On the security of security extensions for IP-based KNX networks

Aljosha Judmayer
ajudmayer@sba-research.org
ajudmayer@auto.tuwien.ac.at

SBA Research

secure sba-research.org

COMET Competence Centers for Excellent Technologies

Area 1 (GRC): Governance, Risk and Compliance

- P1.1: Risk Management and Analysis
- P1.2: Secure BP Modeling, Simulation and Verification
- P1.3: Computer Security Incident Response Team
- P1.4: Awareness and E-Learning

Area 2 (DSP): Data Security and Privacy

- P2.1: Privacy Enhancing Technologies
- P2.2: Enterprise Rights Management
- P2.3: Digital Preservation

Area 3 (SCA): Secure Coding and Code Analysis

- P3.1: Malware Detection and Botnet Economics
- P3.2: Systems and Software Security
- P3.3: Digital Forensics

Area 4 (HNS): Hardware and Network Security

- P4.1: Hardware Security and Differential Fault Analysis
- P4.2: Pervasive Computing
- P4.3: Network Security of the Future Internet

bmvit Bundesministerium für Verkehr, Innovation und Technologie
bmwfi Bundesministerium für Wirtschaft, Familie und Jugend
Christian Doppler Forschungsgesellschaft
FFG
wirtschaftsagentur wien
zit Die Technologieagentur der Stadt Wien

TU Vienna

AUTOMATION SYSTEMS GROUP

- Thesis @ automation systems group

  =>

- Paper @ 10th IEEE Workshop on Factory Communication Systems (WFCS), 2014
  - Lukas Krammer (lkrammer@auto.tuwien.ac.at)
  - Wolfgang Kastner (k@auto.tuwien.ac.at)

What the h3ck is KNX?

What the h3ck is KNX?

- **KNX** is a standard for **home and building automation**
- **K**o**N**ne**X** Association pool of companies
  - publish KNX Systems specification
  - Develop the ETS (Engineering Tool Software)

What the h3ck is KNX?

- **KNX** is a standard for **home and building automation**
- **K**o**N**ne**X** Association pool of companies
  - publish KNX Systems specification (first version 2002)
  - Develop the ETS (Engineering Tool Software)

- Ensuring the interoperability between *products*, *applications* and *systems*
- Different physical layers e.g. :
  - Twisted pair cable (TP1)
  - Ethernet (IP)
    - called **KNXnet/IP**

Building Automation Systems (BAS)

- Goal: "*intelligent buildings*"
- Old and busted:
  - heating, ventilation and air conditioning (HVAC)
  - BUS networks

Building Automation Systems (BAS)

- Goal: "*intelligent buildings*"
- Old and busted:
  - heating, ventilation and air conditioning (HVAC)
  - BUS networks
- New hotness:
  - security and safety stuff (e.g. alarm systems, access control systems)
  - remote management and stuff ...
  - **>> connected to IP based networks << !!!111!**

  What can possibly go wrong?

Building Automation Systems (BAS)

- Goal: "*intelligent buildings*"
- Old and busted:
  - heating, ventilation and air c
  - BUS networks
- New hotness:
  - security and safety stuff (e.g systems)
  - remote management and stuff ...
  - **>> connected to IP based netw**

  What can possibly go wrong?

Source: http://laughingsquid.com/wp-content/uploads/tetris1_img6080.jpg

Security features in current/classical KNX ...

-

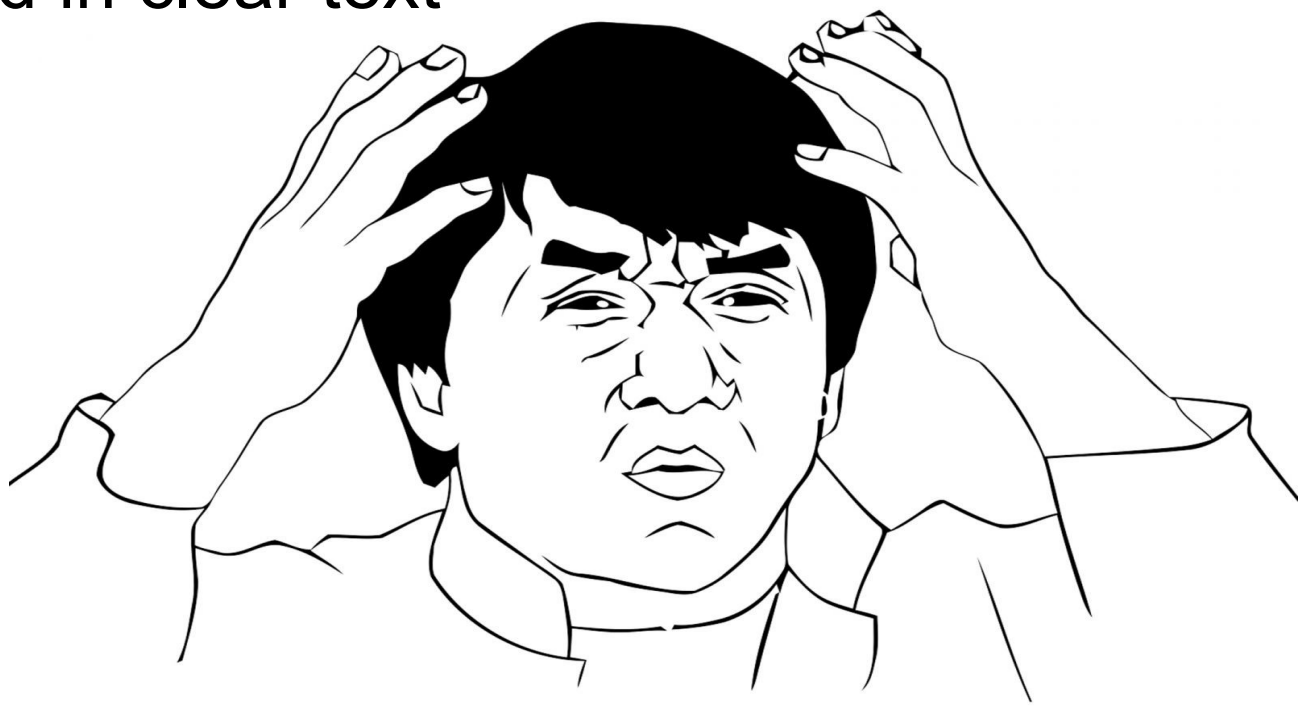
Security features in current/classical KNX ...

- Optional 4 (in words “four”) byte password

Security features in current/classical KNX ...

- Optional 4 (in words “four”) byte password

  .... transmitted in clear text



What the spec has to say ...

“For KNX, security is a minor concern, as any breach of security requires local access to the network”

(KNX Systems Specification)

What the spec has to say ...

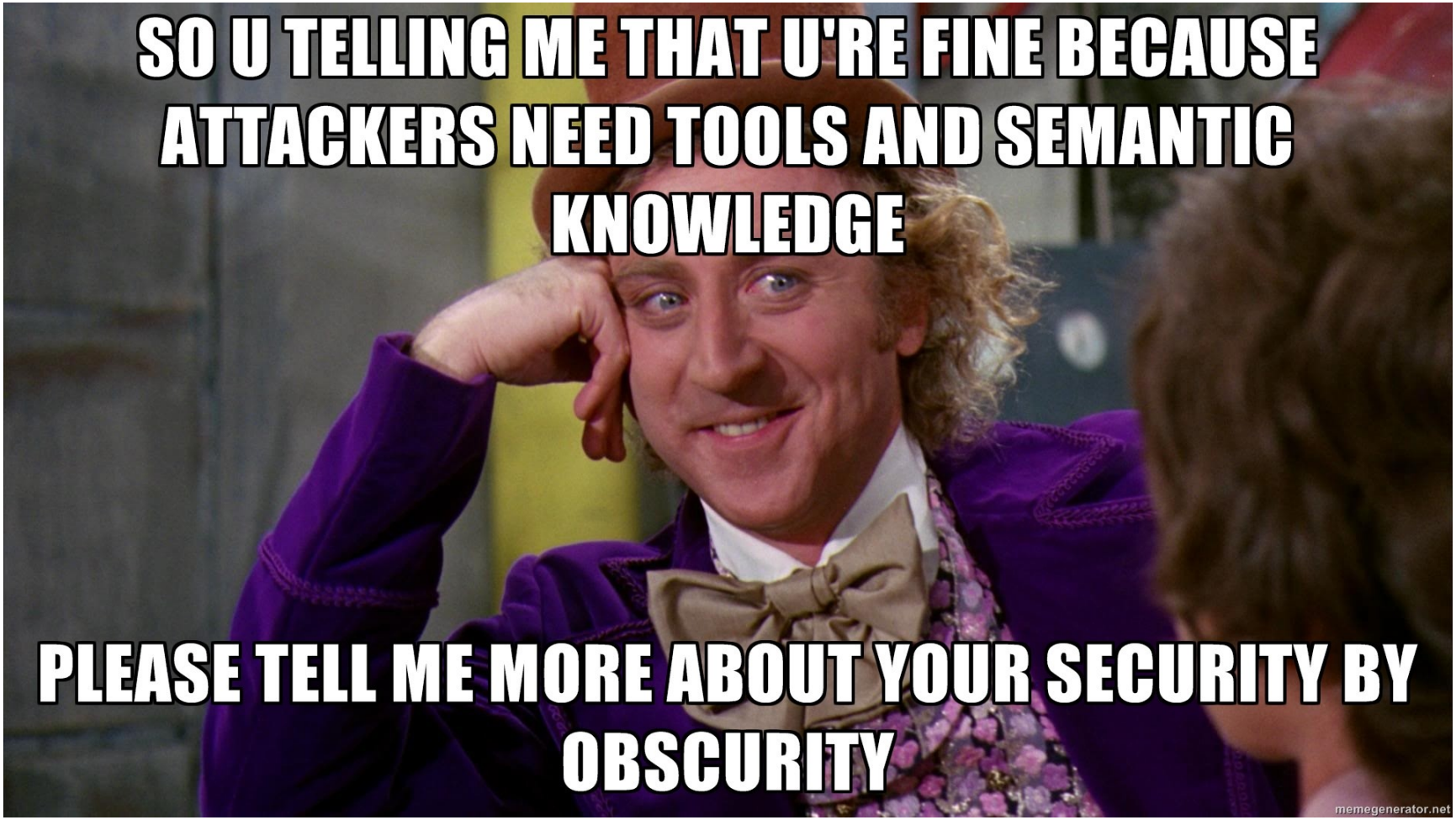
“For KNX, security is a minor concern, as any breach of security requires local access to the network”

(KNX Systems Specification)

“Filtering KNXnet/IP datagrams from the network requires network analysis tools and expertise. The content of a KNXnet/IP message is not self-descriptive but requires semantic knowledge ...”

(KNX Systems Specification)

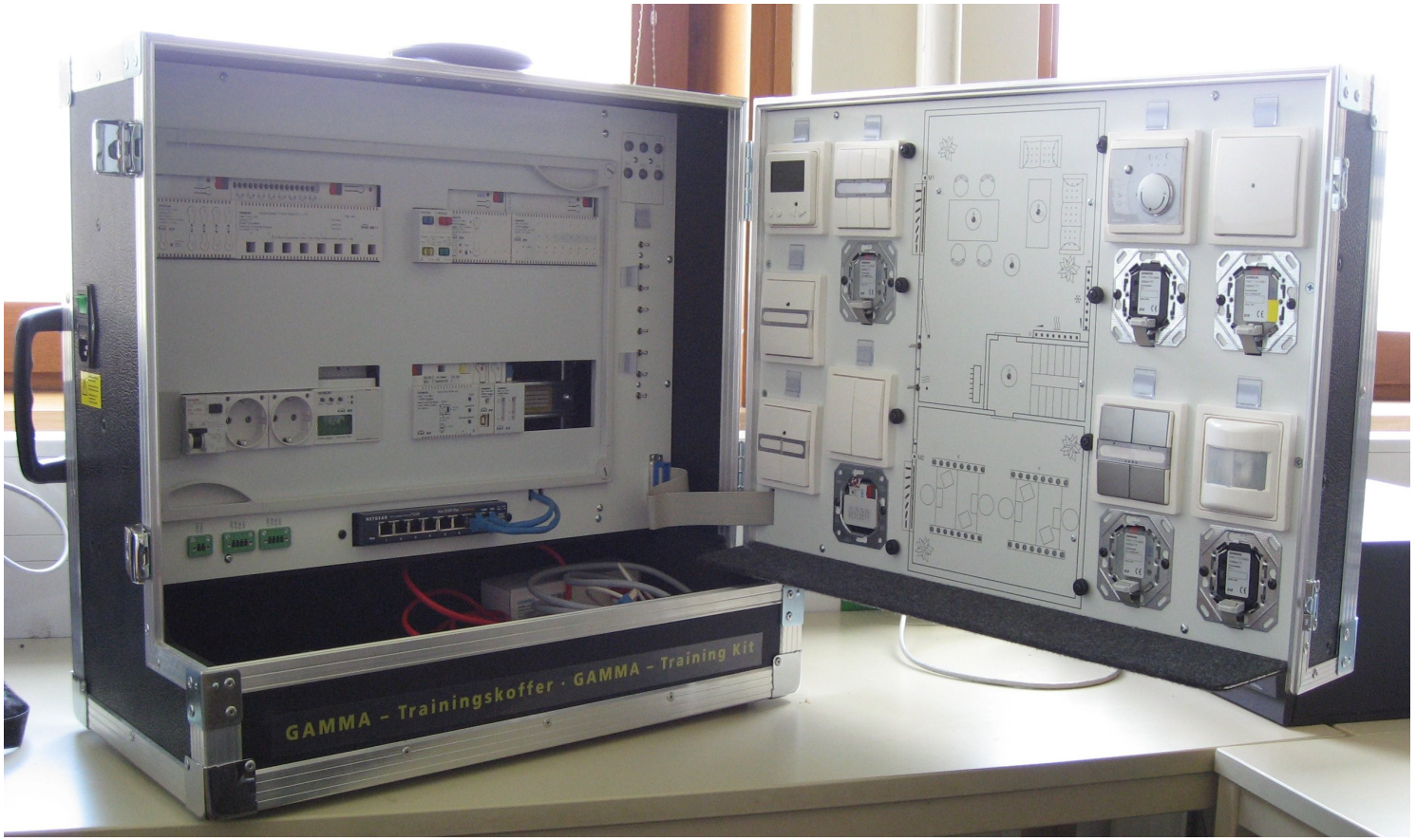
What the spec has to say ...



How does a KNX BAS look like?

How does a KNX BAS look like?

- GAMMA Training Kit (GTK2)



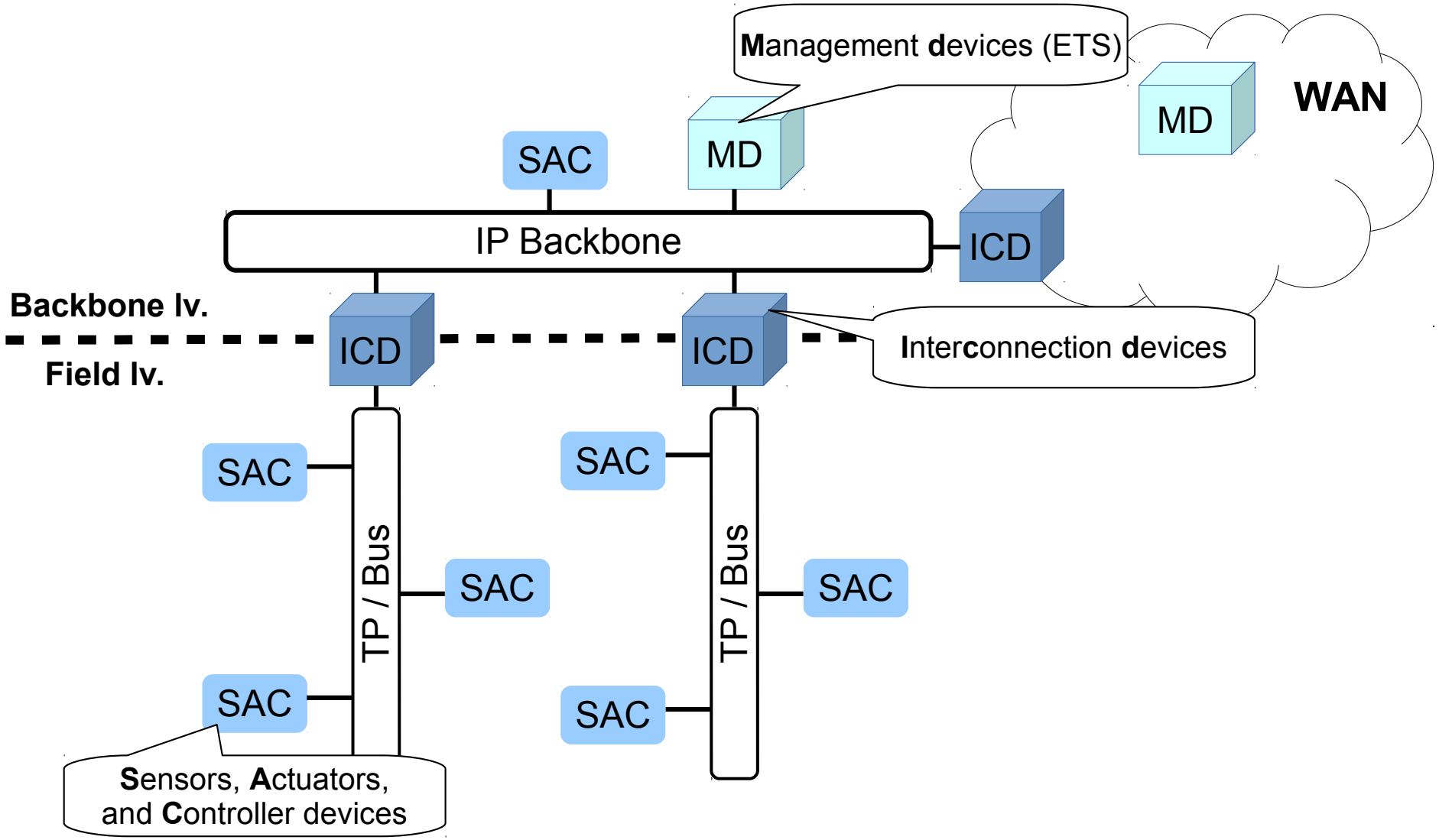
Source:https://www.auto.tuwien.ac.at/images/practicals/siemens_gamma_img_0515.jpg

How does a KNX BAS look like?

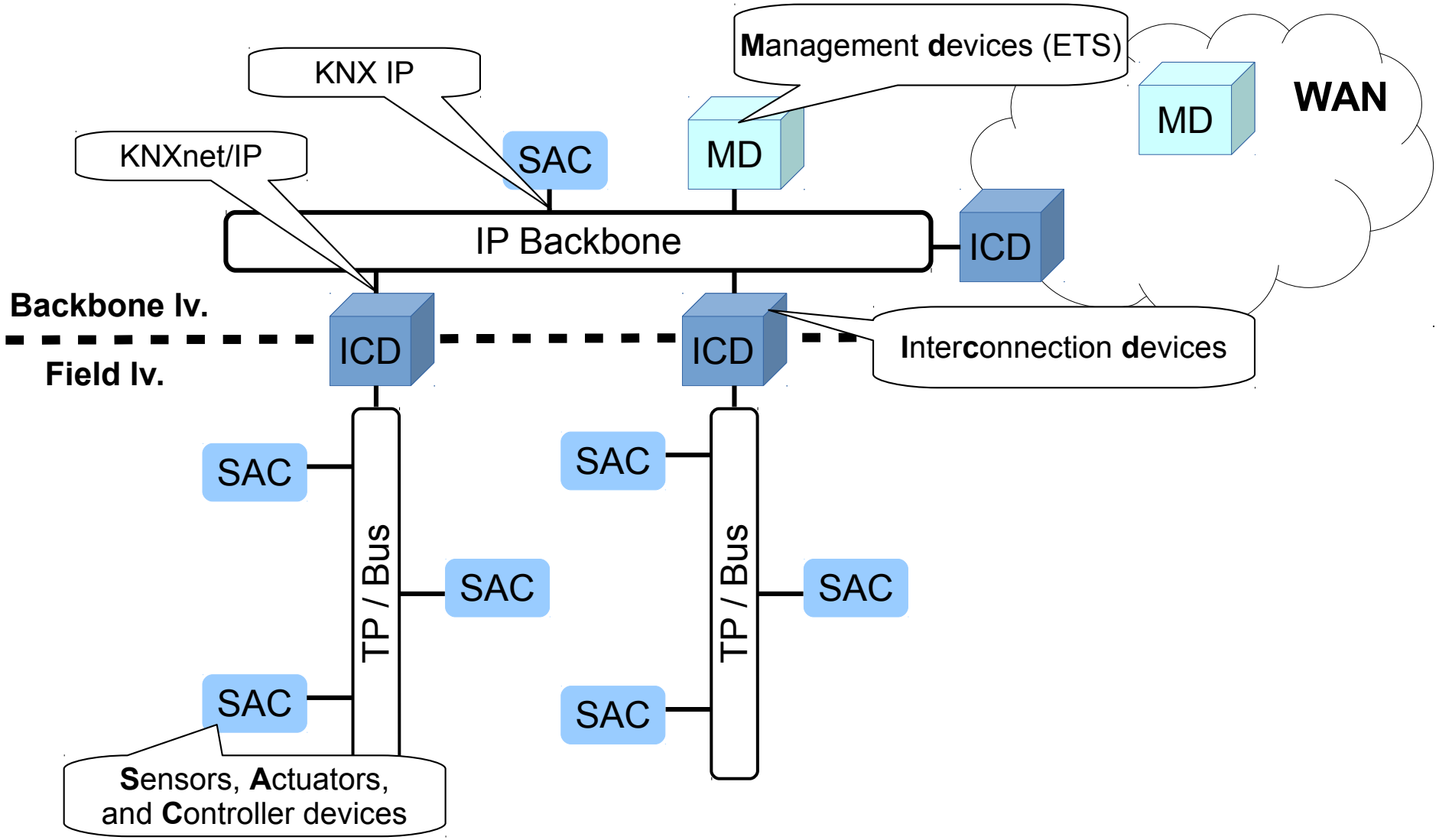
Backbone lv.

Field lv.

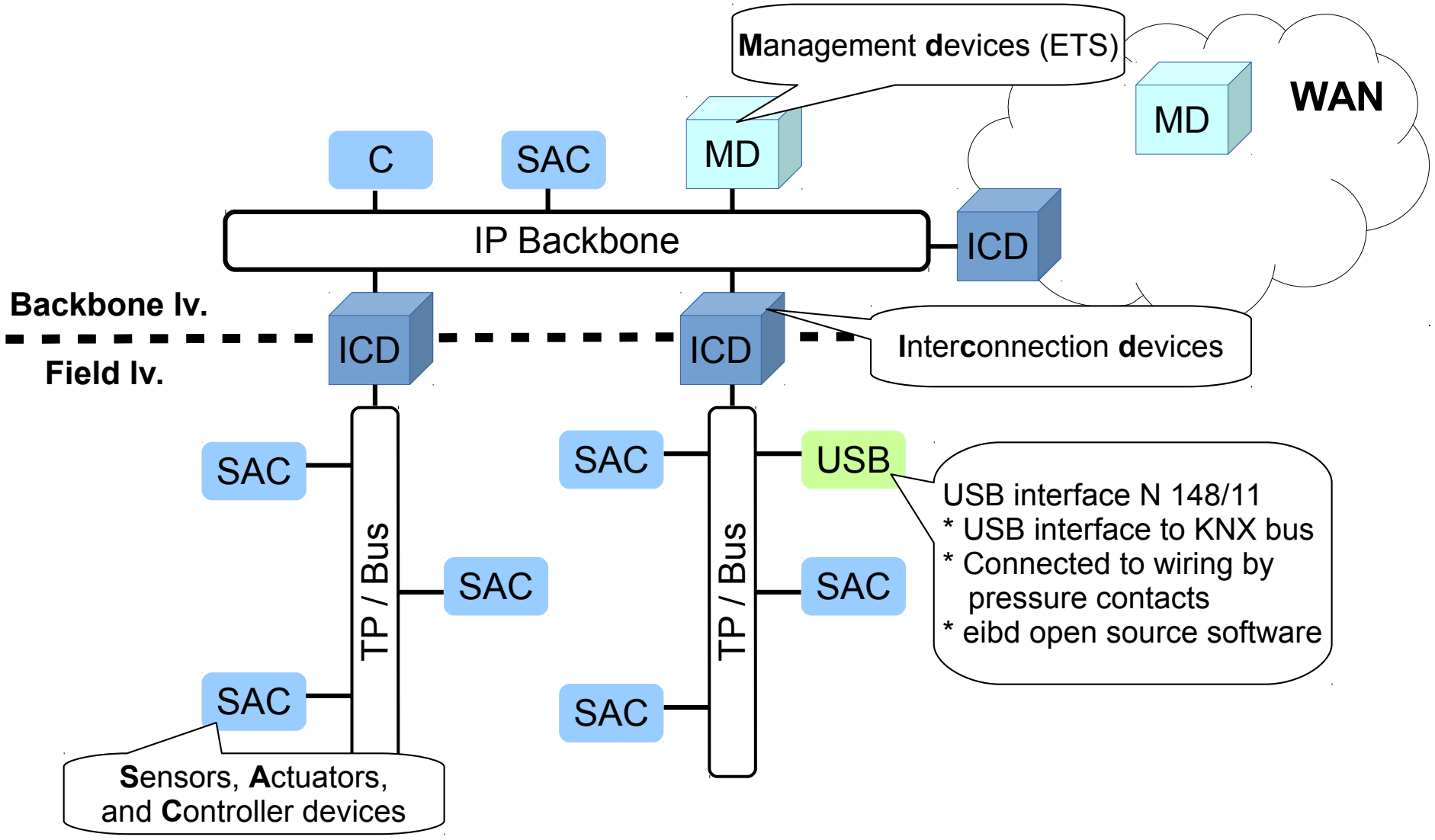
How does a KNX BAS look like?



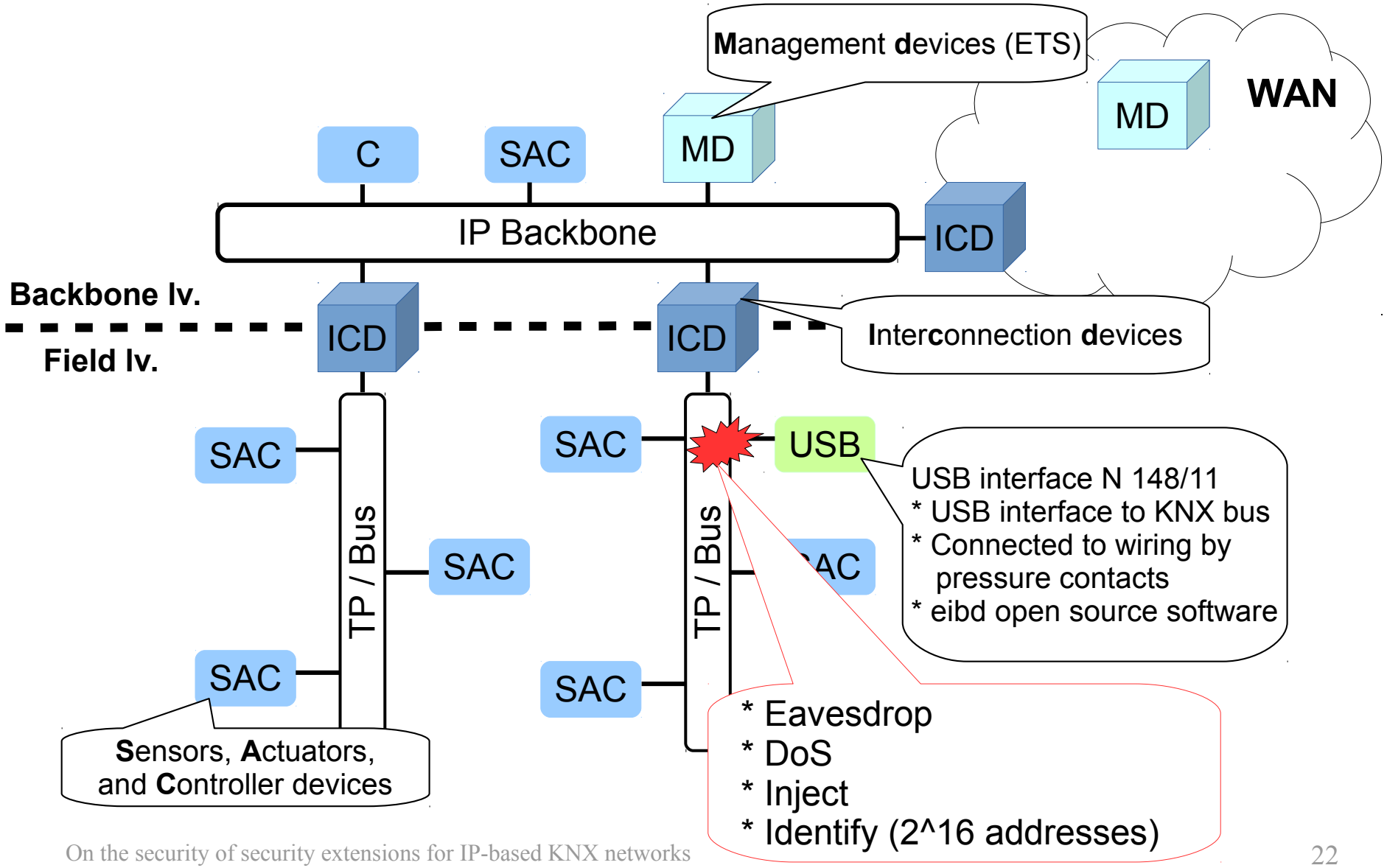
How does a KNX BAS look like?



How does a KNX BAS look like?



How does a KNX BAS look like?



Example

- Record all traffic on bus

```
$ eibd --listen-local=/tmp/eibhandle -t1023 usb:2:4:1:0:0
$ vbusmonitor1 local:/tmp/eibhandle
```

- Send message “on” to group addr.

```
$ groupswrite local:/tmp/eibhandle 1/1/5 1
```

- Read configuration of device

```
$ mread local:/tmp/eibhandle AA04 116 100
09 AA 04 09 00 09 01 09 02 09 03 09 04 09 05 0B 00 0B 02
FE 20 01 00 FE 01 FE 02 FE 03 02 04 FE 05 FE 06 FE 07 03
08 FE 09 FE 0A FE 0B 04 0C FE 0D FE
```

Example

- Record all traffic on bus

```
$ eibd --listen-local=/tmp/eibhandle -t1023 usb:2:4:1:0:0
$ vbusmonitor1 local:/tmp/eibhandle
```

- Send message “on” to group addr.

```
$ groupswrite local:/tmp/eibhandle 1/1/5 1
```

- Read configuration of device

```
$ mread local:/tmp/eibhandle AA04 116 100
09 AA 04 09 00 09 01 09 02 09 03 09 04 09 05 0B 00 0B 02
FE 20 01 00 FE 01 FE 02 FE 03 02 04 FE 05 FE 06 FE 07 03
08 FE 09 FE 0A FE 0B 04 0C FE 0D FE
```

Example

- Record all traffic on bus

```
$ eibd --listen-local=/tmp/eibhandle -t1023 usb:2:4:1:0:0
$ vbusmonitor1 local:/tmp/eibhandle
```

- Send message “on” to group addr.

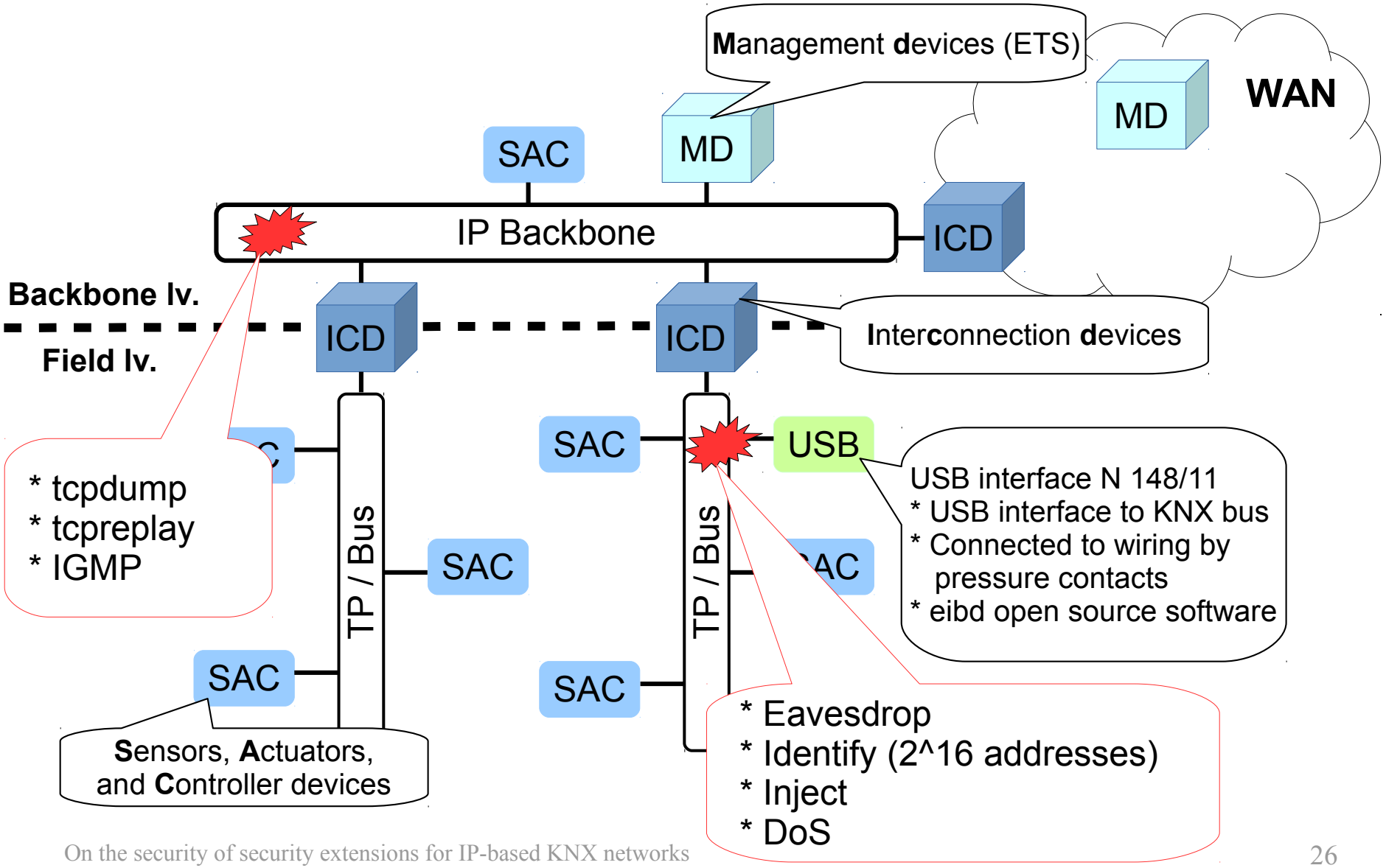
```
$ groupswrite local:/tmp/eibhandle 1/1/5 1
```

Group addr.
1/1/0

- Read configuration of device

```
$ mread local:/tmp/eibhandle AA04 116 100
09 AA 04 09 00 09 01 09 02 09 03 09 04 09 05 0B 00 0B 02
FE 20 01 00 FE 01 FE 02 FE 03 02 04 FE 05 FE 06 FE 07 03
08 FE 09 FE 0A FE 0B 04 0C FE 0D FE
```

How does a KNX BAS look like?



Example

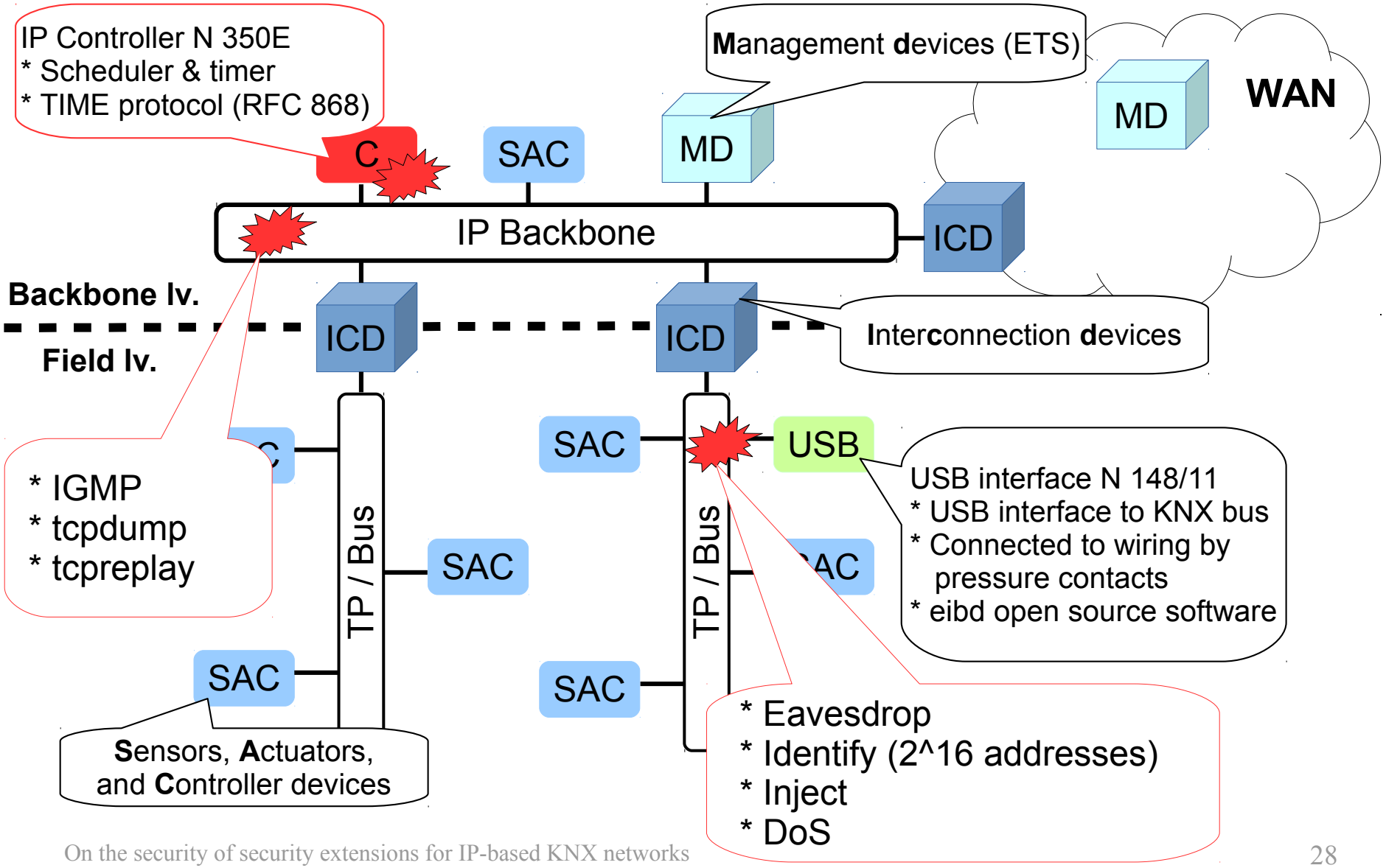
- UDP/IP port 3671
- IPv4 multicast addr. 224.0.23.12

```
0000     01 00 5e 00 17 0c 00 0e 8c 00 8a fa 08 00 45 00
0010     00 2d 00 7e 40 00 10 11 b2 8b c0 a8 00 02 e0 00
0020     17 0c 0e 57 0e 57 00 19 05 01 06 10 05 30 00 11
0030     29 00 bc f0 aa 0f 09 04 01 00 81 81
```

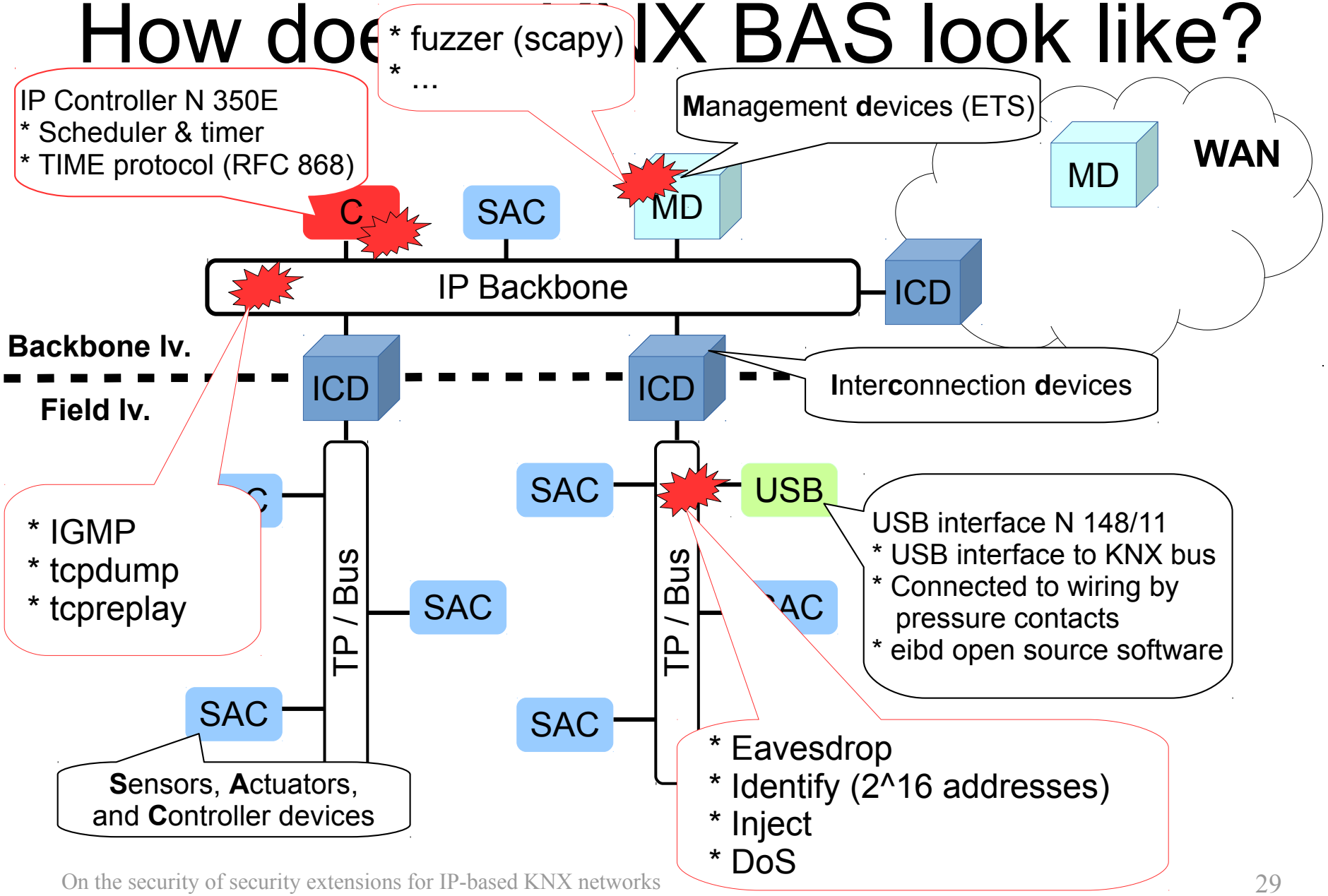
- Just record and replay ...

```
$ tcpdump -nnvvXSw switchon.cap udp port 3671
$ tcpreplay -i eth0 -v switchon.cap
```

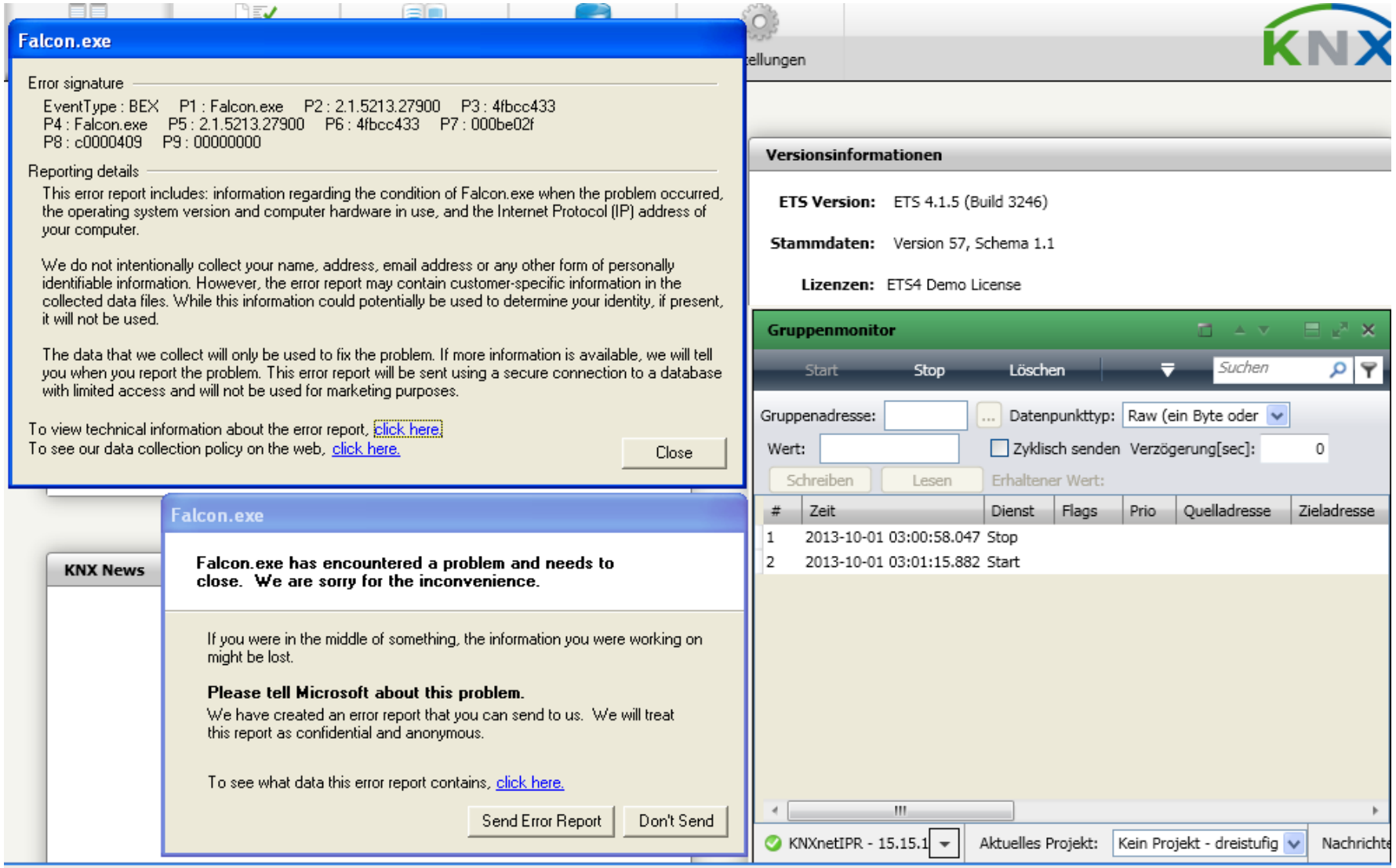
How does a KNX BAS look like?



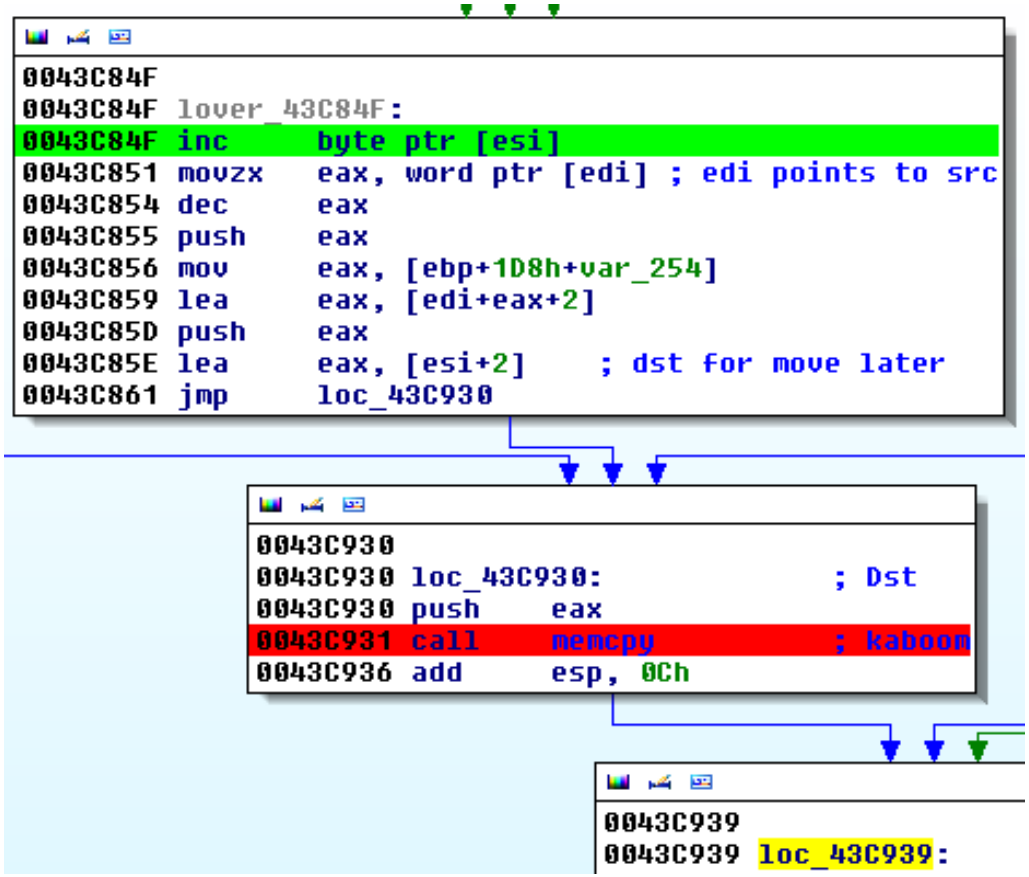
How doe[illegible]IX BAS look like?



How about the software ...?



How about the software ...?



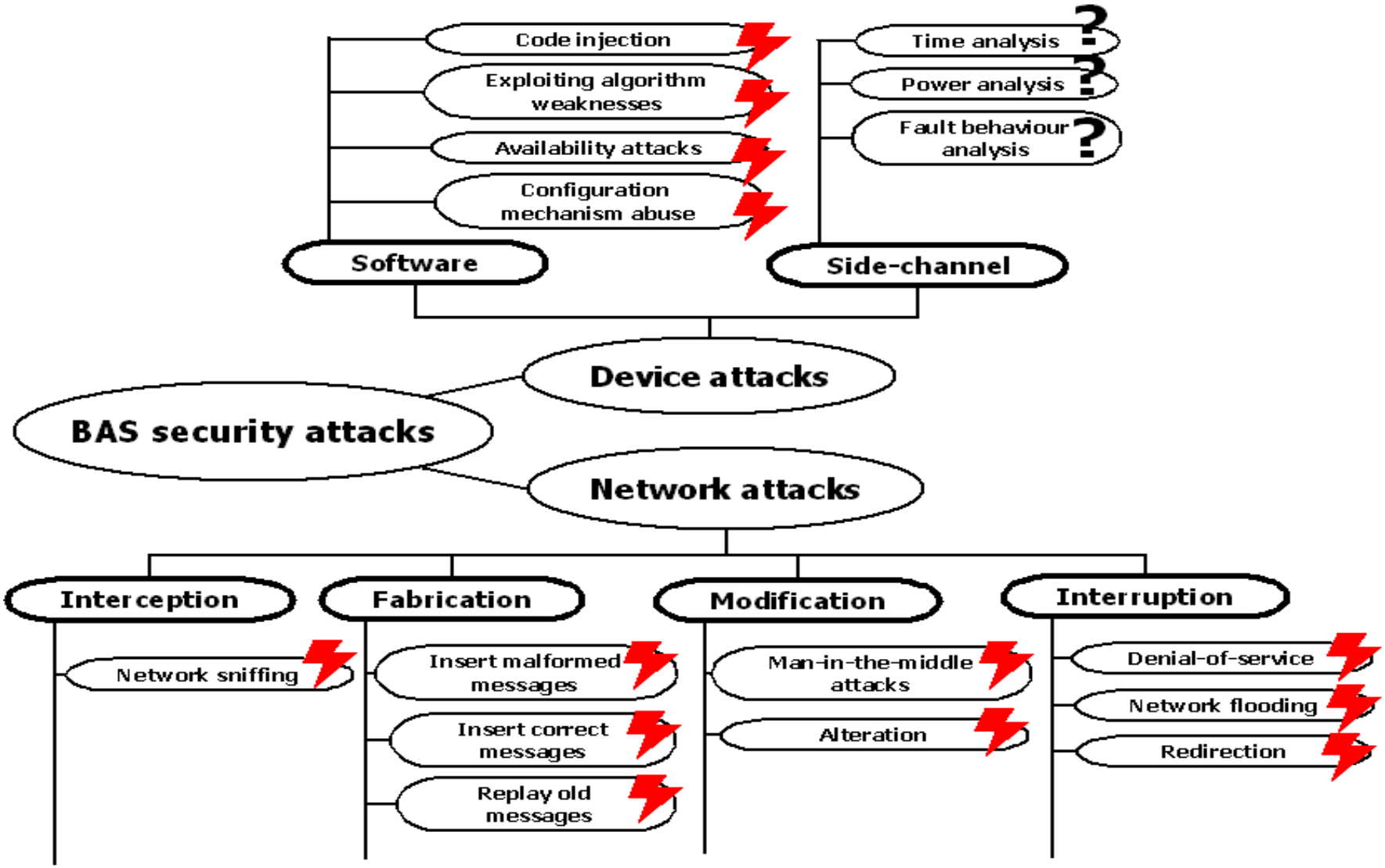
How about the software ...?

```
0043C84F
0043C84F lover_43C84F:
0043C84F inc     byte ptr [esi]
0043C851 movzx   eax, word ptr [edi] ; edi points to src
0043C854 dec     eax
0043C855 push    eax
0043C856 mov     eax, [ebp+1D8h+var_254]
0043C859 lea     eax, [edi+eax+2]
0043C85D push    eax
0043C85E lea     eax, [esi+2]    ; dst for move later
0043C861 jmp     loc_43C930
```

```
0043C930
0043C930 loc_43C930:                ; Dst
0043C930 push    eax
0043C931 call    memcpy             ; kaboom
0043C936 add     esp, 0Ch
```

```
0043C939
0043C939 loc_43C939:
```

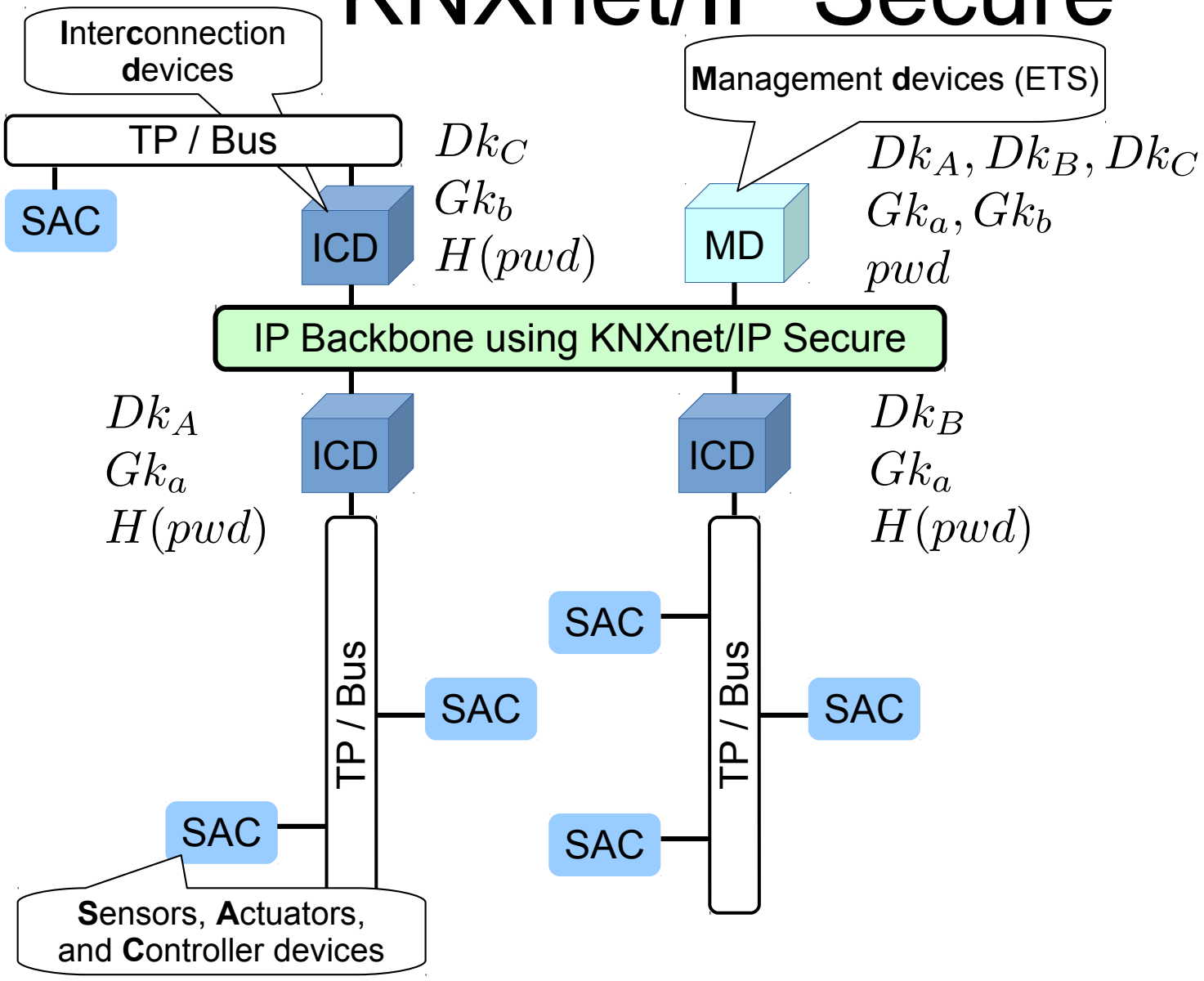
What's possible in classic KNX?



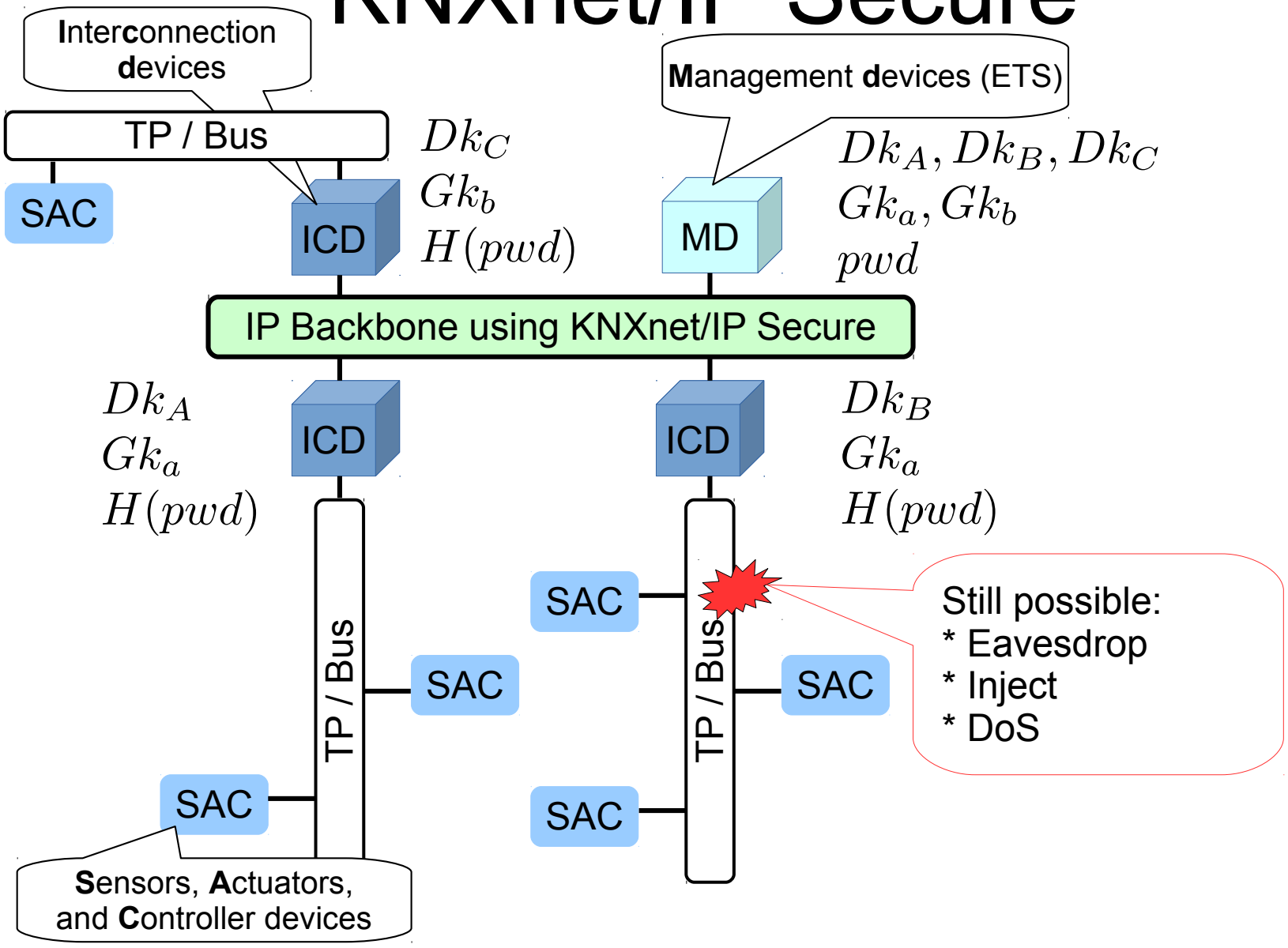
The solution?: KNXnet/IP Secure

- Security extension to KNXnet/IP
- Backward compatible
- “Draft” - now available for members, not yet implemented
- **Multicast** communication
  (*group communication*)
  - Custom version of CCM (CTR + CBC-MAC)
  - AES block cipher
- **Unicast** communication
  - Custom protocol
  - ECDH + Custom version of CCM
  - AES block cipher

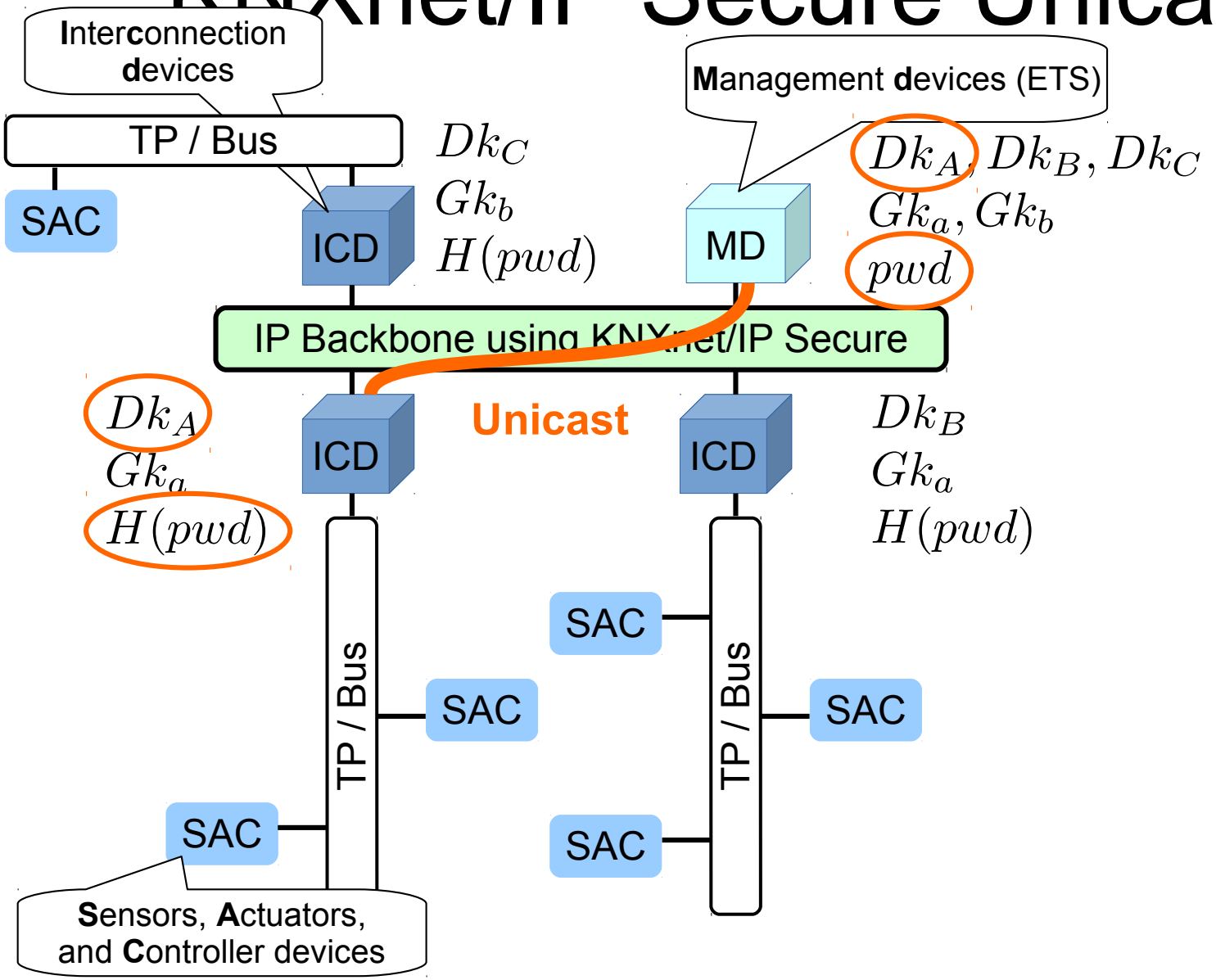
KNXnet/IP Secure



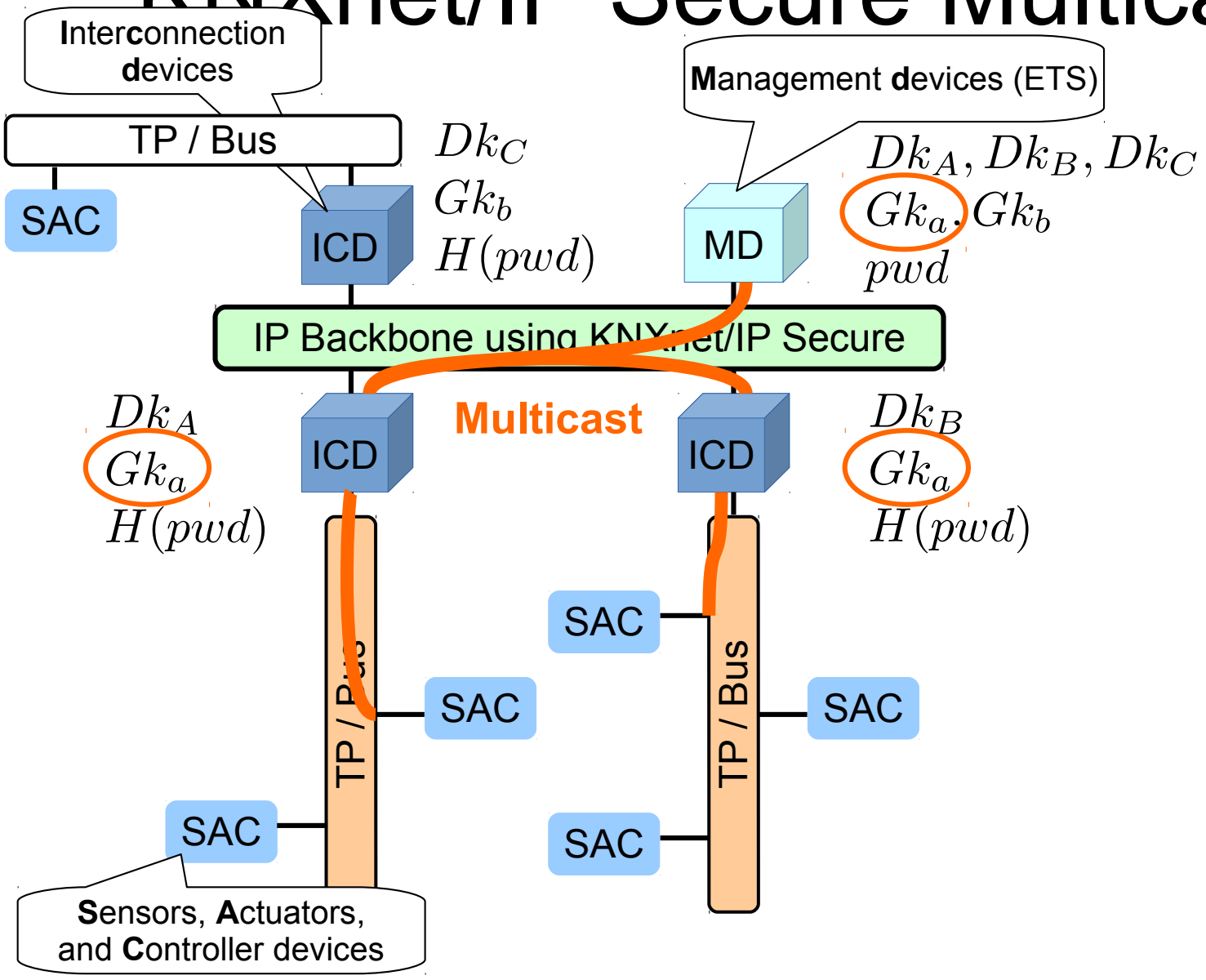
KNXnet/IP Secure



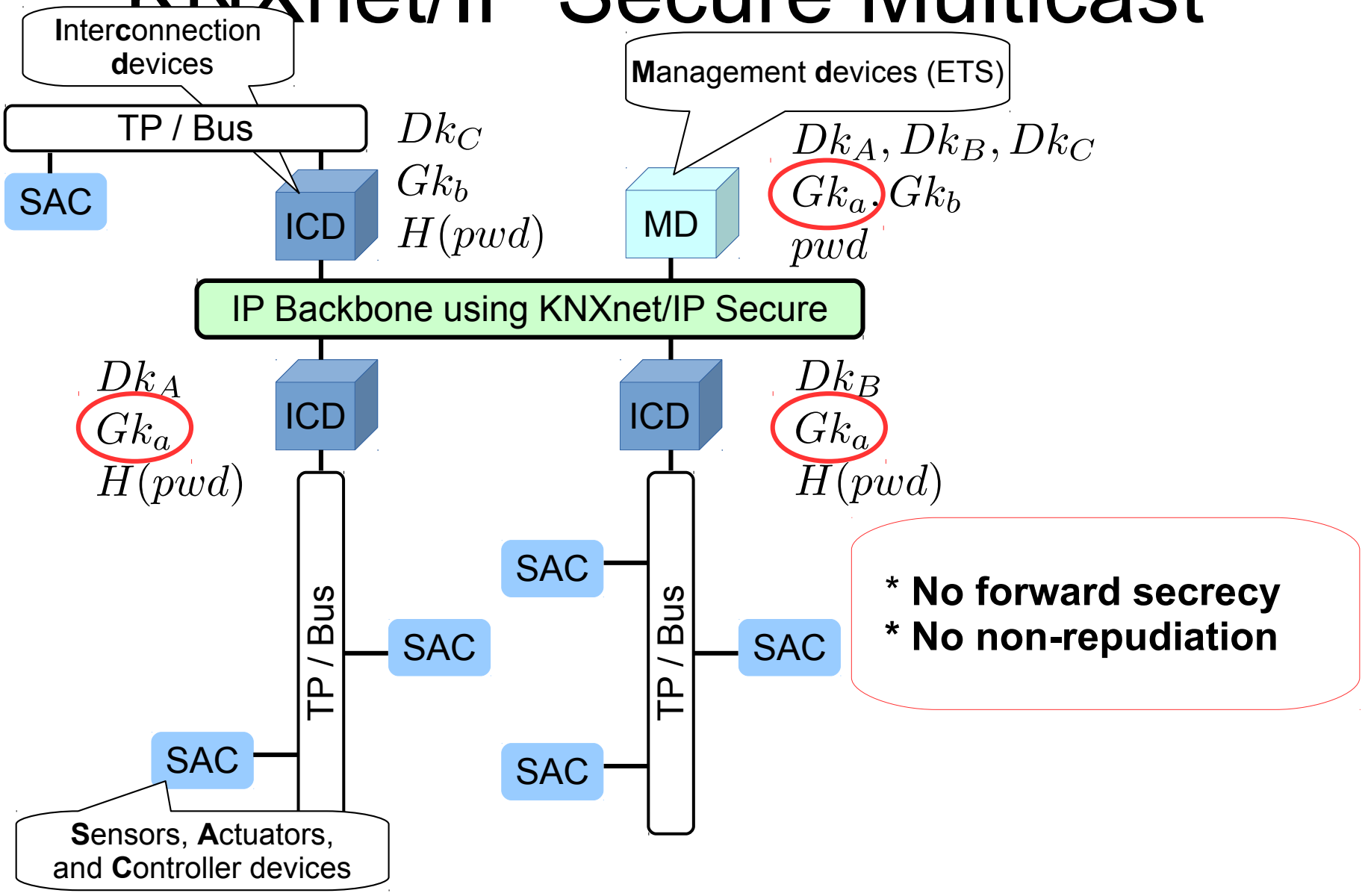
KNXnet/IP Secure Unicast



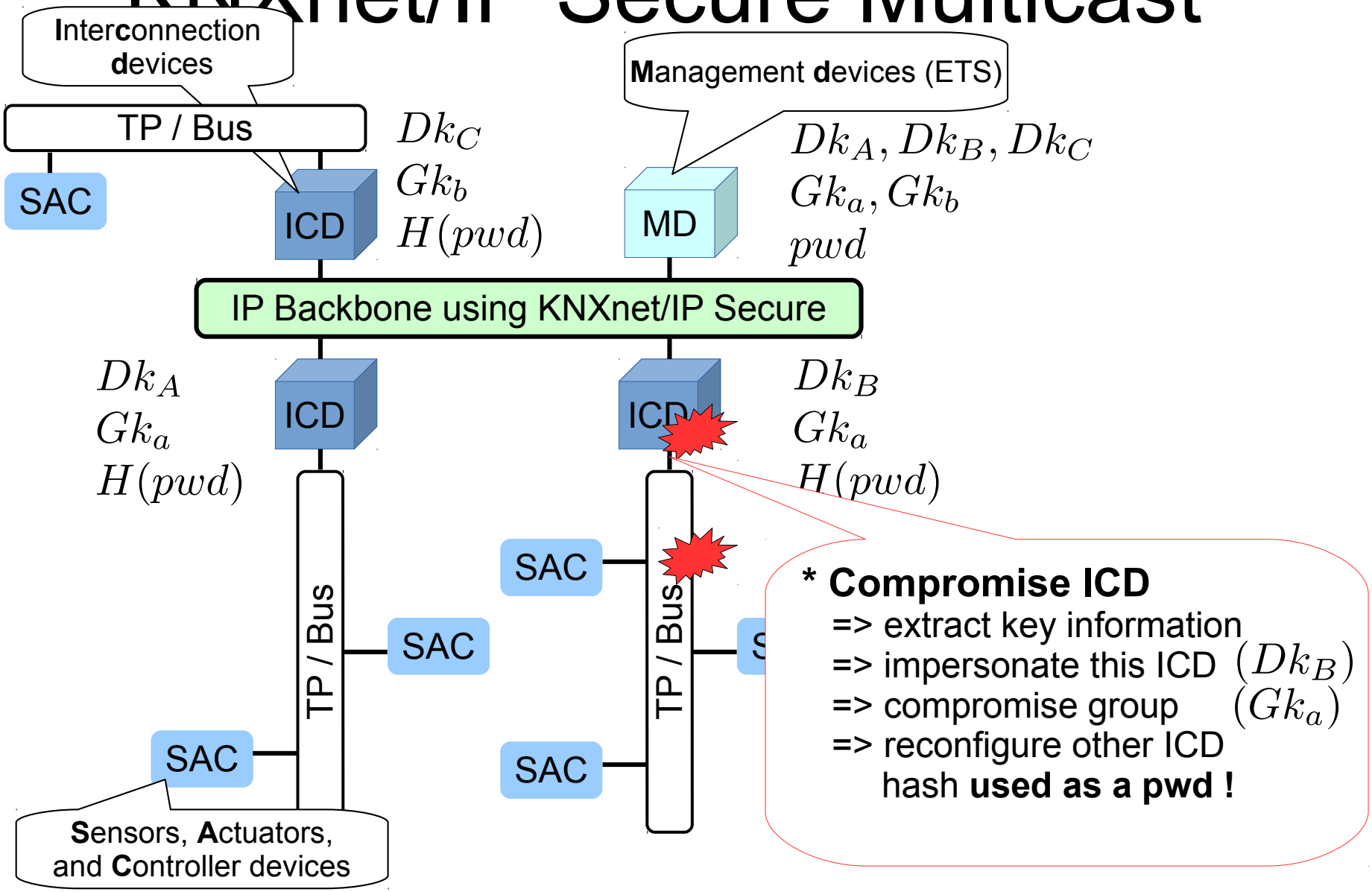
KNXnet/IP Secure Multicast



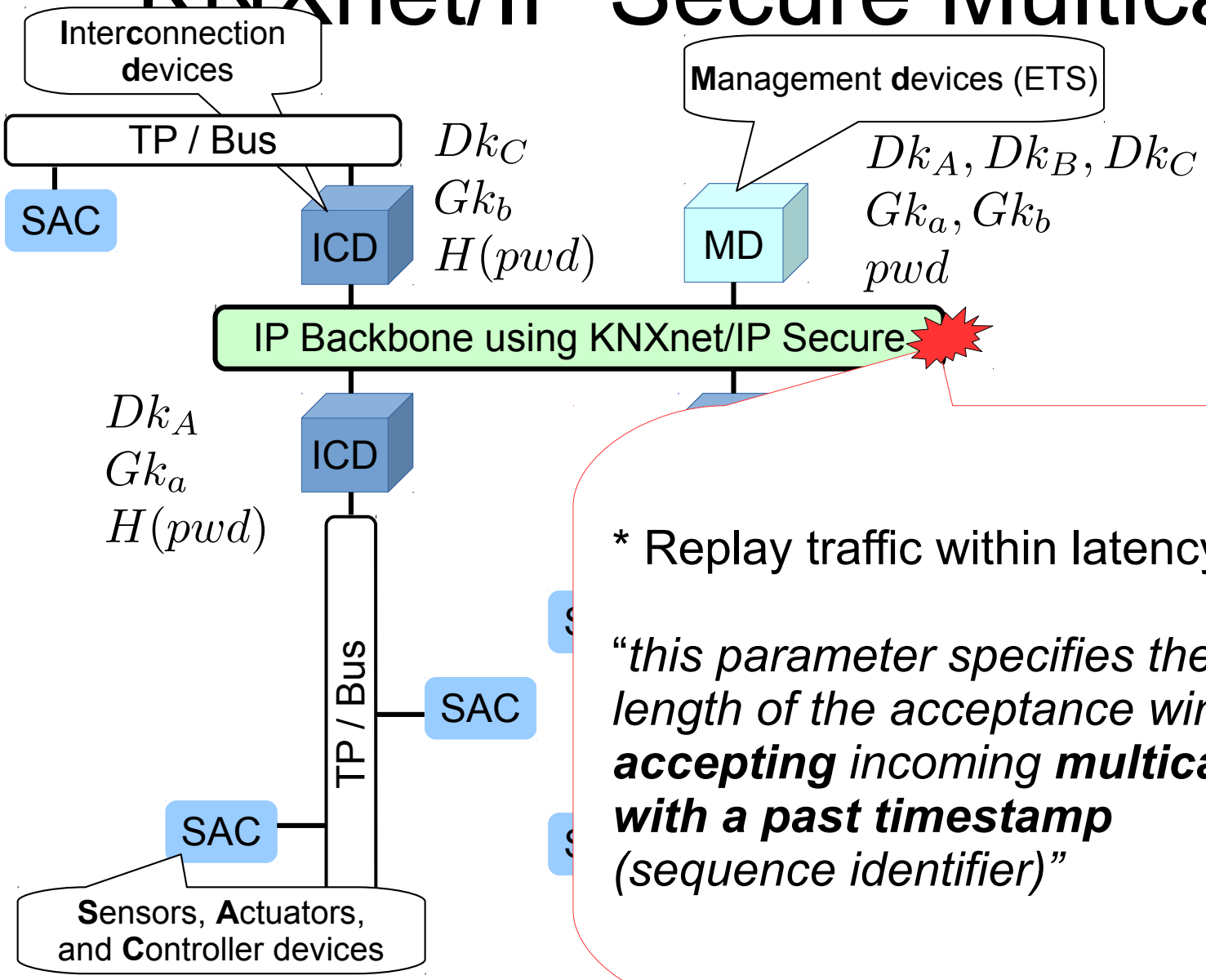
KNXnet/IP Secure Multicast



KNXnet/IP Secure Multicast



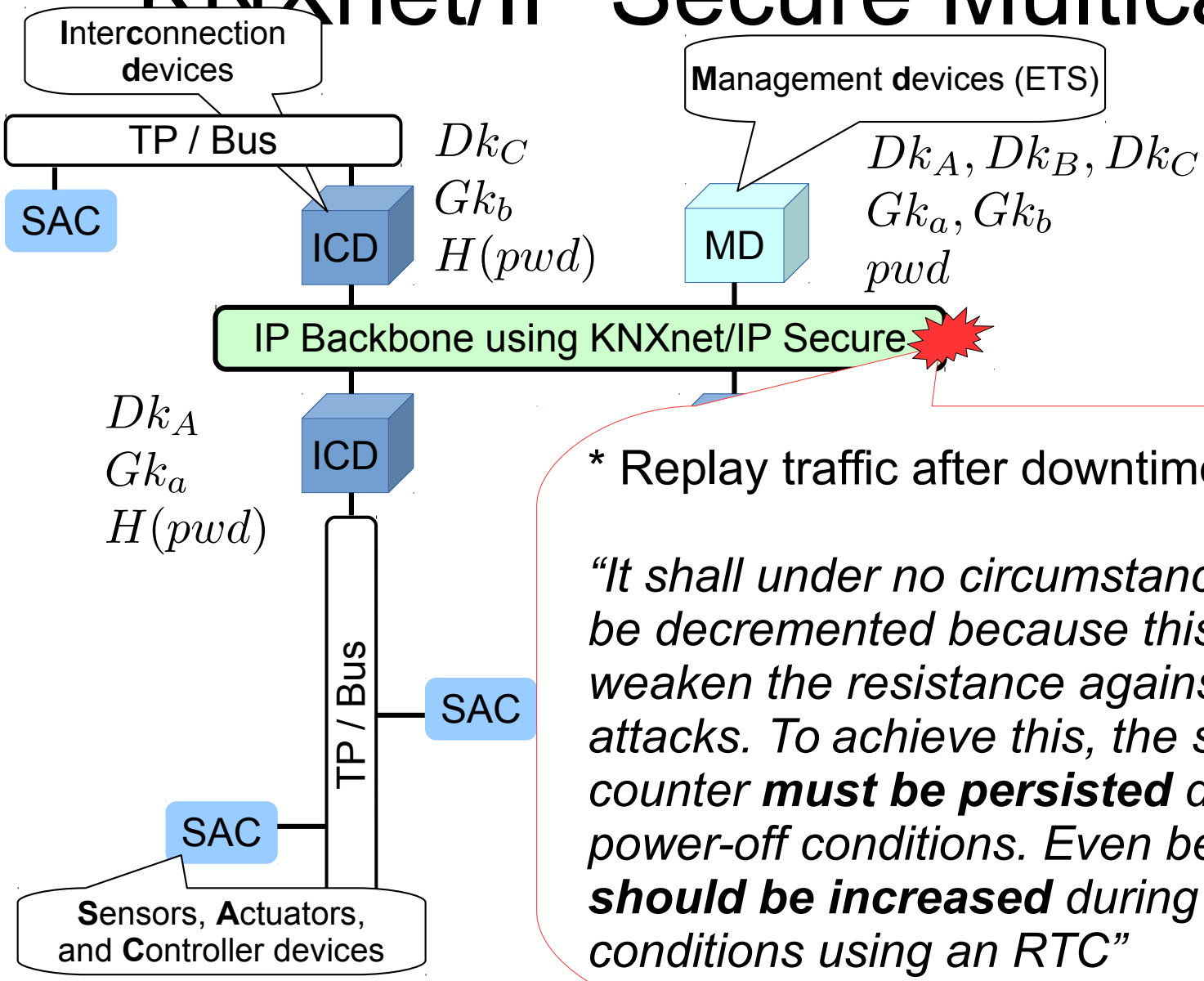
KNXnet/IP Secure Multicast



* Replay traffic within latency tolerance

"*this parameter specifies the length of the acceptance window for* ***accepting*** *incoming* ***multicast frames with a past timestamp*** *(sequence identifier)*"

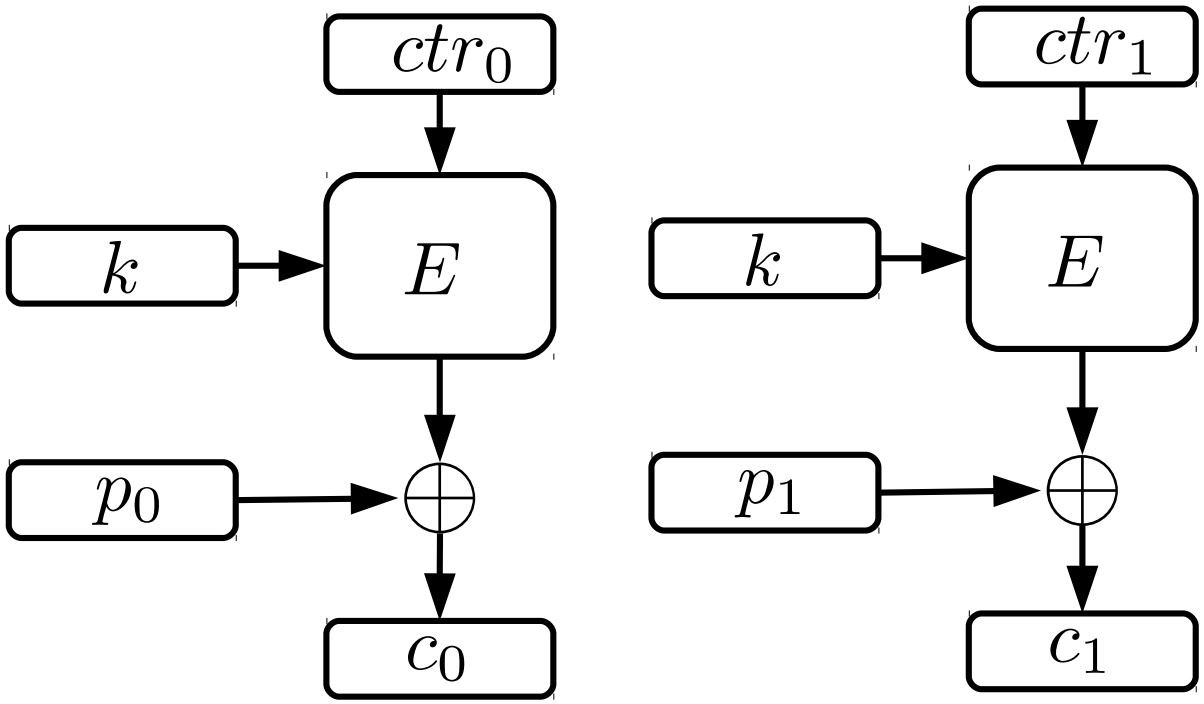
KNXnet/IP Secure Multicast



* Replay traffic after downtime

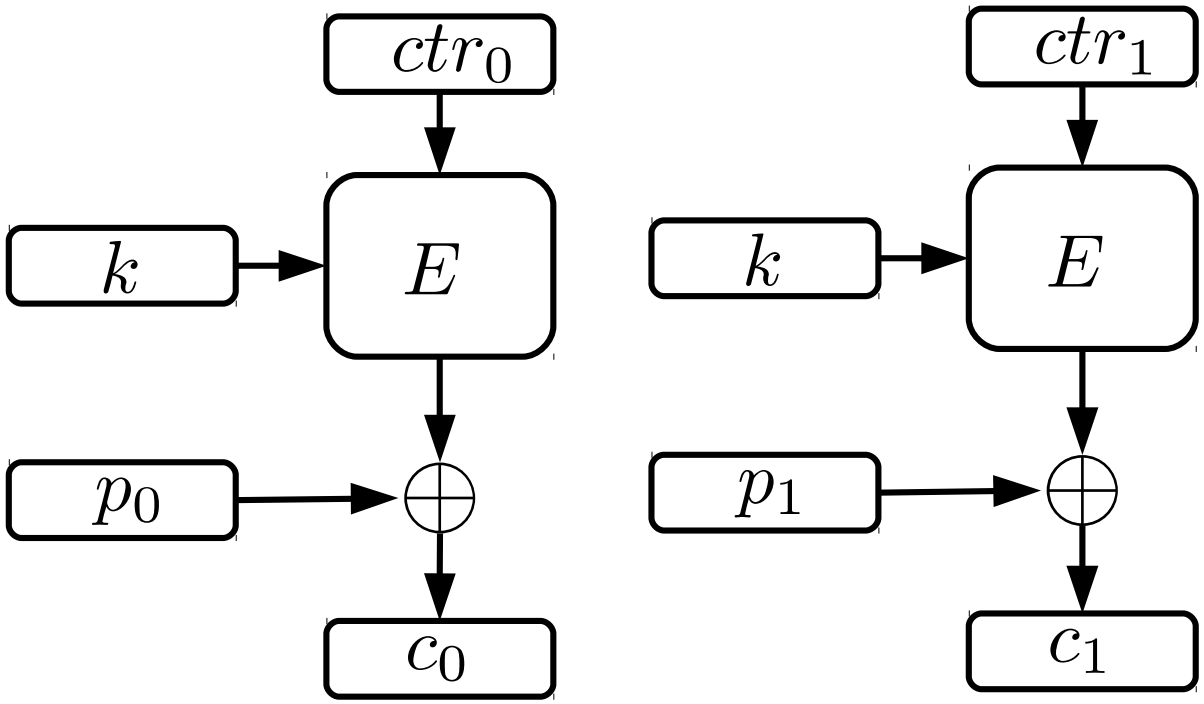
*"It shall under no circumstances be decremented because this would weaken the resistance against replay attacks. To achieve this, the sequence counter **must be persisted** during power-off conditions. Even better it **should be increased** during power-off conditions using an RTC"*

Custom AES CTR



where,
c is the ciphertext,
p is the plaintext,
E is the encryption function (AES),
k is the key,
ctr is the counter

Custom AES CTR



where,
c is the ciphertext,
p is the plaintext,
E is the encryption function (AES),
k is the key,
ctr is the counter

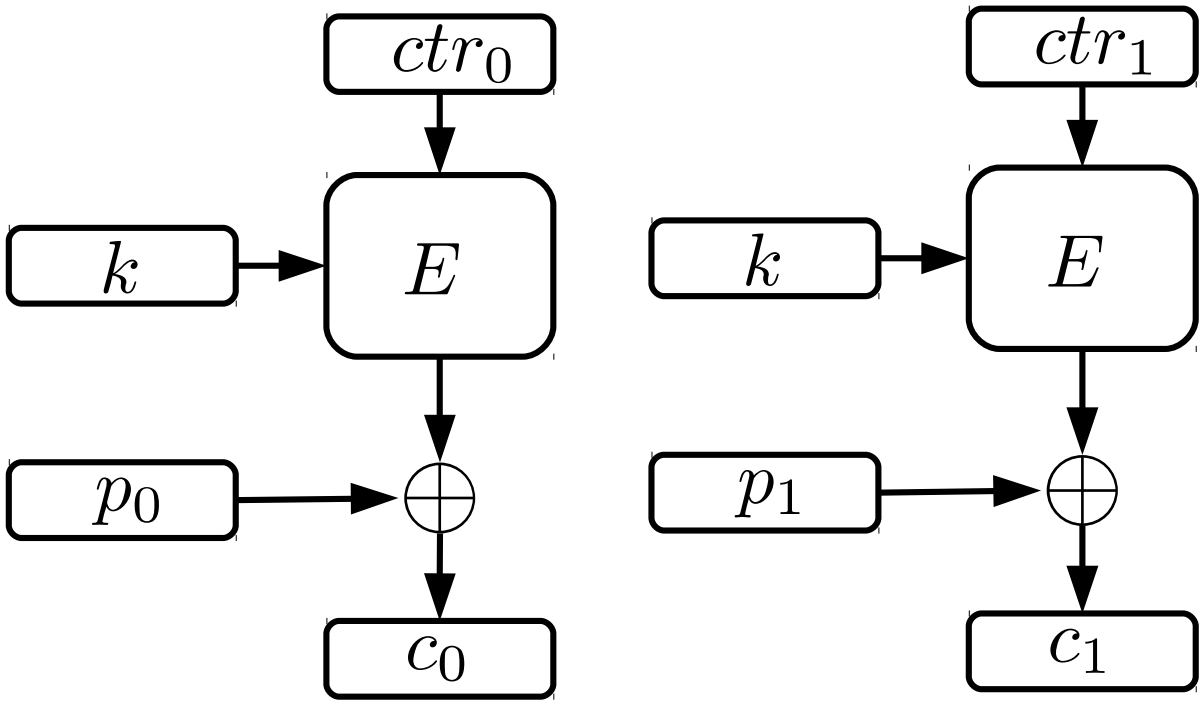
Group identifier (GID) is a timestamp

$ctr_x = GID \mid\mid 00 \ldots 00 \mid\mid 0 - 255$

$ctr_0 = GID \mid\mid 00 \ldots 00 \mid\mid 0$

$ctr_1 = GID \mid\mid 00 \ldots 00 \mid\mid 1$

Custom AES CTR



where,
c is the ciphertext,
p is the plaintext,
E is the encryption function (AES),
k is the key,
ctr is the counter

Group identifier (GID) is a timestamp

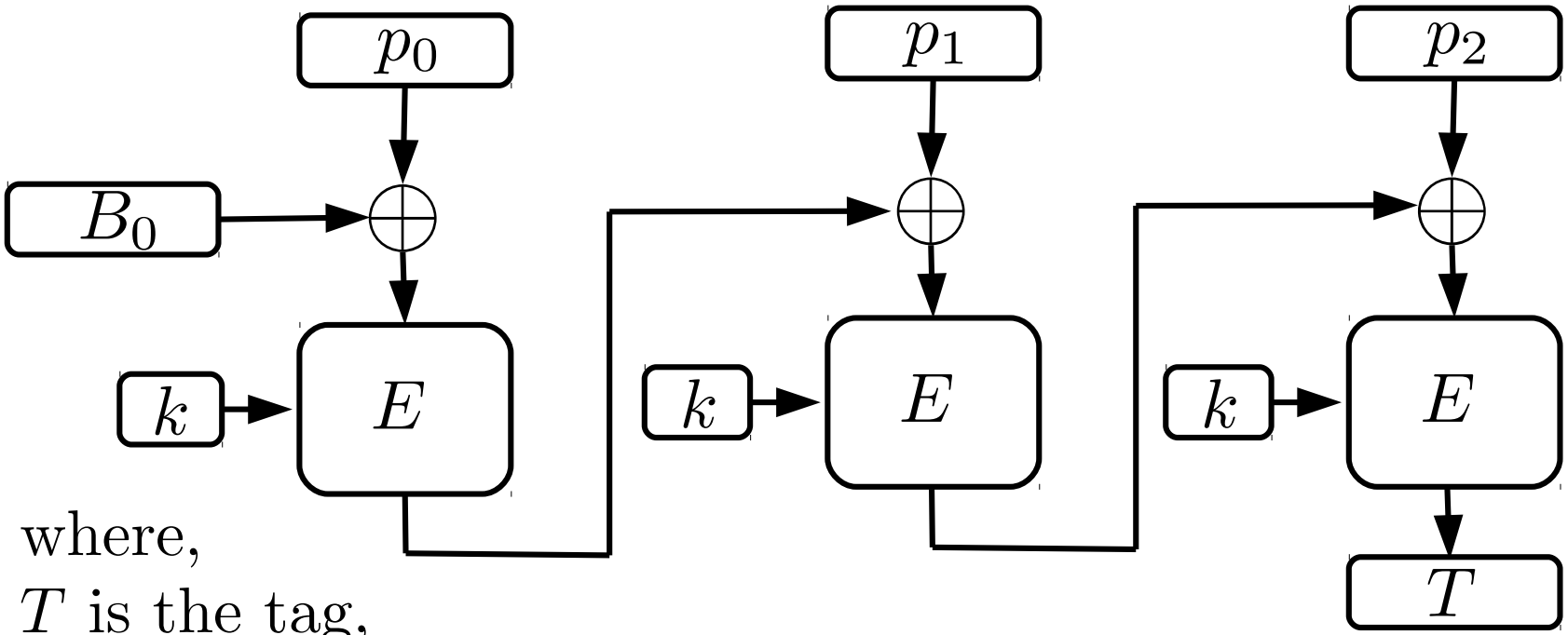
$$ctr_x = GID \,||\, 00 \ldots 00 \,||\, 0 - 255$$
$$ctr_0 = GID \,||\, 00 \ldots 00 \,||\, 0$$
$$ctr_1 = GID \,||\, 00 \ldots 00 \,||\, 1$$

$$ctr_0 = ctr'_0$$
$$c_0 = p_0 \oplus E_k(ctr_0)$$
$$c'_0 = p'_0 \oplus E_k(ctr'_0)$$
$$c_0 \oplus c'_0 = p_0 \oplus p'_0$$

CBC MAC Forgery?

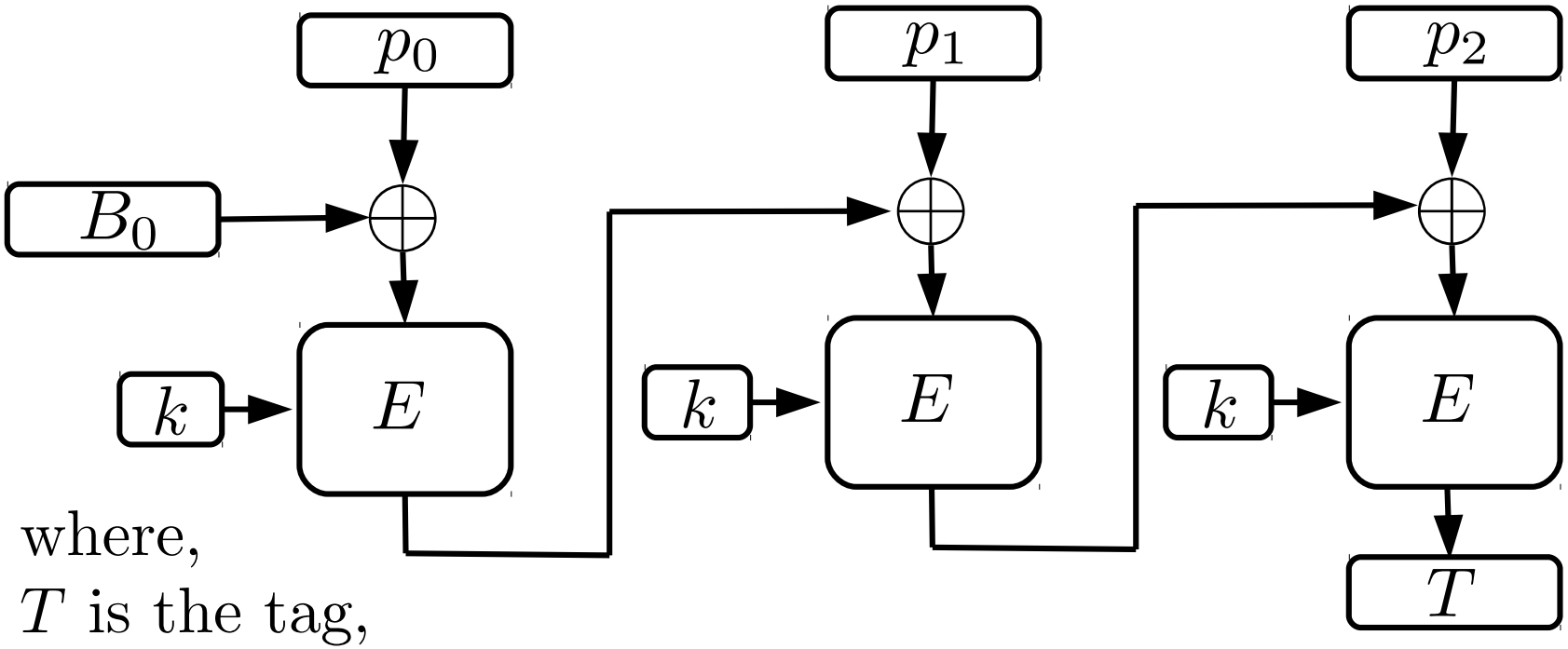
- depends on byte order and detailed construction of and
- Only possible on messages which are authenticated but not encrypted

CBC MAC Forgery?



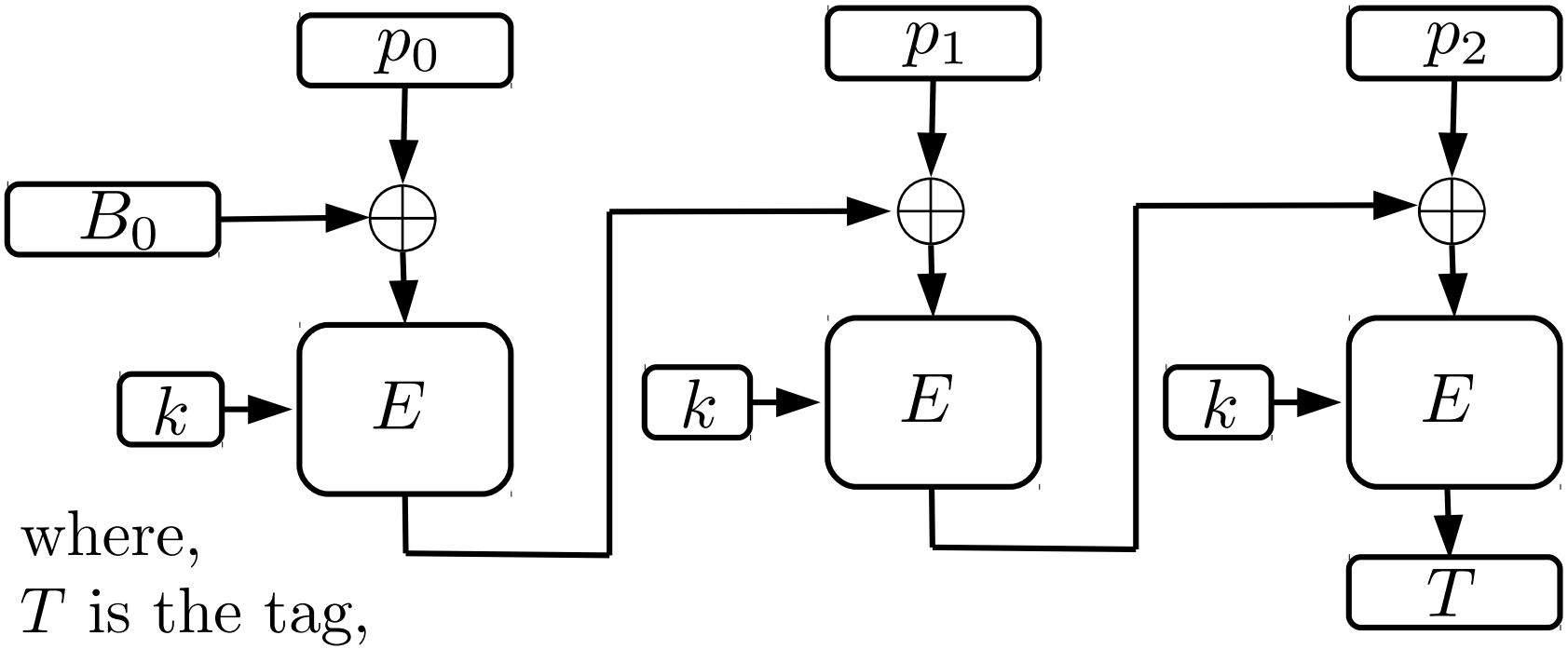
where,
T is the tag,
p is the plaintext,
E is the encryption function (AES),
k is the key,
B_0 is the IV

CBC MAC Forgery?



where,
T is the tag,
p is the plaintext,
E is the encryption function (AES),
k is the key,
B_0 is the IV

CBC MAC Forgery?



where,
T is the tag,
p is the plaintext,
E is the encryption function (AES),
k is the key,
B_0 is the IV

$$p_0 \oplus B_0 = p'_0 \oplus B'_0$$

$$c_0 = E_k(p_0 \oplus B_0)$$

$$c_0 = E_k(p'_0 \oplus B'_0)$$

Conclusio

- Current/classical KNX => no security
- unicast / multicast (+) yes, (-) no, (~) nice try

Property	KNX	KNXnet/IP Secure
Authentication	- / -	~ / -
Authorization	- / -	+ / -
Non-repudiation	- / -	- / -
Integrity	- / -	+ / ~
Freshness	- / -	+ / ~
Confidentiality	- / -	+ / ~
Forward secrecy	- / -	+ / -
Availability	- / -	- / -

EOF