black hat® USA 2017

JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS

ERNW
providing security.

Network Automation is not your Safe Haven: Protocol Analysis and Vulnerabilities of Autonomic Network

Omar Eissa

#sh run

- Security Analyst @ ERNW GmbH

- Network security and reverse-engineering

- Bachelor and Masters theses are done on Autonomic systems

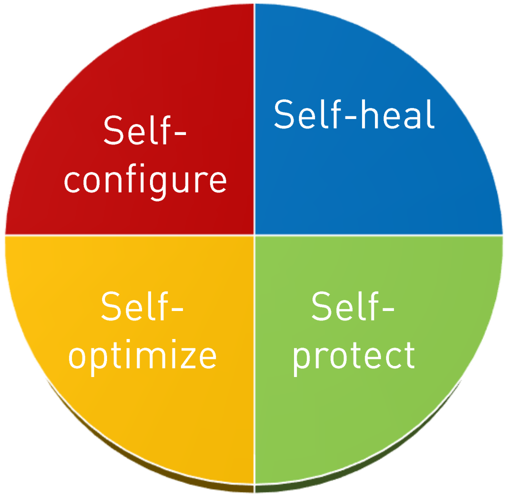
--More--

Agenda

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

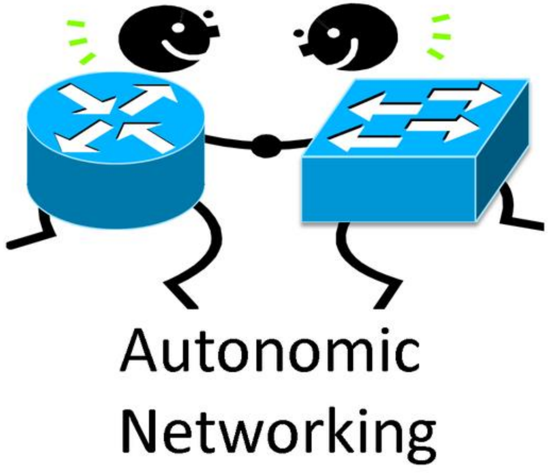
Autonomic Systems

- Smart systems that don’t need human intervention to operate
- They have the ability to “self-manage”



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



Autonomic Network logo as shown by Cisco in their presentations here and here

Live Demo

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

Cisco Deployment

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

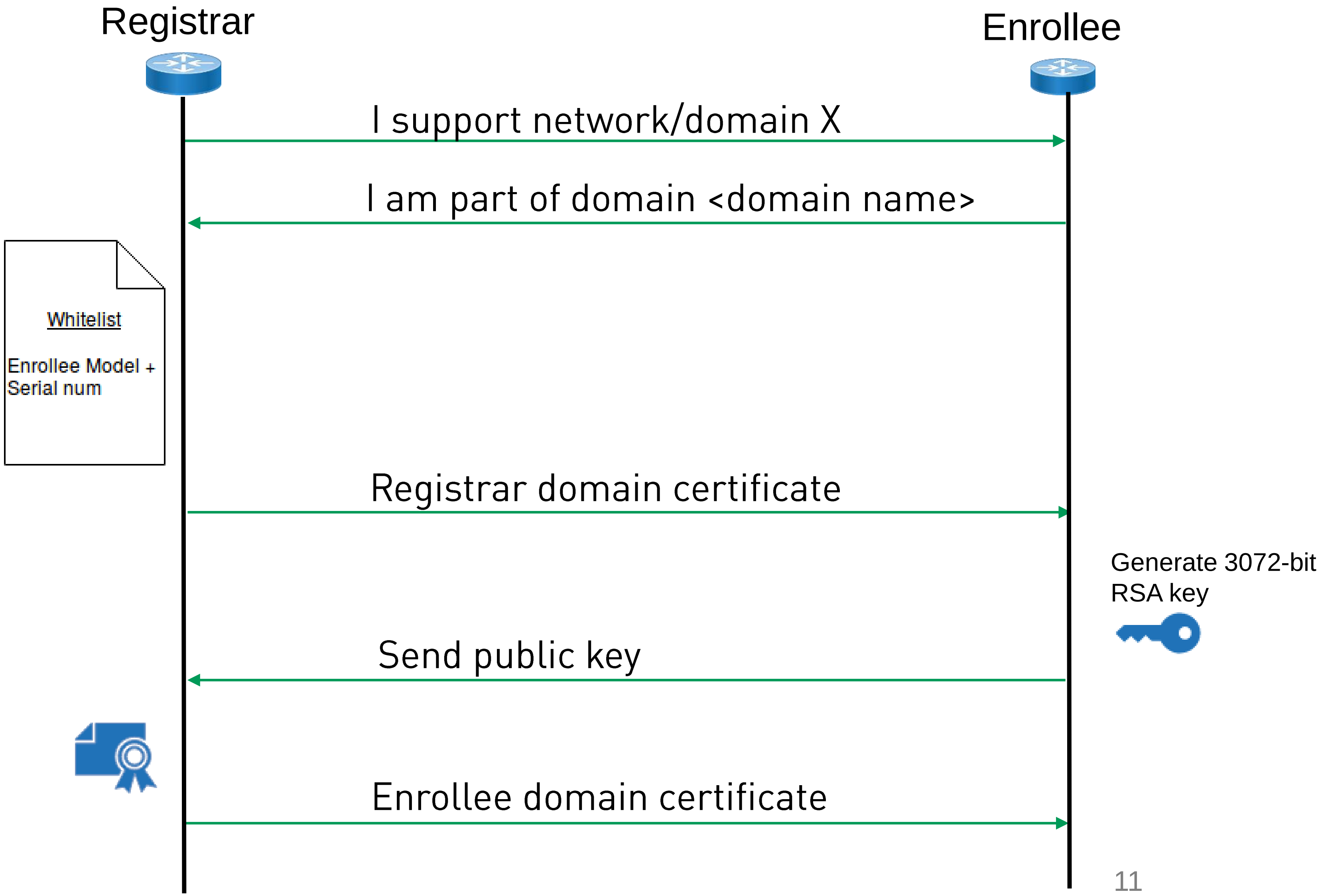
Channel Discovery

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

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

Adjacency Discovery



Registrar

Enrollee

I support network/domain X

I am part of domain <domain name>

Whitelist

Enrollee Model + Serial num

Registrar domain certificate

Generate 3072-bit RSA key

Send public key

Enrollee domain certificate

Secure Channel

- IPSec
  - Port 500
  - Backwards compatibility

- DIKE
  - Data Internet Key Exchange
  - Port 5000
  - Preferred over IPsec

Registrar Configuration

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

Enrollee Needed Configuration

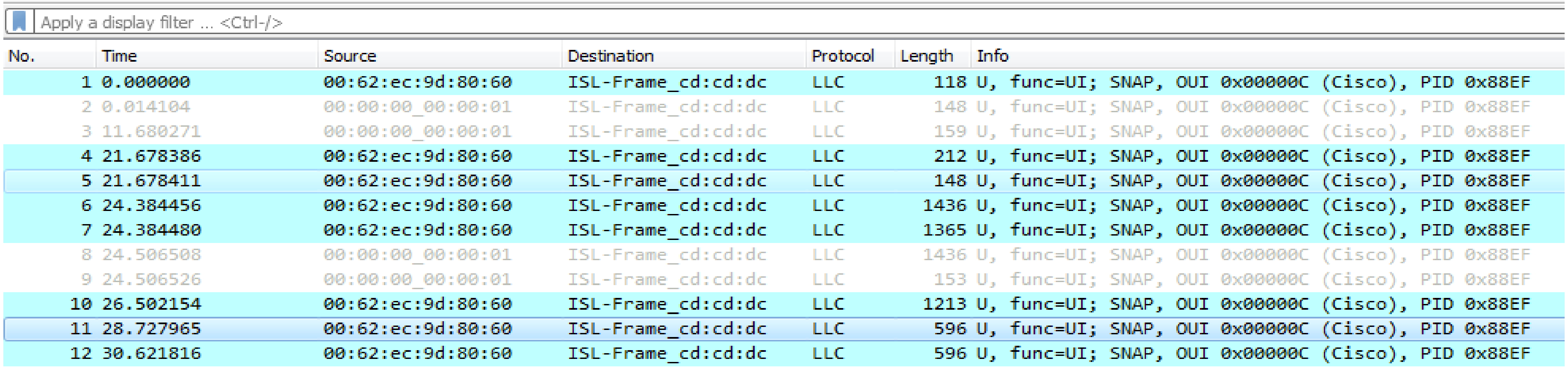
- Brand new (i.e. no configuration file exits)
  - None!
- Configuration file exists
  - `autonomic`

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)

Are you in Control?

Autonomic Network: Under The Hood



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

6 bytes	6 bytes	2 bytes	Till 1500 bytes	
Destination MAC Address	Source MAC Address	EtherType	Payload	FCS

Ethernet II

6 bytes	6 bytes	2 bytes	1 byte	1 byte	1 byte	Till 1500 bytes	
Destination MAC Address	Source MAC Address	Frame Length	DSAP	SSAP	Control	Payload	FCS

802.3
(802.3, 802.2 LLC)

6 bytes	6 bytes	2 bytes	1 byte	1 byte	1 byte	3 bytes	2 bytes	Till 1500 bytes	
Destination MAC Address	Source MAC Address	Frame Length	DSAP	SSAP	Control	OUI	Protocol ID	Payload	FCS

802.3
(802.3, 802.2 SNAP)

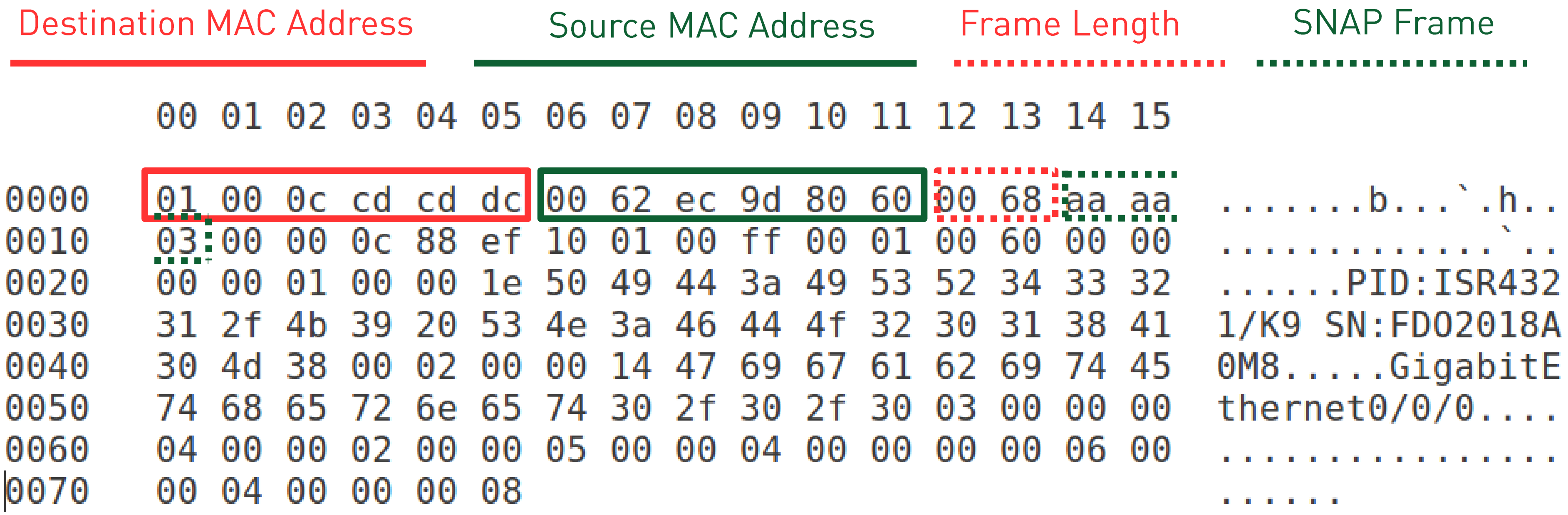
Not Ethernet II

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                                ......
```

Channel Discovery

Ethernet



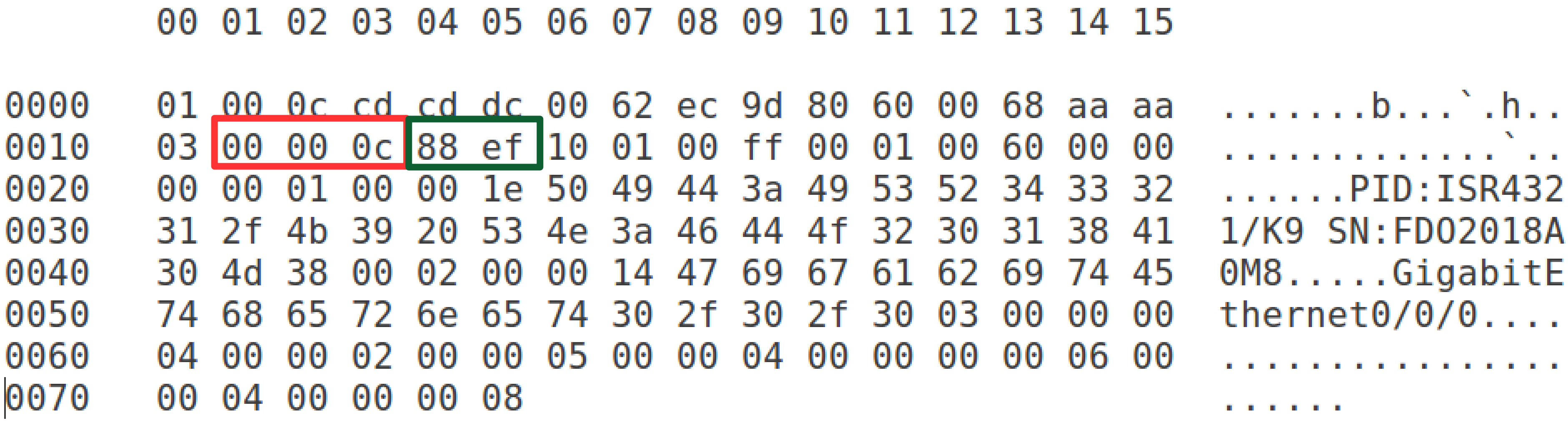
```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

0000    01 00 0c cd cd dc 00 62 ec 9d 80 60 00 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                                 ......
```

Channel Discovery

Ethernet

Organization Unique Identifier

AN Protocol ID

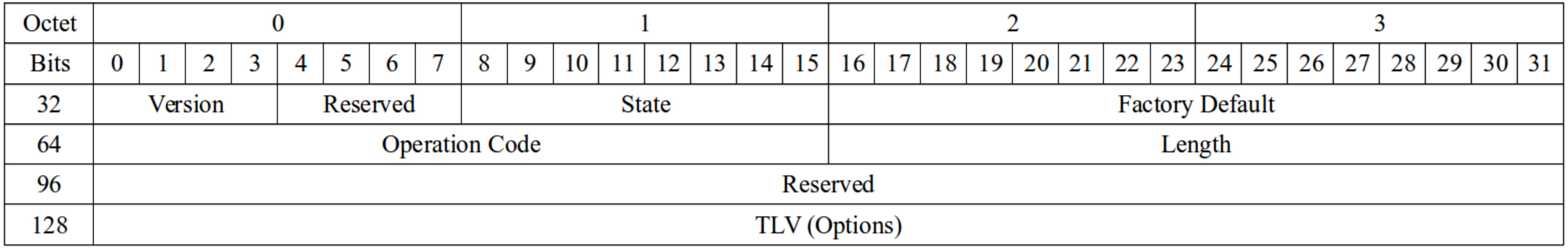


```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

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                                 ......
```

Channel Discovery

Channel Discovery

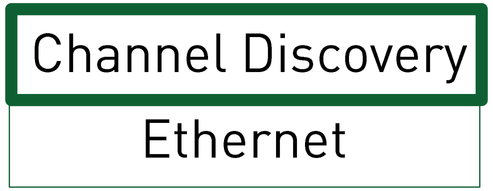
Ethernet



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

Channel Discovery



Version = 1, reserved = 0

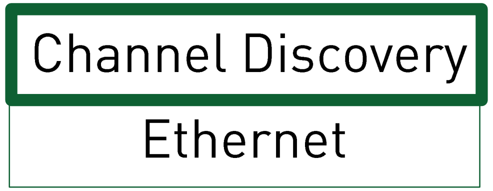
State

Factory Default

Operation Code

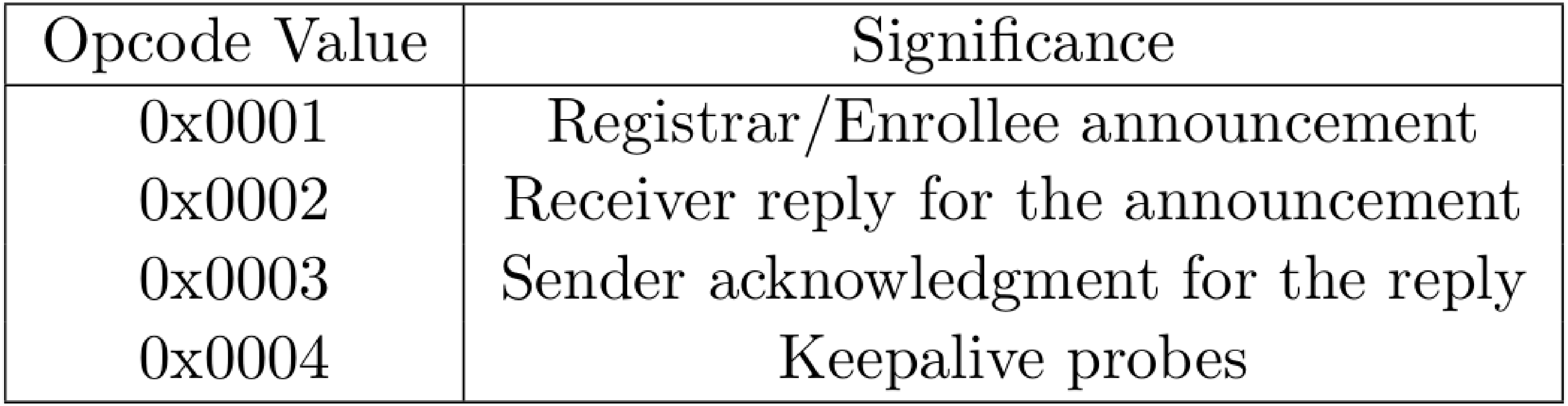
```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

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                                 ......
```

Channel Discovery



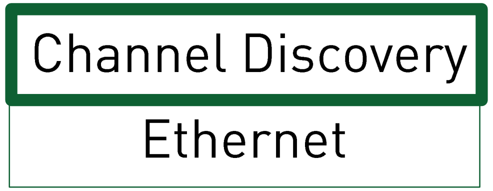
Channel Discovery

Ethernet

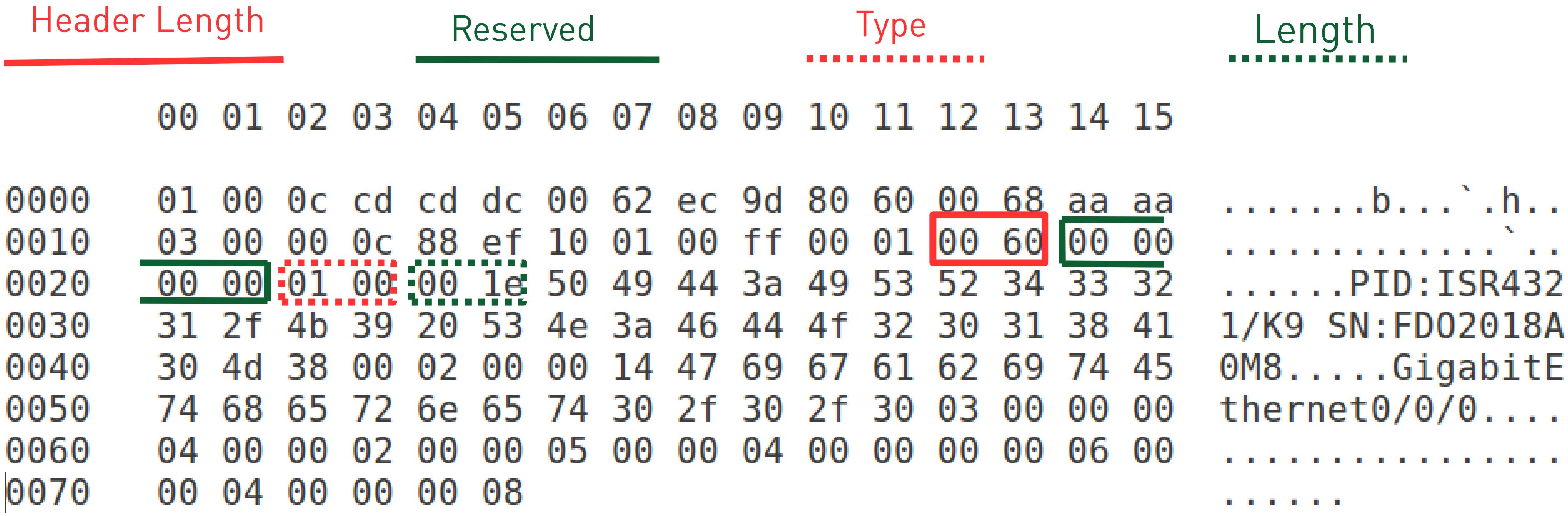


Opcode Value	Significance
0x0001	Registrar/Enrollee announcement
0x0002	Receiver reply for the announcement
0x0003	Sender acknowledgment for the reply
0x0004	Keepalive probes

Channel Discovery

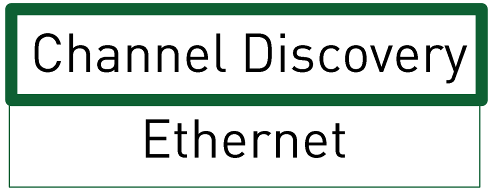

Channel Discovery

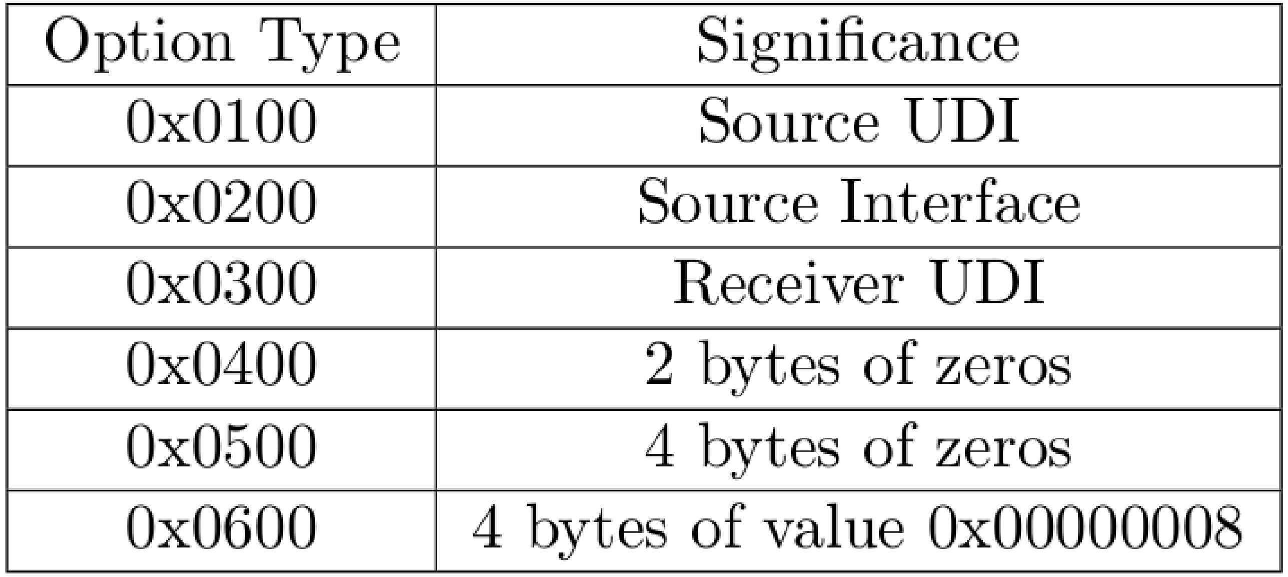
Ethernet



```
        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 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                                 ......
```

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

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
```

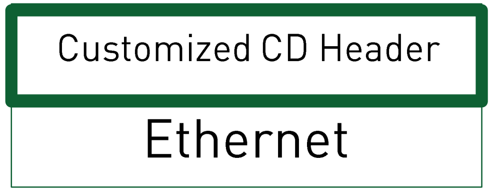
Adjacency Discovery

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

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
```

Customized CD Header

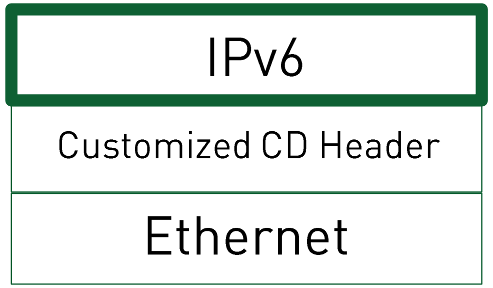
Adjacency Discovery

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


IPv6

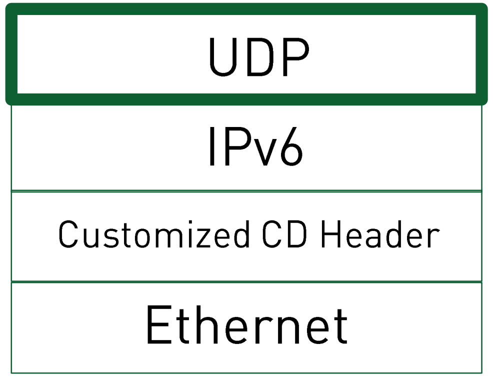
Customized CD Header

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
```

IPv6 Header

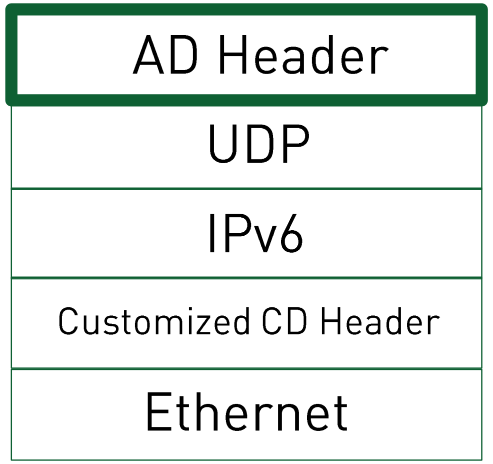
Adjacency Discovery

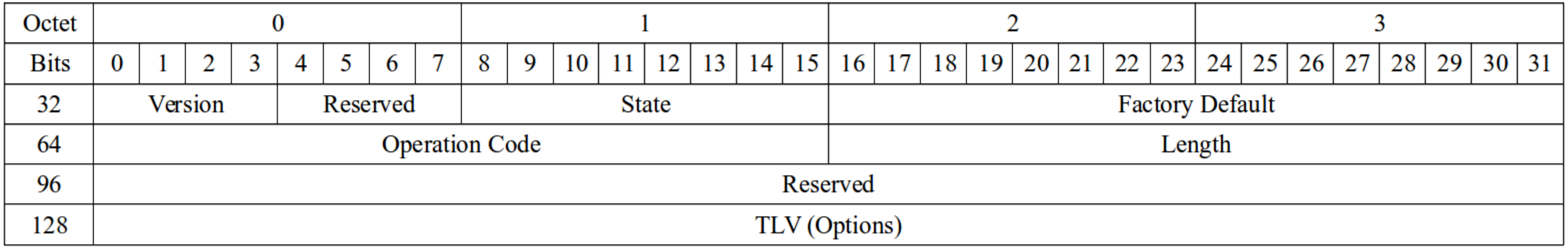


```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

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
```

UDP Header

Adjacency Discovery

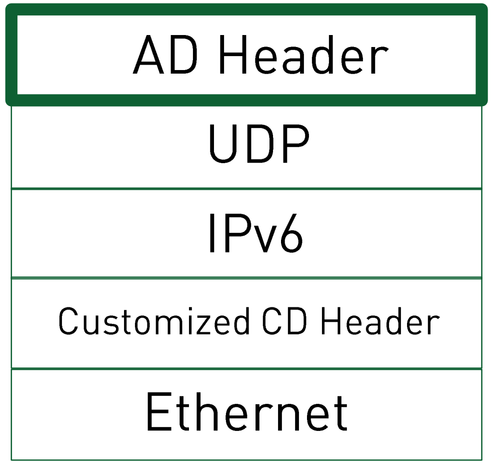




Octet	0								1								2								3							
Bits	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	Version				Reserved				State								Factory Default															
64	Operation Code																Length															
96	Reserved																															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

AN Adjacency Discovery Header

Adjacency Discovery

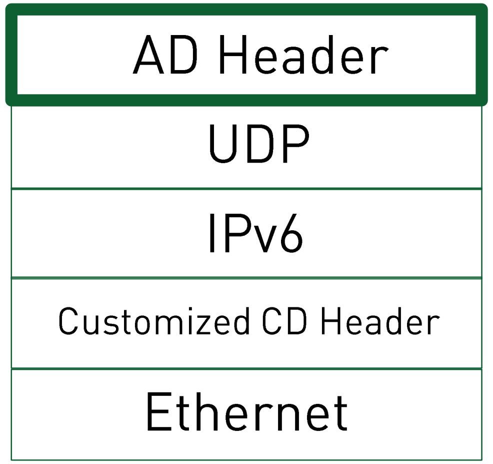


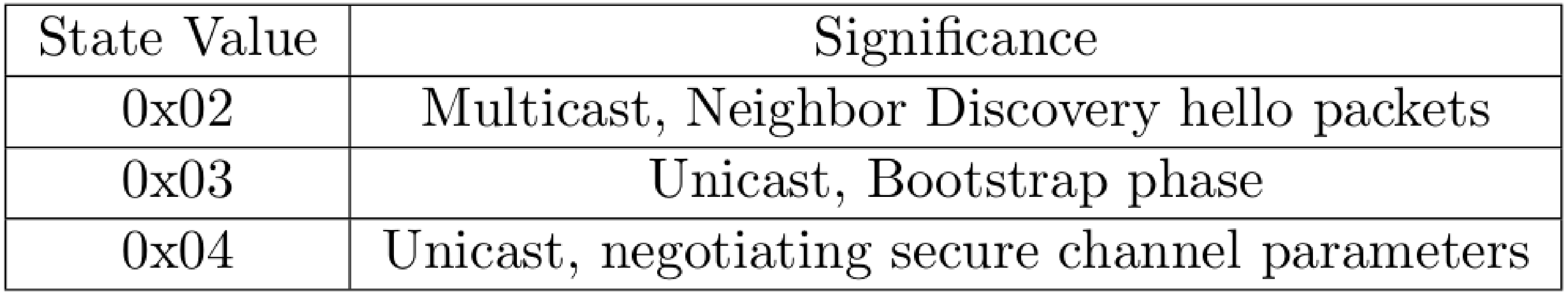
```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

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
```

Version = 2, reserved = 0

State

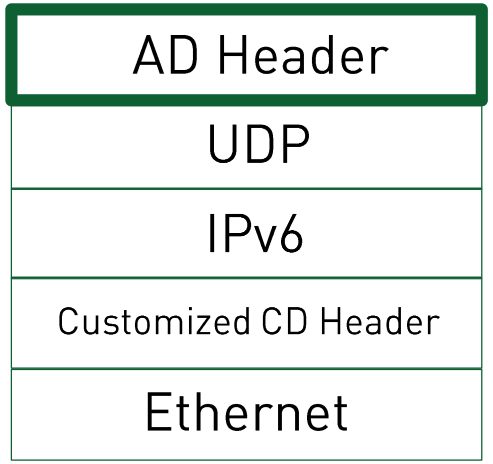
Adjacency Discovery





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

Adjacency Discovery

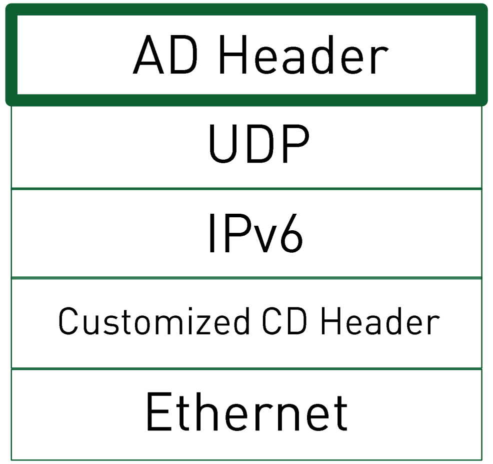


```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

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
```

🟥 Reserved

🟩 Operation Code

Adjacency Discovery

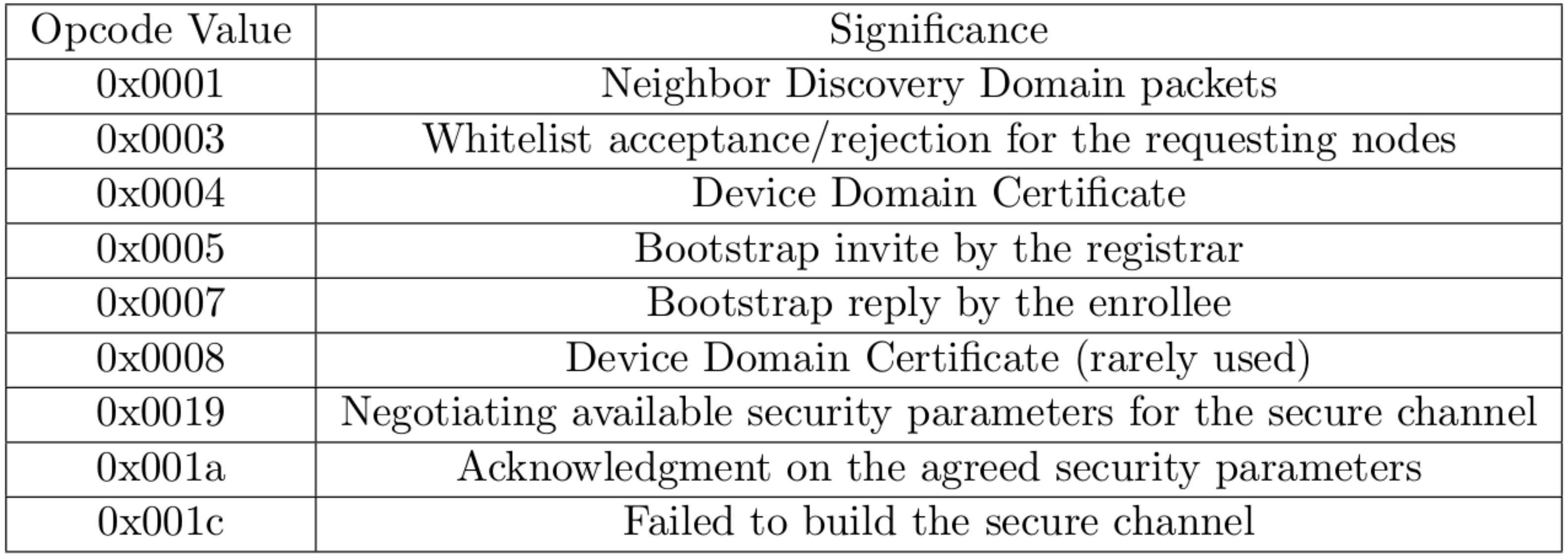

AD Header

UDP

IPv6

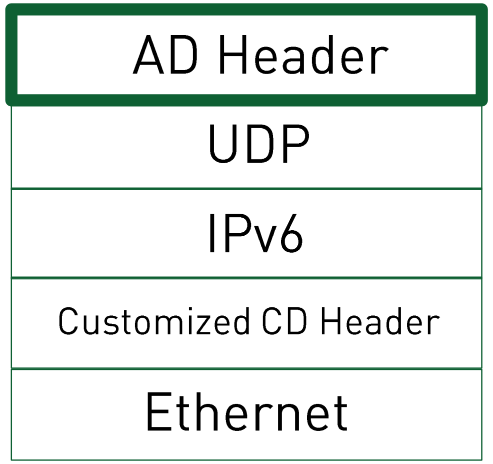
Customized CD Header

Ethernet



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

Adjacency Discovery

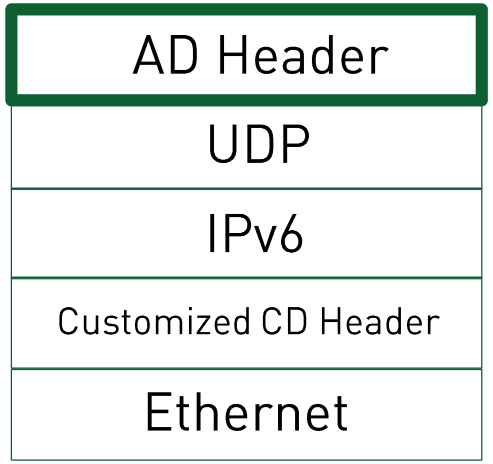


```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

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
```

🟥 Header Length

🟩 Factory Default

Adjacency Discovery

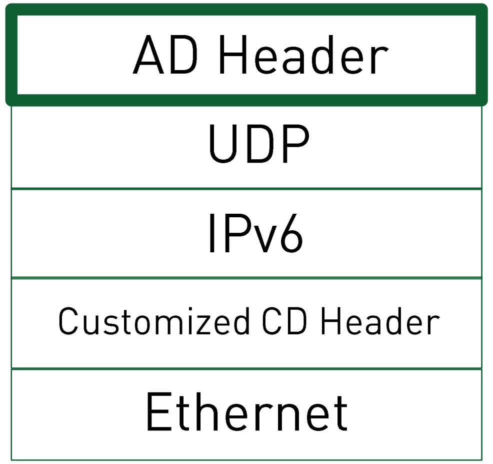


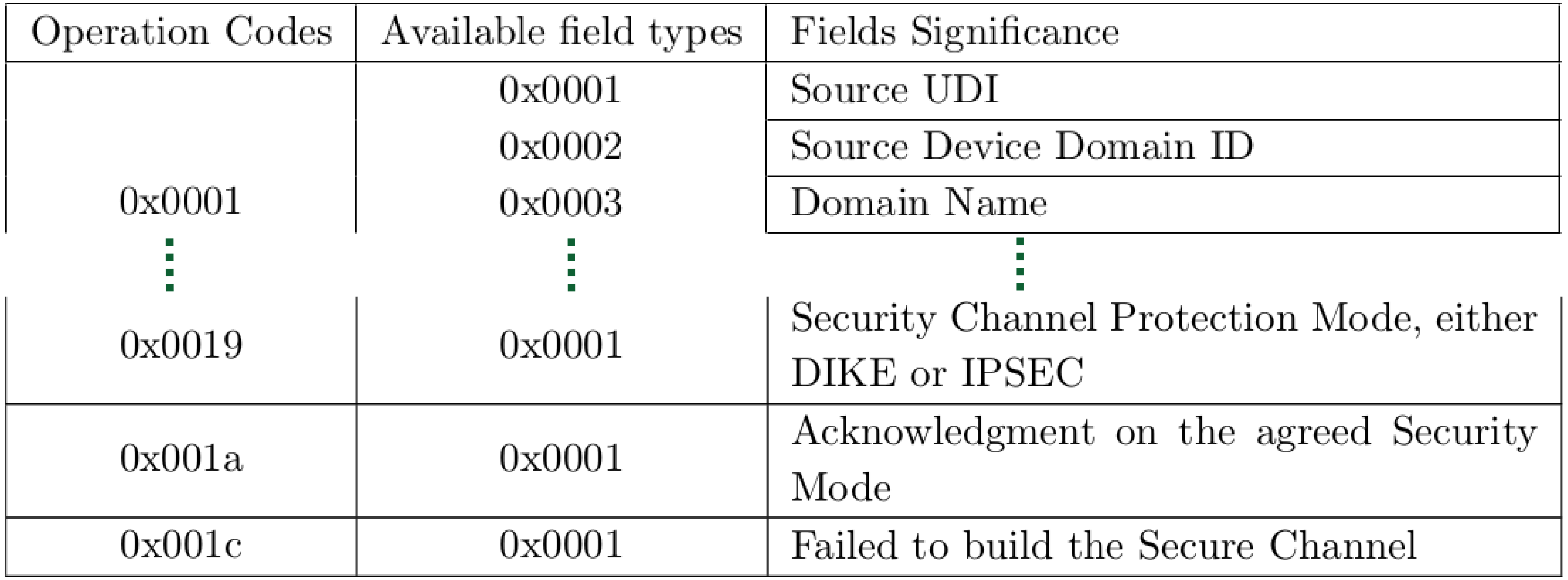
```
        00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

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
```

Type 🟥

Length 🟩

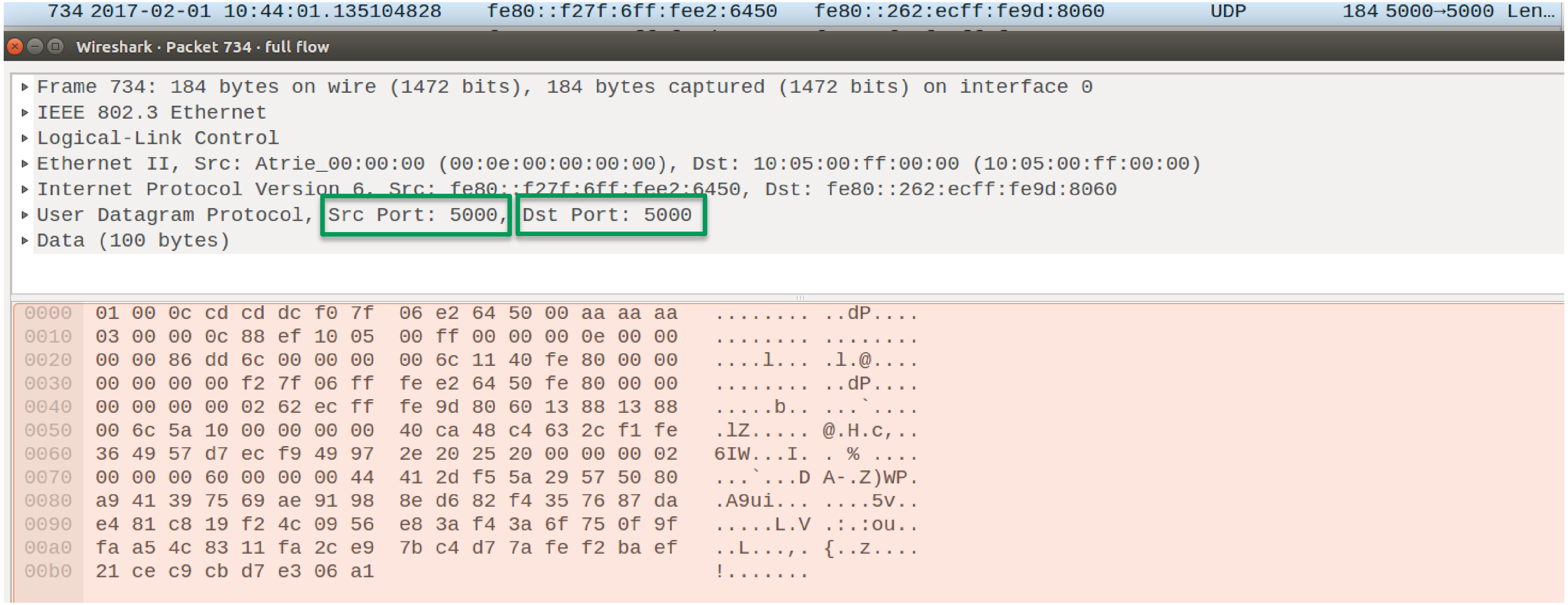
Adjacency Discovery





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

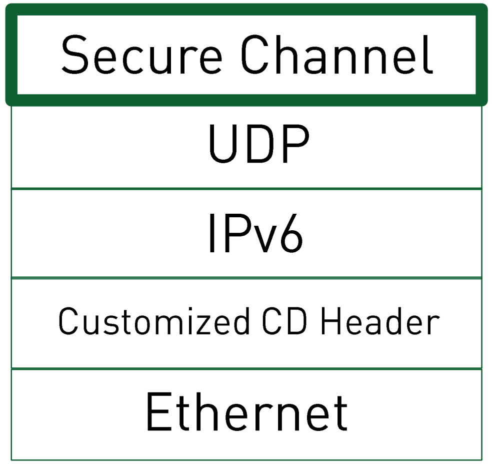
Secure Channel



```
734 2017-02-01 10:44:01.135104828    fe80::f27f:6ff:fee2:6450    fe80::262:ecff:fe9d:8060        UDP        184 5000→5000  Len…
```

```
▸ Frame 734: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits) on interface 0
▸ IEEE 802.3 Ethernet
▸ Logical-Link Control
▸ Ethernet II, Src: Atrie_00:00:00 (00:0e:00:00:00:00), Dst: 10:05:00:ff:00:00 (10:05:00:ff:00:00)
▸ Internet Protocol Version 6, Src: fe80::f27f:6ff:fee2:6450, Dst: fe80::262:ecff:fe9d:8060
▸ User Datagram Protocol, Src Port: 5000, Dst Port: 5000
▸ Data (100 bytes)
```

```
0000  01 00 0c cd cd dc f0 7f  06 e2 64 50 00 aa aa aa   ........ ..dP....
0010  03 00 00 0c 88 ef 10 05  00 ff 00 00 00 0e 00 00   ........ ........
0020  00 00 86 dd 6c 00 00 00  00 6c 11 40 fe 80 00 00   ....l... .l.@....
0030  00 00 00 00 f2 7f 06 ff  fe e2 64 50 fe 80 00 00   ........ ..dP....
0040  00 00 00 00 02 62 ec ff  fe 9d 80 60 13 88 13 88   .....b.. ...`....
0050  00 6c 5a 10 00 00 00 00  40 ca 48 c4 63 2c f1 fe   .lZ..... @.H.c,..
0060  36 49 57 d7 ec f9 49 97  2e 20 25 20 00 00 00 02   6IW...I. . % ....
0070  00 00 00 60 00 00 00 44  41 2d f5 5a 29 57 50 80   ...`...D A-.Z)WP.
0080  a9 41 39 75 69 ae 91 98  8e d6 82 f4 35 76 87 da   .A9ui... ....5v..
0090  e4 81 c8 19 f2 4c 09 56  e8 3a f4 3a 6f 75 0f 9f   .....L.V .:.:ou..
00a0  fa a5 4c 83 11 fa 2c e9  7b c4 d7 7a fe f2 ba ef   ..L...,. {..z....
00b0  21 ce c9 cb d7 e3 06 a1                            !.......
```



Secure Channel

UDP

IPv6

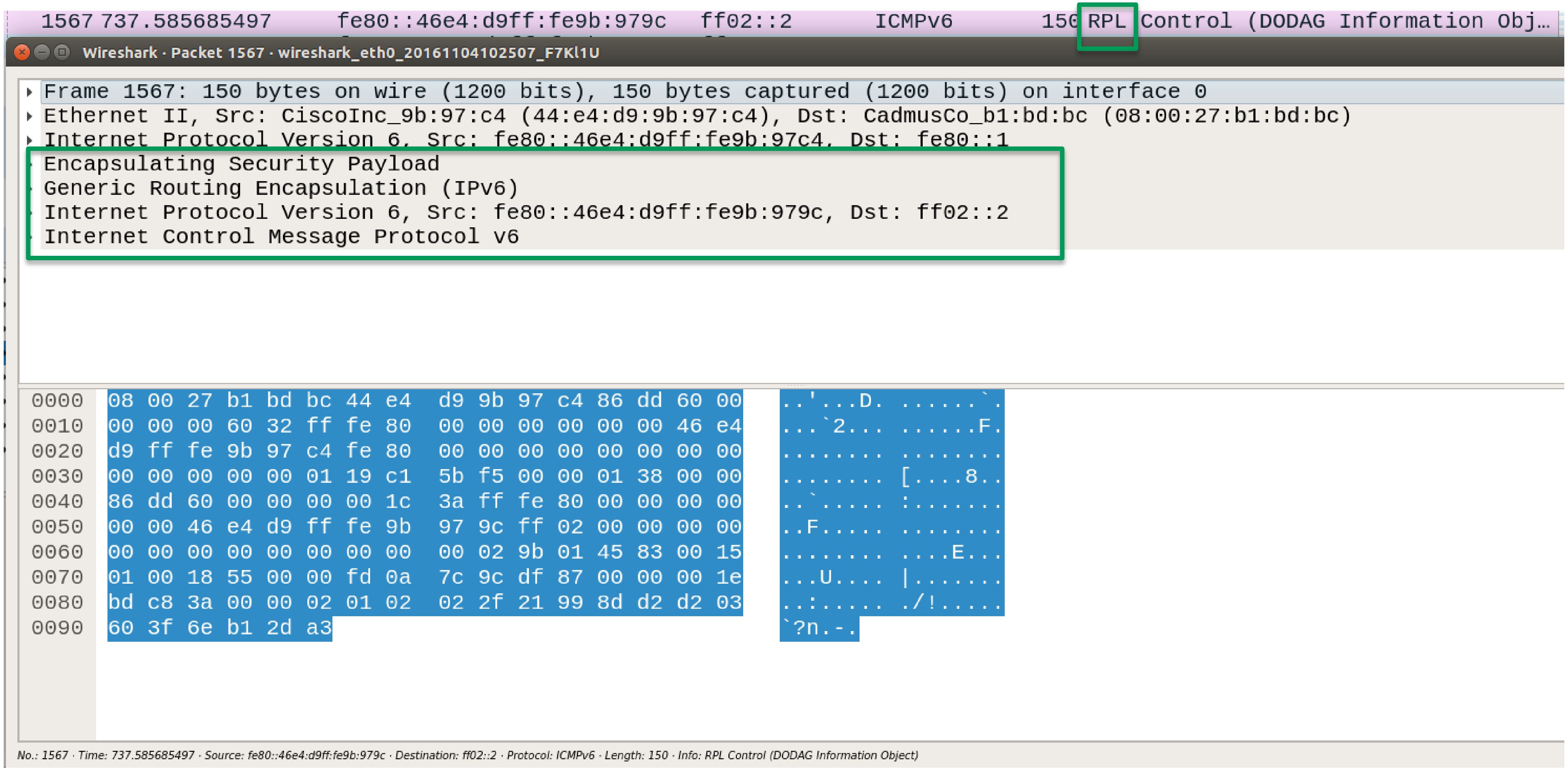
Customized CD Header

Ethernet

Secure Channel

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

ME 3600X-24CX-M



```
1567 737.585685497    fe80::46e4:d9ff:fe9b:979c    ff02::2    ICMPv6    150 RPL Control (DODAG Information Obj…
```

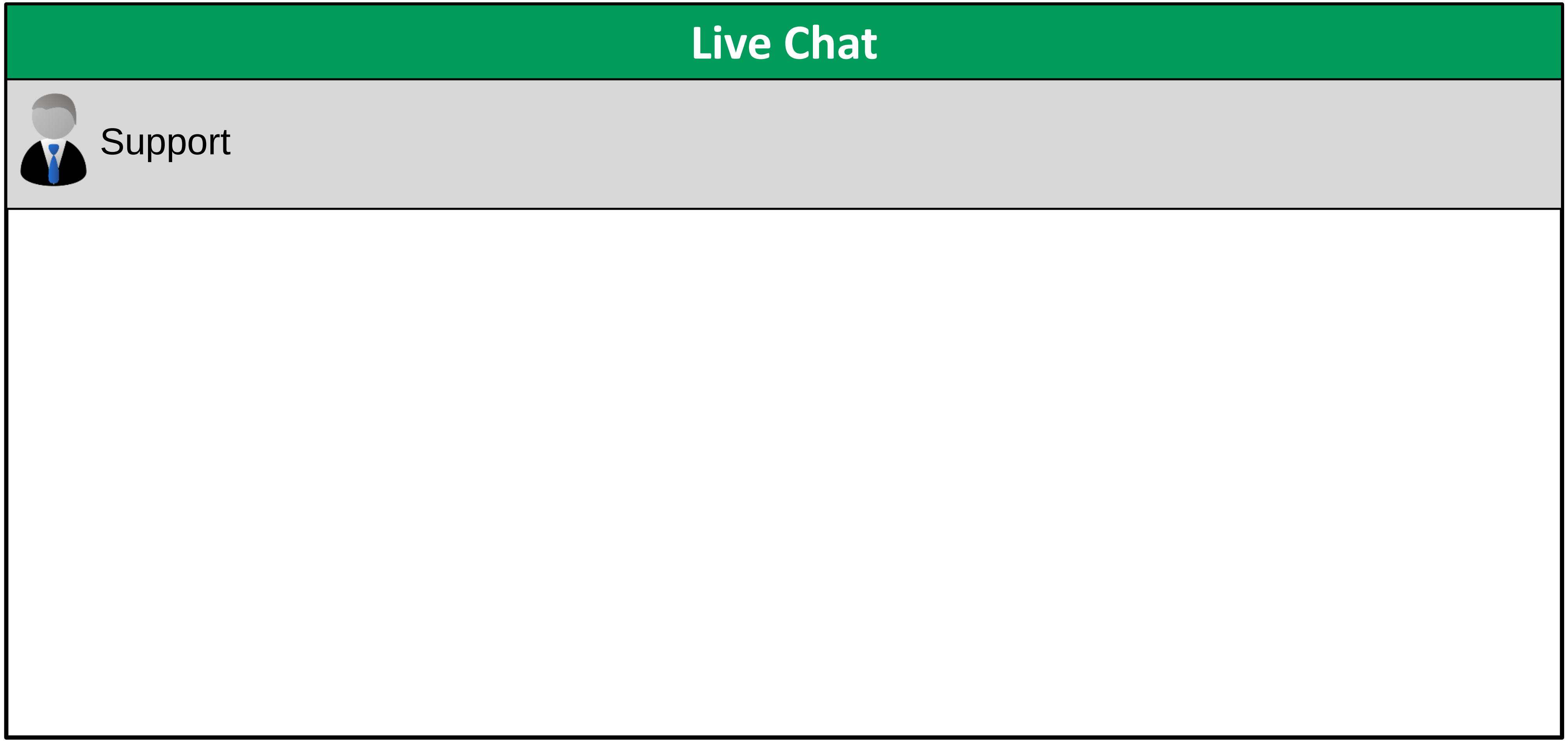
Wireshark · Packet 1567 · wireshark_eth0_20161104102507_F7Kl1U

```
▸ Frame 1567: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
▸ Ethernet II, Src: CiscoInc_9b:97:c4 (44:e4:d9:9b:97:c4), Dst: CadmusCo_b1:bd:bc (08:00:27:b1:bd:bc)
▸ Internet Protocol Version 6, Src: fe80::46e4:d9ff:fe9b:97c4, Dst: fe80::1
▸ Encapsulating Security Payload
▸ Generic Routing Encapsulation (IPv6)
▸ Internet Protocol Version 6, Src: fe80::46e4:d9ff:fe9b:979c, Dst: ff02::2
▸ Internet Control Message Protocol v6
```

```
0000  08 00 27 b1 bd bc 44 e4  d9 9b 97 c4 86 dd 60 00   ..'...D. ......`.
0010  00 00 00 60 32 ff fe 80  00 00 00 00 00 00 46 e4   ...`2... ......F.
0020  d9 ff fe 9b 97 c4 fe 80  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 01 19 c1  5b f5 00 00 01 38 00 00   ........ [....8..
0040  86 dd 60 00 00 00 00 1c  3a ff fe 80 00 00 00 00   ..`..... :.......
0050  00 00 46 e4 d9 ff fe 9b  97 9c ff 02 00 00 00 00   ..F..... ........
0060  00 00 00 00 00 00 00 00  00 02 9b 01 45 83 00 15   ........ ....E...
0070  01 00 18 55 00 00 fd 0a  7c 9c df 87 00 00 00 1e   ...U.... |.......
0080  bd c8 3a 00 00 02 01 02  02 2f 21 99 8d d2 d2 03   ..:..... ./!.....
0090  60 3f 6e b1 2d a3                                  `?n.-.
```

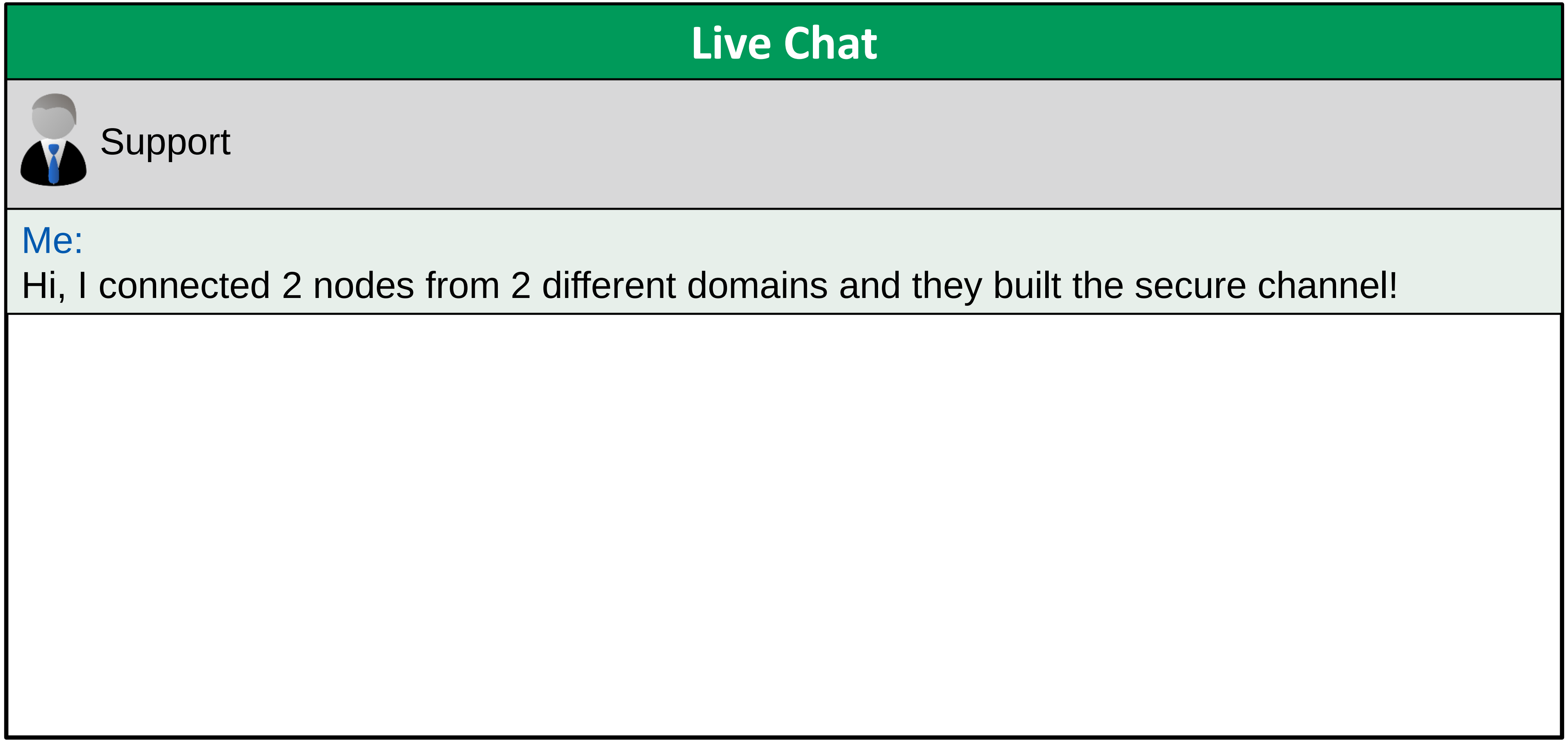
No.: 1567 · Time: 737.585685497 · Source: fe80::46e4:d9ff:fe9b:979c · Destination: ff02::2 · Protocol: ICMPv6 · Length: 150 · Info: RPL Control (DODAG Information Object)

Is it Secure?



Live Chat

Support

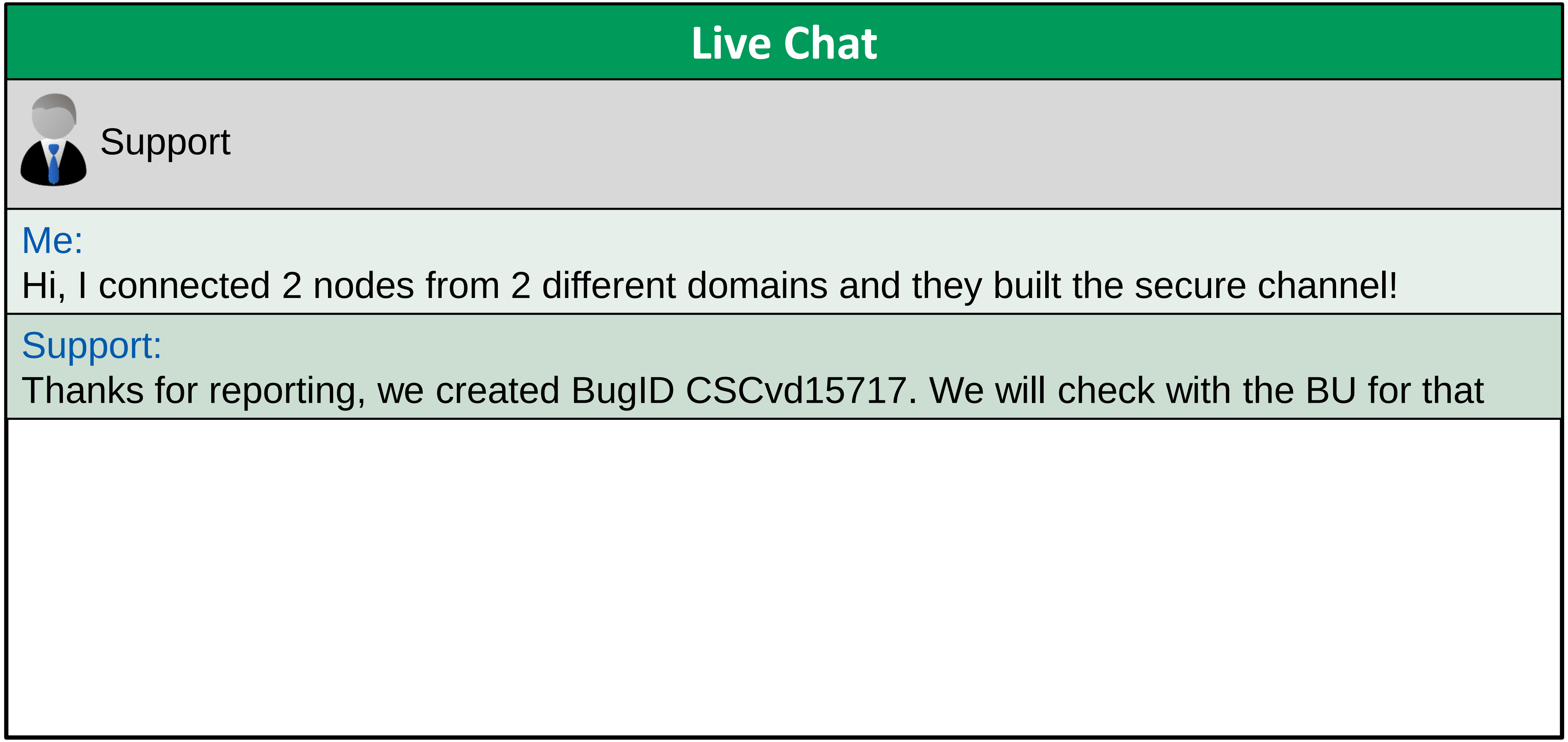


Live Chat

Support

Me:

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

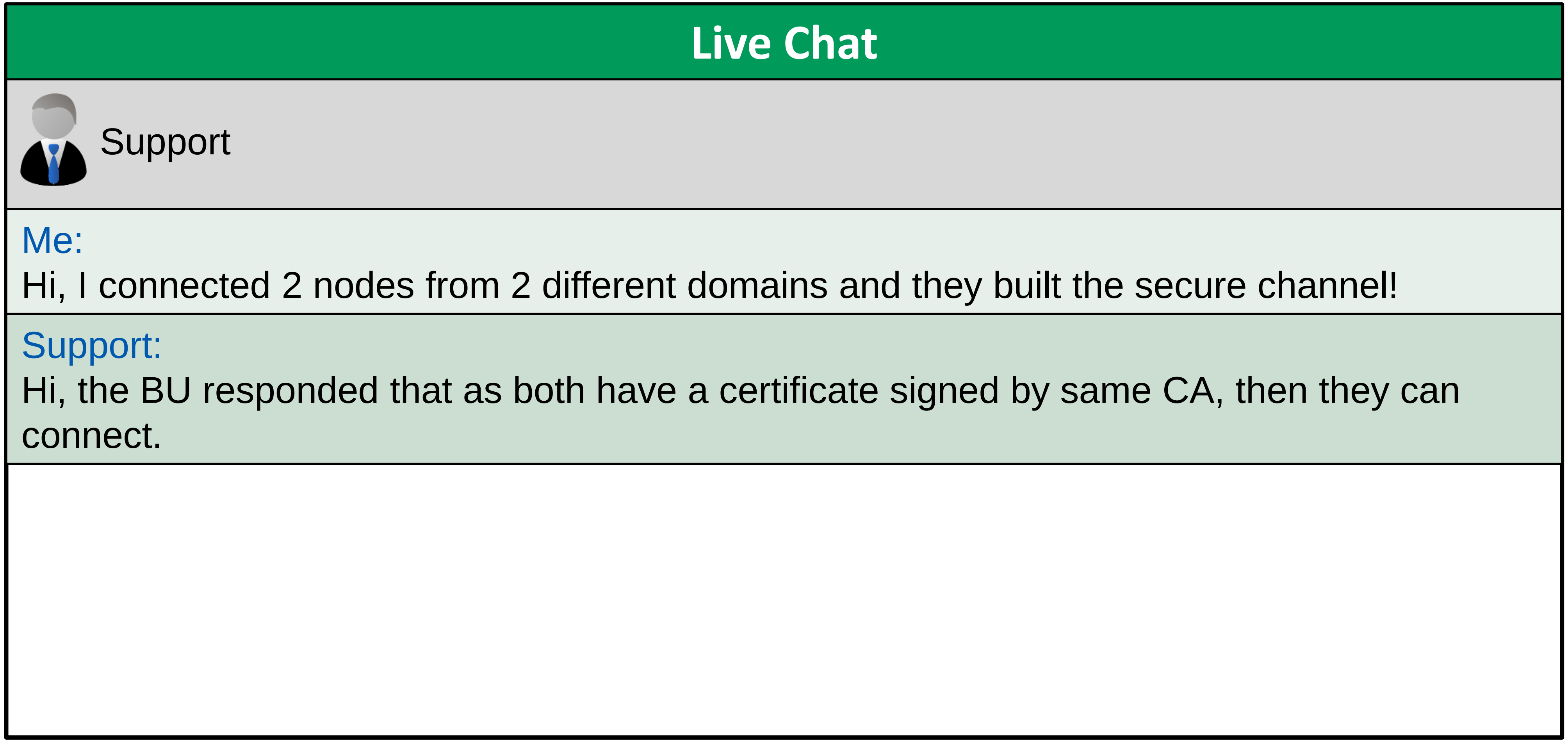


Live Chat

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

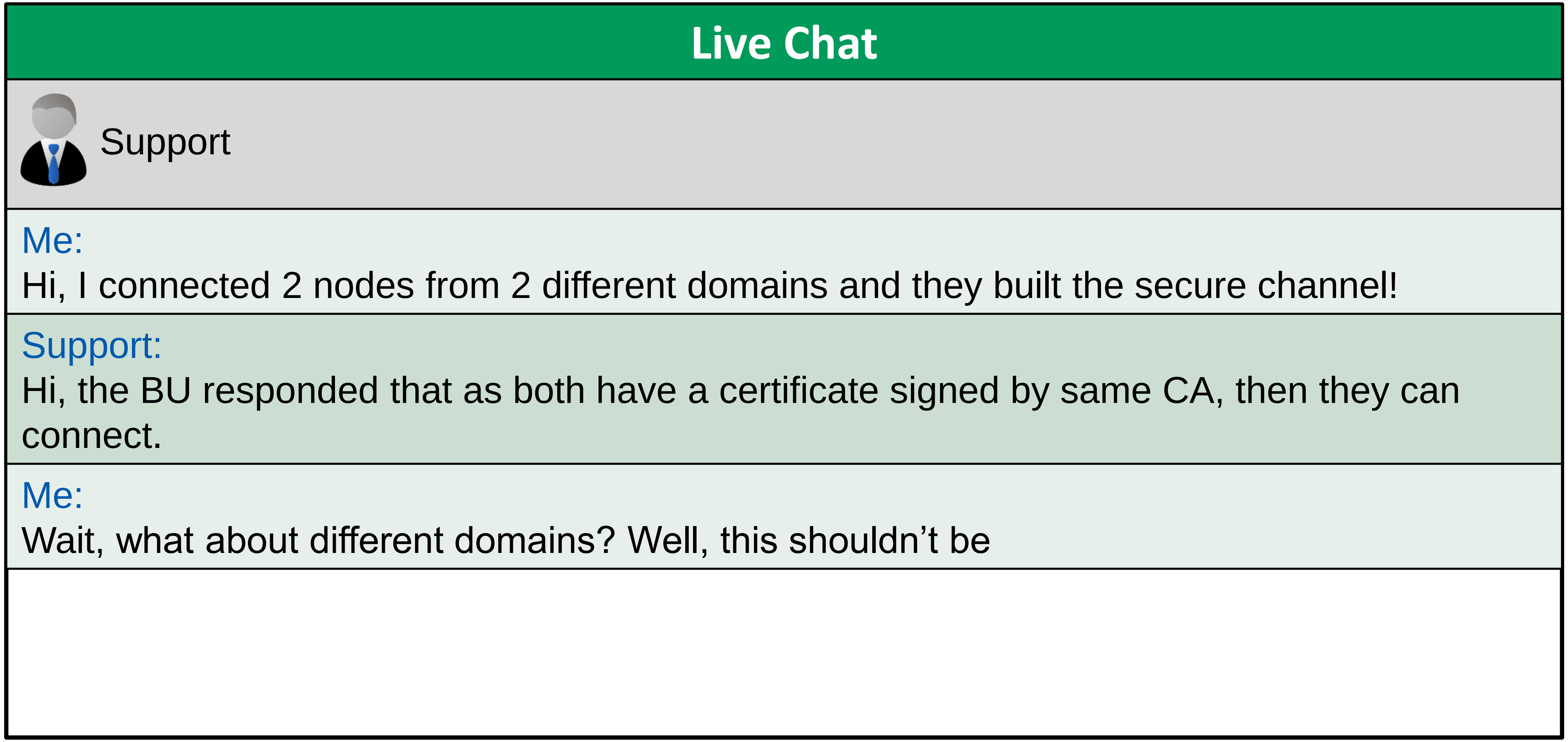


Live Chat

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.



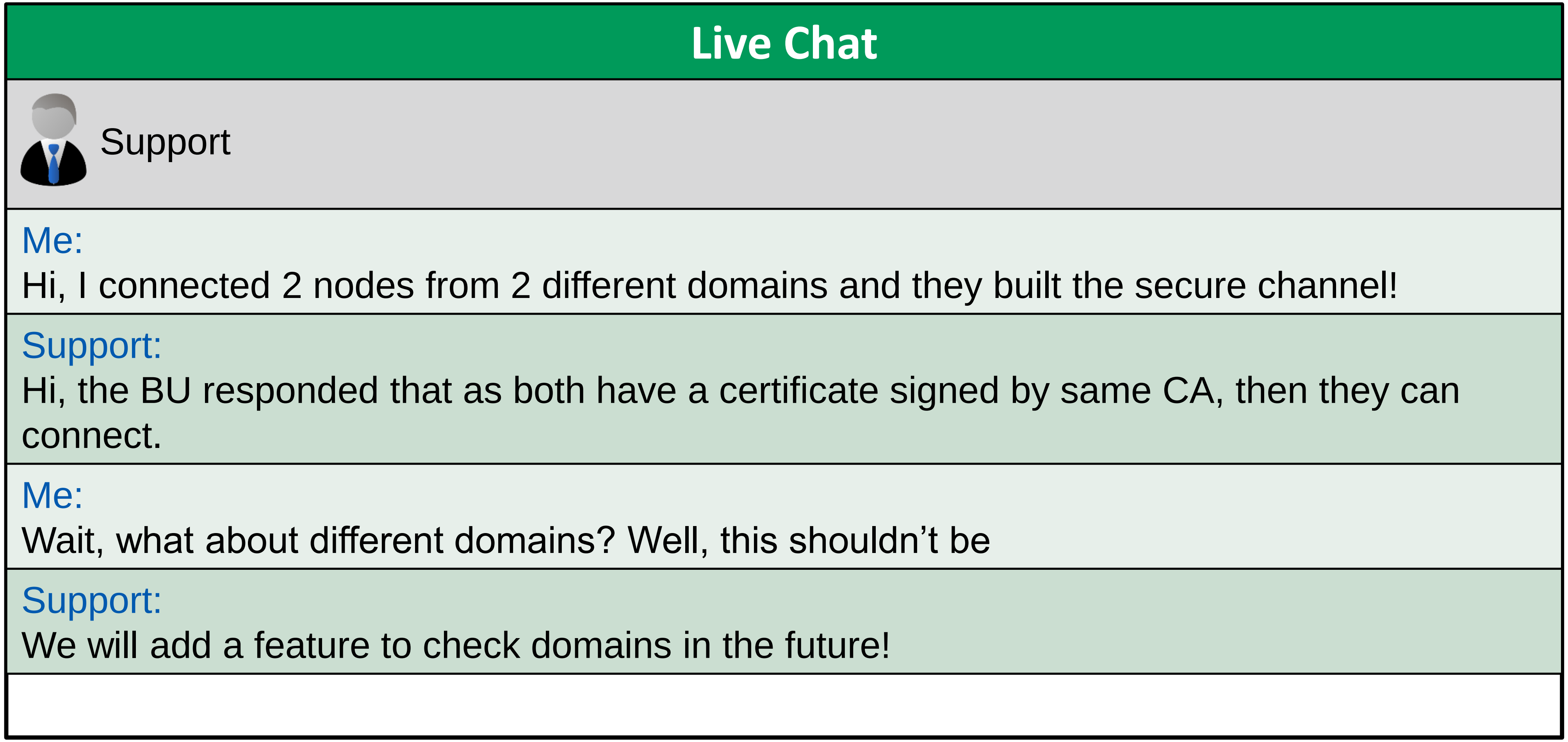
Live Chat

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



Live Chat

Support

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

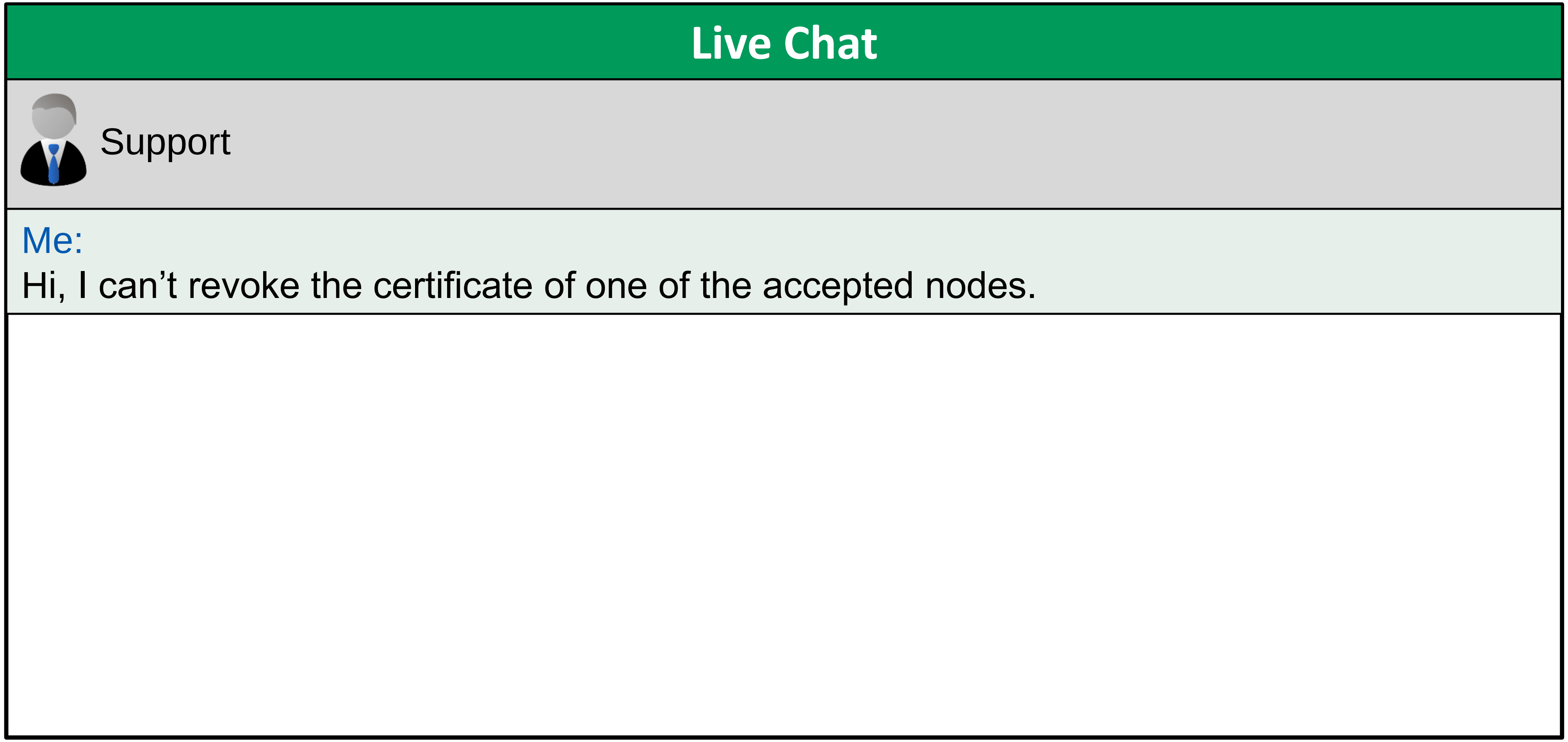
Support:
Hi, the BU responded that as both have a certificate signed by same CA, then they can connect.

Me:
Wait, what about different domains? Well, this shouldn’t be

Support:
We will add a feature to check domains in the future!

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



Live Chat

Support

Me:

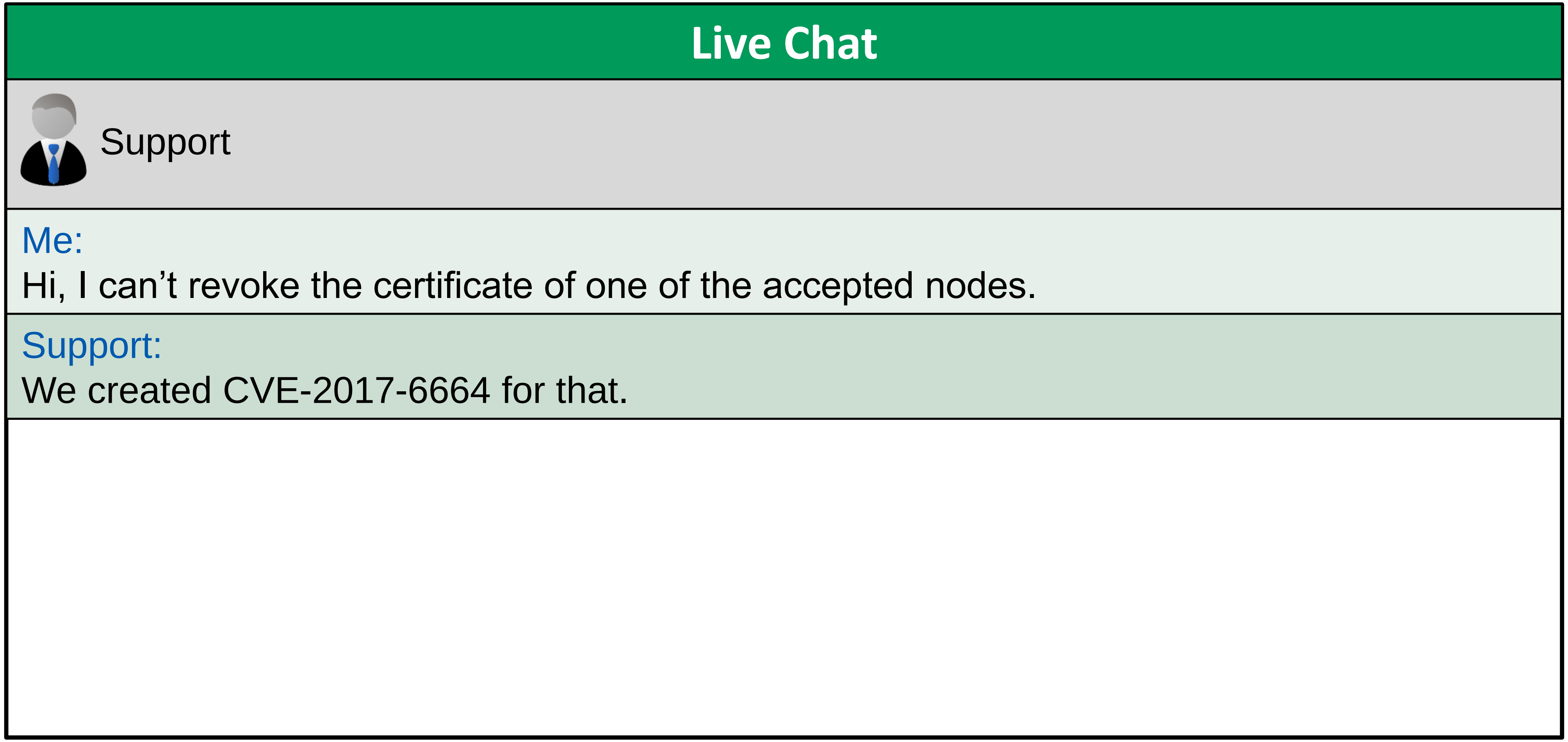
Hi, I can’t revoke the certificate of one of the accepted nodes.

Live Chat

Support

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

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



Live Chat

Support

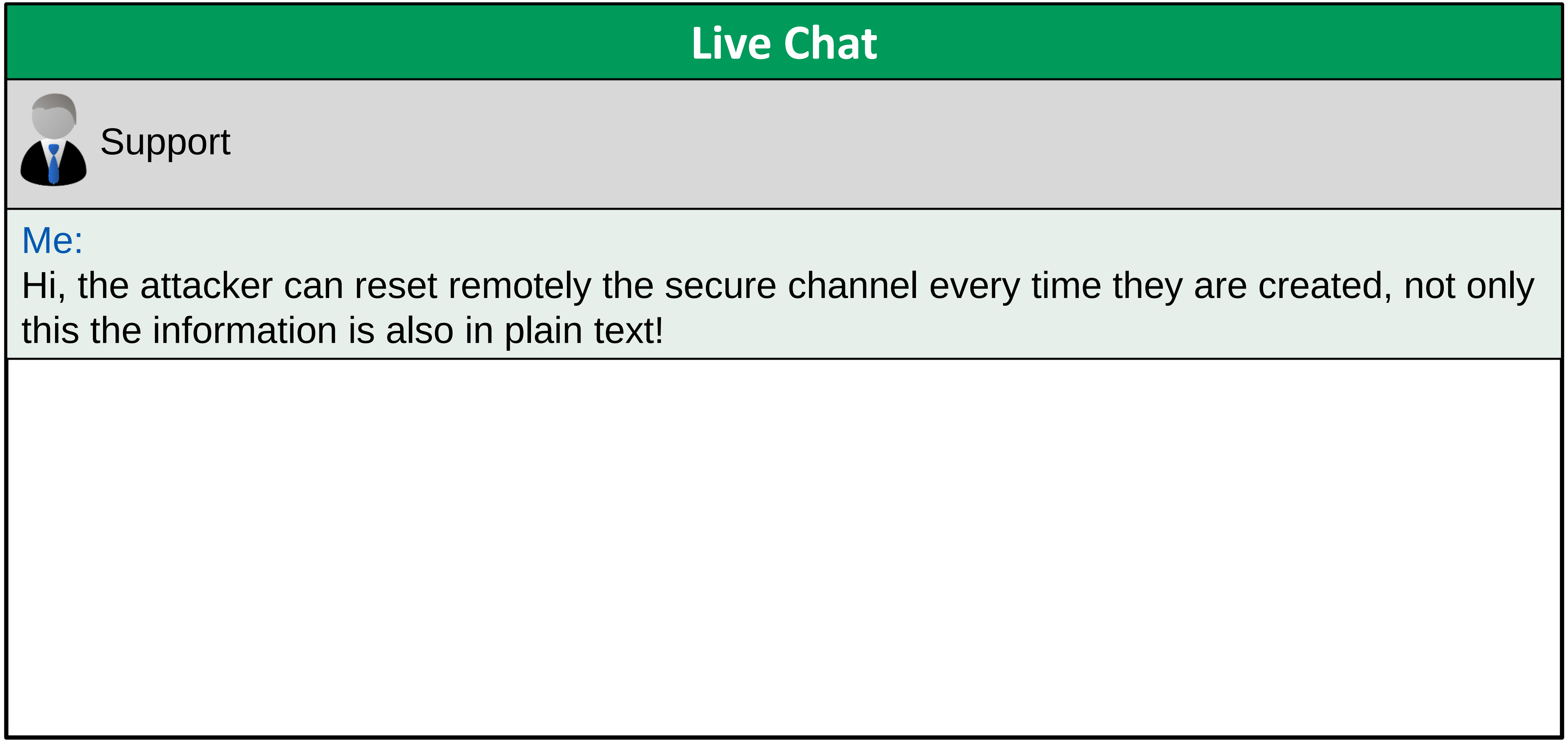
Me:
Hi, I can’t revoke the certificate of one of the accepted nodes.

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

CVE-2017-6664

- Certification Revocation List is not correctly implemented on IOS XE

- No way to protect against malicious nodes within the network

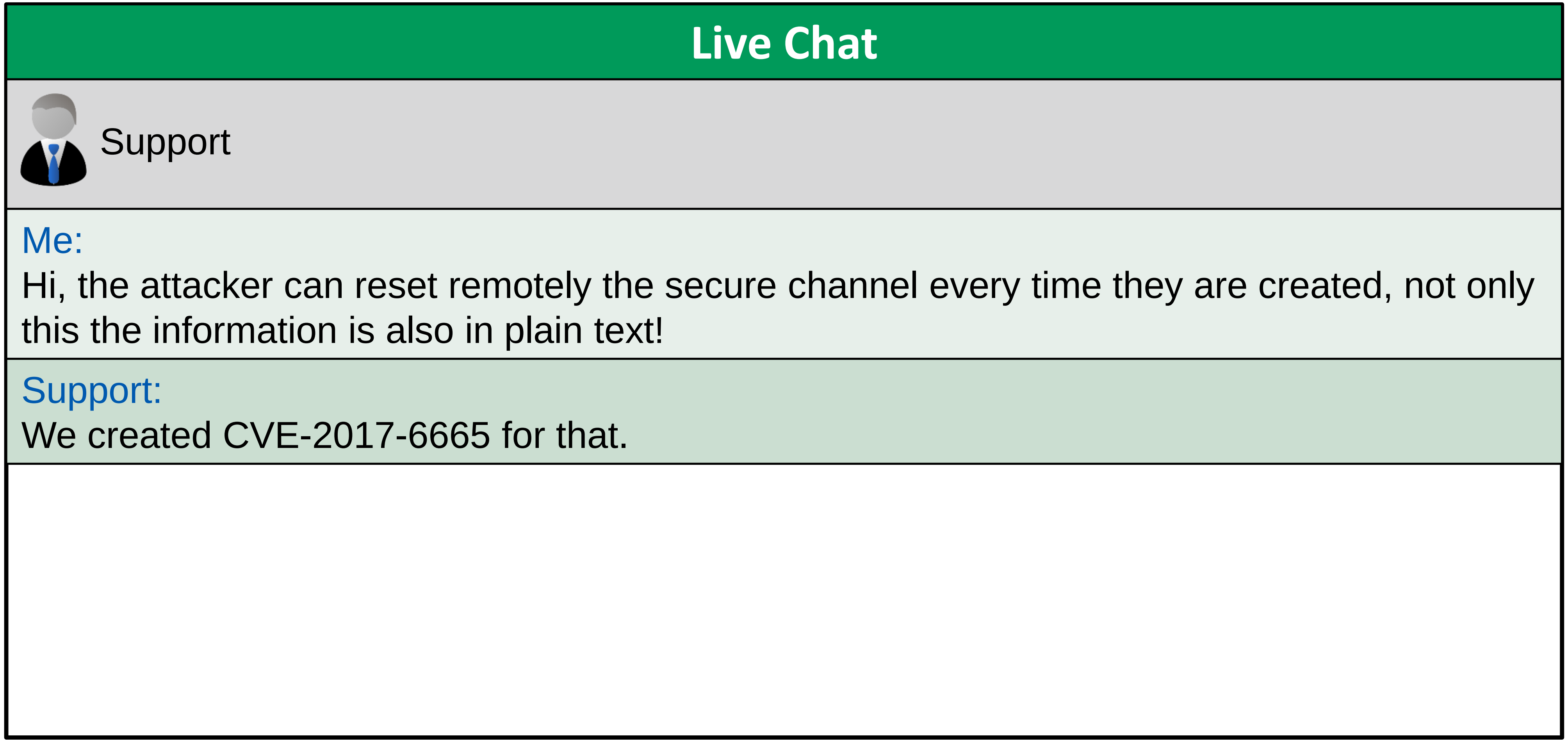


Live Chat

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!



Live Chat

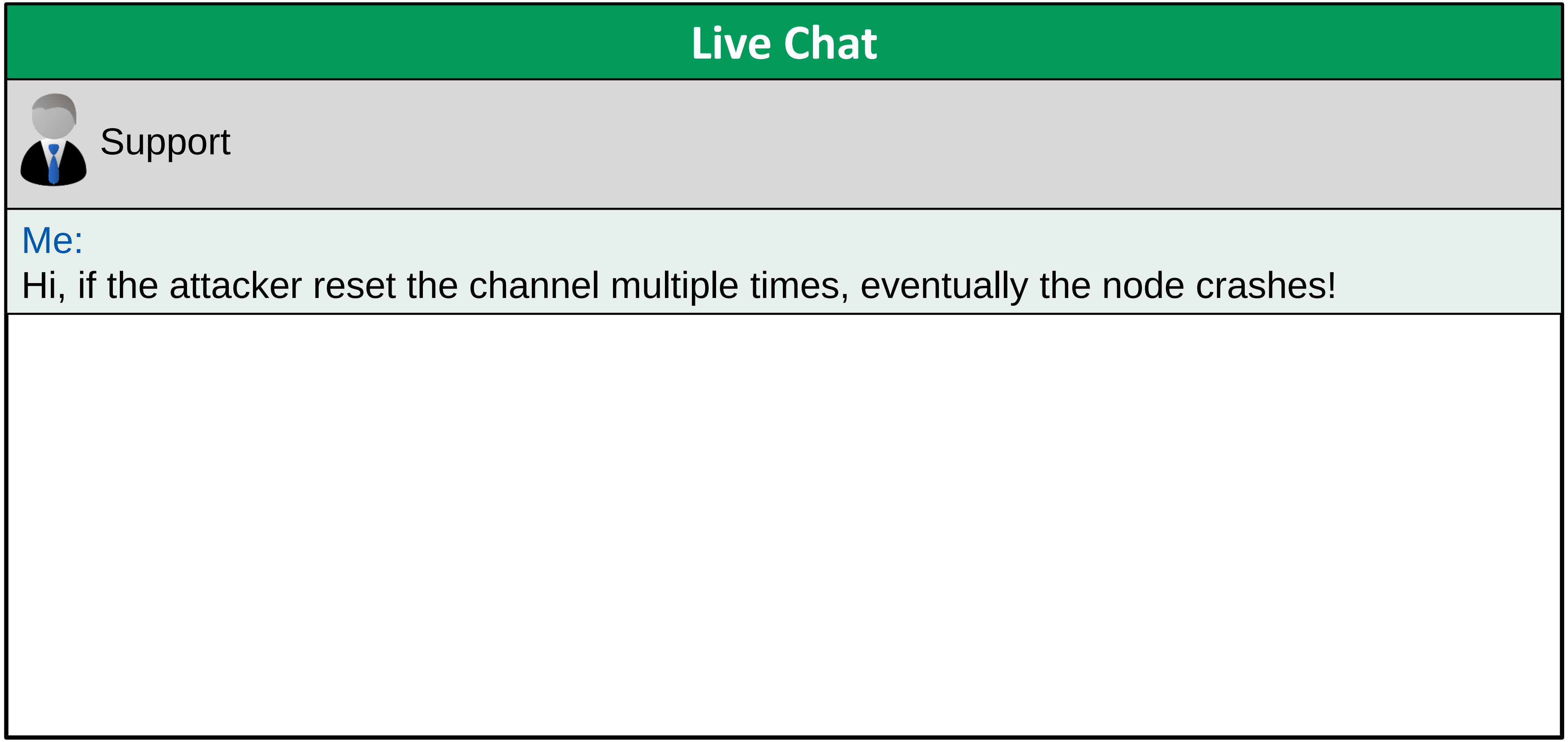
Support

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.

CVE-2017-6665

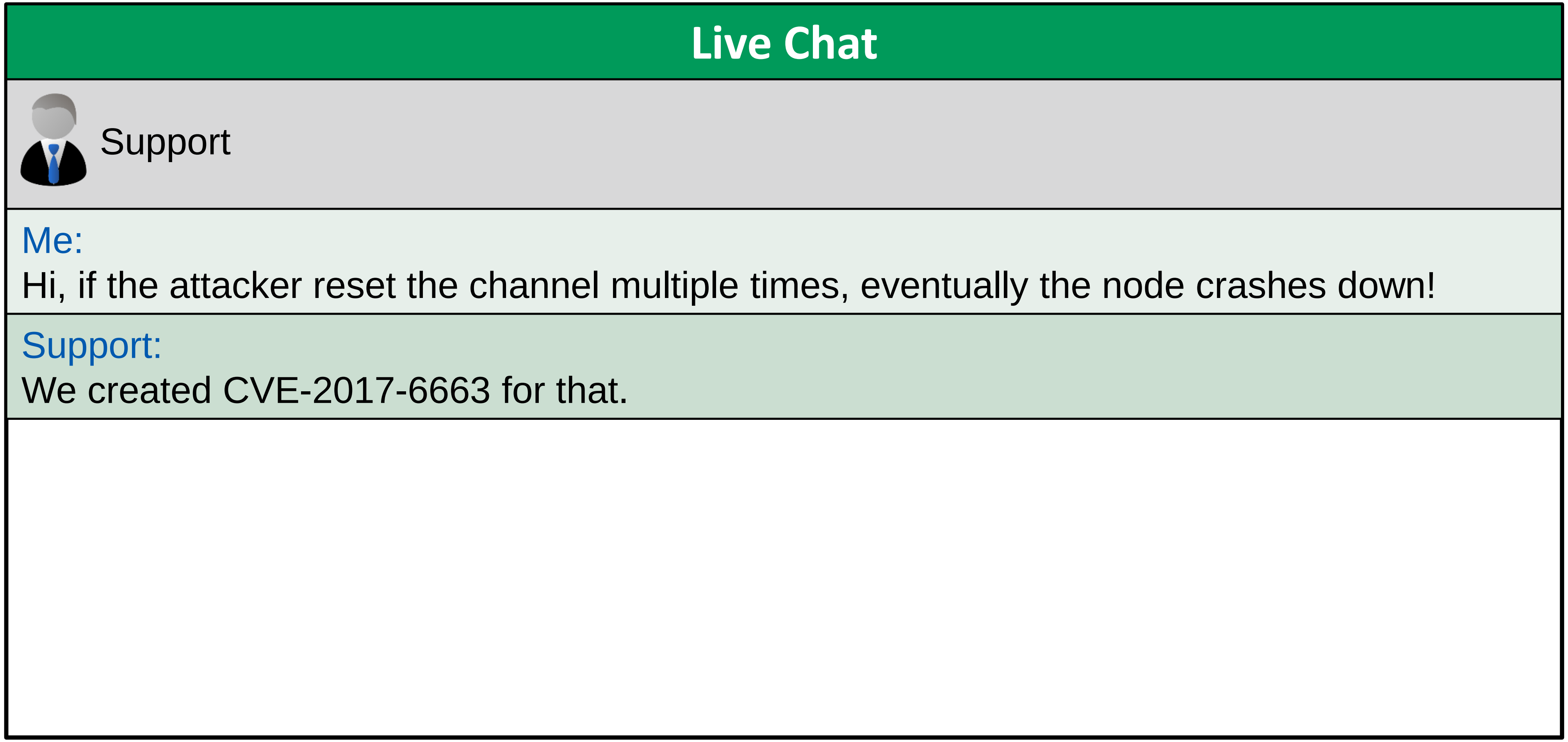
- Replaying the Channel Discovery and Adjacency Discovery packets of any of the accepted nodes reset the Secure channel
- Secure channel is vulnerable to denial-of-service attacks
- Once the secure channel resets, the encrypted information is sent in plain text



Live Chat

Support

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



Live Chat

Support

Me:

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

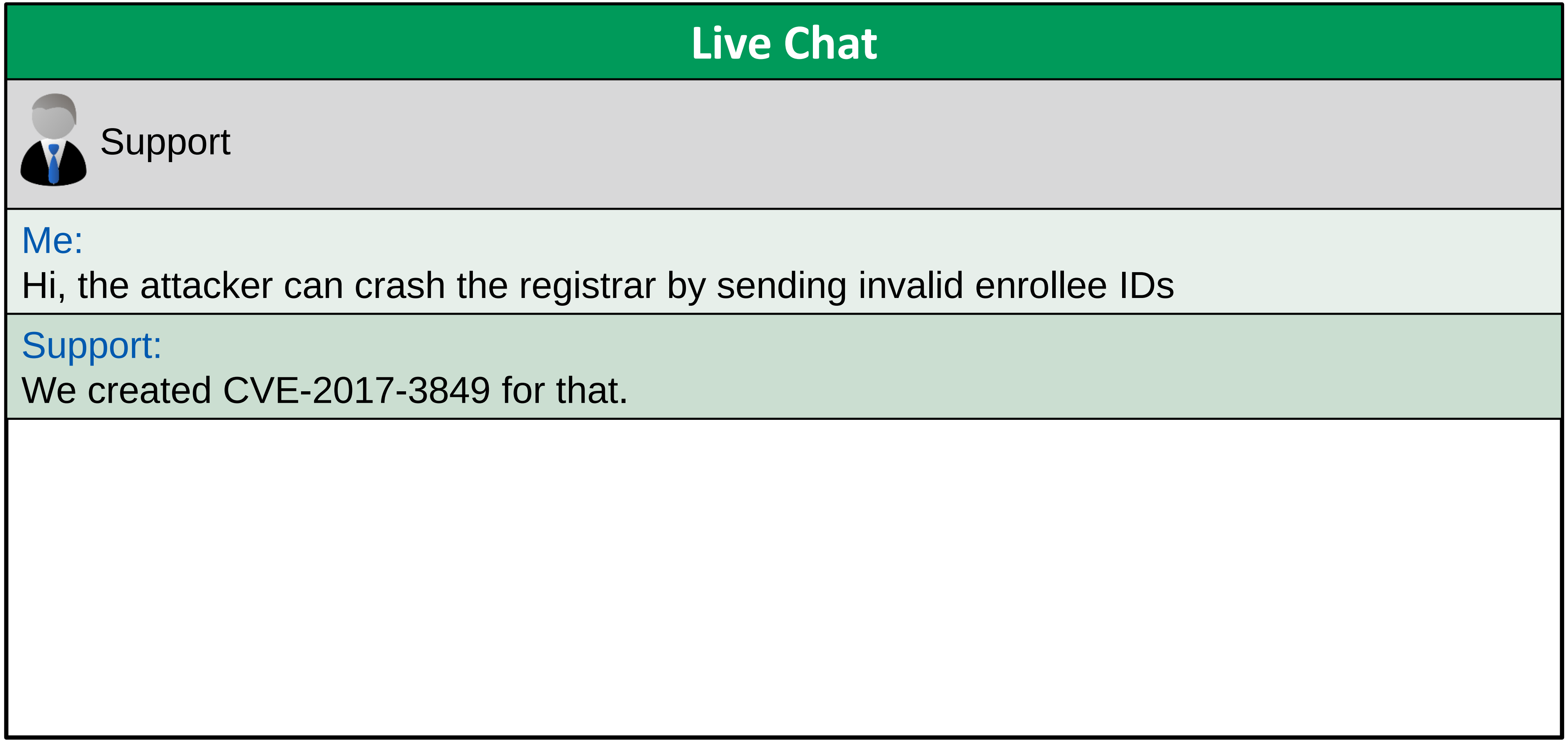
Support:

We created CVE-2017-6663 for that.

CVE-2017-6663

- Resetting the secure channel multiple times will crash the nodes due to a problem in how mDNS packets are handled

- It usually takes about 15 minutes to crash the device



Live Chat

Support

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

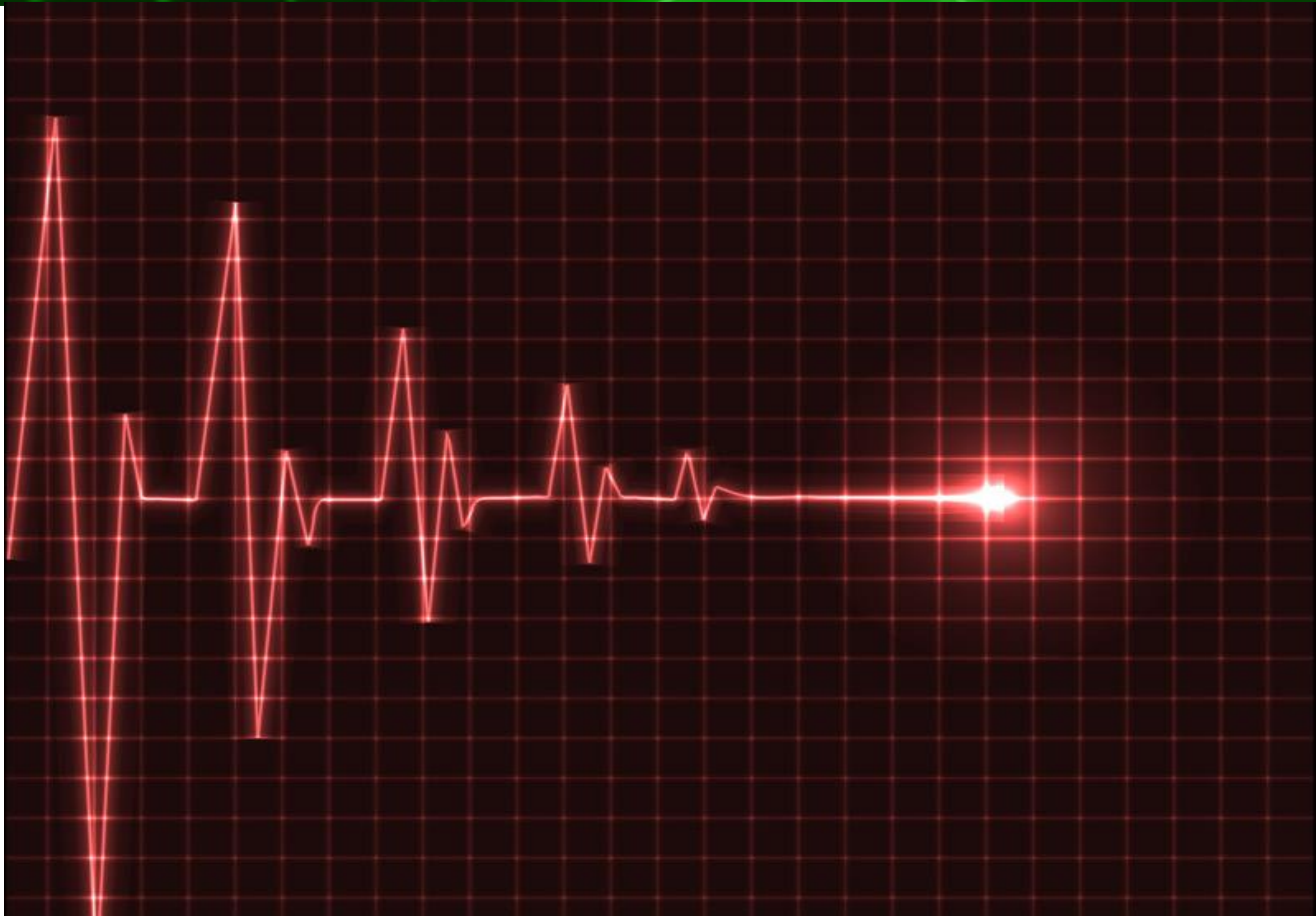
Support:
We created CVE-2017-3849 for that.

CVE-2017-3849

- Sending enrollee UDI as *space byte* or *null byte* crashes the registrar.
- No workaround for that, please upgrade your systems.

DeathKiss!

CVE-2017-3850



CVE-2017-3850

- The device is vulnerable even if the autonomic service is NOT enabled!
- 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

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

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

STAY TUNED
STAY TUNED
STAY TUNED

oeissa@ernw.de

www.ernw.de

@Insinuator

www.insinuator.net