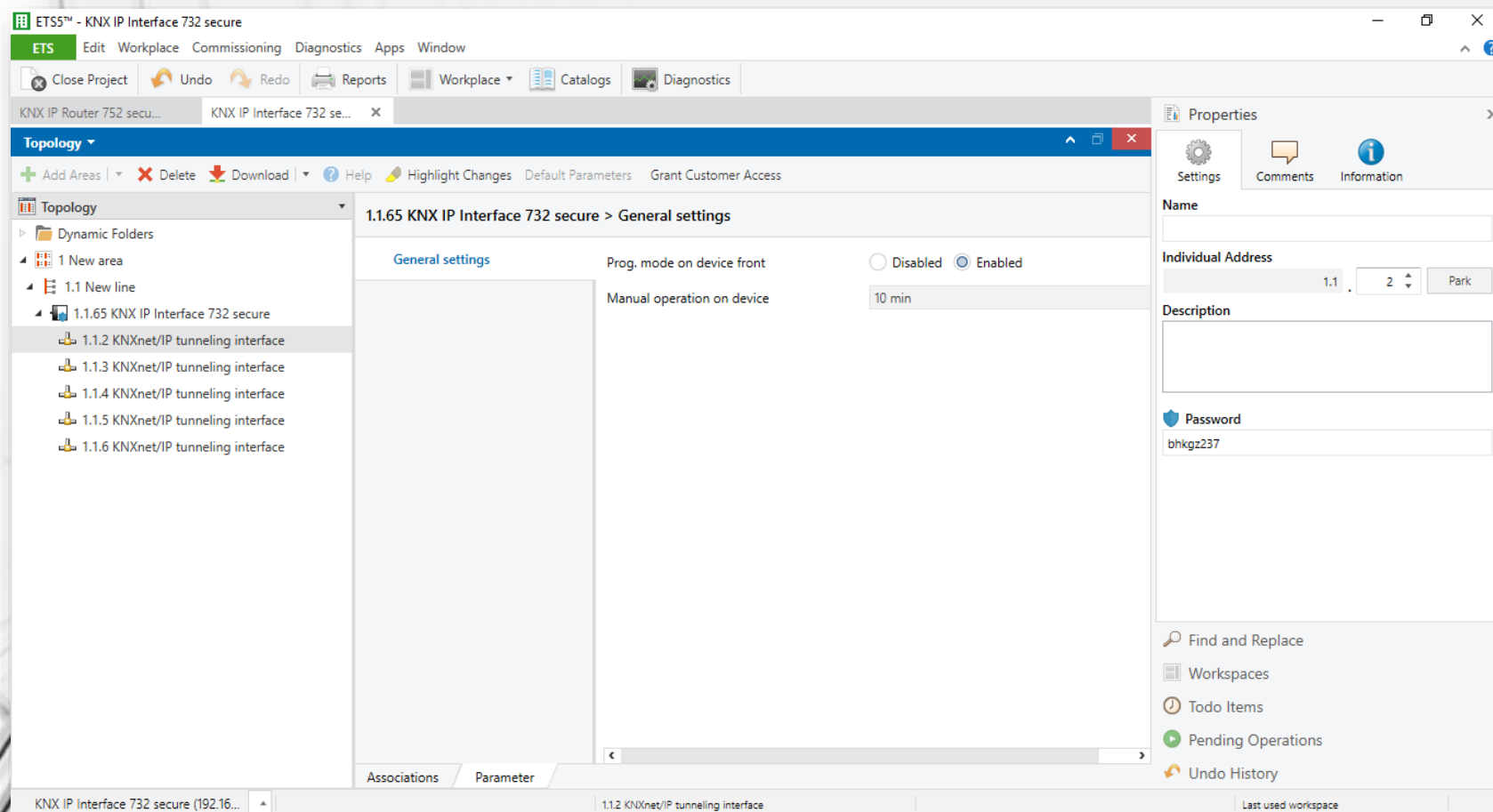
IP Settings with Security



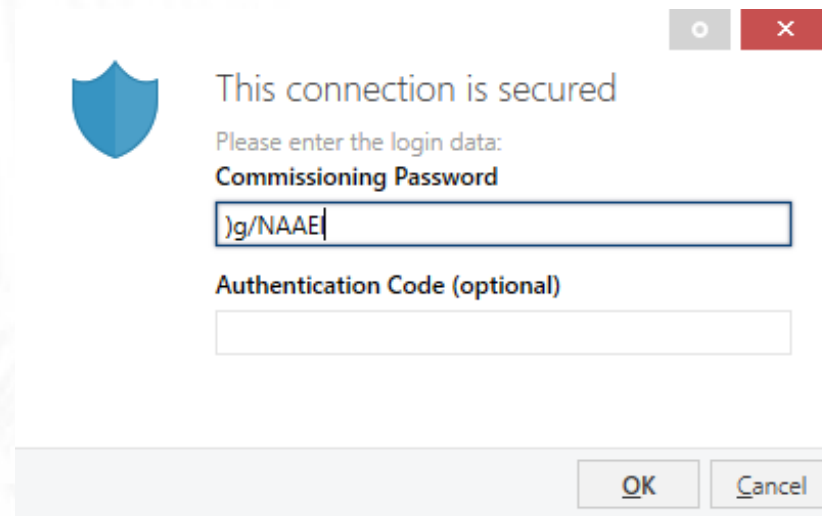
Secure Interface



Secure Tunnel



Password for Tunnel



This connection is secured

Please enter the login data:

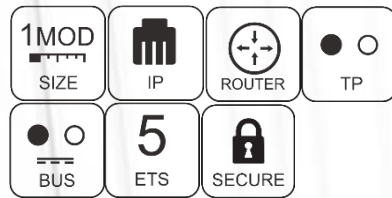
Commissioning Password

)g/NAAE(

Authentication Code (optional)

OK Cancel

KNX IP Router 752 *secure*



First KNX IP Router with 18mm width (1 Unit)

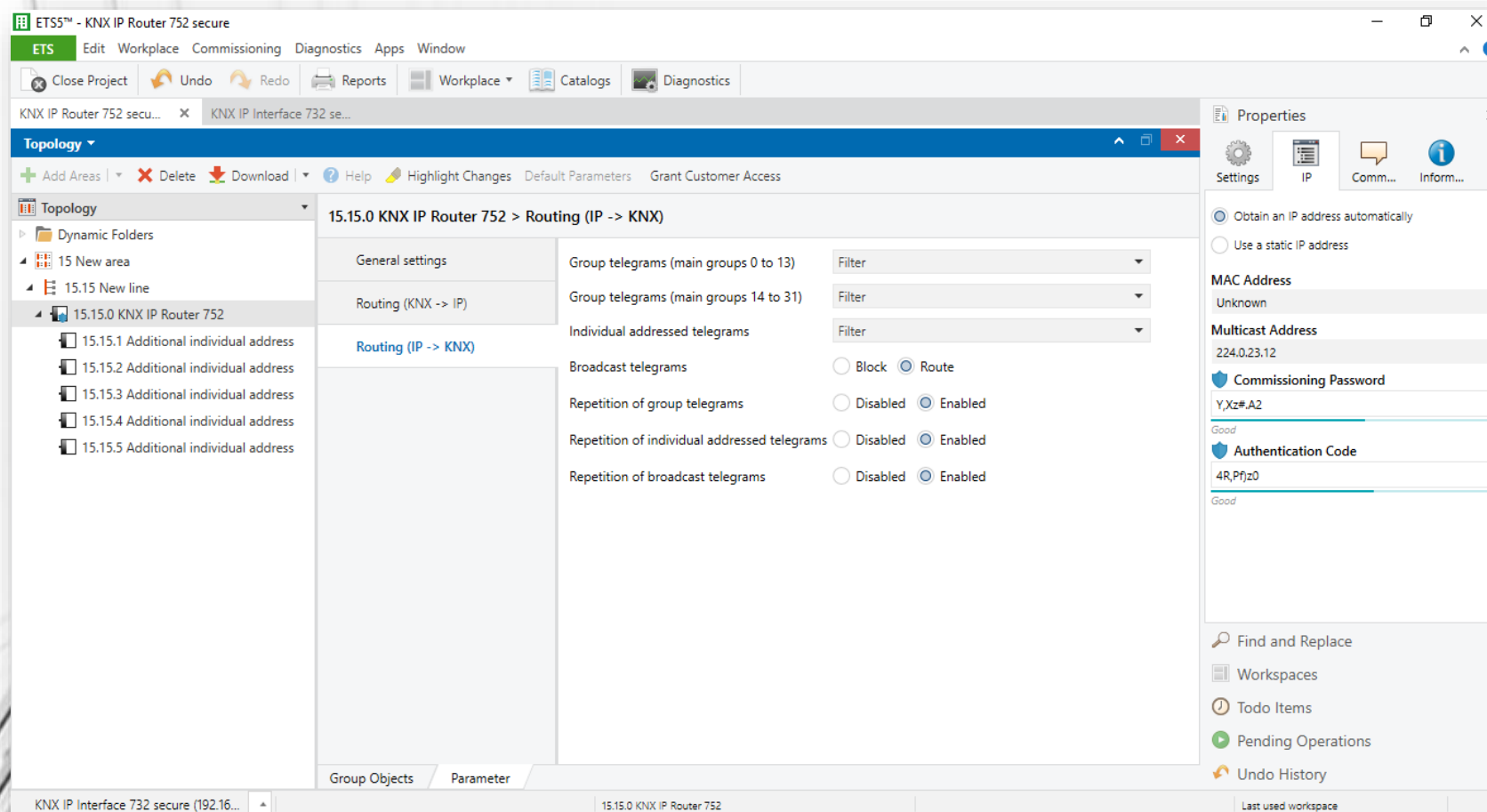
- KNXnet/IP Tunneling
- Up to 8 simultaneous connections
- KNXnet/IP Routing
- Filter table for main groups 0..31

User Interface

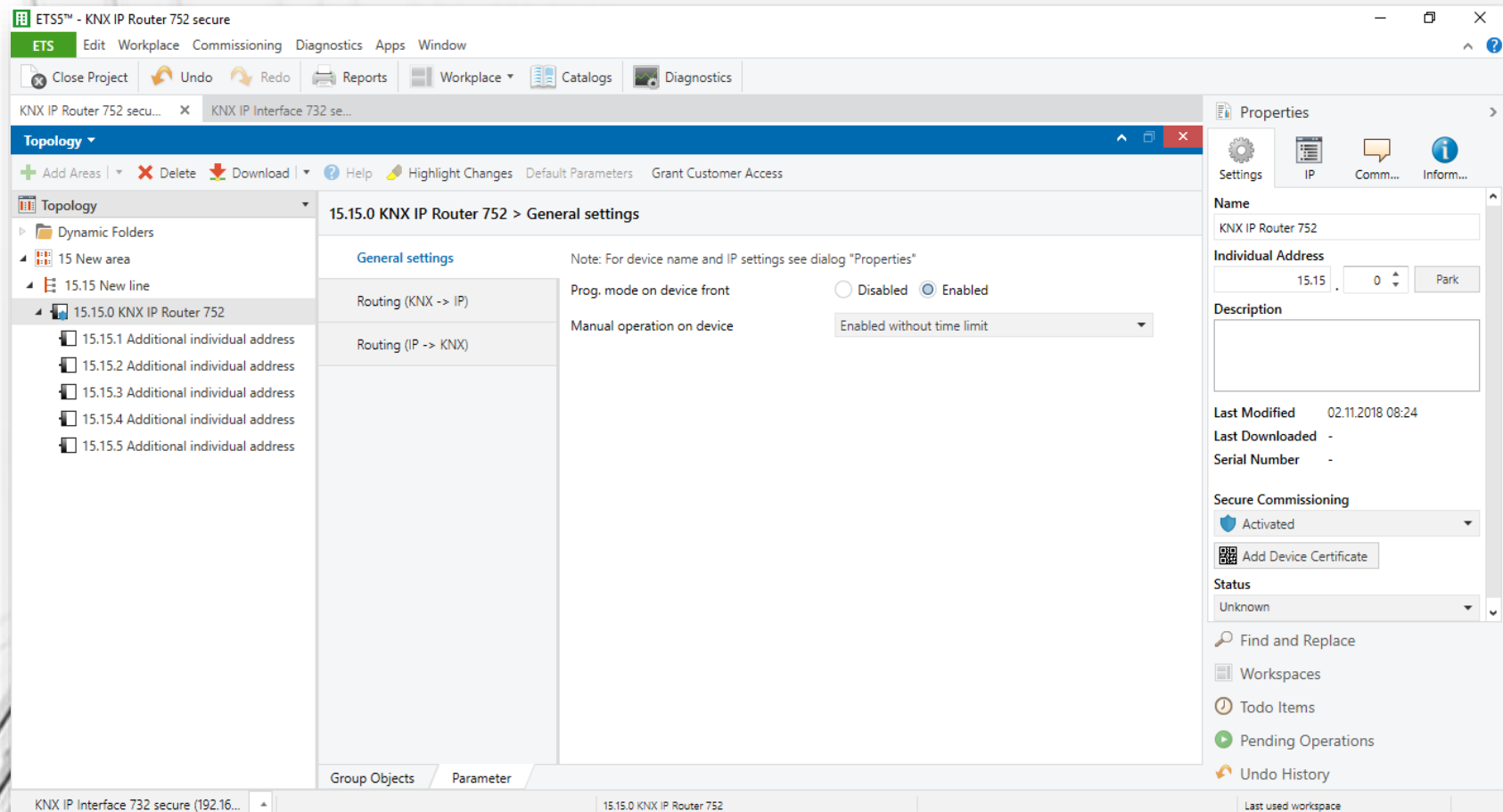
- Diagnosis functions via buttons
- Display of communication errors



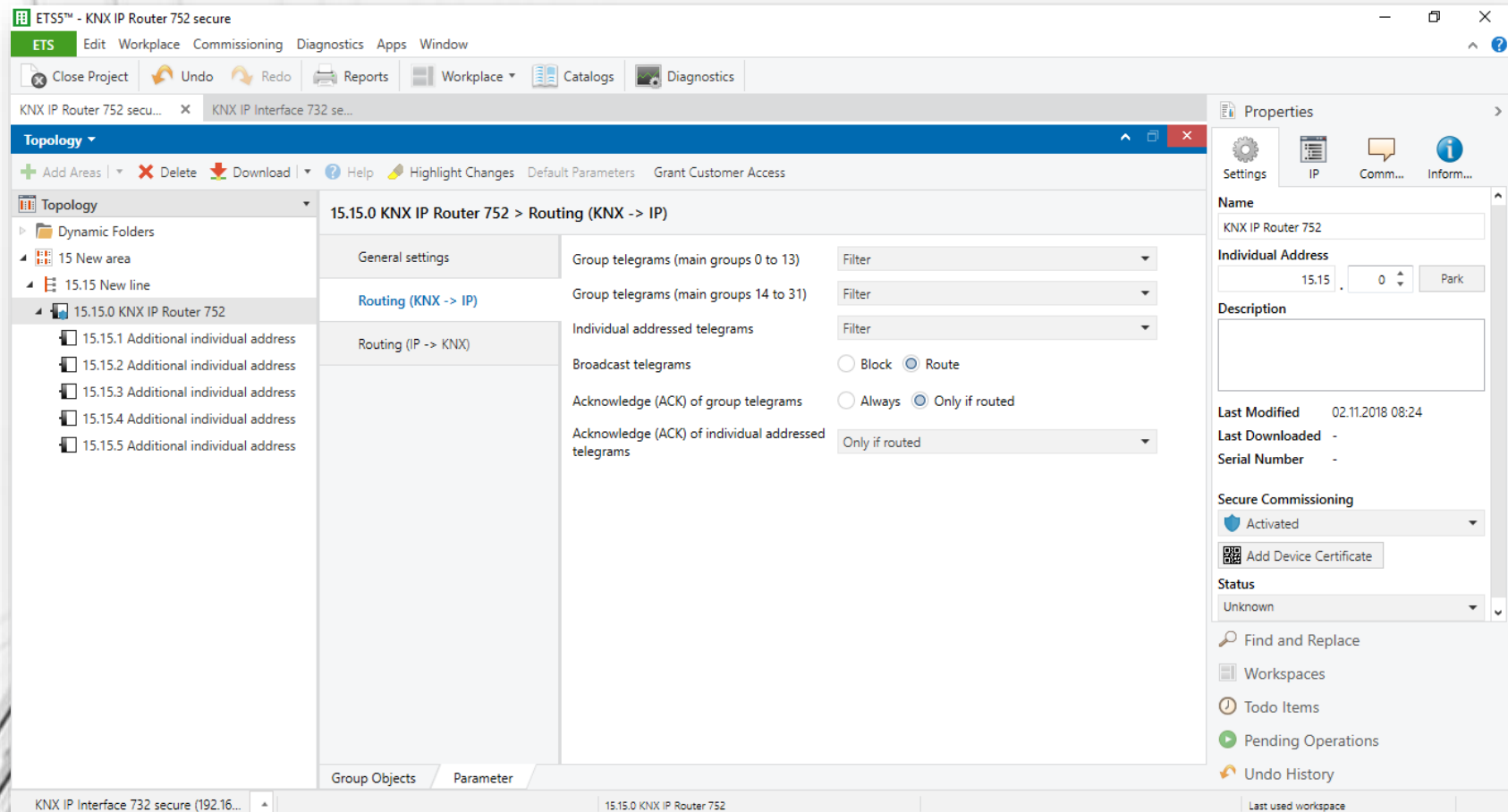
Secure Router



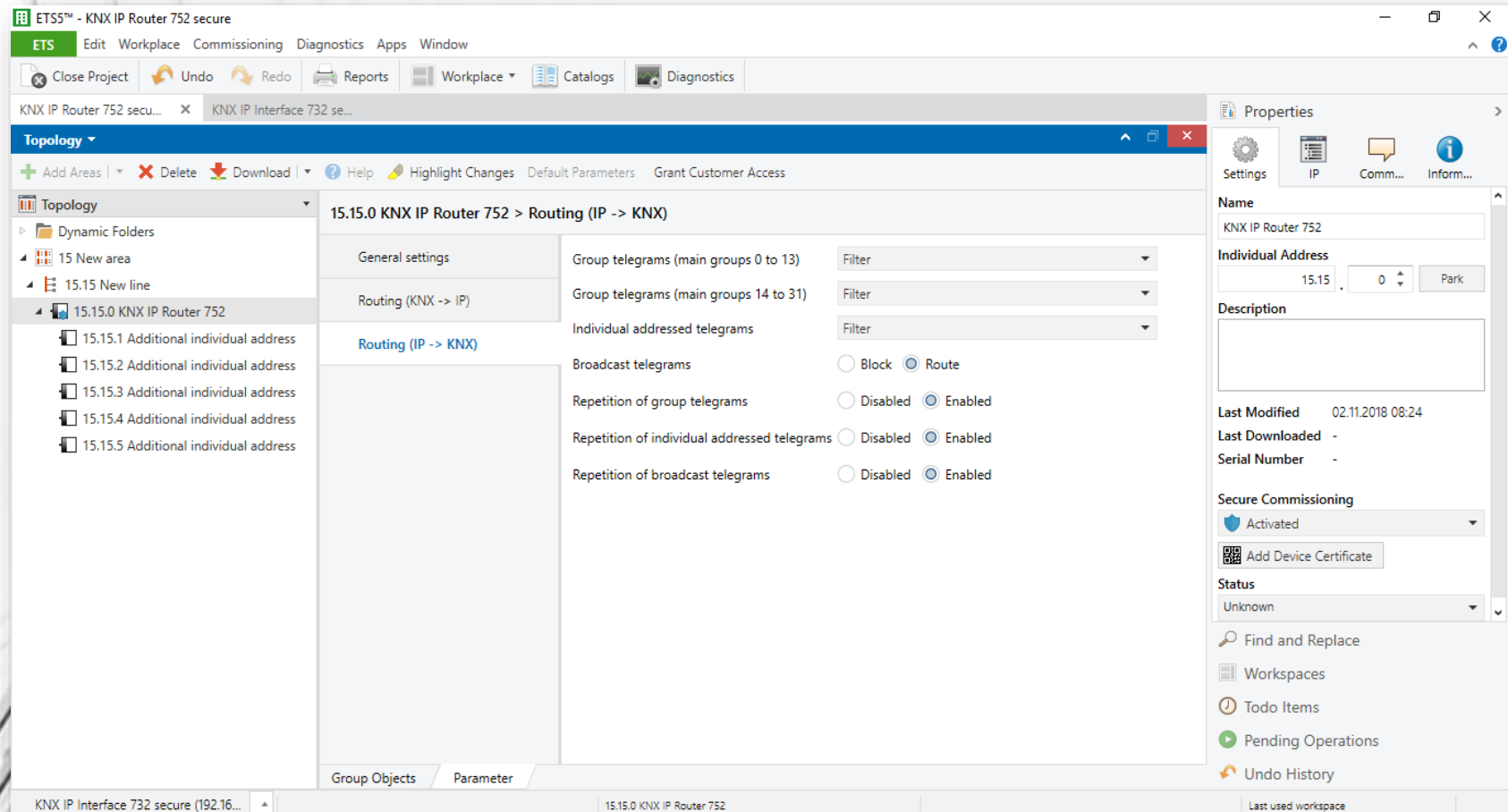
Secure Router general



Secure Router KNX -> IP



Secure Router IP -> KNX



ETS Connection Manager

The screenshot displays the ETS5™ - KNX IP Interface 732 secure software interface. The main window is titled "ETS5™ - KNX IP Interface 732 secure" and features a menu bar with "ETS", "Edit", "Workplace", "Commissioning", "Diagnostics", "Apps", and "Window". Below the menu bar is a toolbar with icons for Overview, Bus, Catalogs, and Settings. The left sidebar contains a tree view with the following items: Connections, Interfaces, Options, Monitor, Group Monitor, Bus Monitor, Diagnostics, Unload Device, Device Info, Individual Addresses, Programming Mode, Individual Address Check, and Line Scan. The main area is divided into two sections: "Current Interface" and "Configured Interfaces". The "Current Interface" section shows the selected interface: "1.1.60 KNX IP Interface 732 secure" with an individual address of 1.1.2. The "Configured Interfaces" section displays a table of discovered interfaces.

Icon	Interface Name	IP Address	MAC Address
🔌	15.15.99 00-24-6D-01-80-68	192.168.1.68:3671	00:24:6D:01:80:68
🔌	1.0.1 KNX IP BAOS 777 - Rt	192.168.1.224:3671	00:24:6D:01:06:94
🔌	15.15.55 KNX IP Baos 777 Ms	192.168.1.45:3671	00:24:6D:00:E1:33
🔌	1.1.60 KNX IP Interface 732 secure	192.168.1.47:3671	00:50:C2:55:40:78

The right sidebar shows the "IP Tunneling" settings for the selected interface. It includes fields for Name, Host Individual Address, Individual Address, IP Address, Port, and MAC Address. The "Test" button is highlighted.

ETS Version: ETS 5.6.6 (Build 1190) License: Demo Apps: 0 active

**Thank
You
for your
Attention!**

Weinzierl Engineering GmbH