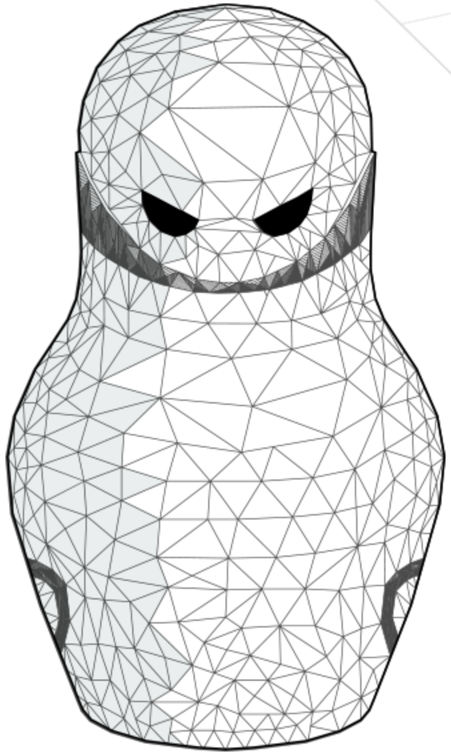


ZERONIGHTS 2015

Security in KNX or how to steal a skyscraper

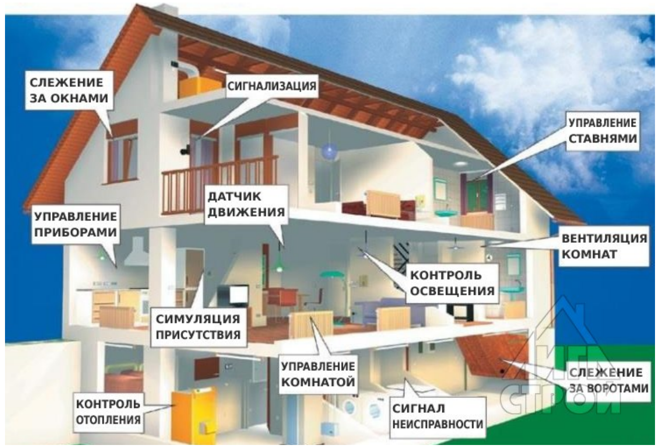
Egor Litvinov

e.litvinov@dsec.ru

Egor Litvinov

Digital Security

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



from «Smart house» to BMS

Building Management System - is a computer-based control system installed in buildings that controls and monitors the building’s mechanical and electrical equipment

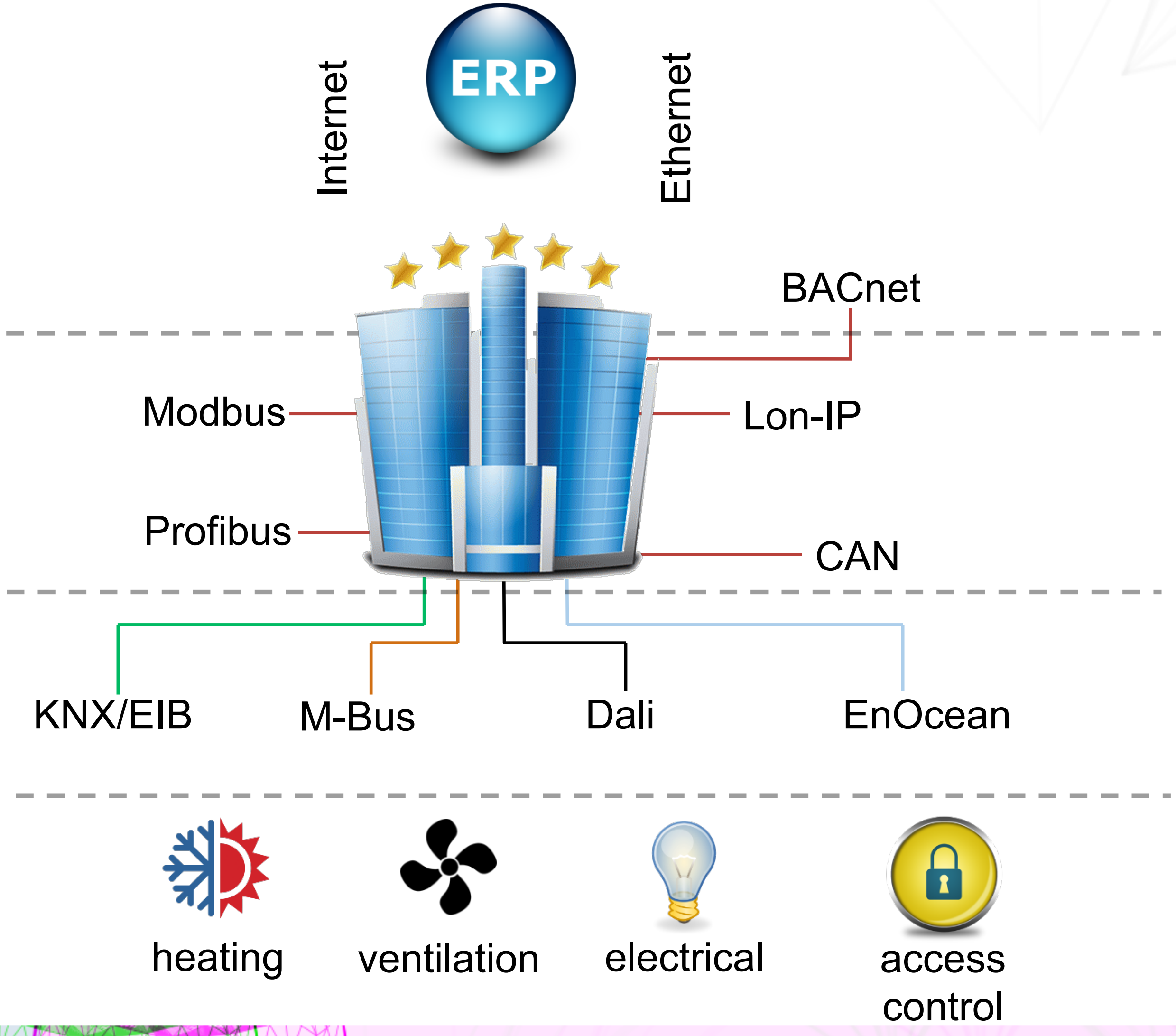
Main objectives of BMS

Reduce power consumption

Control operation of different systems

Provide comfort to visitors

BMS
What is it?



Management level

Internet

ERP

Ethernet

BACnet

Automation level

Modbus

Profibus

Lon-IP

CAN

Field level

KNX/EIB

M-Bus

Dali

EnOcean

heating

ventilation

electrical

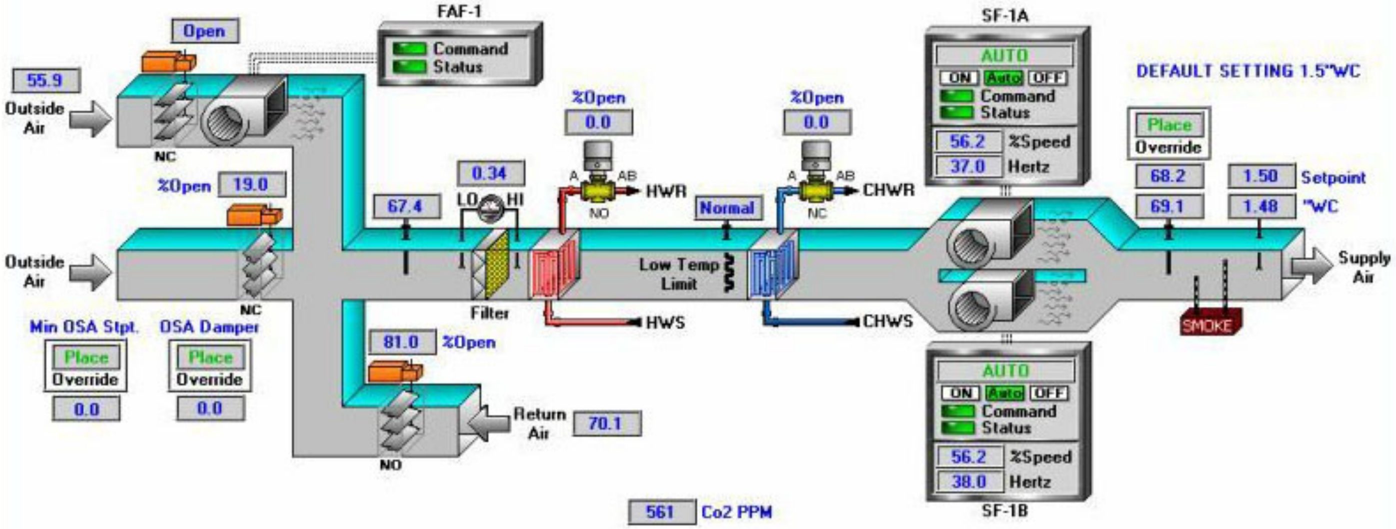
access control

BMS in detail:

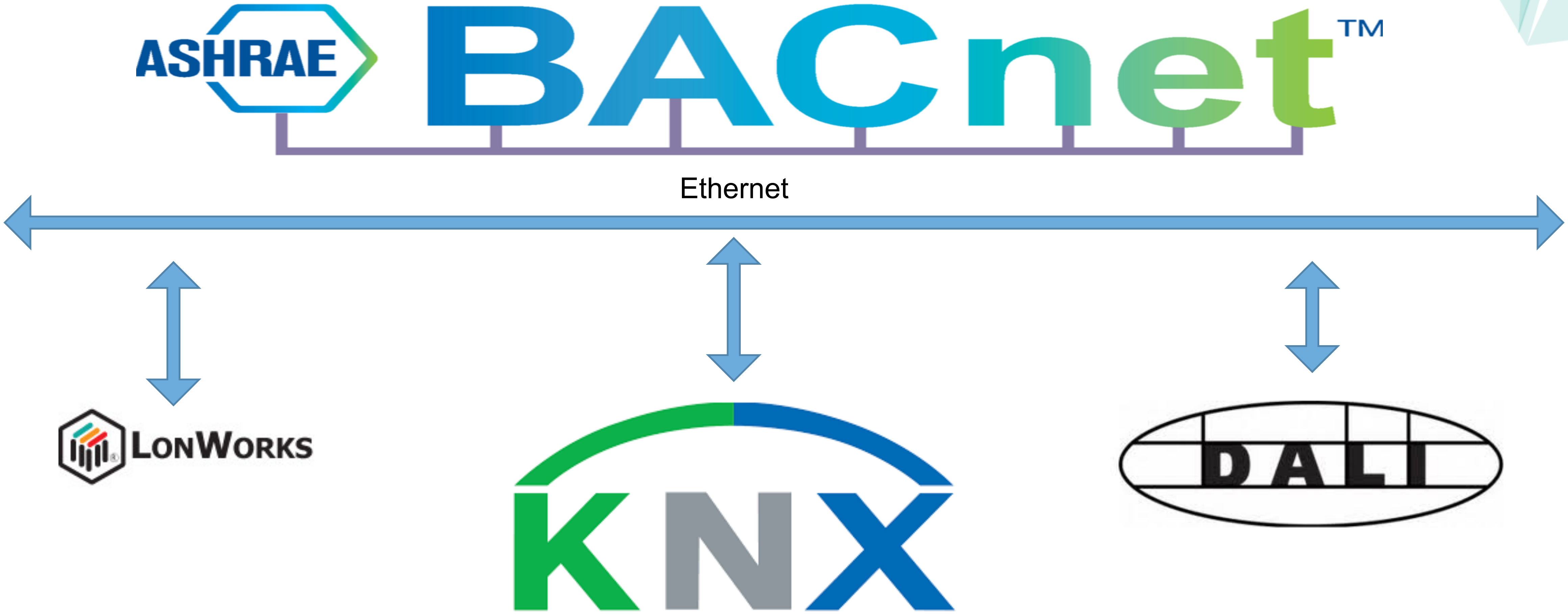
Light Control System

Access Control System

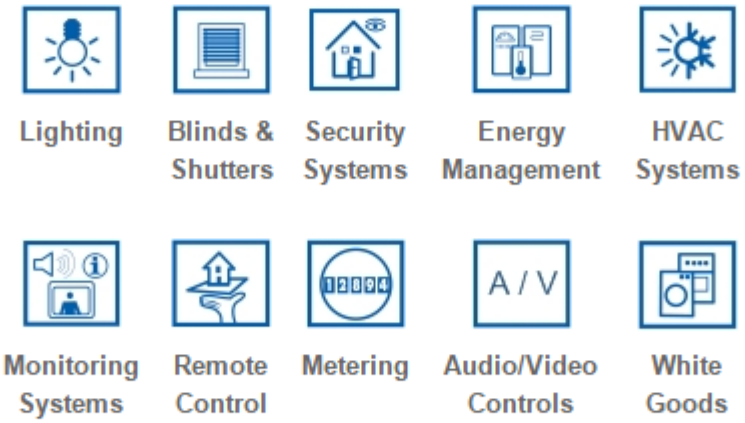
HVAC System



Other Systems …


ASHRAE
BACnet™
Ethernet
LonWorks
KNX
DALI

KNX is a standardized (EN 50090, ISO/IEC 14543), OSI-based network communications protocol for intelligent buildings. KNX is the successor to, and convergence of, three previous standards: the European Home Systems Protocol (EHS), BatiBUS, and the European Installation Bus (EIB or Instabus). The KNX standard is administered by the KNX Association *



https://en.wikipedia.org/wiki/KNX_(standard)

Where KNX/EIB is used:

Hotel

Headquarters of a Turkish corporation GAMA

Air Terminal «Concourse A» at Dubai International Airport

Inside the room

Movement detector

Thermoelectric Valve Drives

Push button sensor

Room Thermostat Fan Coil

Brightness controller

….

What can we manipulate inside KNX network?

Energy consumption measures

Heating/cooling parameters by controlling valves

Ventilation

Air quality sensor

....

My workplace

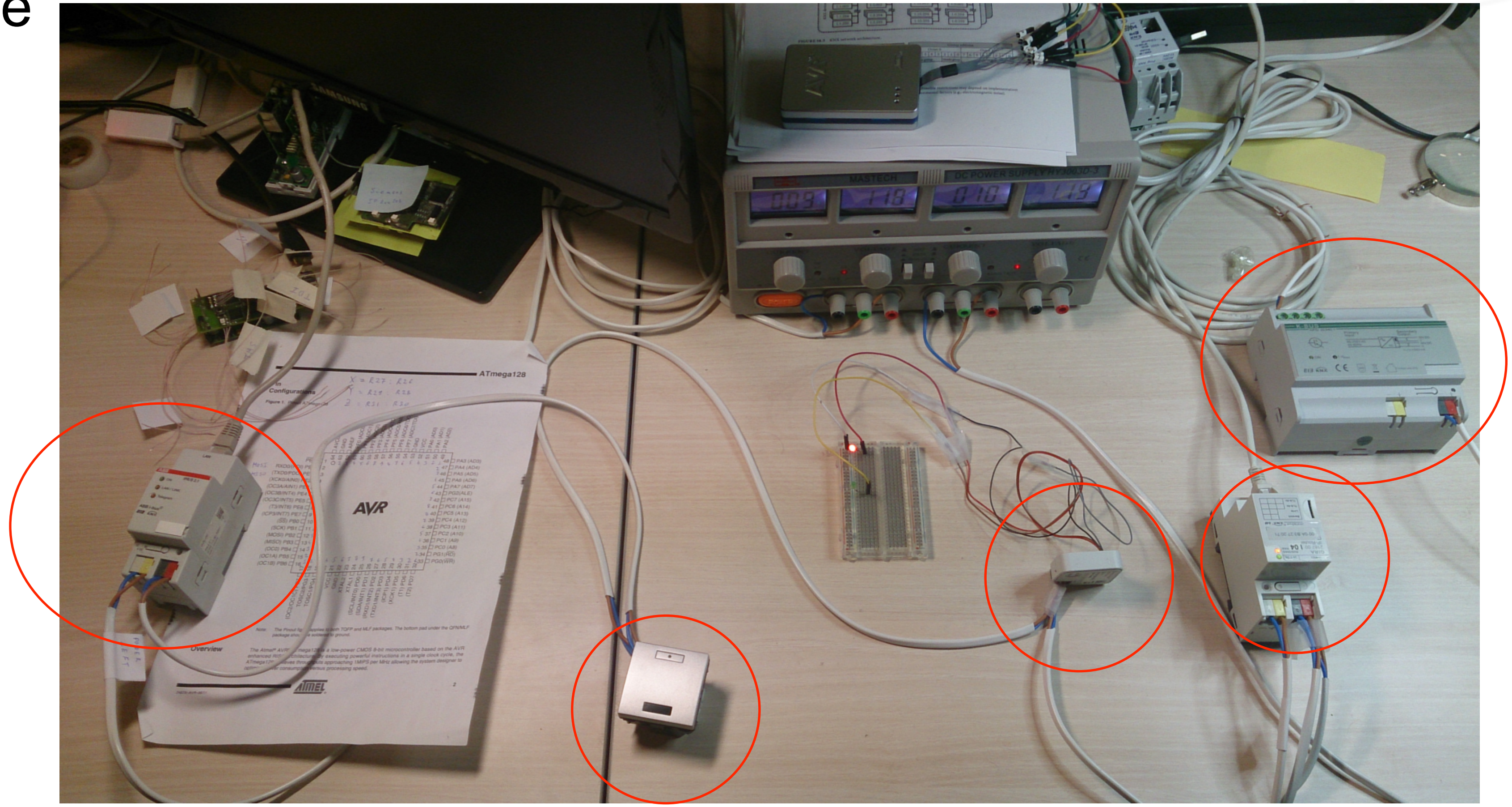


ABB
IPR/S 2.1

Power
module

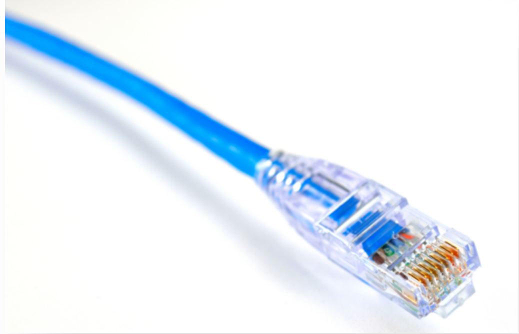
Gira
IP router

button KNX

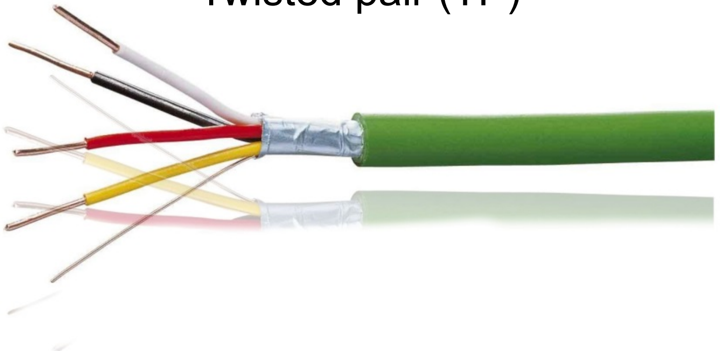
dimmer KNX

Physical communication media*:

KNX
IP



KNX
Twisted pair (TP)



9600 bit/s

KNX
RF

))))

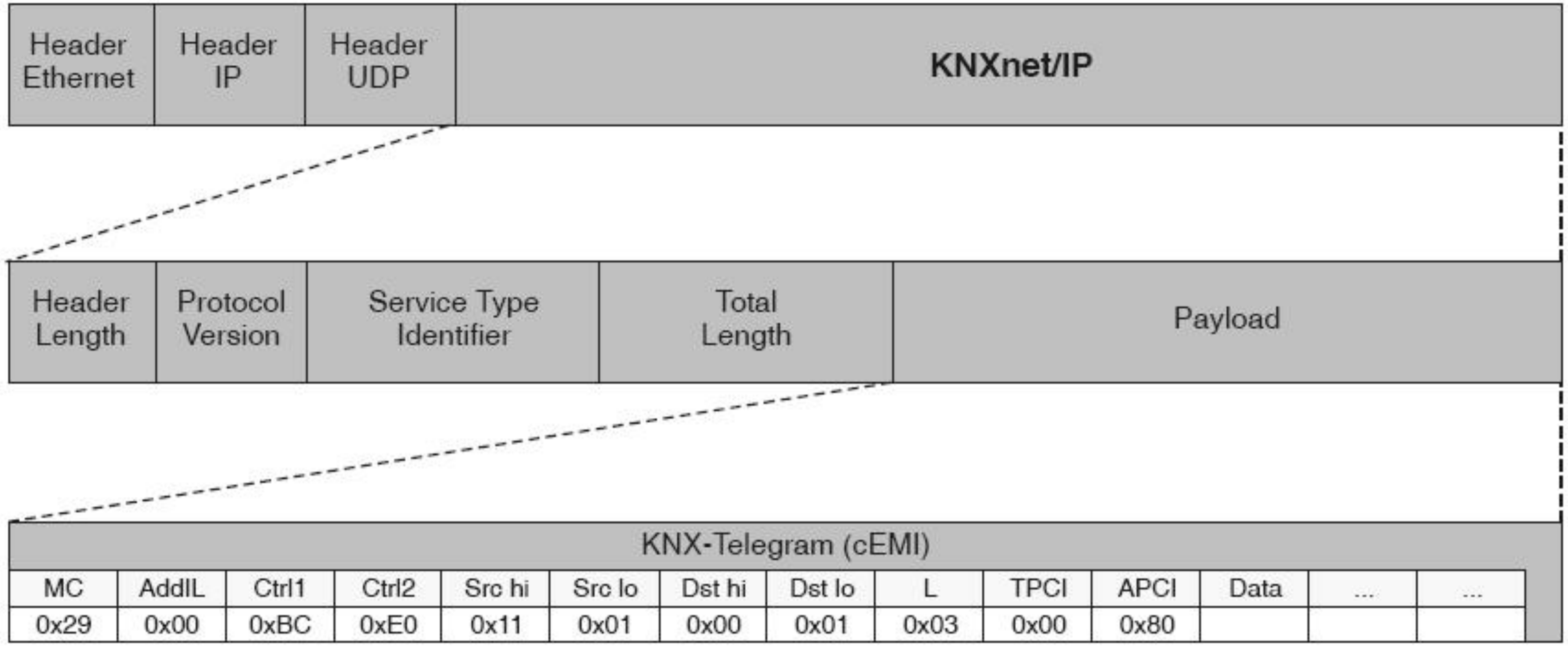
16384 kbit/s
868 MHz

KNX
Power Line (PL110)

1200 bit/s

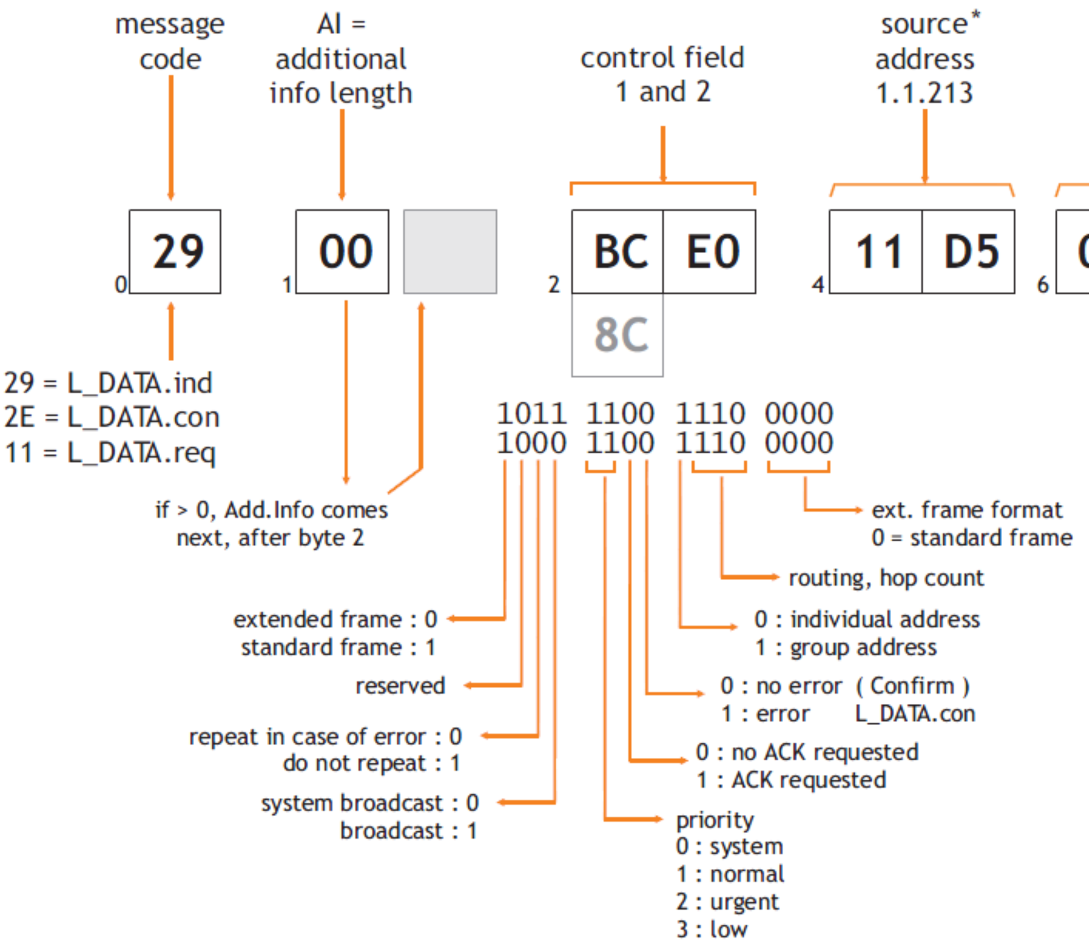
* http://www.konnex-russia.ru/knx-standard/communication-media/

KNXnet/IP



MC	AddIL	Ctrl1	Ctrl2	Src hi	Src lo	Dst hi	Dst lo	L	TPCI	APCI	Data	...	...
0x29	0x00	0xBC	0xE0	0x11	0x01	0x00	0x01	0x03	0x00	0x80			

cEMI



message code

AI = additional info length

control field 1 and 2

source* address 1.1.213

dest. address 0/1/40

data length

TPCI

APCI / data

data

0	1		2		4		6		8	9			
29	00		BC	E0	11	D5	01	28	03	00	80	19	0e
			8C										

29 = L_DATA.ind
2E = L_DATA.con
11 = L_DATA.req

if > 0, Add.Info comes next, after byte 2

data bytes, w/o TPCI/APCI bits

data = EIS5 = 20.64 °C

```
1011 1100 1110 0000
1000 1100 1110 0000
```

ext. frame format
0 = standard frame

routing, hop count

0 : individual address
1 : group address

0 : no error (Confirm)
1 : error L_DATA.con

0 : no ACK requested
1 : ACK requested

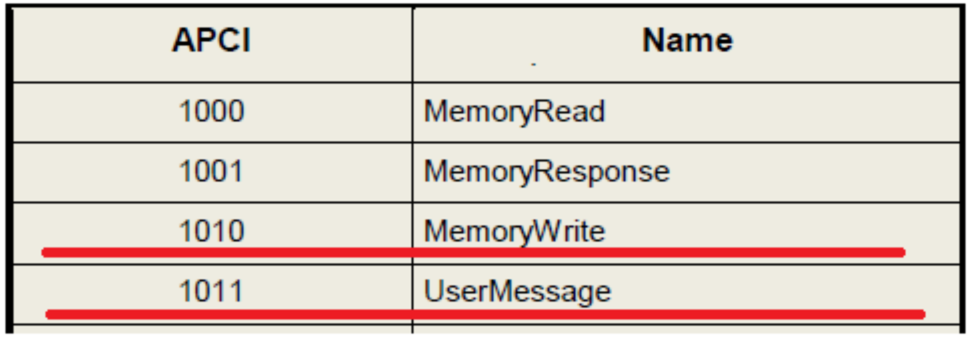
priority
0 : system
1 : normal
2 : urgent
3 : low

extended frame : 0
standard frame : 1

reserved

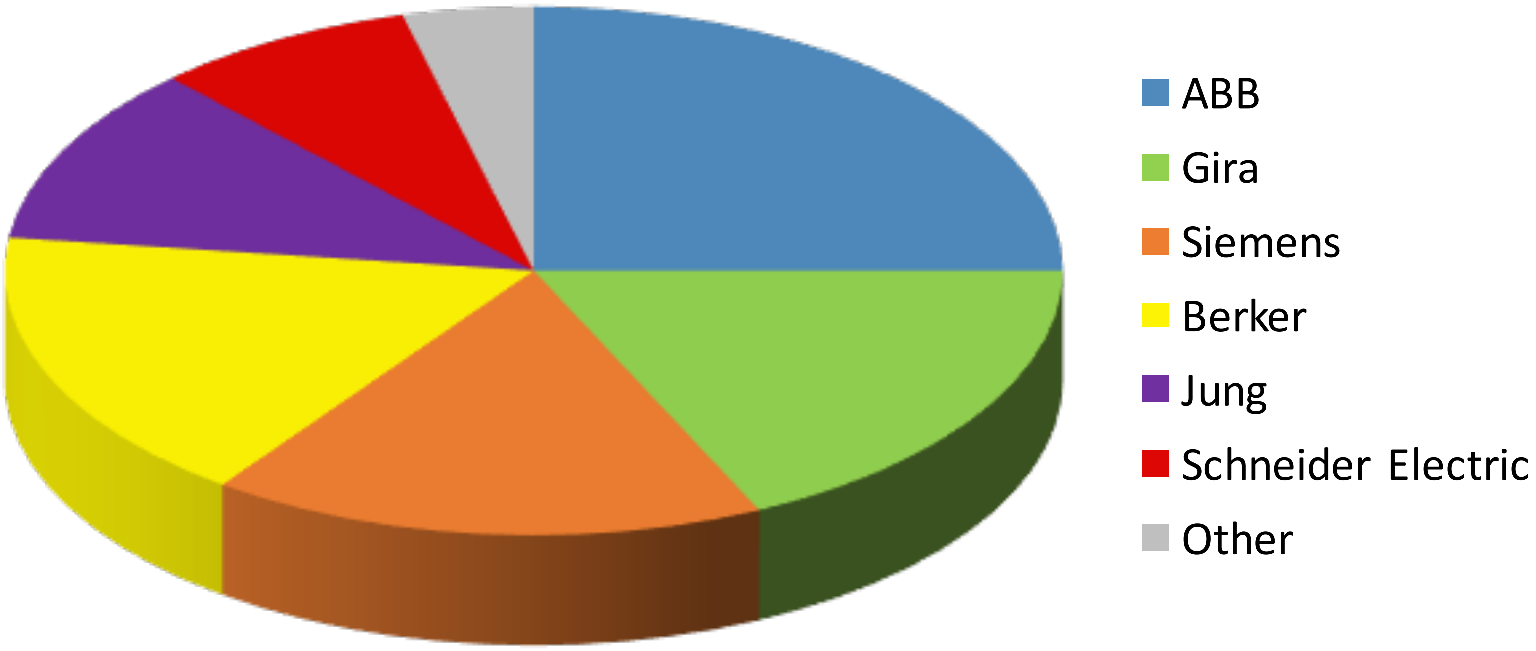
repeat in case of error : 0
do not repeat : 1

system broadcast : 0
broadcast : 1



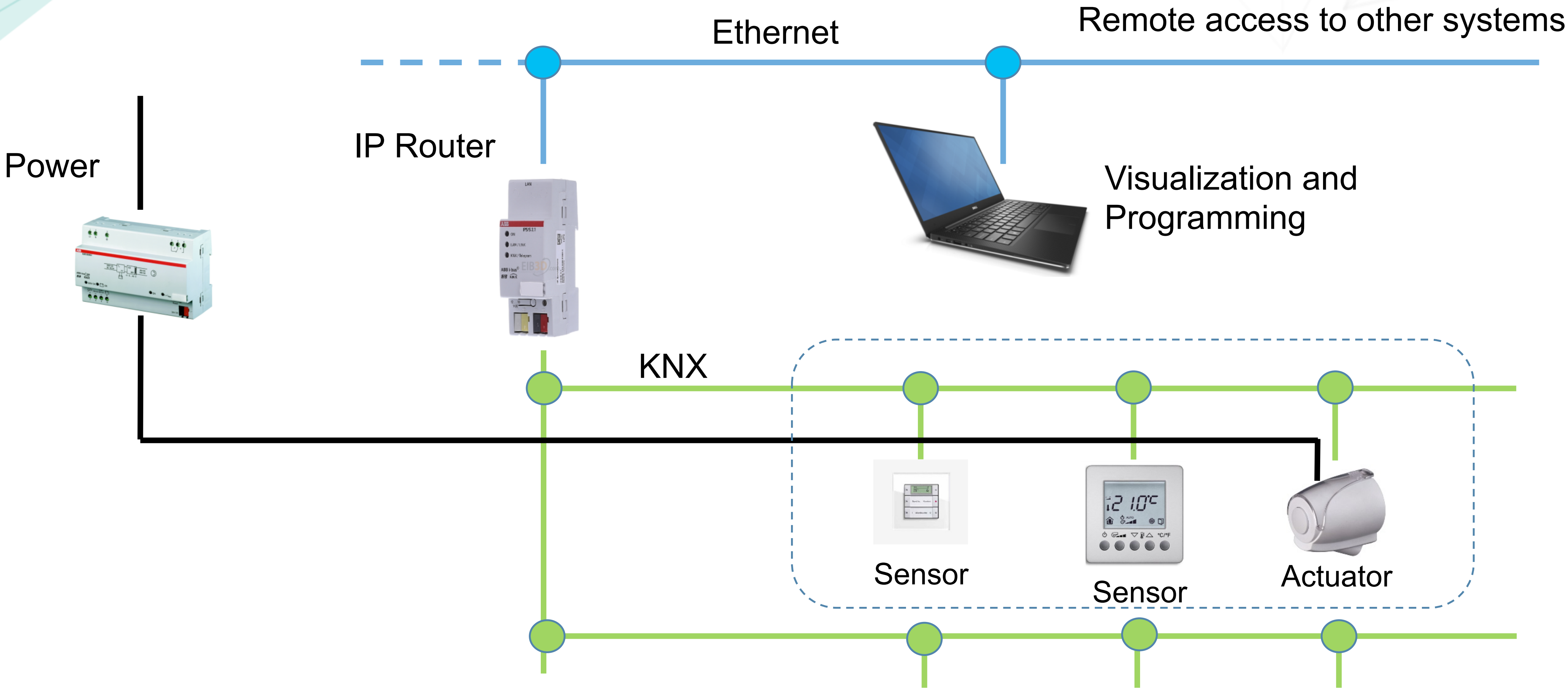
APCI	Name
1000	MemoryRead
1001	MemoryResponse
1010	MemoryWrite
1011	UserMessage

Vendors by popularity *



* http://knxtoday.com/2013/10/2357/research-smart-home-market-in-germany.html

Why choose KNX to IP routers?



ABB

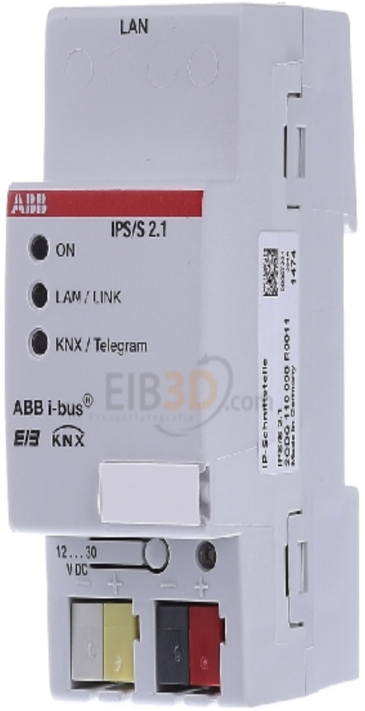
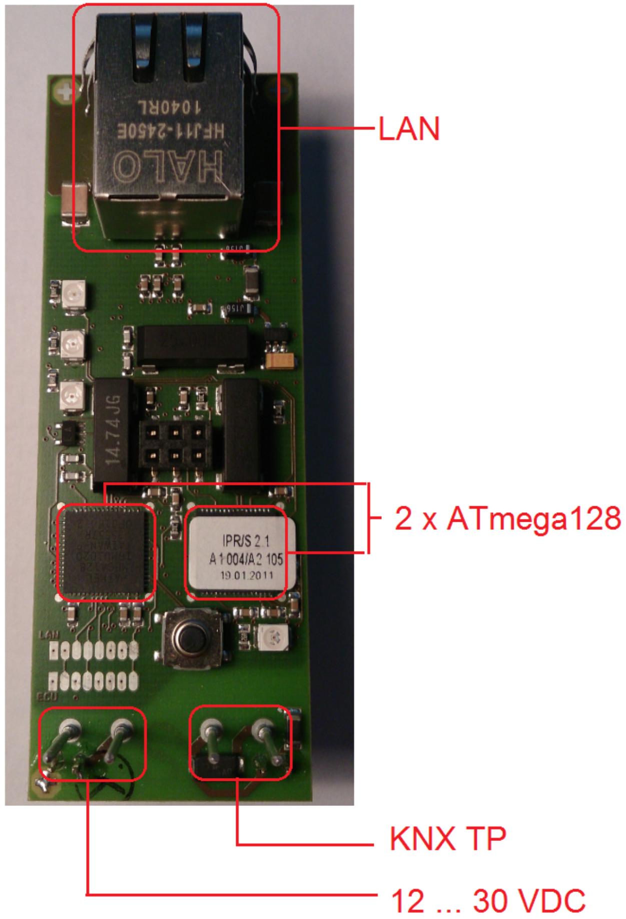
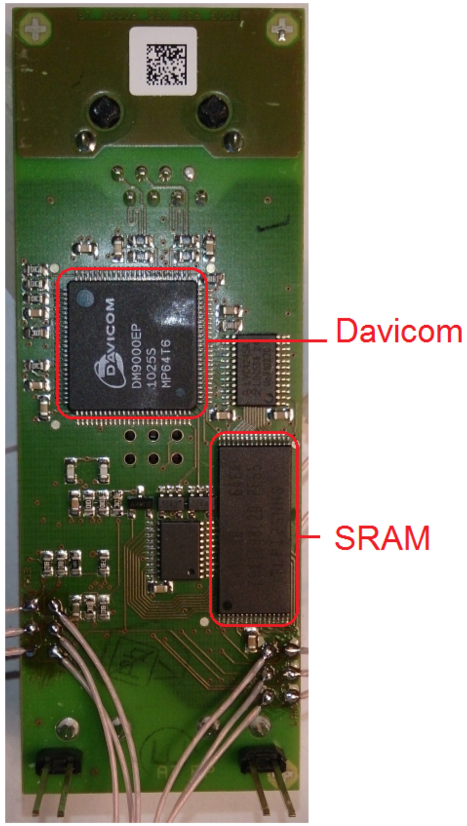


ABB
IPR/S 2.1





CPU:
- ATmega128
  128 Kbytes flash
  4 Kbytes EEPROM
  4 Kbytes internal SRAM

SRAM:
  128Kx8 bit

OS:
- perhaps ethernut

ABB

How to get control over the device:

Connect to the Ethernet

Run ABB i-bus Firmware Tool

Update

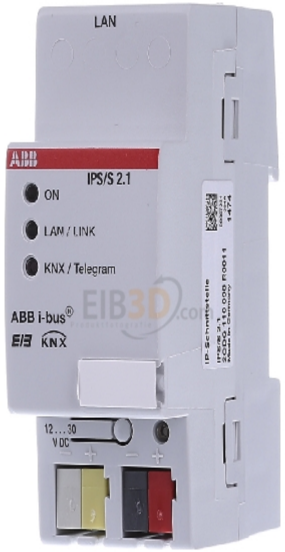
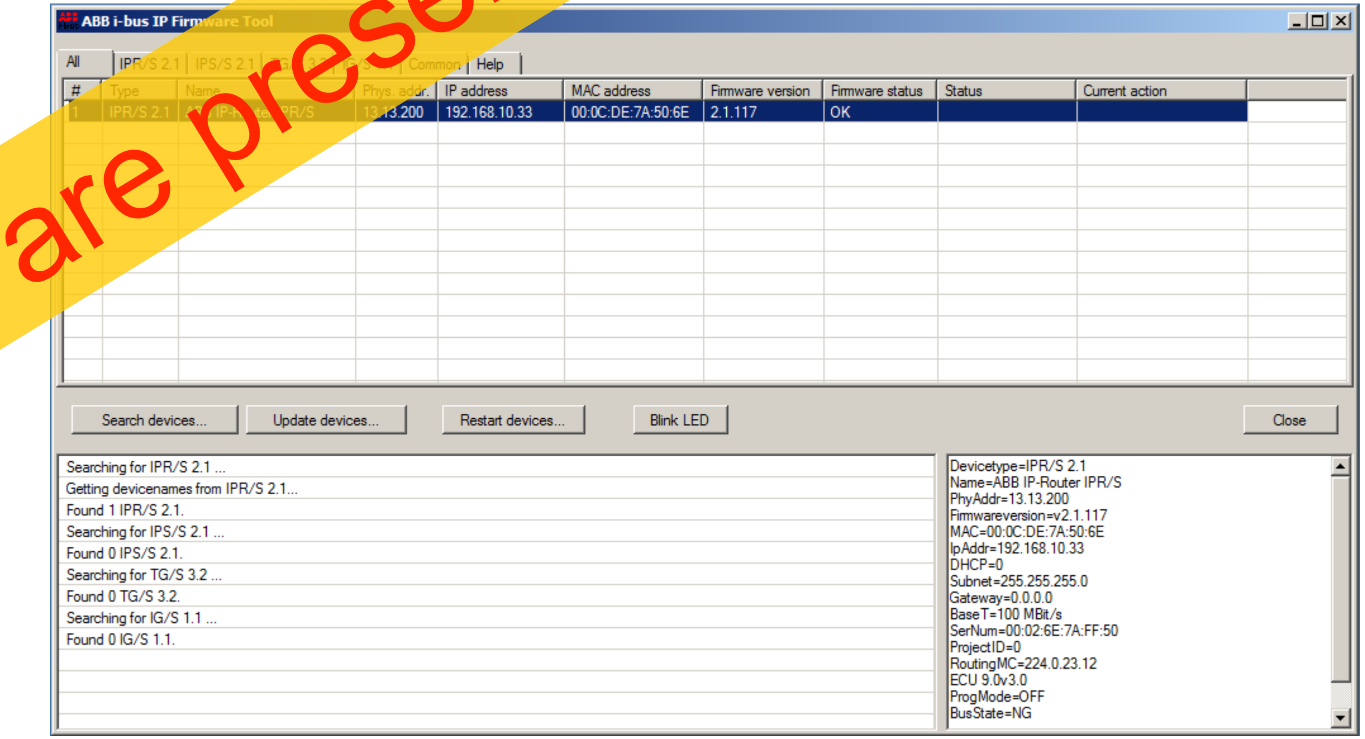


ABB
IPR/S 2.1

No checks are present



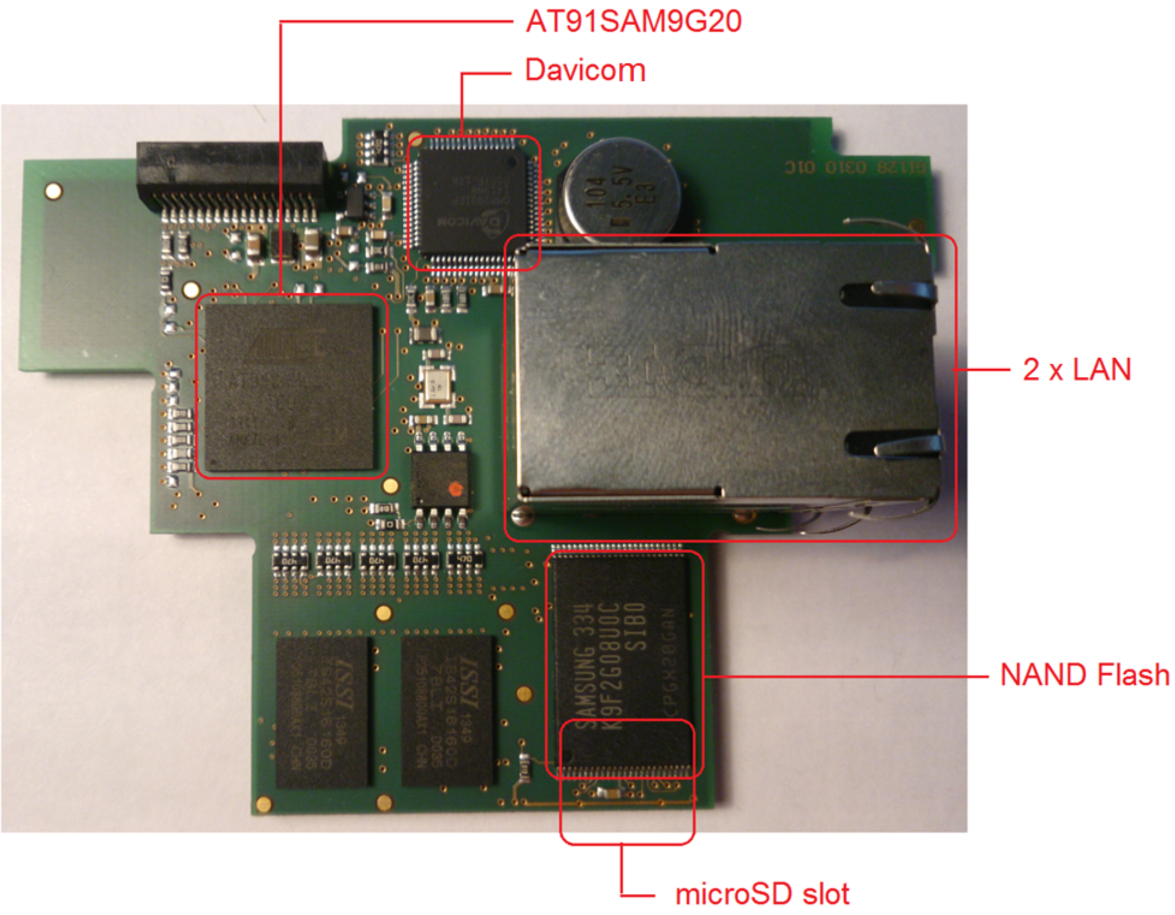
#	Type	Name	Phys. addr.	IP address	MAC address	Firmware version	Firmware status	Status	Current action
1	IPR/S 2.1	ABB IP-Router IPR/S	13.13.200	192.168.10.33	00:0C:DE:7A:50:6E	2.1.117	OK		

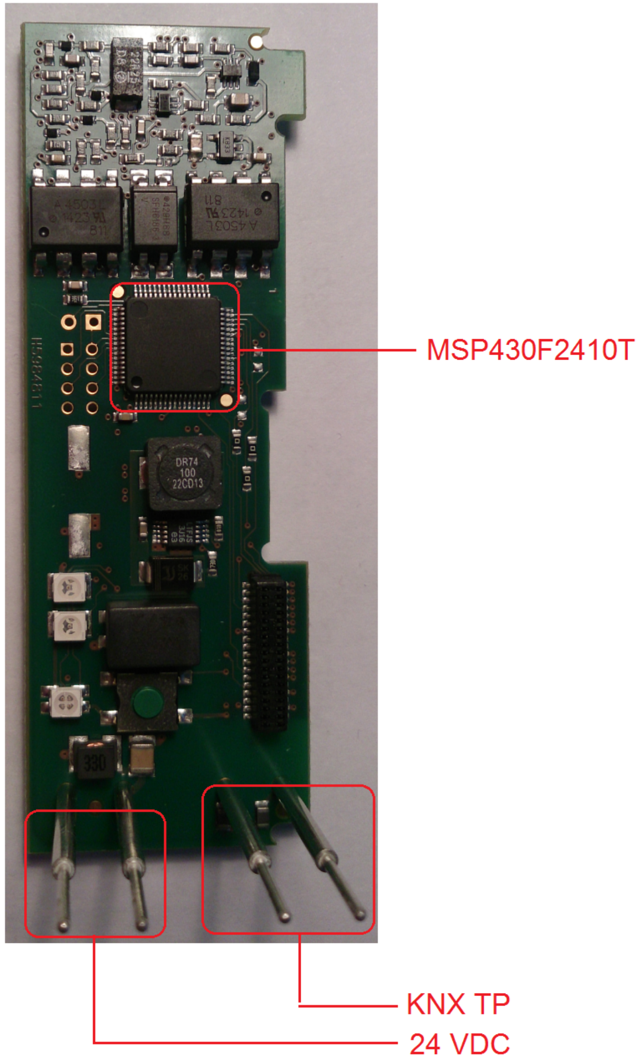
```
Searching for IPR/S 2.1 ...
Getting devicenames from IPR/S 2.1...
Found 1 IPR/S 2.1.
Searching for IPS/S 2.1 ...
Found 0 IPS/S 2.1.
Searching for TG/S 3.2 ...
Found 0 TG/S 3.2.
Searching for IG/S 1.1 ...
Found 0 IG/S 1.1.
```

```
Devicetype=IPR/S 2.1
Name=ABB IP-Router IPR/S
PhyAddr=13.13.200
Firmwareversion=v2.1.117
MAC=00:0C:DE:7A:50:6E
IpAddr=192.168.10.33
DHCP=0
Subnet=255.255.255.0
Gateway=0.0.0.0
BaseT=100 MBit/s
SerNum=00:02:6E:7A:FF:50
ProjectID=0
RoutingMC=224.0.23.12
ECU 9.0v3.0
ProgMode=OFF
BusState=NG
```

Gira

Gira
IP router





Gira

Gira
IP router

AT91SAM9G20:

- ARM926EJ-S
- 64 Kbytes ROM
- 2 x 16 Kbytes SRAM
- Ethernet 10/100 Base-T

NAND Flash (K9F2G08U0C)

- 256Mbytes NAND Flash

MSP430F2410T:

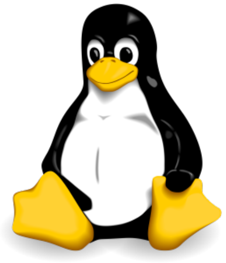
- 56Kbytes + 256 bytes Flash Memory
- 4Kbytes RAM

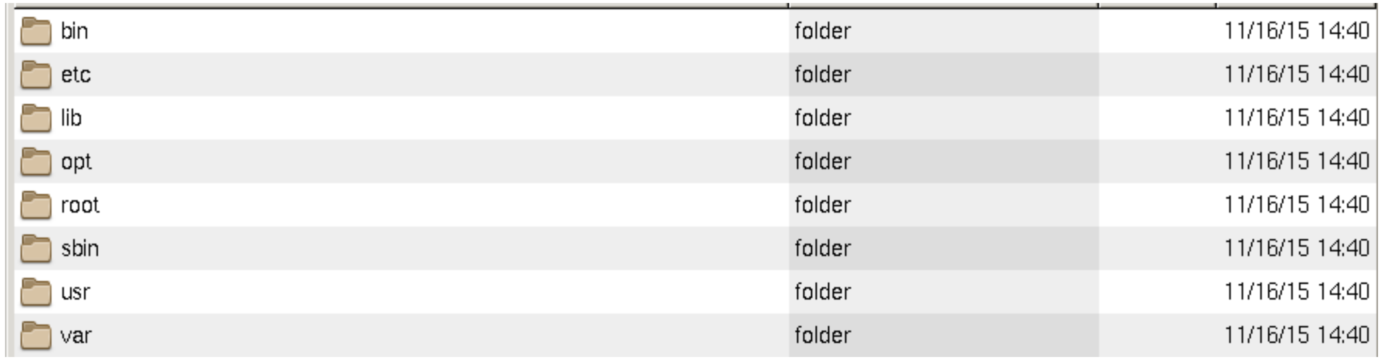
Gira

Gira
IP router

What does its firmware look like:

OS Linux !!!





bin	folder	11/16/15 14:40
etc	folder	11/16/15 14:40
lib	folder	11/16/15 14:40
opt	folder	11/16/15 14:40
root	folder	11/16/15 14:40
sbin	folder	11/16/15 14:40
usr	folder	11/16/15 14:40
var	folder	11/16/15 14:40

+ ssh, gdb-server

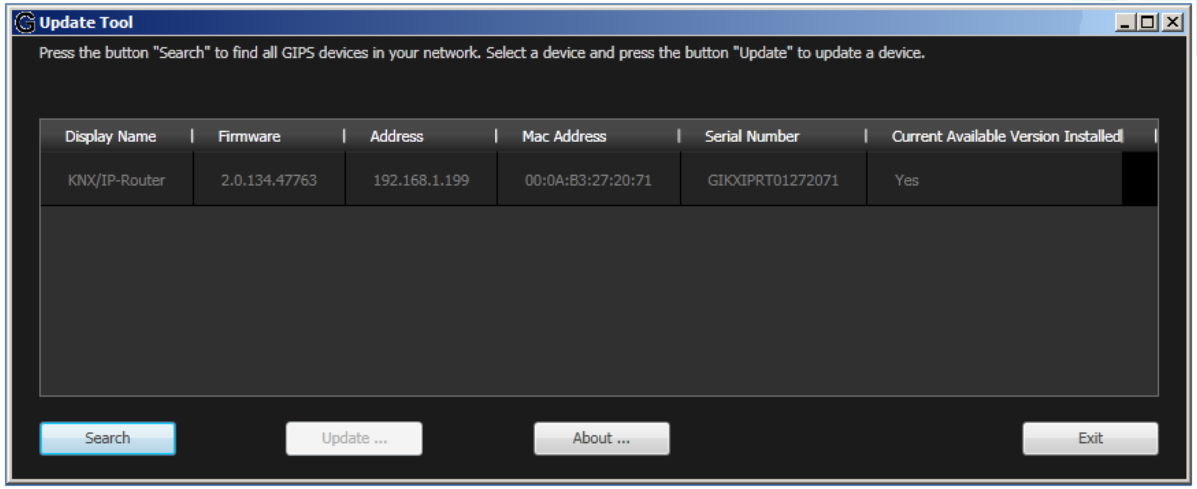
How to get control over the device:

Gira

Gira
IP router

Connect to the Ethernet

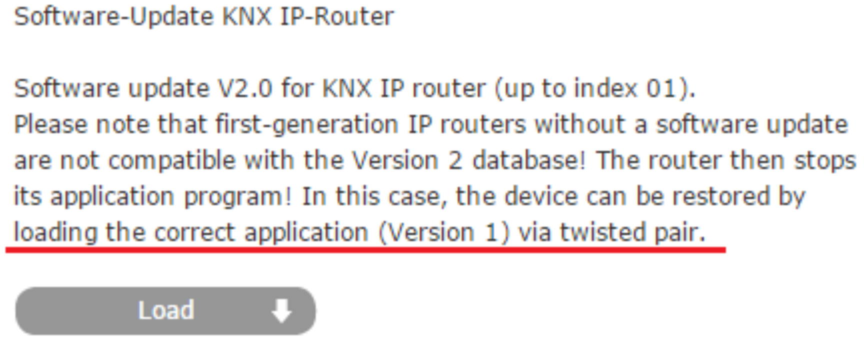
Run Gira Update Tool



Press the button "Search" to find all GIPS devices in your network. Select a device and press the button "Update" to update a device.

Display Name	Firmware	Address	Mac Address	Serial Number	Current Available Version Installed
KNX/IP-Router	2.0.134.47763	192.168.1.199	00:0A:B3:27:20:71	GIKXIPRT01272071	Yes

Update (it is possible to update to the latest version)

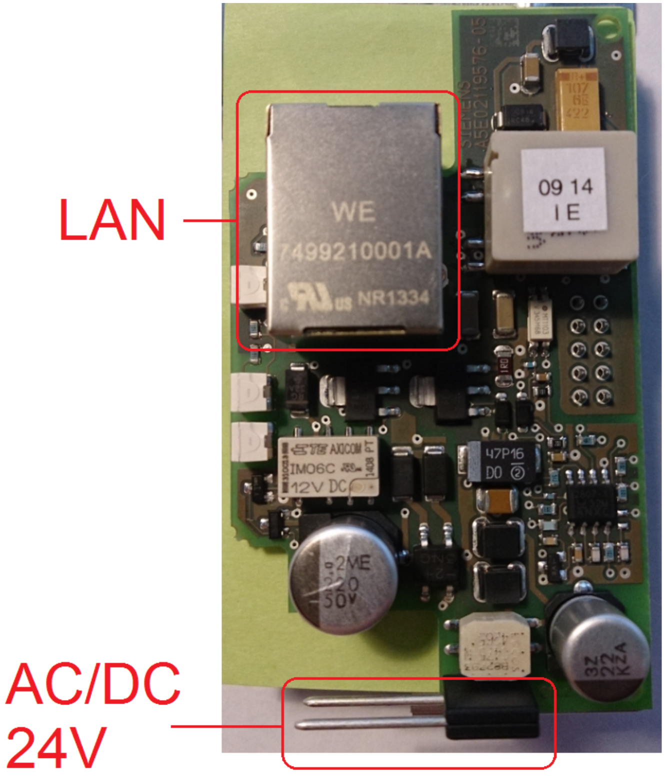


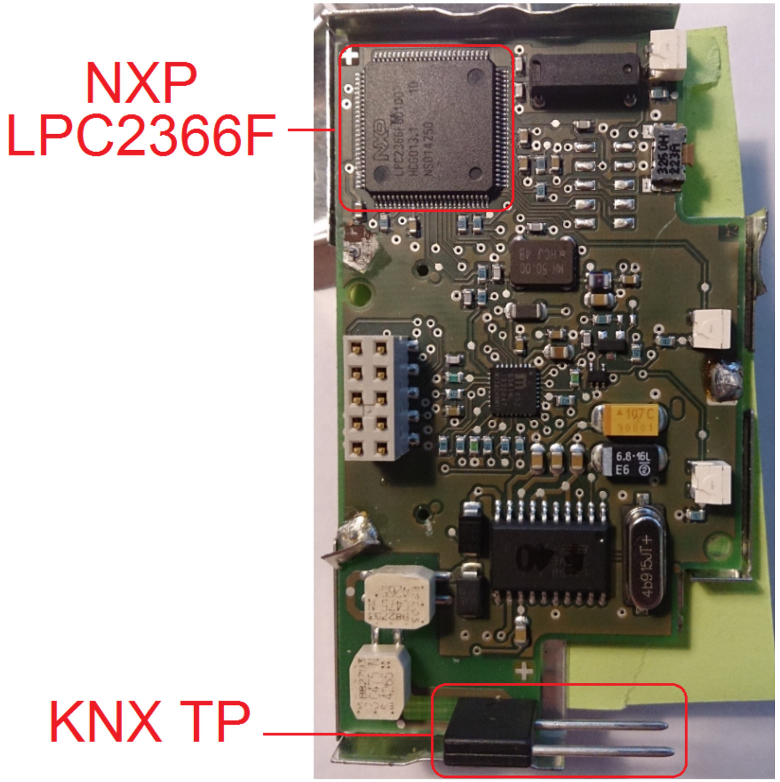
Software-Update KNX IP-Router

Software update V2.0 for KNX IP router (up to index 01).
Please note that first-generation IP routers without a software update are not compatible with the Version 2 database! The router then stops its application program! In this case, the device can be restored by loading the correct application (Version 1) via twisted pair.

Siemens

Siemens IP router





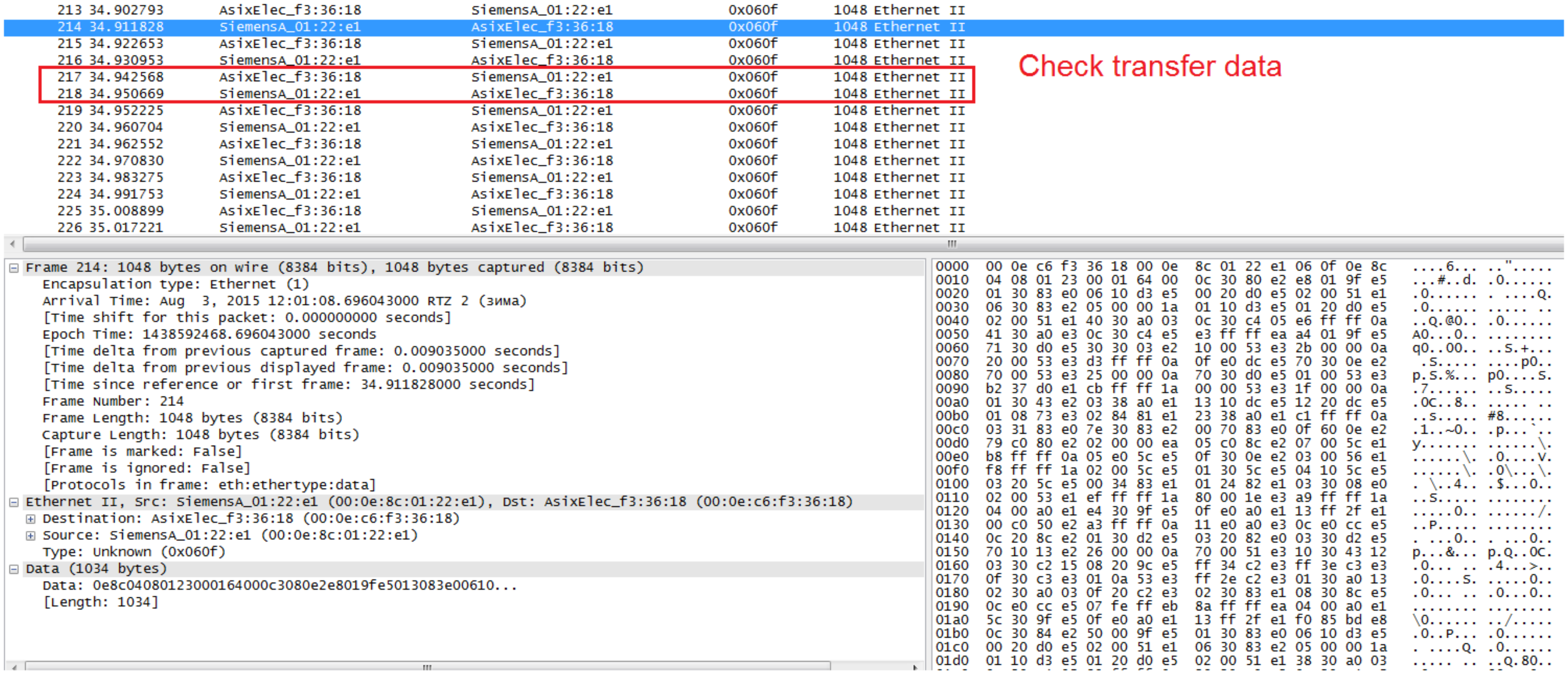
NXP LPC2366:
256 kB flash
32 kB SRAM local bus
16 kB SRAM Ethernet buf
8 kB SRAM GP/USB
2 RTC
2 CAN
6 ADC
1 DAC

Security in KNX or how to steal a skyscraper

Siemens

Siemens
IP router

How to update Siemens firmware



```
213 34.902793    AsixElec_f3:36:18    SiemensA_01:22:e1    0x060f    1048 Ethernet II
214 34.911828    SiemensA_01:22:e1    AsixElec_f3:36:18    0x060f    1048 Ethernet II
215 34.922653    AsixElec_f3:36:18    SiemensA_01:22:e1    0x060f    1048 Ethernet II
216 34.930953    SiemensA_01:22:e1    AsixElec_f3:36:18    0x060f    1048 Ethernet II
217 34.942568    AsixElec_f3:36:18    SiemensA_01:22:e1    0x060f    1048 Ethernet II
218 34.950669    SiemensA_01:22:e1    AsixElec_f3:36:18    0x060f    1048 Ethernet II
219 34.952225    AsixElec_f3:36:18    SiemensA_01:22:e1    0x060f    1048 Ethernet II
220 34.960704    SiemensA_01:22:e1    AsixElec_f3:36:18    0x060f    1048 Ethernet II
221 34.962552    AsixElec_f3:36:18    SiemensA_01:22:e1    0x060f    1048 Ethernet II
222 34.970830    SiemensA_01:22:e1    AsixElec_f3:36:18    0x060f    1048 Ethernet II
223 34.983275    AsixElec_f3:36:18    SiemensA_01:22:e1    0x060f    1048 Ethernet II
224 34.991753    SiemensA_01:22:e1    AsixElec_f3:36:18    0x060f    1048 Ethernet II
225 35.008899    AsixElec_f3:36:18    SiemensA_01:22:e1    0x060f    1048 Ethernet II
226 35.017221    SiemensA_01:22:e1    AsixElec_f3:36:18    0x060f    1048 Ethernet II
```

Check transfer data

```
⊟ Frame 214: 1048 bytes on wire (8384 bits), 1048 bytes captured (8384 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug  3, 2015 12:01:08.696043000 RTZ 2 (зима)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1438592468.696043000 seconds
    [Time delta from previous captured frame: 0.009035000 seconds]
    [Time delta from previous displayed frame: 0.009035000 seconds]
    [Time since reference or first frame: 34.911828000 seconds]
    Frame Number: 214
    Frame Length: 1048 bytes (8384 bits)
    Capture Length: 1048 bytes (8384 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:data]
⊟ Ethernet II, Src: SiemensA_01:22:e1 (00:0e:8c:01:22:e1), Dst: AsixElec_f3:36:18 (00:0e:c6:f3:36:18)
  ⊞ Destination: AsixElec_f3:36:18 (00:0e:c6:f3:36:18)
  ⊞ Source: SiemensA_01:22:e1 (00:0e:8c:01:22:e1)
    Type: Unknown (0x060f)
⊟ Data (1034 bytes)
    Data: 0e8c04080123000164000c3080e2e8019fe5013083e00610...
    [Length: 1034]
```

```
0000  00 0e c6 f3 36 18 00 0e  8c 01 22 e1 06 0f 0e 8c   ....6... ..".....
0010  04 08 01 23 00 01 64 00  0c 30 80 e2 e8 01 9f e5   ...#..d. .0......
0020  01 30 83 e0 06 10 d3 e5  00 20 d0 e5 02 00 51 e1   .0...... . ....Q.
0030  06 30 83 e2 05 00 00 1a  01 10 d3 e5 01 20 d0 e5   .0...... ..... ..
0040  02 00 51 e1 40 30 a0 03  0c 30 c4 05 e6 ff ff 0a   ..Q.@0.. .0......
0050  41 30 a0 e3 0c 30 c4 e5  e3 ff ff ea a4 01 9f e5   A0...0.. ........
0060  71 30 d0 e5 30 30 03 e2  10 00 53 e3 2b 00 00 0a   q0..00.. ..S.+...
0070  20 00 53 e3 d3 ff ff 0a  0f e0 dc e5 70 30 0e e2    .S..... ....p0..
0080  70 00 53 e3 25 00 00 0a  70 30 d0 e5 01 00 53 e3   p.S.%... p0....S.
0090  b2 37 d0 e1 cb ff ff 1a  00 00 53 e3 1f 00 00 0a   .7...... ..S.....
00a0  01 30 43 e2 03 38 a0 e1  13 10 dc e5 12 20 dc e5   .0C..8.. ..... ..
00b0  01 08 73 e3 02 84 81 e1  23 38 a0 e1 c1 ff ff 0a   ..s..... #8......
00c0  03 31 83 e0 7e 30 83 e2  00 70 83 e0 0f 60 0e e2   .1..~0.. .p...`..
00d0  79 c0 80 e2 02 00 00 ea  05 c0 8c e2 07 00 5c e1   y....... ......\.
00e0  b8 ff ff 0a 05 e0 5c e5  0f 30 0e e2 03 00 56 e1   ......\. .0....V.
00f0  f8 ff ff 1a 02 00 5c e5  01 30 5c e5 04 10 5c e5   ......\. .0\...\.
0100  03 20 5c e5 00 34 83 e1  01 24 82 e1 03 30 08 e0   . \..4.. .$...0..
0110  02 00 53 e1 ef ff ff 1a  80 00 1e e3 a9 ff ff 1a   ..S..... ........
0120  04 00 a0 e1 e4 30 9f e5  0f e0 a0 e1 13 ff 2f e1   .....0.. ....../.
0130  00 c0 50 e2 a3 ff ff 0a  11 e0 a0 e3 0c e0 cc e5   ..P..... ........
0140  0c 20 8c e2 01 30 d2 e5  03 20 82 e0 03 30 d2 e5   . ...0.. . ...0..
0150  70 10 13 e2 26 00 00 0a  70 00 51 e3 10 30 43 12   p...&... p.Q..0C.
0160  03 30 c2 15 08 20 9c e5  ff 34 c2 e3 ff 3e c3 e3   .0... .. .4...>..
0170  0f 30 c3 e3 01 0a 53 e3  ff 2e c2 e3 01 30 a0 13   .0....S. .....0..
0180  02 30 a0 03 0f 20 c2 e3  02 30 83 e1 08 30 8c e5   .0... .. .0...0..
0190  0c e0 cc e5 07 fe ff eb  8a ff ff ea 04 00 a0 e1   ........ ........
01a0  5c 30 9f e5 0f e0 a0 e1  13 ff 2f e1 f0 85 bd e8   \0...... ../.....
01b0  0c 30 84 e2 50 00 9f e5  01 30 83 e0 06 10 d3 e5   .0..P... .0......
01c0  00 20 d0 e5 02 00 51 e1  06 30 83 e2 05 00 00 1a   . ....Q. .0......
01d0  01 10 d3 e5 01 20 d0 e5  02 00 51 e1 38 30 a0 03   ..... .. ..Q.80..
```

Before I tell you a “little fairy tale”,
let us have a look at the available works in this field

Jesus Molina

“Learn how to control every room at a luxury hotel remotely: the dangers of insecure home automation deployment.”

Daniel Lechner, Wolfgang Granzer, Wolfgang Kastner

“Security for KNXnet/IP”

How to connect to KNX TP?

Do it yourself or buy in EBay*

~ 20 Euro (it’s just the transceiver)

Buy USB to KNX TP

~ 210 Euro

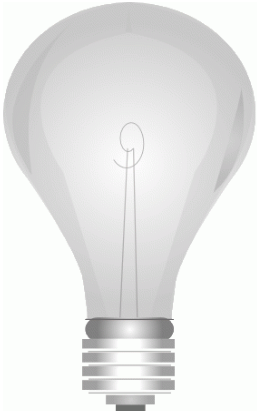
Buy KNX IP router

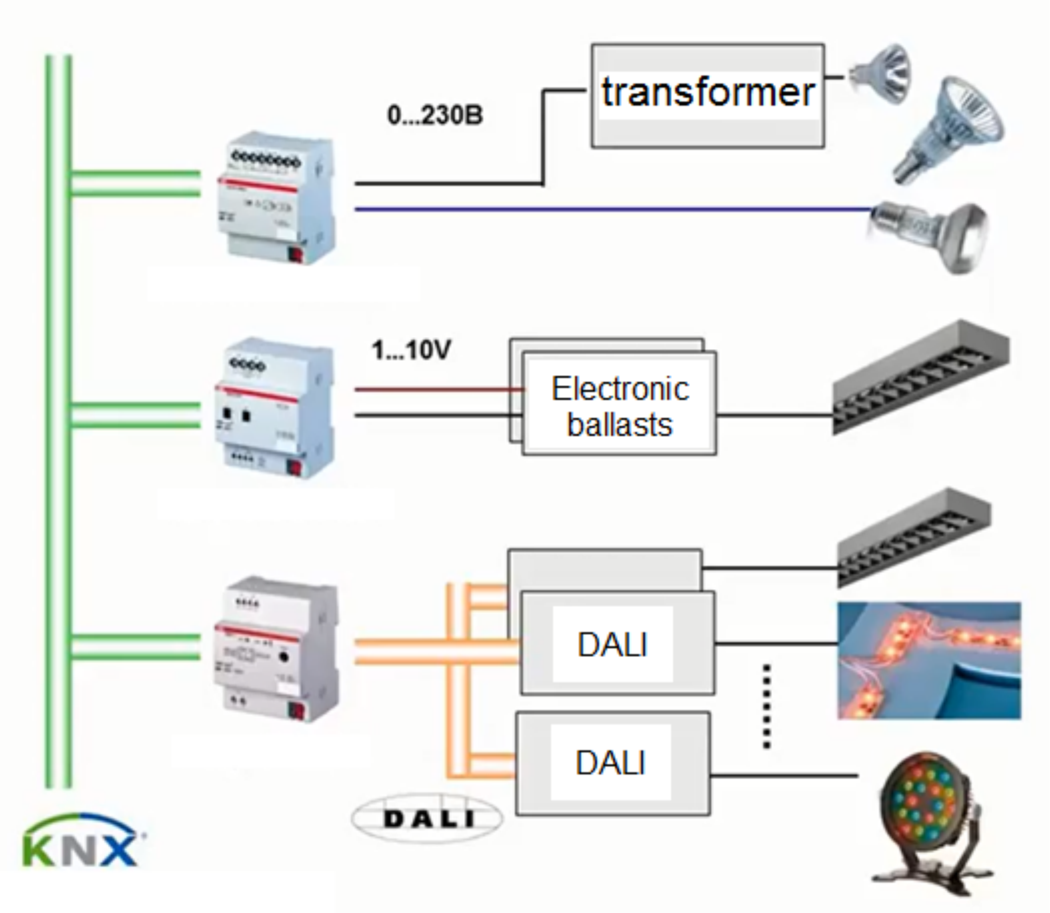
~ 100 Euro or higher

* http://www.ebay.it/itm/knxgate-interfaccia-bus-domotico-knx-konnex-vimar-pic-arduino-raspberry-/301802382190?hash=item4644d2e36e:g:uqgAAOSweuxWTG5q

A walk inside KNX network

A walk inside KNX network



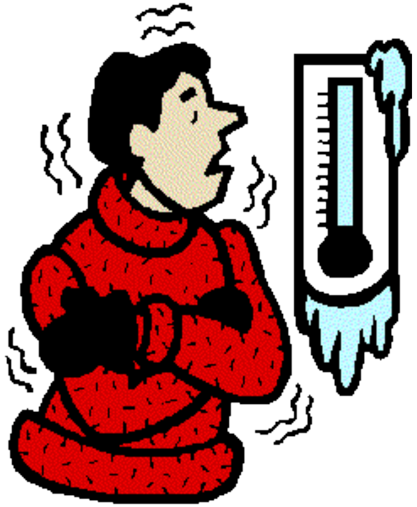


A walk inside KNX network

Setting up:

- Light
- Heat
- Ventilation
- ….

A walk inside KNX network



Cold

Wake up

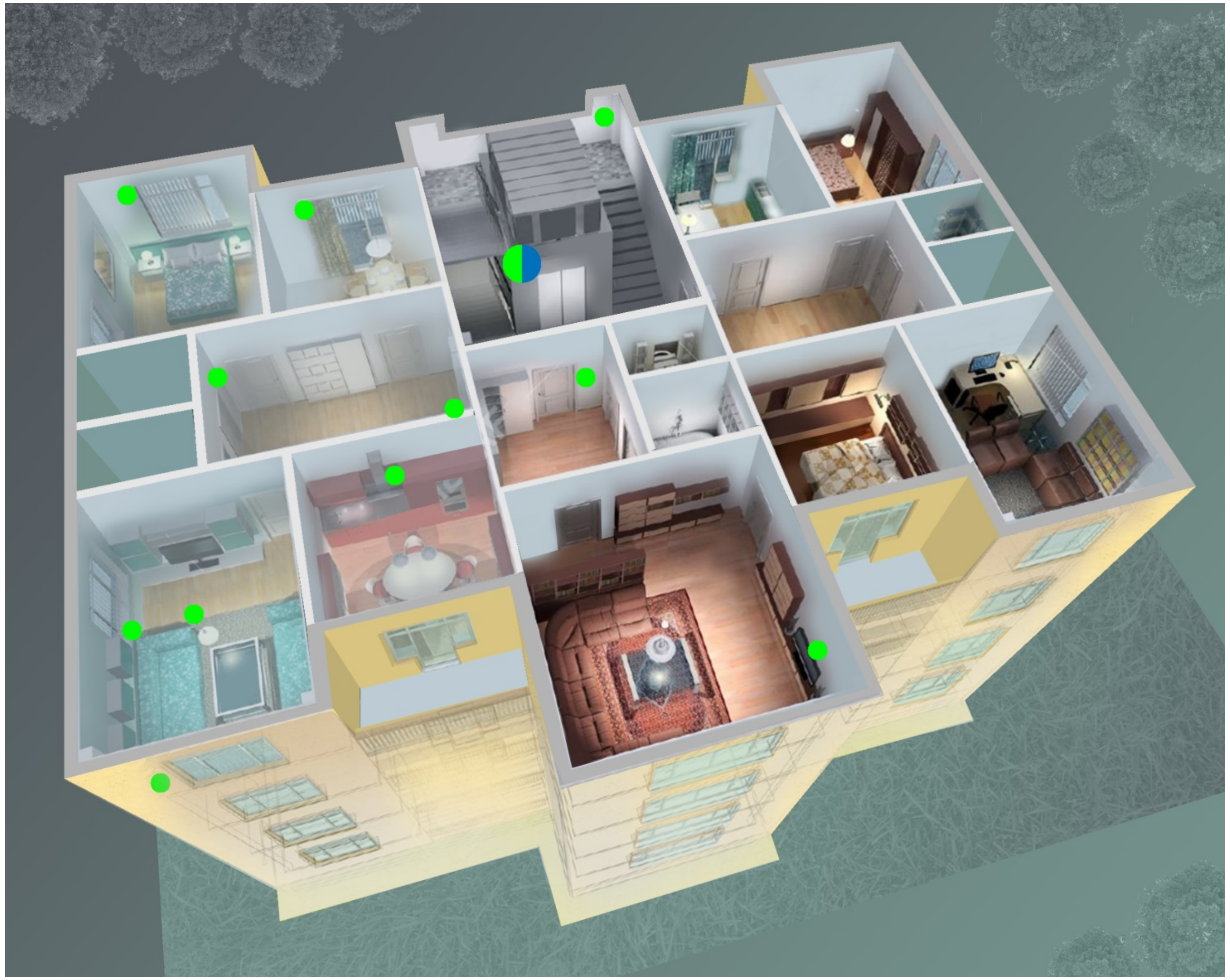
fire siren

Increased energy consumption

Malfunctioning control systems

Discomfort for visitors

Reality



● KNX node

◐ IP router
KNX TP <-> KNX IP

Reality

You need ETS software

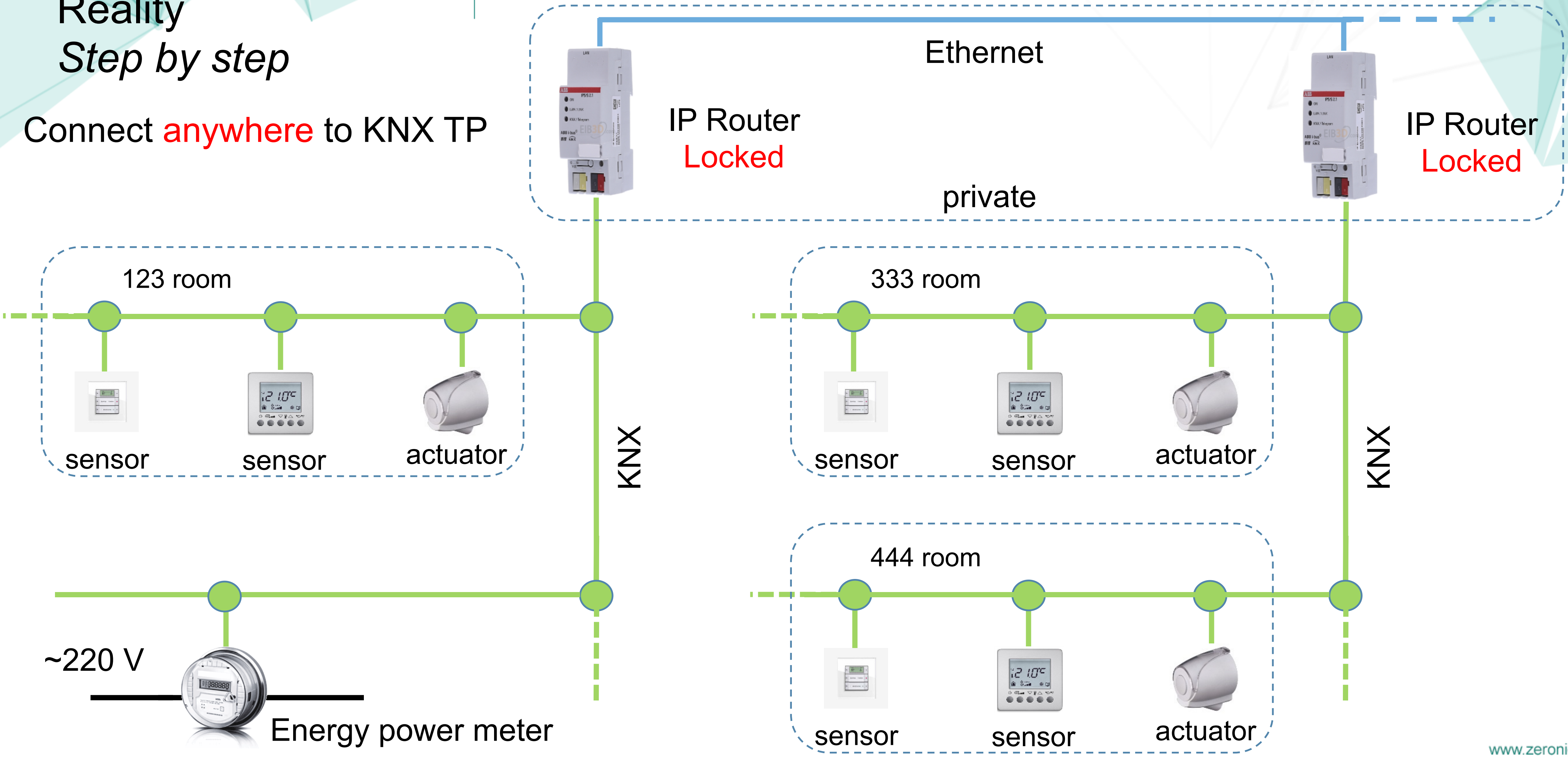
Enable program mode in router or node

Configure

Reality

Step by step

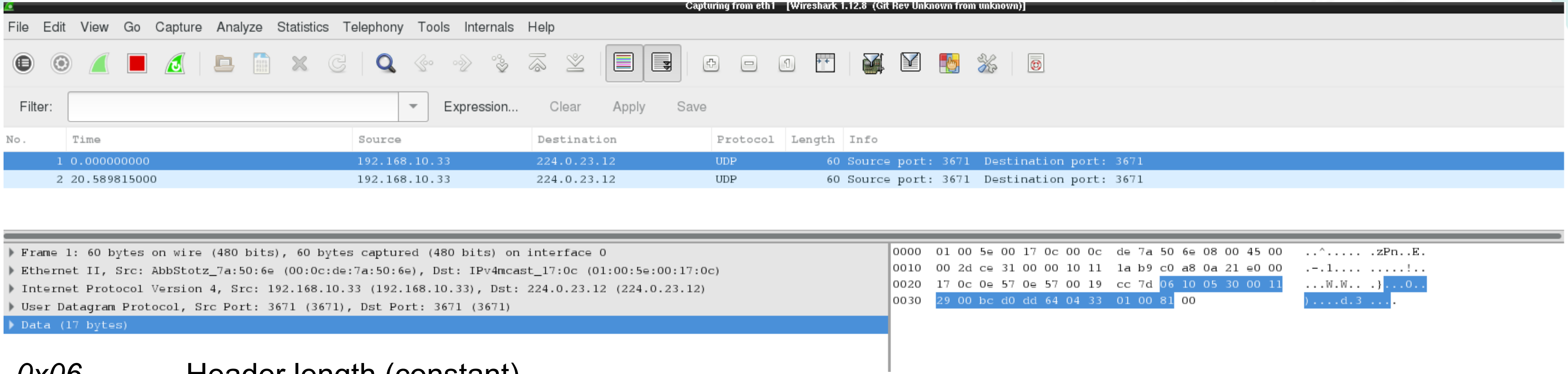
Connect anywhere to KNX TP



Reality

Step by step

To manage any device



Capturing from eth1 [Wireshark 1.12.8 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save

```
No.  Time          Source          Destination   Protocol  Length  Info
  1  0.000000000   192.168.10.33   224.0.23.12   UDP          60  Source port: 3671  Destination port: 3671
  2  20.589815000  192.168.10.33   224.0.23.12   UDP          60  Source port: 3671  Destination port: 3671
```

```
▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: AbbStotz_7a:50:6e (00:0c:de:7a:50:6e), Dst: IPv4mcast_17:0c (01:00:5e:00:17:0c)
▸ Internet Protocol Version 4, Src: 192.168.10.33 (192.168.10.33), Dst: 224.0.23.12 (224.0.23.12)
▸ User Datagram Protocol, Src Port: 3671 (3671), Dst Port: 3671 (3671)
▸ Data (17 bytes)
```

```
0000  01 00 5e 00 17 0c 00 0c  de 7a 50 6e 08 00 45 00   ..^..... .zPn..E.
0010  00 2d ce 31 00 00 10 11  1a b9 c0 a8 0a 21 e0 00   .-.1.... .....!..
0020  17 0c 0e 57 0e 57 00 19  cc 7d 06 10 05 30 00 11   ...W.W.. .}...0..
0030  29 00 bc d0 dd 64 04 33  01 00 81 00               )....d.3 ....
```

0x06 – Header length (constant)
0x10 – Protocol version (constant)
0x05 0x30 – Service Type ID
0x00 0x11 – Total length
0x29 – Message code
0x00 – Additional info
0xbc 0xd0 – Control Field
0xdd 0x64 – Source address
0x04 0x33 – Destination address
0x01 0x00 0x81 – TPCI, APCI and Data

Reality

Step by step

To unlock IP router (stage 1)

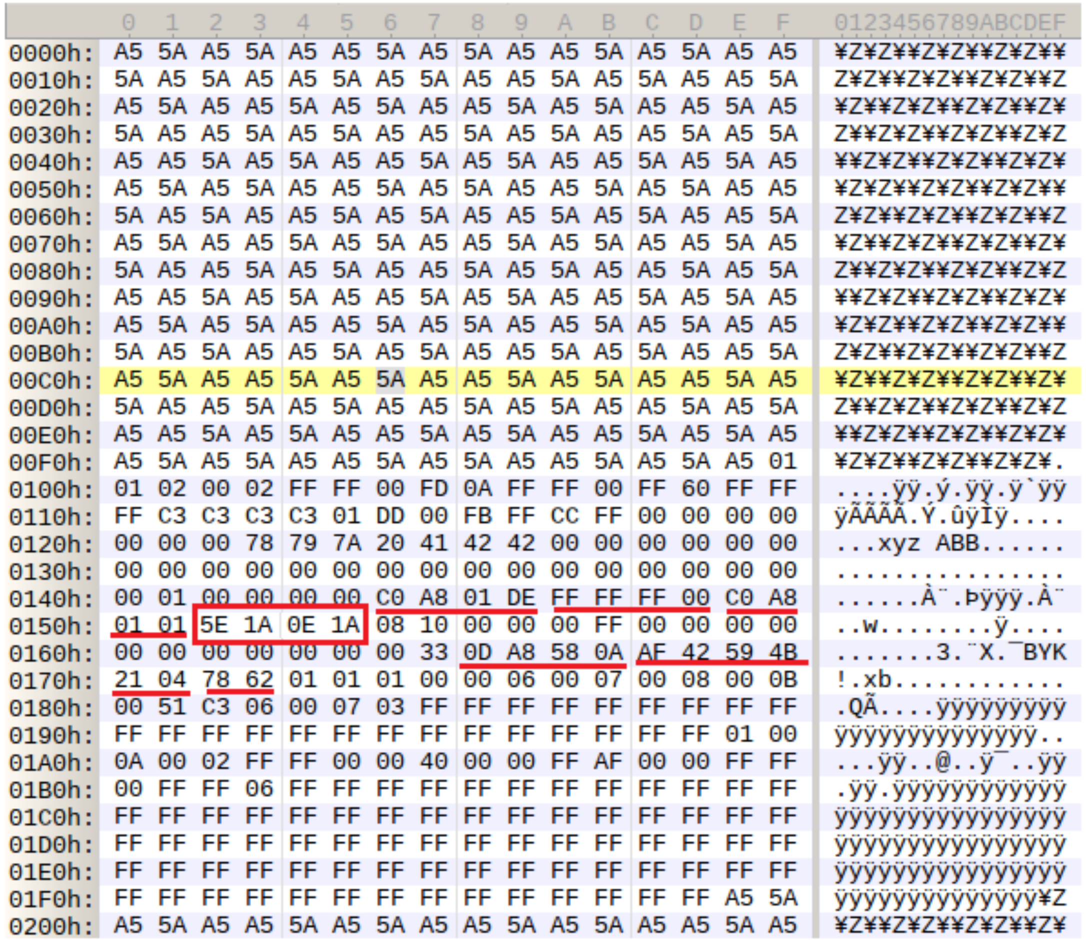
Read memory of a router *and get:*

IP	192.168.1.222
Mask	*255.255.255.0*
Gateway	192.168.1

Router is Locked: *0x5E 0x1A 0x0E 0x1A*

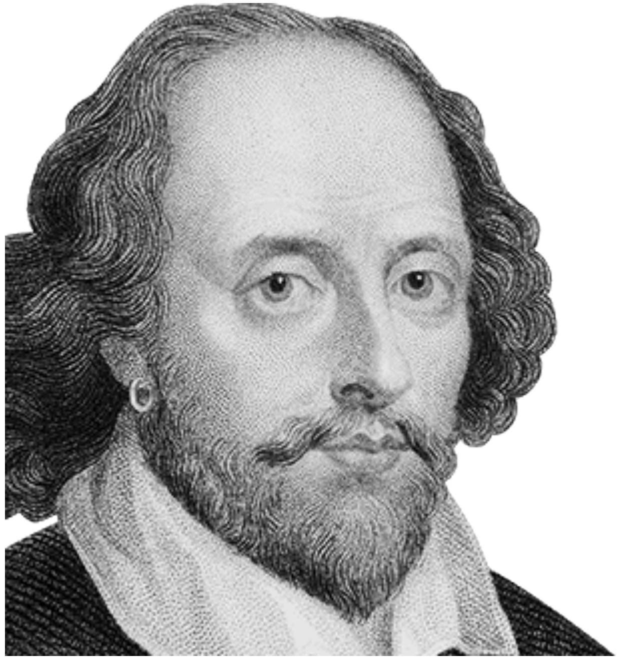
in additional:

IP Routing Unicast 1	13.168.88.10
Unicast IP port1	8452
IP Routing Unicast 2	175.66.89.75
Unicast IP port2	30818

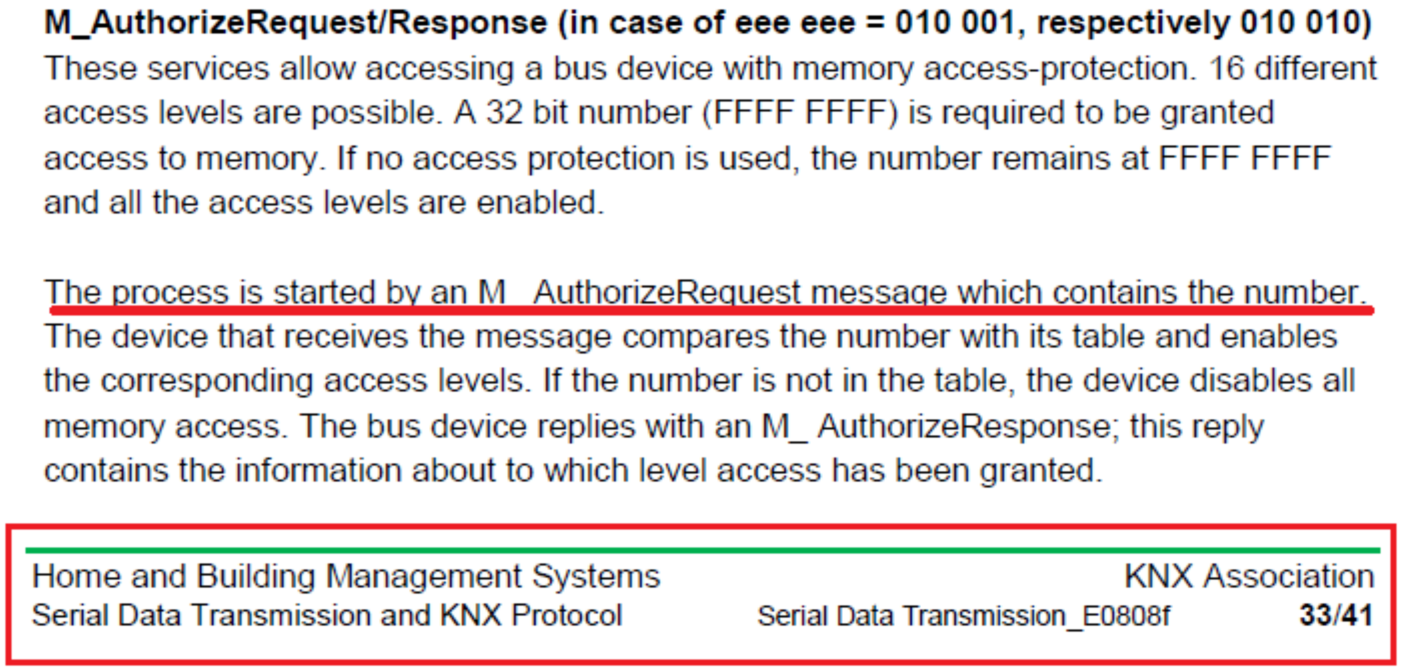


```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: A5 5A A5 5A A5 A5 5A A5 5A A5 A5 5A A5 5A A5 A5   ¥Z¥Z¥¥Z¥Z¥¥Z¥Z¥¥
0010h: 5A A5 5A A5 A5 5A A5 5A A5 A5 5A A5 5A A5 A5 5A   Z¥Z¥¥Z¥Z¥¥Z¥Z¥¥Z
0020h: A5 5A A5 A5 5A A5 5A A5 A5 5A A5 5A A5 A5 5A A5   ¥Z¥¥Z¥Z¥¥Z¥Z¥¥Z¥
0030h: 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.ÿ`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.ÿÿÿÿÿÿÿÿÿÿÿÿ
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¥
```

Reality
Step by step



To unlock IP router



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.

Home and Building Management Systems — KNX Association
Serial Data Transmission and KNX Protocol — Serial Data Transmission_E0808f — **33/41**

To be or not to be

Reality
Step by step

To unlock IP router (stage 2)

Just write some bytes to memory to *unlock router :* 0x77 0x15 0x07 0x15

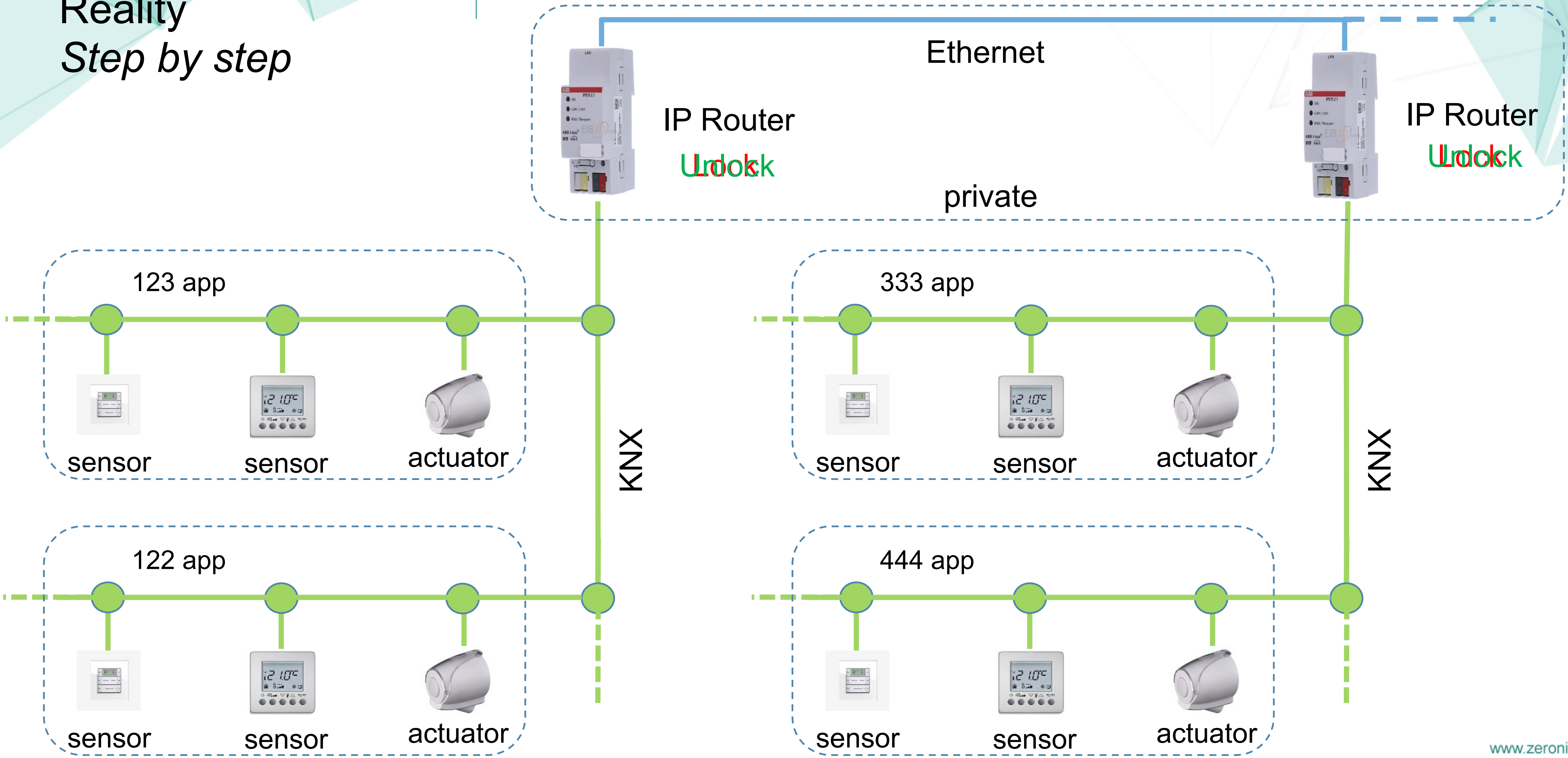
How do you do it?

Use “Write Memory” command without any checks or authorization

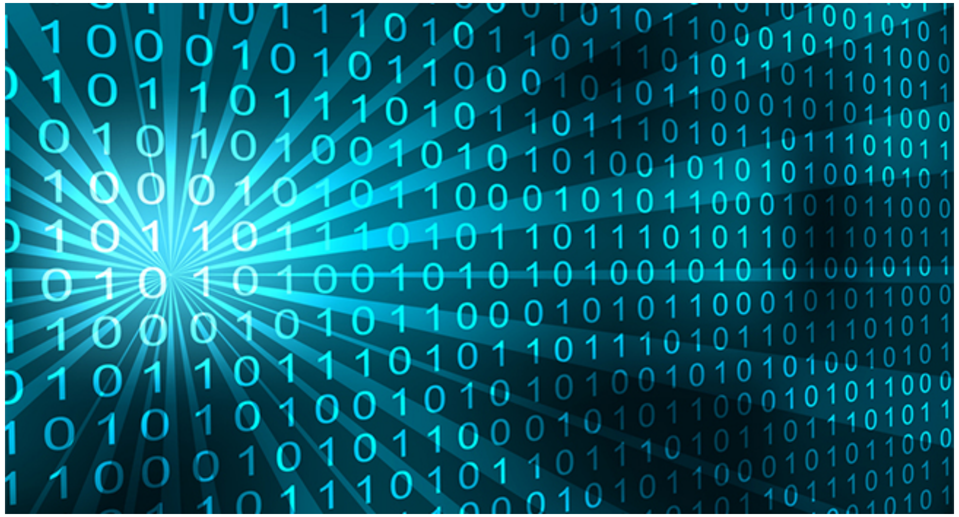
Moreover, you can use “User Message” command to send up to 69 bytes, not 15 bytes

Reality

Step by step



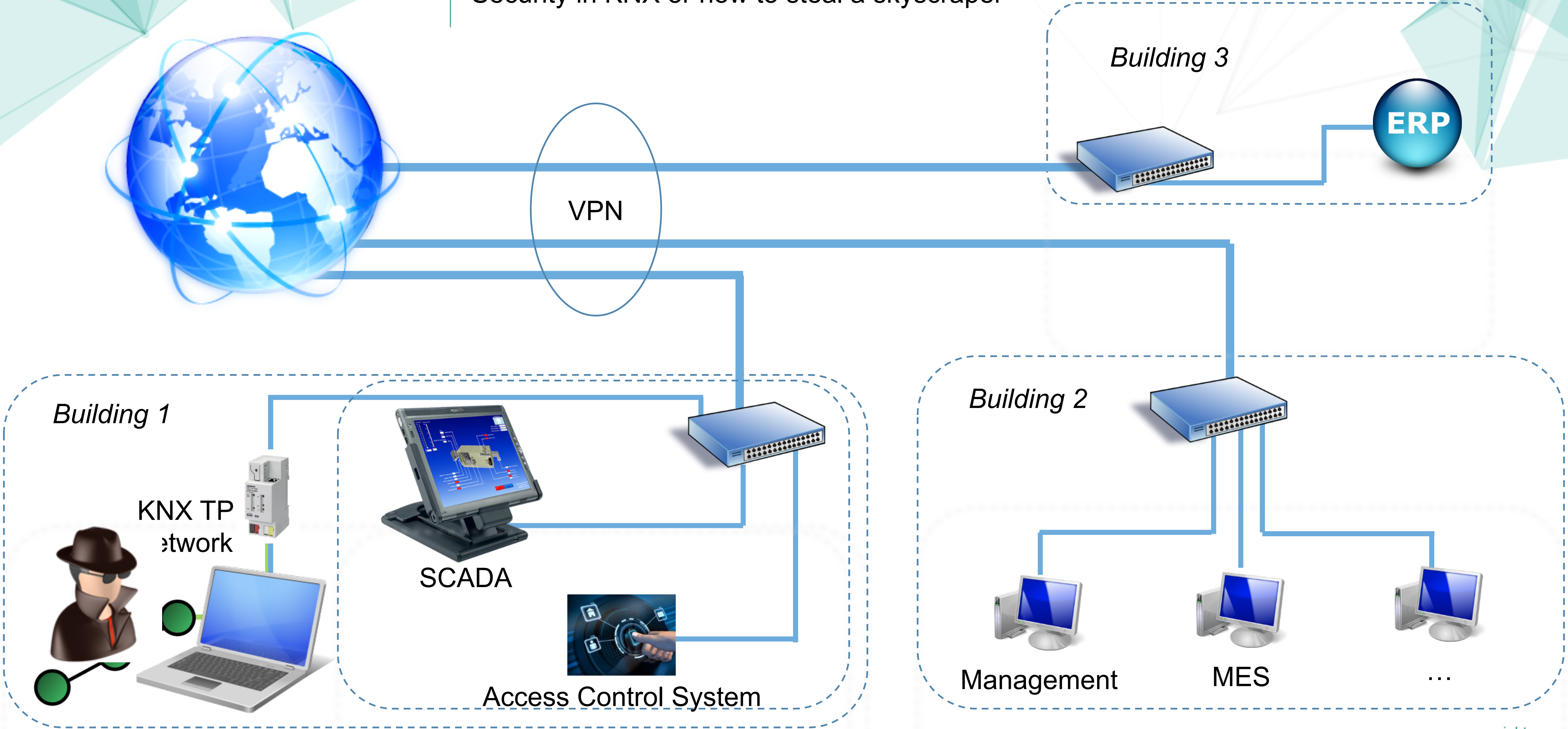
- DoS for any node in KNX
- Opportunity to manage any device in KNX
- Change router configuration



RCE on the router allows turning your router into a laptop

Work in progress…

Security in KNX or how to steal a skyscraper



www.dsec.ru
info@dsec.ru