ERNW
providing security.

Attacking Autonomic Networks

Omar Eissa

ERNW
providing security.

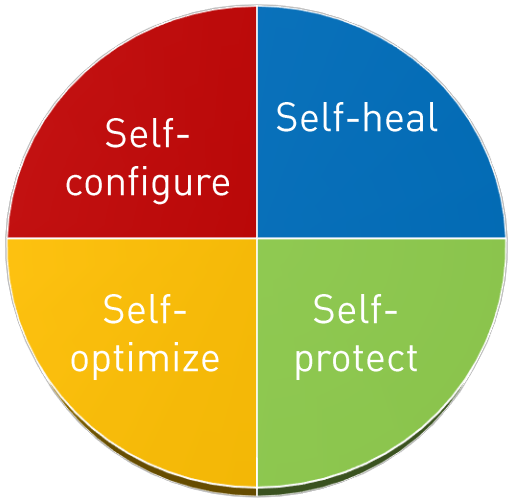
Agenda

- Autonomic System
- Cisco deployment of the Autonomic Network
- Reverse-engineer the proprietary protocol
- Discover and exploit multiple vulnerabilities

ERNW
providing security.

Autonomic Systems

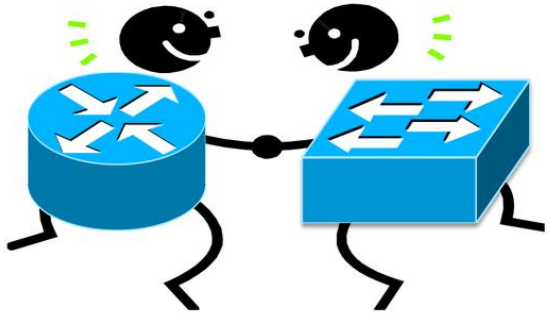
- Smart systems that don't need human intervention to operate
- They have the ability to self-manage themselves



ERNW
providing security.

Autonomic Network

- IETF ANIMA working group
- One device that configures everything else
- Only 5 commands are needed
- Nothing has to be configured on the new devices



credits

Live Demo

ERNW
providing security.

Demo Results

- Plug and Play
- There is no need to configure any command on the greenfield devices
- Only a single command needs to be configured on the brownfield devices

ERNW
providing security.

Cisco Deployment

- Communication is divided into 3 phases:
  - Channel Discovery
  - Adjacency Discovery
  - Secure Channel

ERNW
providing security.

Channel Discovery

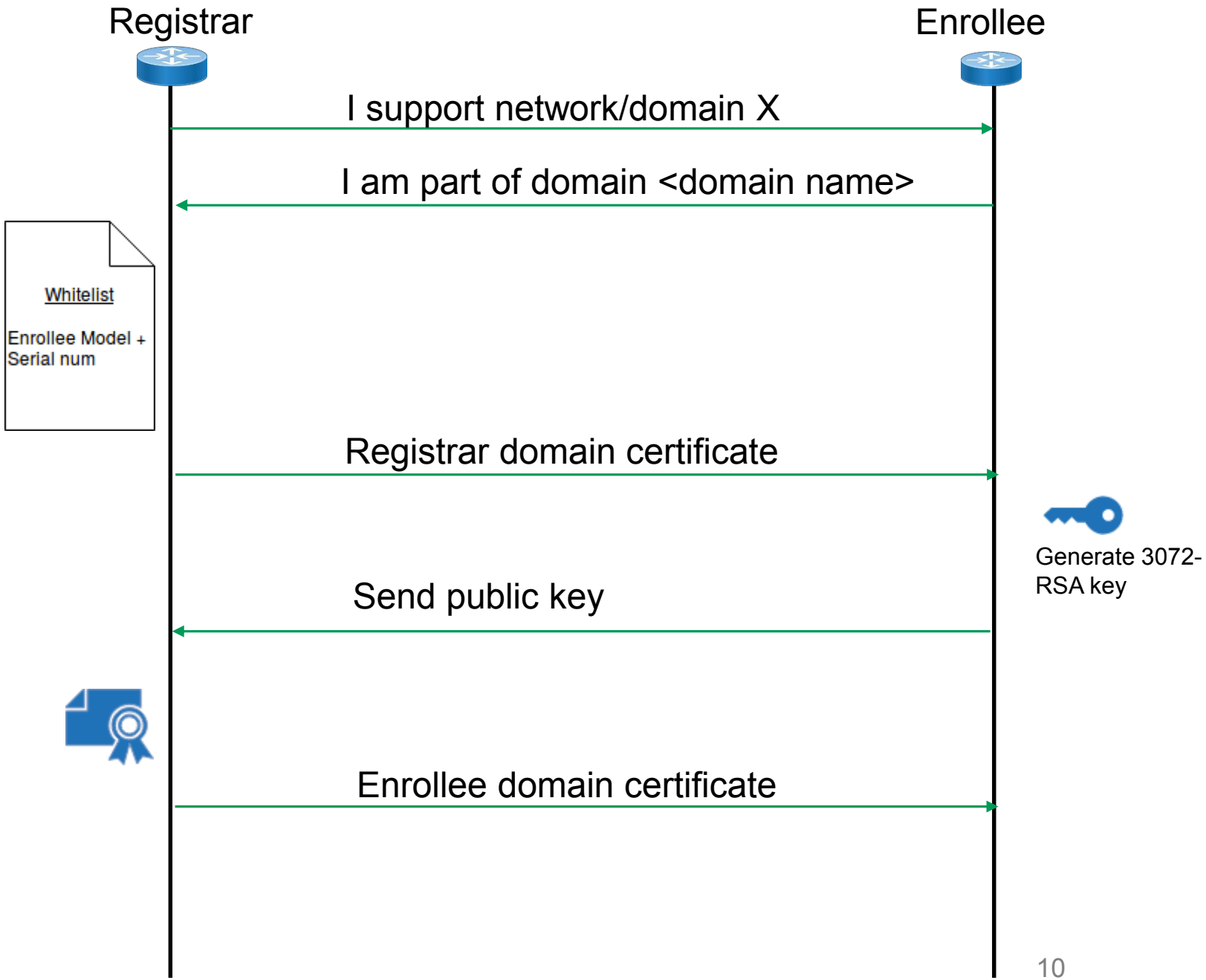
- Discover any autonomic devices around
- Layer 2 probes sent by registrar

ERNW
providing security.

Adjacency Discovery

- Domain name
- Are you allowed to join the domain or not?
  - Rejected: stay at channel discovery phase
  - Allowed: let's issue a certificate then
- UDP port 4936

ERNW
providing security.



Adjacency Discovery

ERNW
providing security.

Secure Channel

- IPSec
  - Port 500
  - Backwards compatibility
- DIKE
  - Data Internet Key Exchange
  - Port 5000
  - Preferred over IPsec

ERNW
providing security.

Registrar Configuration

```
autonomic registrar
domain-id ERNW.de
whitelist flash:whitelist.txt
CA local
no shut
autonomic
```

ERNW
providing security.

Enrollee Configuration

- Brand new (i.e. no configuration file exit)
  - None!
- Configuration file exist
  - `autonomic`

ERNW
providing security.

Autonomic Effect

- IPv6 address based on the domain name and device ID
- Domain Certificate
- VRF cisco_autonomic
- Virtual Interface, ANI1
- Tunnel Interface, Tunnel100000
- AAA (Authentication, Authorization and Accounting) will be enabled
- RADIUS, TFTP, Syslog (if available)

ERNW
providing security.

Are you in Control?

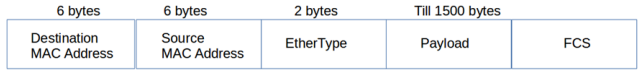
ERNW
providing security.

Autonomic Network: Under The Hood

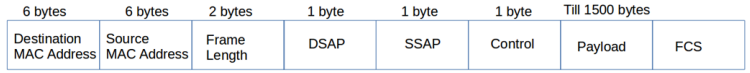
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:62:ec:9d:80:60	ISL-Frame_cd:cd:dc	LLC	118	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF
2	0.014104	00:00:00_00:00:01	ISL-Frame_cd:cd:dc	LLC	148	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF
3	11.680271	00:00:00_00:00:01	ISL-Frame_cd:cd:dc	LLC	159	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF
4	21.678386	00:62:ec:9d:80:60	ISL-Frame_cd:cd:dc	LLC	212	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF
5	21.678411	00:62:ec:9d:80:60	ISL-Frame_cd:cd:dc	LLC	148	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF
6	24.384456	00:62:ec:9d:80:60	ISL-Frame_cd:cd:dc	LLC	1436	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF
7	24.384480	00:62:ec:9d:80:60	ISL-Frame_cd:cd:dc	LLC	1365	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF
8	24.506508	00:00:00_00:00:01	ISL-Frame_cd:cd:dc	LLC	1436	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF
9	24.506526	00:00:00_00:00:01	ISL-Frame_cd:cd:dc	LLC	153	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF
10	26.502154	00:62:ec:9d:80:60	ISL-Frame_cd:cd:dc	LLC	1213	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF
11	28.727965	00:62:ec:9d:80:60	ISL-Frame_cd:cd:dc	LLC	596	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF
12	30.621816	00:62:ec:9d:80:60	ISL-Frame_cd:cd:dc	LLC	596	U, func=UI; SNAP, OUI 0x00000C (Cisco), PID 0x88EF

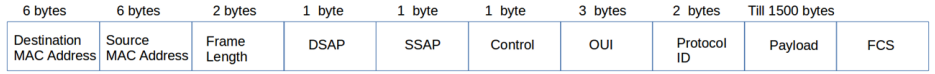
Channel Discovery



Ethernet II



802.3
(802.3, 802.2 LLC)



802.3
(802.3, 802.2 SNAP)

Not Ethernet II

SNAP Frame

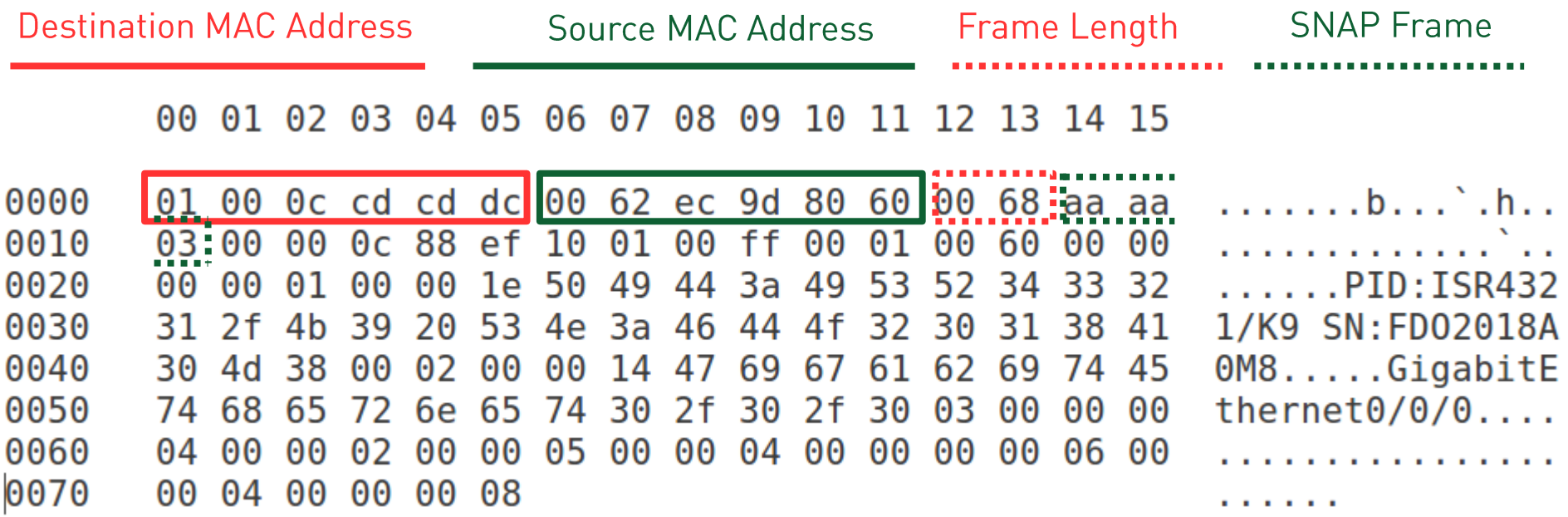
```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000    01 00 0c cd cd dc 00 62 ec 9d 80 60 00 68 aa aa  .......b...`.h..
0010    03 00 00 0c 88 ef 10 01 00 ff 00 01 00 60 00 00  .............`..
0020    00 00 01 00 00 1e 50 49 44 3a 49 53 52 34 33 32  ......PID:ISR432
0030    31 2f 4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41  1/K9 SN:FDO2018A
0040    30 4d 38 00 02 00 00 14 47 69 67 61 62 69 74 45  0M8.....GigabitE
0050    74 68 65 72 6e 65 74 30 2f 30 2f 30 03 00 00 00  thernet0/0/0....
0060    04 00 00 02 00 00 05 00 00 04 00 00 00 00 06 00  ................
0070    00 04 00 00 00 08                                ......
```

ERNW
providing security.

Ethernet

Channel Discovery



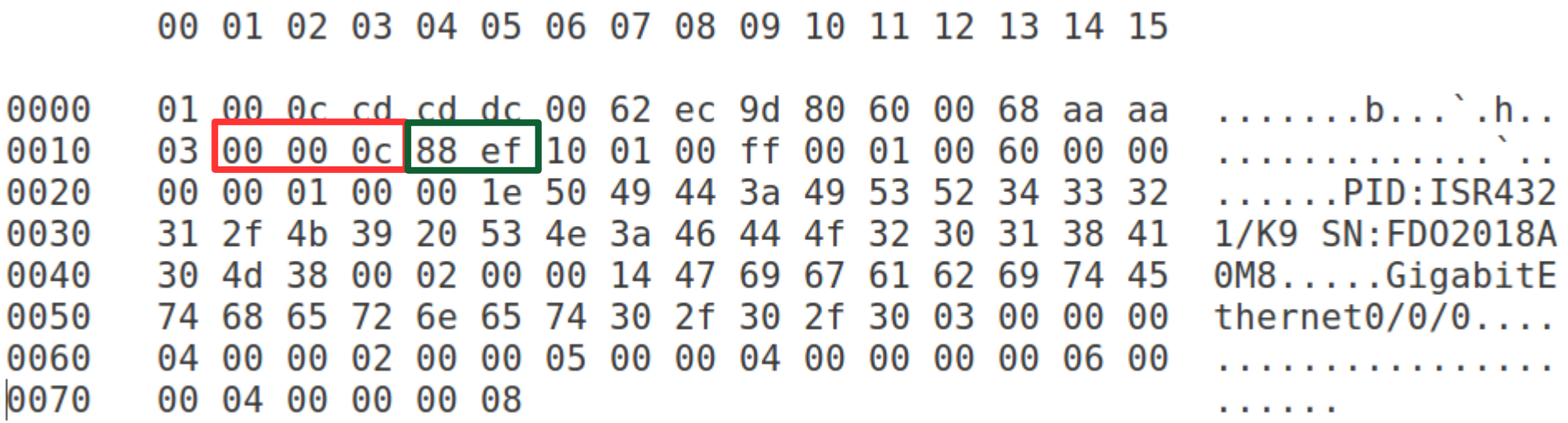
ERNW
providing security.

Ethernet

Channel Discovery

Organization Unique Identifier

AN Protocol ID



ERNW
providing security.

Channel Discovery

Ethernet

Channel Discovery

Octet	0								1								2								3							
Bits	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	Version				Reserved				State								Factory Default															
64	Operation Code																Length															
96	Reserved																															
128	TLV (Options)																															

AN Channel Discovery Header

ERNW
providing security.

Channel Discovery

Ethernet

Channel Discovery

Version = 1, reserved = 0 | State | Factory Default | Operation Code

```
      00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000  01 00 0c cd cd dc 00 62 ec 9d 80 60 00 68 aa aa  .......b...`.h..
0010  03 00 00 0c 88 ef 10 01 00 ff 00 01 00 60 00 00  .............`..
0020  00 00 01 00 00 1e 50 49 44 3a 49 53 52 34 33 32  ......PID:ISR432
0030  31 2f 4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41  1/K9 SN:FDO2018A
0040  30 4d 38 00 02 00 00 14 47 69 67 61 62 69 74 45  0M8.....GigabitE
0050  74 68 65 72 6e 65 74 30 2f 30 2f 30 03 00 00 00  thernet0/0/0....
0060  04 00 00 02 00 00 05 00 00 04 00 00 00 00 06 00  ................
0070  00 04 00 00 00 08                                ......
```

ERNW
providing security.

Channel Discovery

Opcode Value	Significance
0x0001	Registrar/Enrollee announcement
0x0002	Receiver reply for the announcement
0x0003	Sender acknowledgment for the reply
0x0004	Keepalive probes

ERNW
providing security.

Channel Discovery

Ethernet

Channel Discovery

Header Length Reserved Type Length

```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000    01 00 0c cd cd dc 00 62 ec 9d 80 60 00 68 aa aa   .......b...`.h..
0010    03 00 00 0c 88 ef 10 01 00 ff 00 01 00 60 00 00   .............`..
0020    00 00 01 00 00 1e 50 49 44 3a 49 53 52 34 33 32   ......PID:ISR432
0030    31 2f 4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41   1/K9 SN:FDO2018A
0040    30 4d 38 00 02 00 00 14 47 69 67 61 62 69 74 45   0M8.....GigabitE
0050    74 68 65 72 6e 65 74 30 2f 30 2f 30 03 00 00 00   thernet0/0/0....
0060    04 00 00 02 00 00 05 00 00 04 00 00 00 00 06 00   ................
0070    00 04 00 00 00 08                                 ......
```

ERNW
providing security.

Channel Discovery

Option Type	Significance
0x0100	Source UDI
0x0200	Source Interface
0x0300	Receiver UDI
0x0400	2 bytes of zeros
0x0500	4 bytes of zeros
0x0600	4 bytes of value 0x00000008

ERNW
providing security.

Adjacency Discovery

```
      00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000  01 00 0c cd cd dc 00 62 ec 9d 80 60 00 c6 aa aa  .......b...`....
0001  03 00 00 0c 88 ef 10 05 00 ff 00 00 00 0e 00 00  ................
0002  00 00 86 dd 60 00 00 00 00 88 11 ff fe 80 00 00  ....`...........
0003  00 00 00 00 02 62 ec ff fe 9d 80 60 ff 02 00 00  .....b.....`....
0004  00 00 00 00 00 00 00 00 00 00 01 50 13 48 13 48  ...........P.H.H
0005  00 88 86 00 20 02 00 ff 00 01 00 80 00 00 00 00  .... ...........
0006  00 01 00 22 50 49 44 3a 49 53 52 34 33 32 31 2f  ..."PID:ISR4321/
0007  4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41 30 4d  K9 SN:FDO2018A0M
0008  38 00 00 02 00 15 30 30 36 32 2e 65 63 39 64 2e  8.....0062.ec9d.
0009  38 30 36 30 2d 31 00 00 03 00 0c 45 52 4e 57 2e  8060-1.....ERNW.
0010  64 65 00 00 07 00 14 fe 80 00 00 00 00 00 00 02  de..............
0011  62 ec ff fe 9d 80 60 00 08 00 09 41 4e 49 31 00  b.....`....ANI1.
0012  00 05 00 14 fd b6 67 6a 9a 78 00 00 00 62 ec 9d  ......gj.x...b..
0013  80 60 00 01
```

ERNW
providing security.

Adjacency Discovery

Ethernet

```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000    01 00 0c cd cd dc 00 62 ec 9d 80 60 00 c6 aa aa  .......b...`....
0001    03 00 00 0c 88 ef 10 05 00 ff 00 00 00 0e 00 00  ................
0002    00 00 86 dd 60 00 00 00 00 88 11 ff fe 80 00 00  ....`...........
0003    00 00 00 00 02 62 ec ff fe 9d 80 60 ff 02 00 00  .....b.....`....
0004    00 00 00 00 00 00 00 00 00 00 01 50 13 48 13 48  ...........P.H.H
0005    00 88 86 00 20 02 00 ff 00 01 00 80 00 00 00 00  .... ...........
0006    00 01 00 22 50 49 44 3a 49 53 52 34 33 32 31 2f  ..."PID:ISR4321/
0007    4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41 30 4d  K9 SN:FDO2018A0M
0008    38 00 00 02 00 15 30 30 36 32 2e 65 63 39 64 2e  8.....0062.ec9d.
0009    38 30 36 30 2d 31 00 00 03 00 0c 45 52 4e 57 2e  8060-1.....ERNW.
0010    64 65 00 00 07 00 14 fe 80 00 00 00 00 00 00 02  de..............
0011    62 ec ff fe 9d 80 60 00 08 00 09 41 4e 49 31 00  b.....`....ANI1.
0012    00 05 00 14 fd b6 67 6a 9a 78 00 00 00 62 ec 9d  ......gj.x...b..
0013    80 60 00 01
```

Ethernet 802.3 /802.2 SNAP

ERNW
providing security.

Adjacency Discovery


```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000    01 00 0c cd cd dc 00 62 ec 9d 80 60 00 c6 aa aa  .......b...`....
0001    03 00 00 0c 88 ef 10 05 00 ff 00 00 00 0e 00 00  ................
0002    00 00 86 dd 60 00 00 00 00 00 88 11 ff fe 80 00  ....`...........
0003    00 00 00 00 02 62 ec ff fe 9d 80 60 ff 02 00 00  .....b.....`....
0004    00 00 00 00 00 00 00 00 00 00 01 50 13 48 13 48  ...........P.H.H
0005    00 88 86 00 20 02 00 ff 00 01 00 80 00 00 00 00  .... ...........
0006    00 01 00 22 50 49 44 3a 49 53 52 34 33 32 31 2f  ..."PID:ISR4321/
0007    4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41 30 4d  K9 SN:FDO2018A0M
0008    38 00 00 02 00 15 30 30 36 32 2e 65 63 39 64 2e  8.....0062.ec9d.
0009    38 30 36 30 2d 31 00 00 03 00 0c 45 52 4e 57 2e  8060-1.....ERNW.
0010    64 65 00 00 07 00 14 fe 80 00 00 00 00 00 00 02  de..............
0011    62 ec ff fe 9d 80 60 00 08 00 09 41 4e 49 31 00  b.....`....ANI1.
0012    00 05 00 14 fd b6 67 6a 9a 78 00 00 00 62 ec 9d  ......gj.x...b..
0013    80 60 00 01
```

Customized CD Header

ERNW
providing security.

Adjacency Discovery

CD Header Field	Value (hex)
Version	1
Reserved	0
State	05
Factory Default	00 ff
Operation Code	00
Length	0e
Reserved	00 00 00 00
Ethertype	86 dd

```
       00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000   01 00 0c cd cd dc 00 62 ec 9d 80 60 00 c6 aa aa  .......b...`....
0001   03 00 00 0c 88 ef 10 05 00 ff 00 00 00 0e 00 00  ................
0002   00 00 86 dd 60 00 00 00 00 88 11 ff fe 80 00 00  ....`...........
0003   00 00 00 00 02 62 ec ff fe 9d 80 60 ff 02 00 00  .....b.....`....
0004   00 00 00 00 00 00 00 00 00 00 01 50 13 48 13 48  ...........P.H.H
0005   00 88 86 00 20 02 00 ff 00 01 00 80 00 00 00 00  .... ...........
0006   00 01 00 22 50 49 44 3a 49 53 52 34 33 32 31 2f  ..."PID:ISR4321/
0007   4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41 30 4d  K9 SN:FDO2018A0M
0008   38 00 00 02 00 15 30 30 36 32 2e 65 63 39 64 2e  8.....0062.ec9d.
0009   38 30 36 30 2d 31 00 00 03 00 0c 45 52 4e 57 2e  8060-1.....ERNW.
0010   64 65 00 00 07 00 14 fe 80 00 00 00 00 00 00 02  de..............
0011   62 ec ff fe 9d 80 60 00 08 00 09 41 4e 49 31 00  b.....`....ANI1.
0012   00 05 00 14 fd b6 67 6a 9a 78 00 00 00 62 ec 9d  ......gj.x...b..
0013   80 60 00 01
```

Customized CD Header

Adjacency Discovery

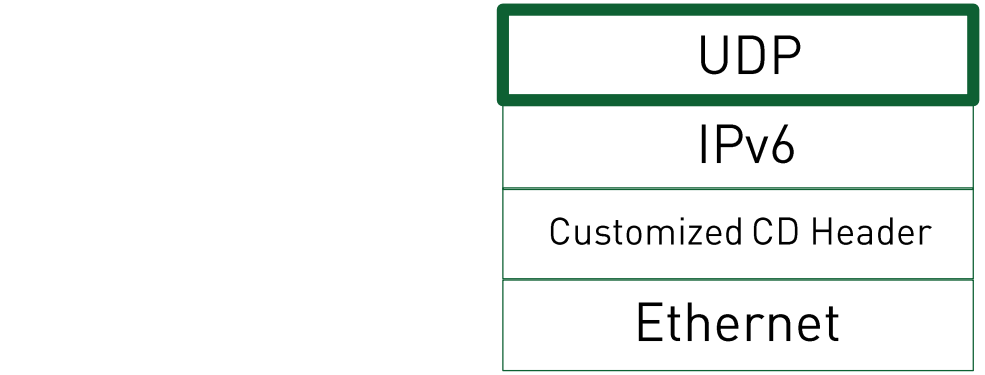

```
       00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000   01 00 0c cd cd dc 00 62 ec 9d 80 60 00 c6 aa aa  .......b...`....
0001   03 00 00 0c 88 ef 10 05 00 ff 00 00 00 0e 00 00  ................
0002   00 00 86 dd 60 00 00 00 00 88 11 ff fe 80 00 00  ....`...........
0003   00 00 00 00 02 62 ec ff fe 9d 80 60 ff 02 00 00  .....b.....`....
0004   00 00 00 00 00 00 00 00 00 00 01 50 13 48 13 48  ...........P.H.H
0005   00 88 86 00 20 02 00 ff 00 01 00 80 00 00 00 00  .... ...........
0006   00 01 00 22 50 49 44 3a 49 53 52 34 33 32 31 2f  ..."PID:ISR4321/
0007   4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41 30 4d  K9 SN:FDO2018A0M
0008   38 00 00 02 00 15 30 30 36 32 2e 65 63 39 64 2e  8.....0062.ec9d.
0009   38 30 36 30 2d 31 00 00 03 00 0c 45 52 4e 57 2e  8060-1.....ERNW.
0010   64 65 00 00 07 00 14 fe 80 00 00 00 00 00 00 02  de..............
0011   62 ec ff fe 9d 80 60 00 08 00 09 41 4e 49 31 00  b.....`....ANI1.
0012   00 05 00 14 fd b6 67 6a 9a 78 00 00 00 62 ec 9d  ......gj.x...b..
0013   80 60 00 01
```

IPv6 Header

ERNW
providing security.

Adjacency Discovery

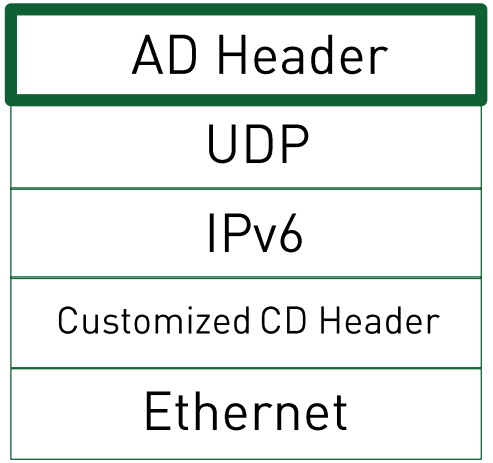



```
      00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000  01 00 0c cd cd dc 00 62 ec 9d 80 60 00 c6 aa aa  .......b...`....
0001  03 00 00 0c 88 ef 10 05 00 ff 00 00 00 0e 00 00  ................
0002  00 00 86 dd 60 00 00 00 00 88 11 ff fe 80 00 00  ....`...........
0003  00 00 00 00 02 62 ec ff fe 9d 80 60 ff 02 00 00  .....b.....`....
0004  00 00 00 00 00 00 00 00 00 00 01 50 13 48 13 48  ...........P.H.H
0005  00 88 86 00 20 02 00 ff 00 01 00 80 00 00 00 00  .... ...........
0006  00 01 00 22 50 49 44 3a 49 53 52 34 33 32 31 2f  ..."PID:ISR4321/
0007  4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41 30 4d  K9 SN:FDO2018A0M
0008  38 00 00 02 00 15 30 30 36 32 2e 65 63 39 64 2e  8.....0062.ec9d.
0009  38 30 36 30 2d 31 00 00 03 00 0c 45 52 4e 57 2e  8060-1.....ERNW.
0010  64 65 00 00 07 00 14 fe 80 00 00 00 00 00 00 02  de..............
0011  62 ec ff fe 9d 80 60 00 08 00 09 41 4e 49 31 00  b.....`....ANI1.
0012  00 05 00 14 fd b6 67 6a 9a 78 00 00 00 62 ec 9d  ......gj.x...b..
0013  80 60 00 01
```

UDP Header

ERNW
providing security.



Adjacency Discovery

Octet	0								1								2								3							
Bits	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	Version				Reserved				State								Factory Default															
64	Operation Code																Length															
96	Reserved																															
128	TLV (Options)																															

AN Adjacency Discovery Header

ERNW
providing security.

Adjacency Discovery

AD Header
UDP
IPv6
Customized CD Header
Ethernet

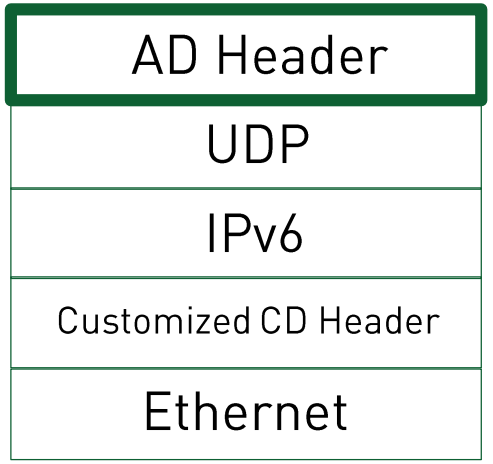
```
       00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000   01 00 0c cd cd dc 00 62 ec 9d 80 60 00 c6 aa aa  .......b...`....
0001   03 00 00 0c 88 ef 10 05 00 ff 00 00 00 0e 00 00  ................
0002   00 00 86 dd 60 00 00 00 00 88 11 ff fe 80 00 00  ....`...........
0003   00 00 00 00 02 62 ec ff fe 9d 80 60 ff 02 00 00  .....b.....`....
0004   00 00 00 00 00 00 00 00 00 00 01 50 13 48 13 48  ...........P.H.H
0005   00 88 86 00 20 02 00 ff 00 01 00 80 00 00 00 00  .... ...........
0006   00 01 00 22 50 49 44 3a 49 53 52 34 33 32 31 2f  ..."PID:ISR4321/
0007   4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41 30 4d  K9 SN:FDO2018A0M
0008   38 00 00 02 00 15 30 30 36 32 2e 65 63 39 64 2e  8.....0062.ec9d.
0009   38 30 36 30 2d 31 00 00 03 00 0c 45 52 4e 57 2e  8060-1.....ERNW.
0010   64 65 00 00 07 00 14 fe 80 00 00 00 00 00 00 02  de..............
0011   62 ec ff fe 9d 80 60 00 08 00 09 41 4e 49 31 00  b.....`....ANI1.
0012   00 05 00 14 fd b6 67 6a 9a 78 00 00 00 62 ec 9d  ......gj.x...b..
0013   80 60 00 01
```

Version = 2, reserved = 0

State

ERNW
providing security.

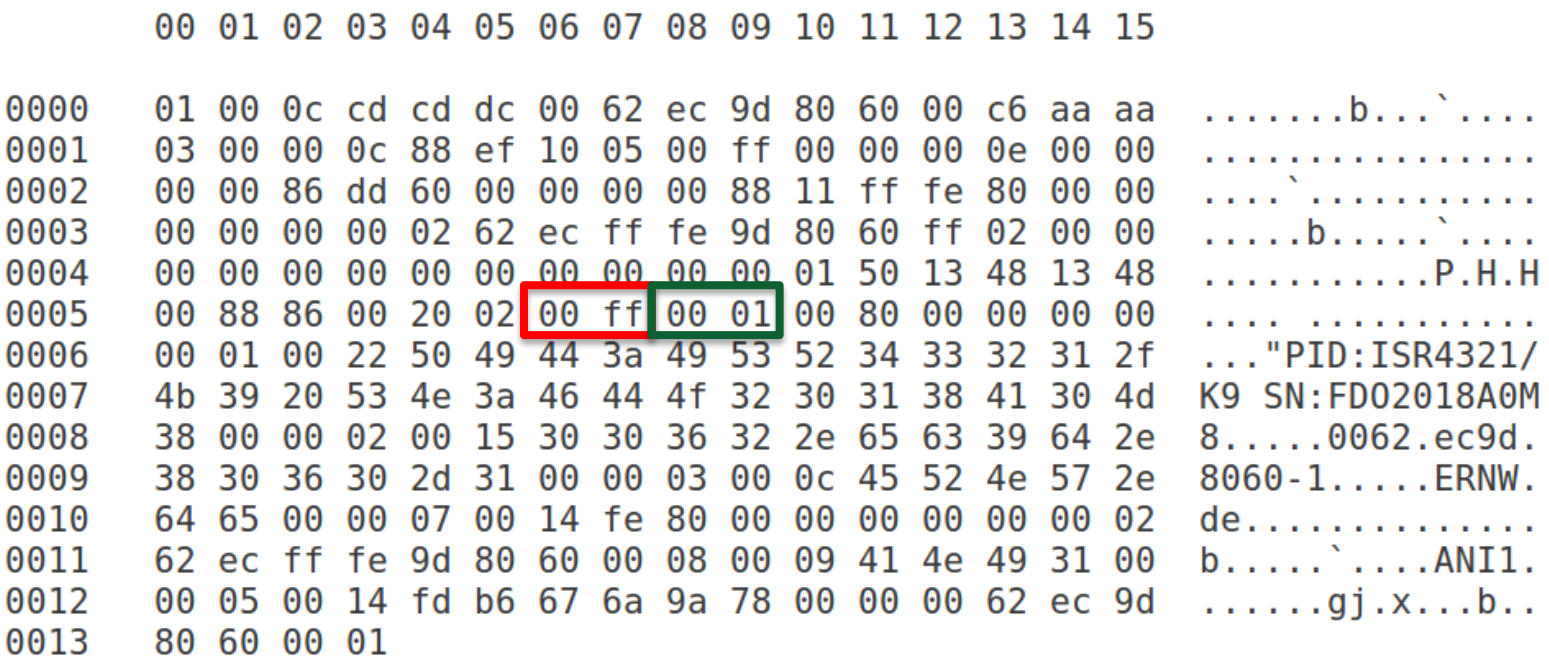


Adjacency Discovery

State Value	Significance
0x02	Multicast, Neighbor Discovery hello packets
0x03	Unicast, Bootstrap phase
0x04	Unicast, negotiating secure channel parameters

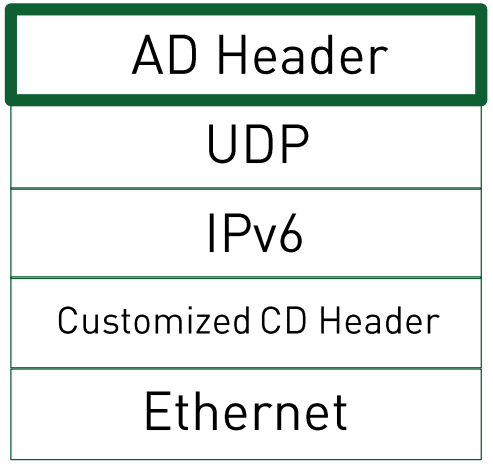
ERNW
providing security.

Adjacency Discovery

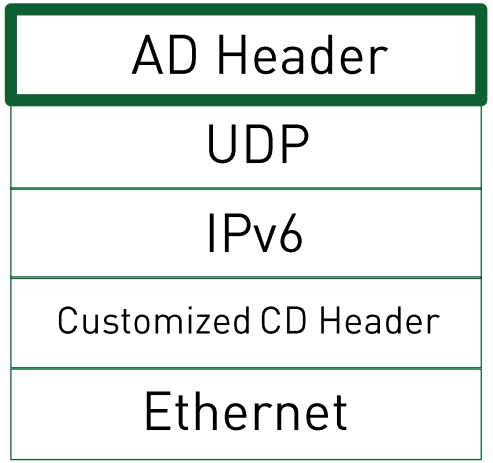


```
       00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000   01 00 0c cd cd dc 00 62 ec 9d 80 60 00 c6 aa aa  .......b...`....
0001   03 00 00 0c 88 ef 10 05 00 ff 00 00 00 0e 00 00  ................
0002   00 00 86 dd 60 00 00 00 00 88 11 ff fe 80 00 00  ....`...........
0003   00 00 00 00 02 62 ec ff fe 9d 80 60 ff 02 00 00  .....b.....`....
0004   00 00 00 00 00 00 00 00 00 00 01 50 13 48 13 48  ...........P.H.H
0005   00 88 86 00 20 02 00 ff 00 01 00 80 00 00 00 00  .... ...........
0006   00 01 00 22 50 49 44 3a 49 53 52 34 33 32 31 2f  ..."PID:ISR4321/
0007   4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41 30 4d  K9 SN:FDO2018A0M
0008   38 00 00 02 00 15 30 30 36 32 2e 65 63 39 64 2e  8.....0062.ec9d.
0009   38 30 36 30 2d 31 00 00 03 00 0c 45 52 4e 57 2e  8060-1.....ERNW.
0010   64 65 00 00 07 00 14 fe 80 00 00 00 00 00 00 02  de..............
0011   62 ec ff fe 9d 80 60 00 08 00 09 41 4e 49 31 00  b.....`....ANI1.
0012   00 05 00 14 fd b6 67 6a 9a 78 00 00 00 62 ec 9d  ......gj.x...b..
0013   80 60 00 01
```

ERNW
providing security.

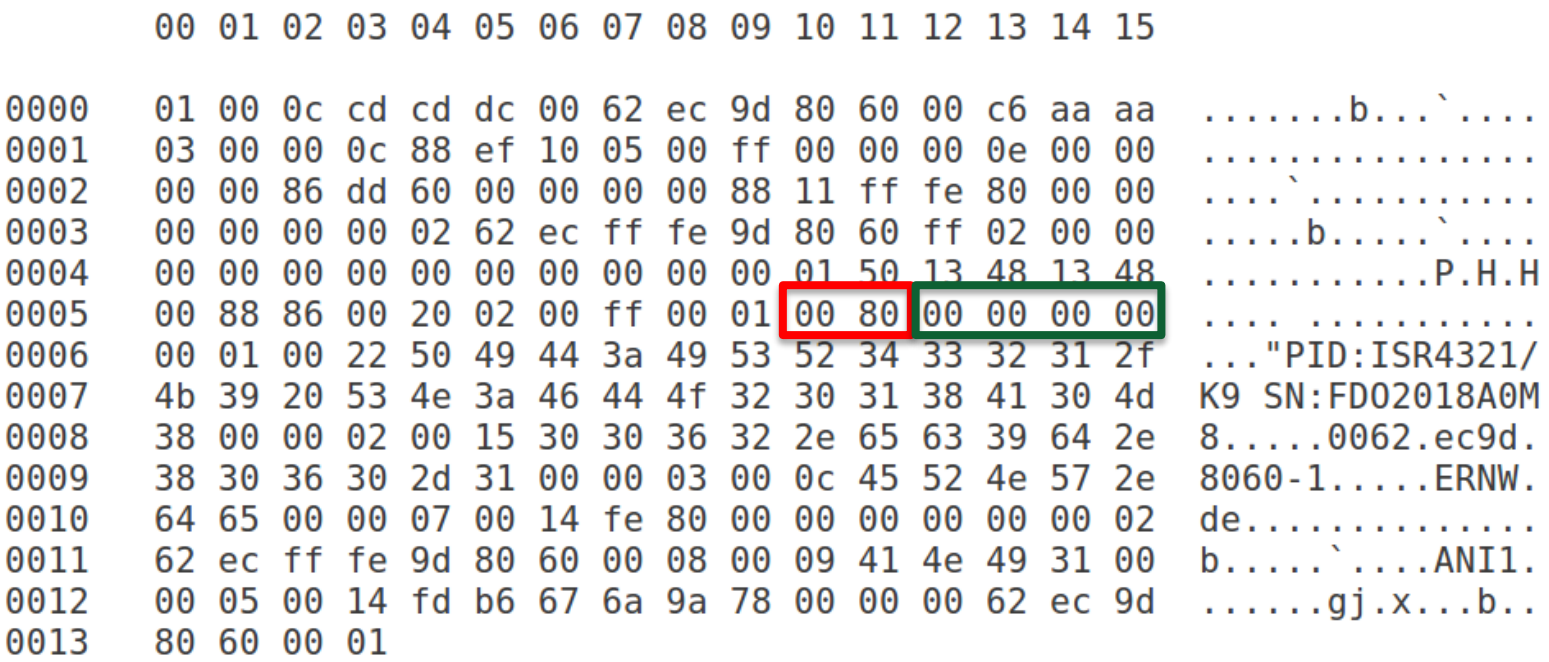


Adjacency Discovery

Opcode Value	Significance
0x0001	Neighbor Discovery Domain packets
0x0003	Whitelist acceptance/rejection for the requesting nodes
0x0004	Device Domain Certificate
0x0005	Bootstrap invite by the registrar
0x0007	Bootstrap reply by the enrollee
0x0008	Device Domain Certificate (rarely used)
0x0019	Negotiating available security parameters for the secure channel
0x001a	Acknowledgment on the agreed security parameters
0x001c	Failed to build the secure channel

ERNW
providing security.

Adjacency Discovery



```
      00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000  01 00 0c cd cd dc 00 62 ec 9d 80 60 00 c6 aa aa  .......b...`....
0001  03 00 00 0c 88 ef 10 05 00 ff 00 00 00 0e 00 00  ................
0002  00 00 86 dd 60 00 00 00 00 88 11 ff fe 80 00 00  ....`...........
0003  00 00 00 00 02 62 ec ff fe 9d 80 60 ff 02 00 00  .....b.....`....
0004  00 00 00 00 00 00 00 00 00 00 01 50 13 48 13 48  ...........P.H.H
0005  00 88 86 00 20 02 00 ff 00 01 00 80 00 00 00 00  .... ...........
0006  00 01 00 22 50 49 44 3a 49 53 52 34 33 32 31 2f  ..."PID:ISR4321/
0007  4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41 30 4d  K9 SN:FDO2018A0M
0008  38 00 00 02 00 15 30 30 36 32 2e 65 63 39 64 2e  8.....0062.ec9d.
0009  38 30 36 30 2d 31 00 00 03 00 0c 45 52 4e 57 2e  8060-1.....ERNW.
0010  64 65 00 00 07 00 14 fe 80 00 00 00 00 00 00 02  de..............
0011  62 ec ff fe 9d 80 60 00 08 00 09 41 4e 49 31 00  b.....`....ANI1.
0012  00 05 00 14 fd b6 67 6a 9a 78 00 00 00 62 ec 9d  ......gj.x...b..
0013  80 60 00 01
```

ERNW
providing security.

Adjacency Discovery

AD Header
UDP
IPv6
Customized CD Header
Ethernet

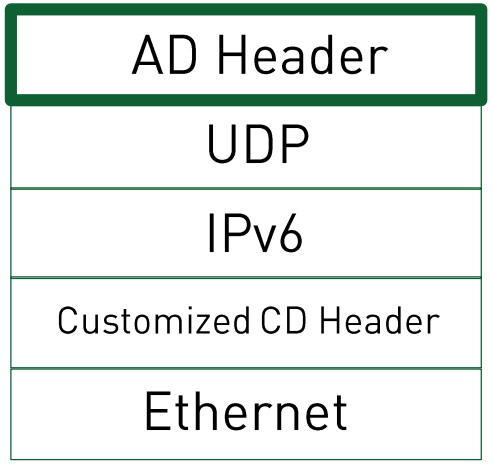
```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000    01 00 0c cd cd dc 00 62 ec 9d 80 60 00 c6 aa aa  .......b...`....
0001    03 00 00 0c 88 ef 10 05 00 ff 00 00 00 0e 00 00  ................
0002    00 00 86 dd 60 00 00 00 00 88 11 ff fe 80 00 00  ....`...........
0003    00 00 00 00 02 62 ec ff fe 9d 80 60 ff 02 00 00  .....b.....`....
0004    00 00 00 00 00 00 00 00 00 00 01 50 13 48 13 48  ...........P.H.H
0005    00 88 86 00 20 02 00 ff 00 01 00 80 00 00 00 00  .... ...........
0006    00 01 00 22 50 49 44 3a 49 53 52 34 33 32 31 2f  ..."PID:ISR4321/
0007    4b 39 20 53 4e 3a 46 44 4f 32 30 31 38 41 30 4d  K9 SN:FDO2018A0M
0008    38 00 00 02 00 15 30 30 36 32 2e 65 63 39 64 2e  8.....0062.ec9d.
0009    38 30 36 30 2d 31 00 00 03 00 0c 45 52 4e 57 2e  8060-1.....ERNW.
0010    64 65 00 00 07 00 14 fe 80 00 00 00 00 00 00 02  de..............
0011    62 ec ff fe 9d 80 60 00 08 00 09 41 4e 49 31 00  b.....`....ANI1.
0012    00 05 00 14 fd b6 67 6a 9a 78 00 00 00 62 ec 9d  ......gj.x...b..
0013    80 60 00 01
```

Type

Length

ERNW
providing security.



Adjacency Discovery

Operation Codes	Available field types	Fields Significance
0x0001	0x0001	Source UDI
	0x0002	Source Device Domain ID
	0x0003	Domain Name
⋮	⋮	⋮
0x0019	0x0001	Security Channel Protection Mode, either DIKE or IPSEC
0x001a	0x0001	Acknowledgment on the agreed Security Mode
0x001c	0x0001	Failed to build the Secure Channel

ERNW
providing security.

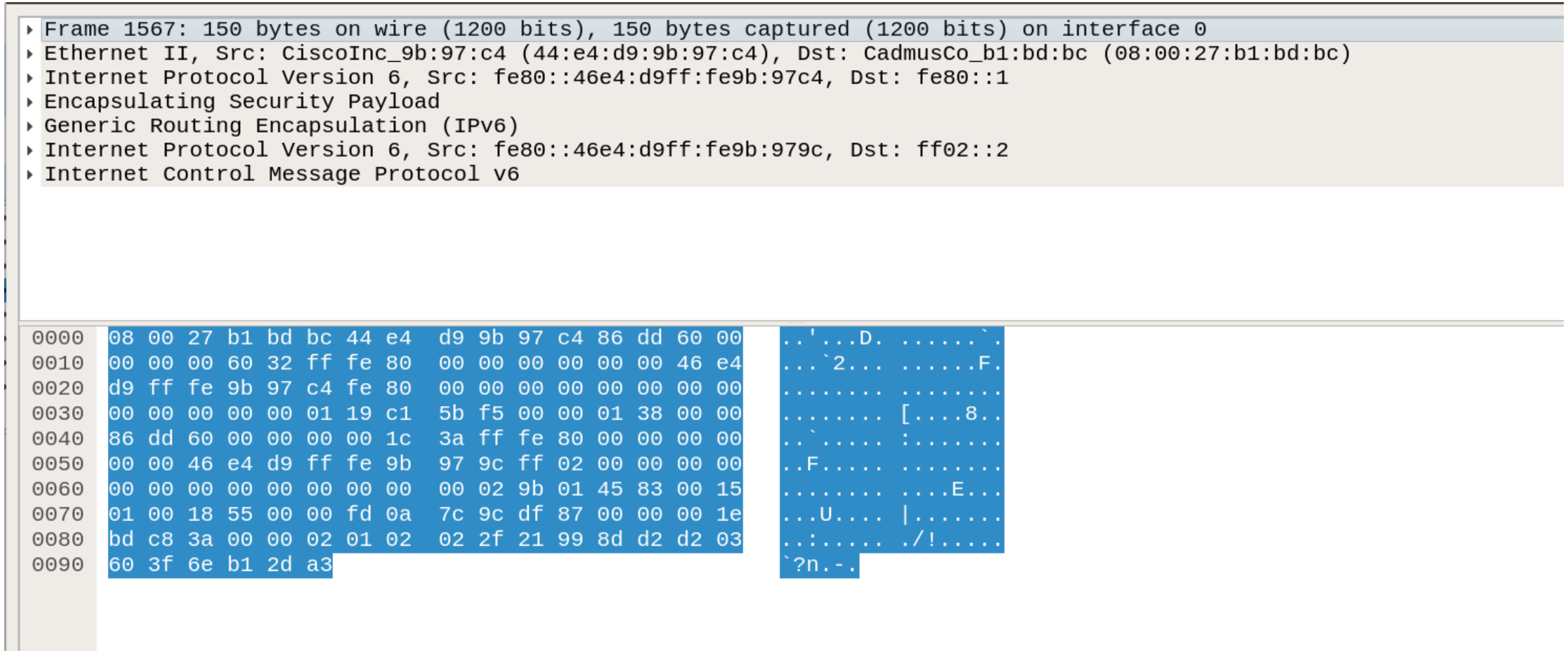
Secure Channel
UDP
IPv6
Customized CD Header
Ethernet

Secure Channel

- Supports AN since 2014
- DIKE only supported on newer operating Systems
- IPSec NULL ☺

ME 3600X-24CX-M

ERNW
providing security.



Is it Secure?

ERNW
providing security.

Live Chat

Support

ERNW
providing security.

Live Chat


Support

Me:
Hi, I connected 2 nodes from 2 different domains and they built the secure channel!

ERNW
providing security.

Live Chat


Support

Me:
Hi, I connected 2 nodes from 2 different domains and they built the secure channel!

Support:
….

ERNW
providing security.

Live Chat


Support

Me:
Hi, I connected 2 nodes from 2 different domains and they built the secure channel!

Support:
Thanks for reporting, we created BugID CSCvd15717. We will check with the BU for that

ERNW
providing security.

Live Chat


Support

Me:
Hi, I connected 2 nodes from 2 different domains and they built the secure channel!

Support:
Hi, the BU responded that as both have a certificate signed by same CA, then they can connect.

ERNW
providing security.

Live Chat
 Support
Me: Hi, I connected 2 nodes from 2 different domains and they built the secure channel!
Support: Hi, the BU responded that as both have a certificate signed by same CA, then they can connect.
Me: Wait, what about different domains? Well, this shouldn't be

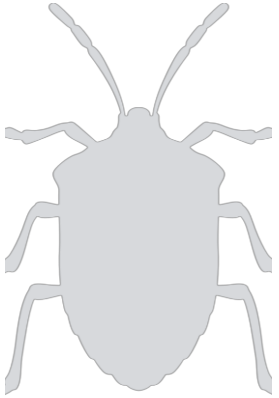
ERNW
providing security.

Live Chat
 Support
Me: Hi, I connected 2 nodes from 2 different domains and they built the secure channel!
Support: Hi, the BU responded that as both have a certificate signed by same CA, then they can connect.
Me: Wait, what about different domains? Well, this shouldn't be
Support: We will add a feature to check domains in the future!

ERNW
providing security.

Bug: CSCvd15717

- Different domains can connect as long as they have certificates from the same CA
- A feature of checking domains will be added in the future
- Whitelist is not checked when the enrollee has a certificate
- No mechanism to stop enrollee with a certificate from joining your domain



ERNW
providing security.

Live Chat


Support

Me:
Hi, I can’t revoke the certificate of one of the accepted nodes.

ERNW
providing security.

Live Chat


Support

Me:
Hi, I can’t revoke the certificate of one of the accepted nodes.

Support:
We will check that. Please note the revoking certificates is not supported on local CA.

ERNW
providing security.

Live Chat


Support

Me:
Hi, I can’t revoke the certificate of one of the accepted nodes.

Support:
We created CVE-2017-6664 for that.

ERNW
providing security.

CVE-2017-6664

- Certification Revocation List is not correctly implemented on IOS XE
- No way to protect against malicious nodes within the network

ERNW
providing security.

Live Chat


Support

Me:
Hi, the attacker can reset remotely the secure channel every time they are created, not only this the information is also in plain text!

ERNW
providing security.

Live Chat
 Support
Me: Hi, the attacker can reset remotely the secure channel every time they are created, not only this the information is also in plain text!
Support: We created CVE-2017-6665 for that.

ERNW
providing security.

CVE-2017-6665

- Replaying the Channel Discovery and Adjacency Discovery packets of any of the accepted nodes reset the Secure channel
- Secure channel is vulnerable to denial-of-service attacks
- Once the secure channel resets, the encrypted information is sent in plain text

ERNW
providing security.

Live Chat


Support

Me:
Hi, if the attacker reset the channel multiple times, eventually the node crashes down!

ERNW
providing security.

Live Chat


Support

Me:
Hi, if the attacker reset the channel multiple times, eventually the node crashes down!

Support:
We created CVE-2017-6663 for that.

ERNW
providing security.

CVE-2017-6663

- Resetting the secure channel multiple times will cause the nodes to crash
- It usually takes about 15 minutes to crash the device

ERNW
providing security.

Live Chat


Support

Me:
Hi, the attacker can crash the registrar by sending invalid enrollee IDs

Support:
We created CVE-2017-3849 for that.

CVE-2017-3849

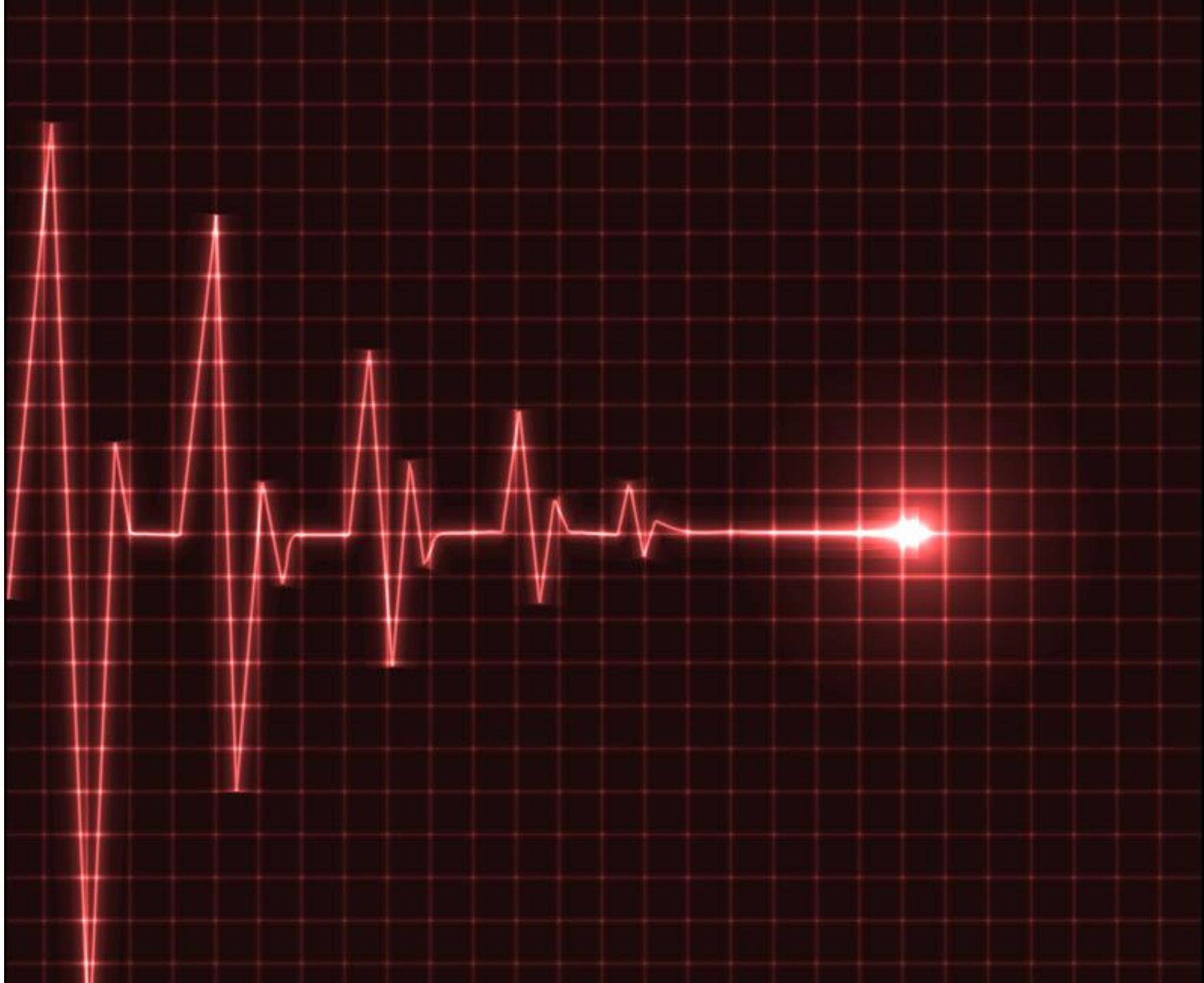
- Sending enrollee UDI as *space byte* or null byte crashes the registrar.

- No workaround for that, please upgrade your systems.

ERNW
providing security.

DeathKiss!

CVE-2017-3850



ERNW
providing security.

CVE-2017-3850

- Regardless Autonomic services are enabled or not, the device is still vulnerable
- Using 1st packet of adjacency discovery, with invalid TLVs crashes the device
- This attack can be launched remotely to crash the devices anywhere
- Block UDP for ports 8888, 4936. If you run AN then upgrade the software

ERNW
providing security.

Conclusion

- Autonomic Systems are smart systems that don't need human intervention to operate.
- Cisco AN protocol with its 3 phases has been reverse-engineered
- Cisco AN is vulnerable to:
  - CVE-2017-3849: crashing registrar with invalid UDIs
  - CVE-2017-3850: crashing IPv6 systems that supports AN
  - CVE-2017-6663: crashing the nodes by resetting secure channel multiple times
  - CVE-2017-6664: CRL on IOS XE not correctly implemented
  - CVE-2017-6665: denial-of-service for secure channel + Information disclosure

ERNW
providing security.

Finally…

- WireEdit 1.10.118 is the first application to support editing and the analyzing of the Cisco Autonomic Network protocol based on our analysis
- I would like to thank Marc Heuse for his contributions with protocol analysis
- 3-part series about Autonomic Network on insinuator.net
  - Introduction
  - Analysis
  - Vulnerabilities

oeissa@ernw.de
www.ernw.de
@Insinuator
www.insinuator.net