Crashing Cisco's Autonomic Network

Omar Eissa

ERNW
providing security.

Goal of the presentation

- Security Assessment for a network implementation
- The network is based on a new technology developed by Cisco under the name Autonomic Network
- *It is first work of its kind to analyze a commercial implementation of Autonomic Network*

ERNW
providing security.

Expectations

- Understand Autonomic Network, its architecture and how different components work together.
- Reverse engineer Cisco's proprietary Autonomic Network protocol.
- *Multiple vulnerabilities will be for the first time disclosed throughout the presentation*

© Can Stock Photo

ERNW
providing security.

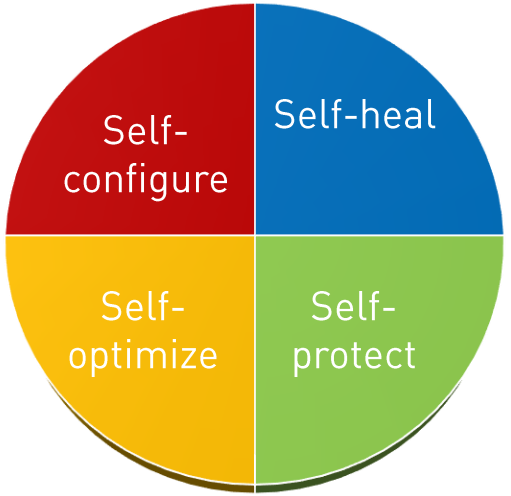
Agenda

- Introduce Cisco's Autonomic Network
- Discuss Autonomic Network (AN) architecture
- Explain Cisco's deployment for the AN through multiple scenarios
- Reverse engineering AN protocol phases
  - Channel Discovery
  - Adjacency Discovery
  - Secure Channel
- Attacking the network
  - Discover and exploit multiple vulnerabilities

ERNW
providing security.

Introduction

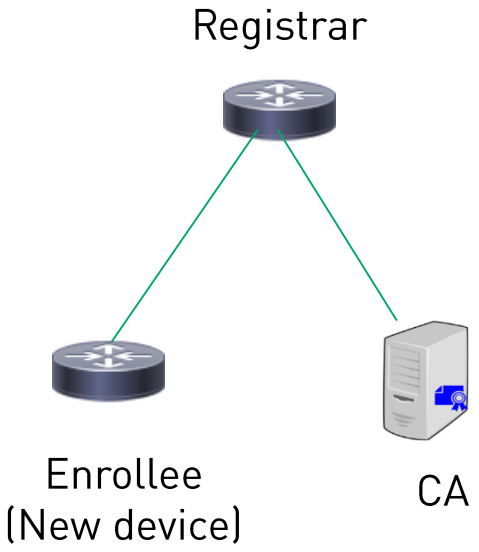
- Technology developed in the IETF under the name ANIMA (Autonomic Networking Integrated Model and Approach)

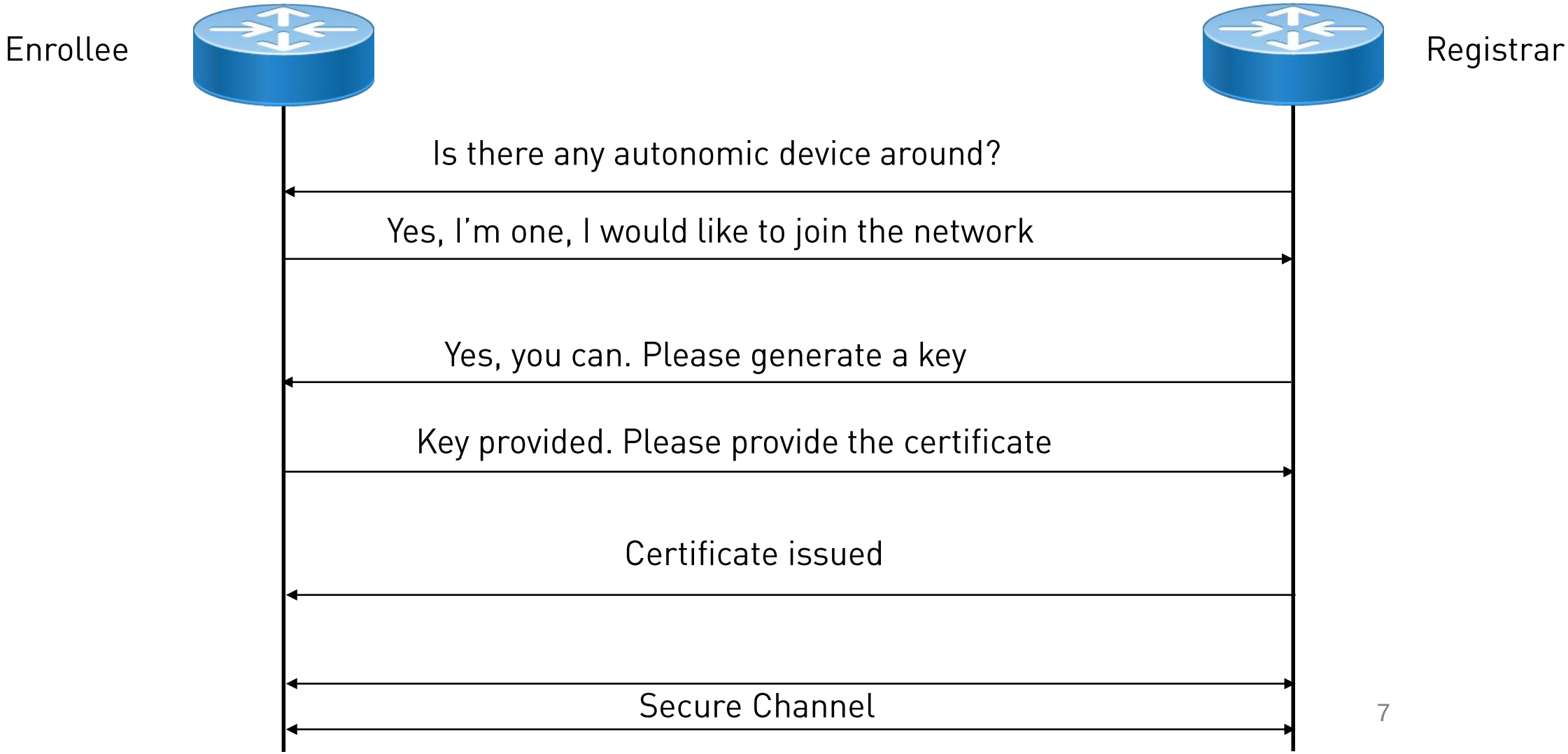


- Based on the Autonomic Computing Systems approach developed by IBM which introduced Self-managing Systems.

General Overview

- Network control point, simply known as registrar
- Enrollee, can be a new device or an already working device
- Certificate Authority (either local or external)




Enrollee
Registrar
Is there any autonomic device around?
Yes, I'm one, I would like to join the network
Yes, you can. Please generate a key
Key provided. Please provide the certificate
Certificate issued
Secure Channel

Live Demo

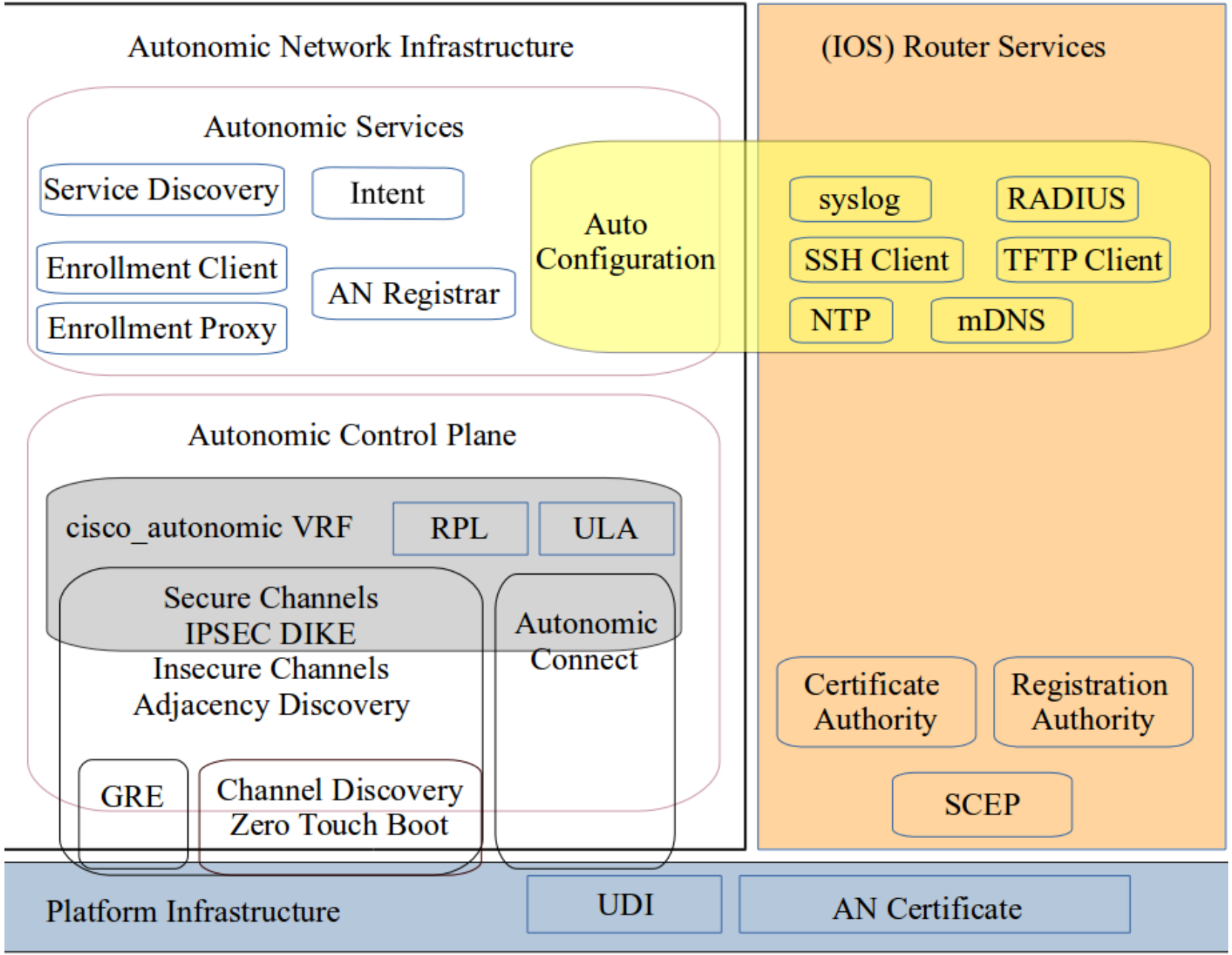
ERNW
providing security.

Demo Results

- 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.

Autonomic Network Architecture



ERNW
providing security.

Scenario 1: Single Registrar with a Local CA

- Autonomic registrar configuration mode
- Domain name for the registrar
- Node acts as both CA and a registrar
- Enabling both CA and registrar functions
- Enabling autonomic functions

```
autonomic registrar
 domain-id ERNW.de
 CA local
 no shut
autonomic
```

ERNW
providing security.

Scenario 1: Single Registrar with a Local CA

- 3072-bit RSA key for the CA is generated

- CA root certificate is generated

Scenario 1: Single Registrar with a Local CA

- Unique Device Identifier, is a combination of device model and serial number, e.g: PID:ISR4321/K9 SN:FDO2018A0M8
- 3072-bit key is generated
- Registrar becomes aware of its domain name
- Registrar generates its domain ID

Interface MAC Address	Device number within the domain

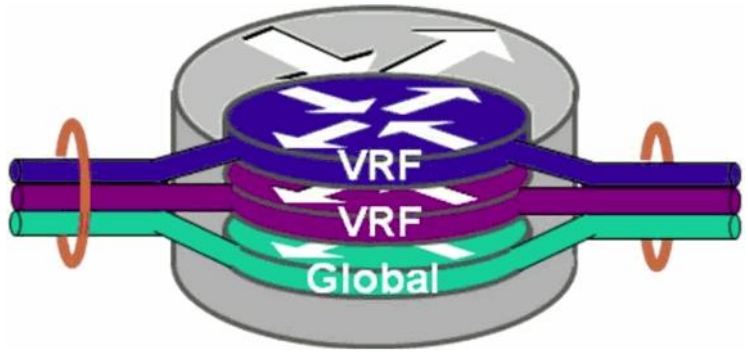
Scenario 1: Single Registrar with a Local CA

- Registrar sends to the CA its UDI, domain name, domain ID and public key to acquire a domain certificate

```
Certificate:
     Data:
        Version:  3 (0x2)
        Serial Number:  2 (0x2)
     Signature Algorithm:  sha512WithRSAEncryption
        Issuer:
            commonName = ioscs RA
        Validity
            Not Before:  Jan 2 15:00:12 2017 GMT
            Not After :  Jan 2 15:00:12 2018 GMT
        Subject:
            serialNumber = PID:ISR4321/K9 SN:FDO2018A0M8 + organizationalUnitName
= ERNW.de
            commonName = 0062.ec9d.8060-1
        Subject Public Key Info:
            Public Key Algorithm:  rsaEncryption
              Public-Key:  (3072 bit)
```

Scenario 1: Single Registrar with a Local CA

- After receiving its domain certificate from the CA
- Registrar creates cisco_autonomic VRF



Cisco.com

Scenario 1: Single Registrar with a Local CA

- Registrar creates new interface under the name loopback100000 and adds it to the VRF
- The IPv6 address of the loopback100000 interface is assigned as the following:

8 bits	40 bits	16 bits	64 bits: 48 bits MAC, 16 bits device number
FD	1st 40 bits of SHA-1 of domain name	0000	Domain ID

ERNW
providing security.

Scenario 1: Single Registrar with a Local CA

- 1st phase of AN protocol, Channel Discovery, starts

- Registrar sends out layer 2 probes advertising the presence of autonomic registrar and looking for any new devices supporting autonomic features

ERNW
providing security.

Scenario 2: Registrar with a Local CA and a Client

- Once the client receives registrar's layer 2 probes, it responds back
- 2nd phase of AN protocol, Adjacency Discovery, starts
- UDP service which runs on protocol 4936

Scenario 2: Registrar with a Local CA and a Client

Client Side

Registrar Side

1) Domain announcement

2) Current Domain & UDI

3) Whitelist check

4) Domain and CA certificates

5) Request Domain Certificate

6) New issued certificate

7) Security parameters negotiation

8) Acknowledgment

3rd phase *Secure Channel*

ERNW
providing security.

Scenario 2: Registrar with a Local CA and a Client

- Secure Channel protection mechanism:
  - DIKE on UDP port 5000 (preferred)
  - IPSec on UDP port 500 (backwards compatibility)

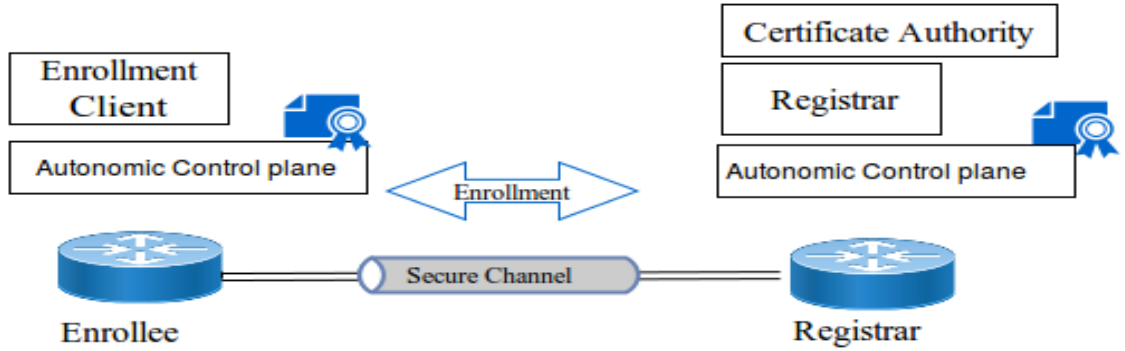
ERNW
providing security.

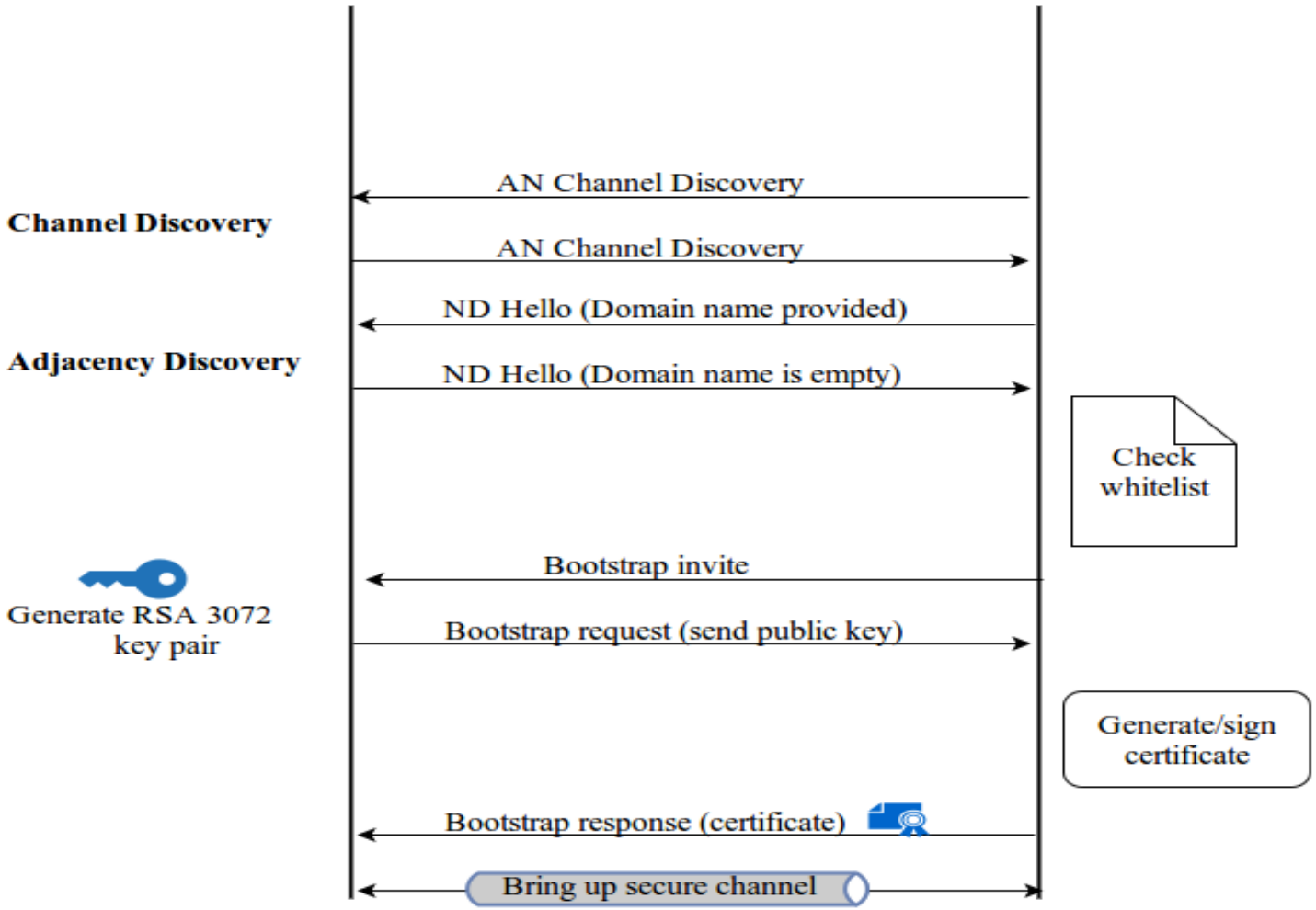
Autonomic Network Features

- Autonomic Control Plane (i.e.: loopback100000 interface)
  - Self-configuring
  - Self-protection
  - Self-healing

ERNW
providing security.

Scenarios Summary





ERNW
providing security.

AN Protocol Analysis

- Wireshark is used to capture packets between the ISR4321 nodes

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

AN Protocol Analysis

- Reverse engineering tools: netzob
- Registrar layer 2 announcements

```
        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.

AN Protocol Analysis

- Network protocol types:
  - Text-based

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

0000   47 45 54 20 2f 64 6f 77 6e 6c 6f 61 64 2e 68 74  GET /download.ht
0010   6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73  ml HTTP/1.1..Hos
0020   74 3a 20 77 77 77 2e 65 74 68 65 72 65 61 6c 2e  t: www.ethereal.
0030   63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a  com..User-Agent:
0040   20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69   Mozilla/5.0 (Wi
0050   6e 64 6f 77 73 3b 20 55 3b 20 57 69 6e 64 6f 77  ndows; U; Window
0060   73 20 4e 54 20 35 2e 31 3b 20 65 6e 2d 55 53 3b  s NT 5.1; en-US;
0070   20 72 76 3a 31 2e 36 29 20 47 65 63 6b 6f 2f 32   rv:1.6) Gecko/2
0080   30 30 34 30 31 31 33 0d 0a 41 63 63 65 70 74 3a  0040113..Accept:
```

ERNW
providing security.

AN Protocol Analysis

- Network protocol types:
  - Binary-based

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

0000  00 00 c0 9f a0 97 00 a0 cc 3b bf fa 08 00 45 10  .........;....E.
0010  00 4f 16 a9 40 00 40 06 a2 9c c0 a8 00 02 c0 a8  .O..@.@.........
0020  00 01 04 e6 00 17 04 53 d8 70 c0 40 87 cf 80 18  .......S.p.@....
0030  7d 78 79 0a 00 00 01 01 08 0a 00 16 0a 27 00 05  }xy..........'..
0040  4b 63 ff fd 03 ff fb 18 ff fb 1f ff fb 20 ff fb  Kc........... ..
0050  21 ff fb 22 ff fb 27 ff fd 05 ff fb 23           !.."..'.....#
```

AN Protocol Analysis

- Binary protocols encoding formats:
  - Fixed fields

```
        00 01 02 03 04 05 06 07

0000    13 48 13 48 00 8f 89 5a     |.H.H...Z
```

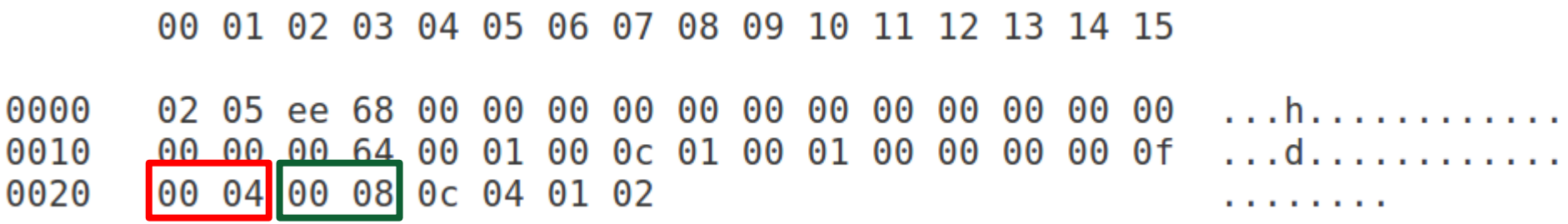
Octet	0								1								2								3							
Bits	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	Source port																Destination port															
64	Length																Checksum															

UDP header

ERNW
providing security.

AN Protocol Analysis

- Binary protocols encoding formats:
  - Variable-sized fields (Type-length-value)



AN Protocol Analysis

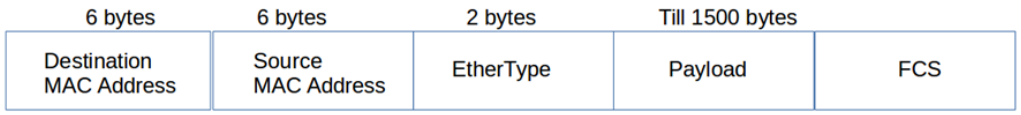
- Looking on our frame, which encoding format does it follow ?

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

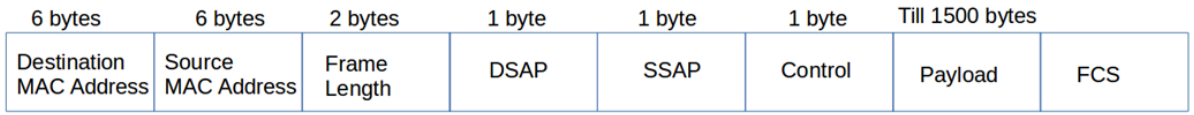
Type-Length-Value

AN Protocol Analysis

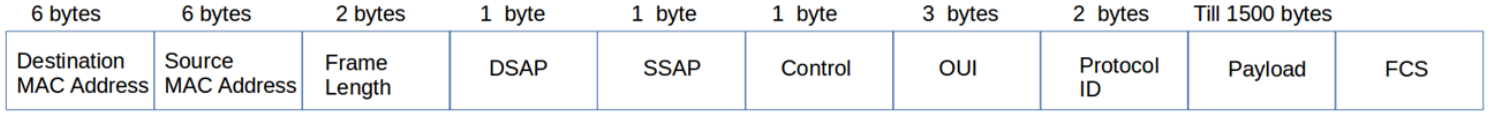
- Ethernet header formats



Ethernet II



802.3 (802.3, 802.2 LLC)



802.3 (802.3, 802.2 SNAP)

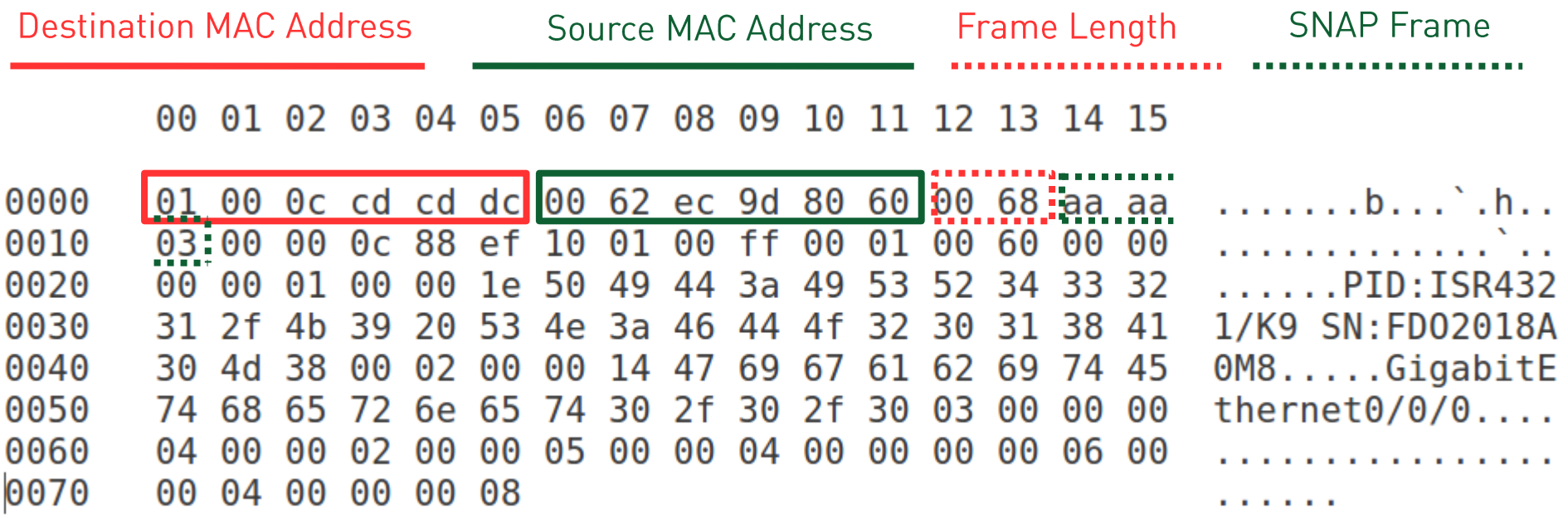
ERNW
providing security.

Channel Discovery

Ethernet

AN Protocol Analysis

- Channel Discovery frame analysis



ERNW
providing security.

Channel Discovery

Ethernet

AN Protocol Analysis

- Channel Discovery frame analysis

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                                ......
```

ERNW
providing security.

Channel Discovery

Ethernet

AN Protocol Analysis

- Channel Discovery frame analysis

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

AN Protocol Analysis

- Channel Discovery frame analysis

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

Ethernet

AN Protocol Analysis

- Channel Discovery frame analysis

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

AN Protocol Analysis

- Channel Discovery frame analysis

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

Ethernet

AN Protocol Analysis

- Channel Discovery frame analysis

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.

AD Header
UDP
IPv6
Customized CD Header
Ethernet

AN Protocol Analysis

- Adjacency Discovery phase on port 4936

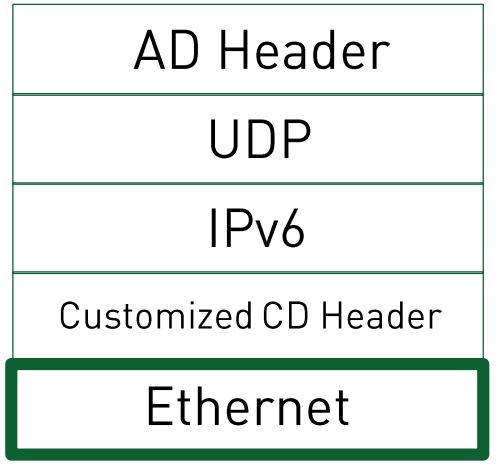
```
      00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

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.

AN Protocol Analysis

- Adjacency Discovery phase on port 4936

```
      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
```



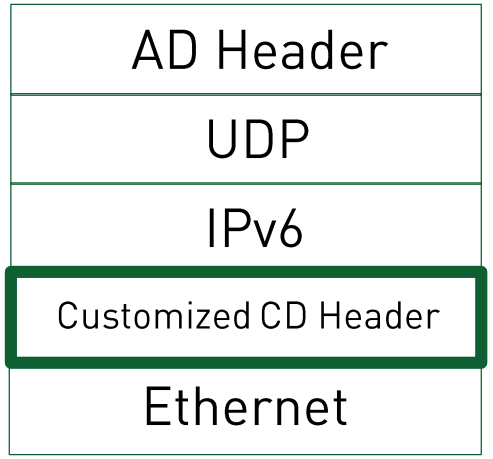
Ethernet 802.3 /802.2 SNAP

ERNW
providing security.

AN Protocol Analysis

- Adjacency Discovery phase on port 4936

```
      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.

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

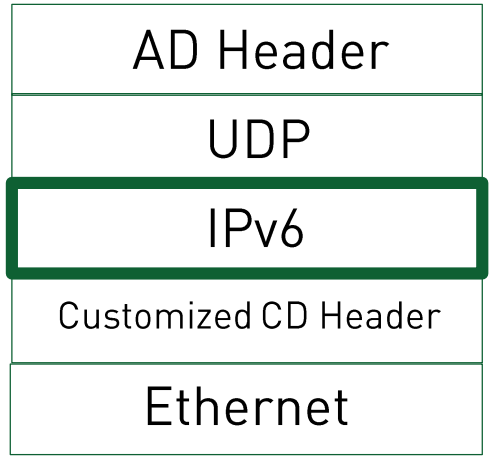
AN Protocol Analysis

- Adjacency Discovery phase on port 4936

```
      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

ERNW
providing security.



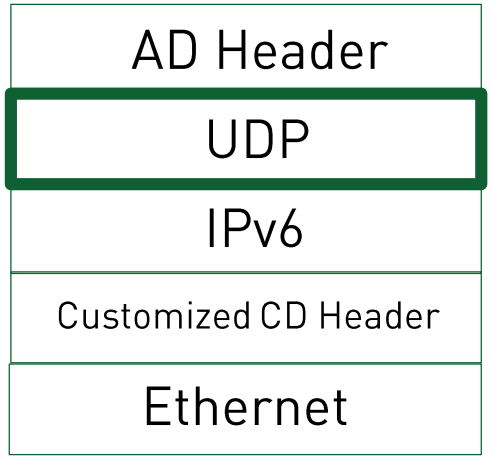
AN Protocol Analysis

- Adjacency Discovery phase on port 4936

```
      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.



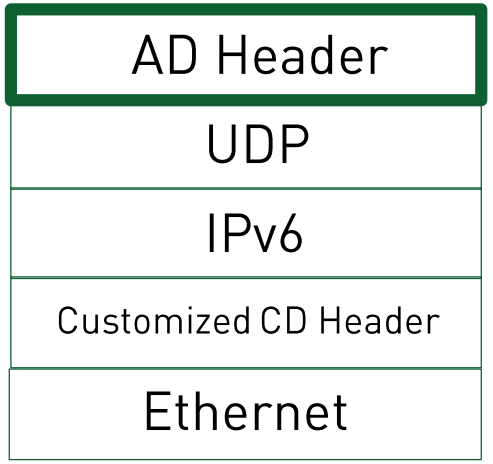
AN Protocol Analysis

- Adjacency Discovery phase on port 4936

```
      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.



AN Protocol Analysis

- Adjacency Discovery phase on port 4936

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)																															

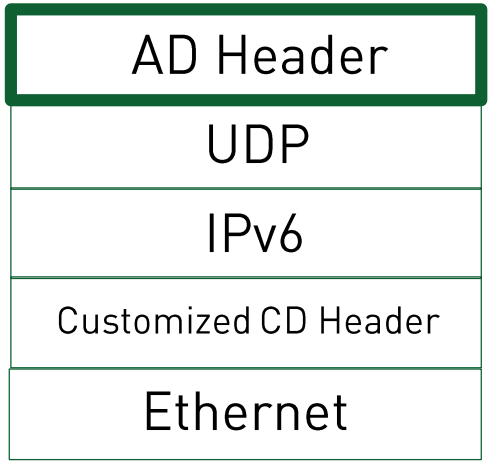
AN Adjacency Discovery Header

ERNW
providing security.

AN Protocol Analysis

- Adjacency Discovery phase on port 4936

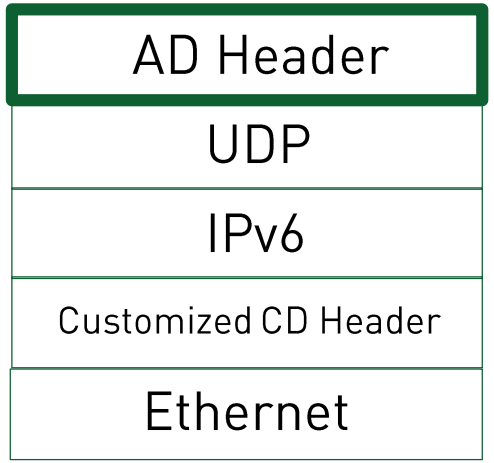
```
      00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

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.



AN Protocol Analysis

- Adjacency Discovery phase on port 4936

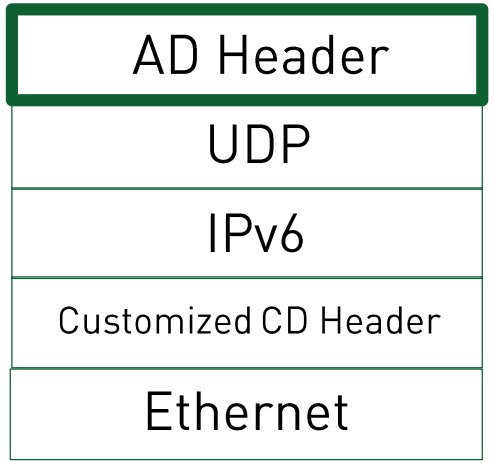
State Value	Significance
0x02	Multicast, Neighbor Discovery hello packets
0x03	Unicast, Bootstrap phase
0x04	Unicast, negotiating secure channel parameters

ERNW
providing security.

AN Protocol Analysis

- Adjacency Discovery phase on port 4936

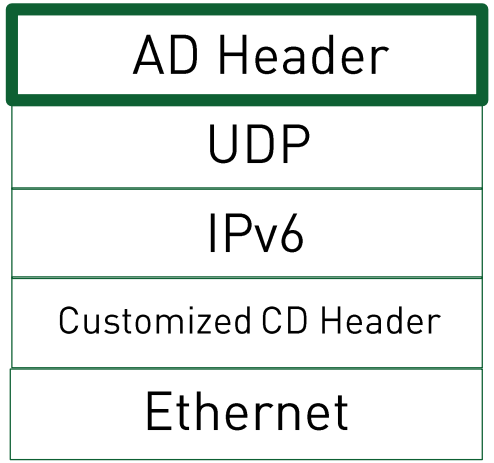
```
      00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

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

ERNW
providing security.



AN Protocol Analysis

- Adjacency Discovery phase on port 4936

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

ERNW
providing security.

AD Header
UDP
IPv6
Customized CD Header
Ethernet

AN Protocol Analysis

- Adjacency Discovery phase on port 4936

```
      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

ERNW
providing security.

AD Header
UDP
IPv6
Customized CD Header
Ethernet

AN Protocol Analysis

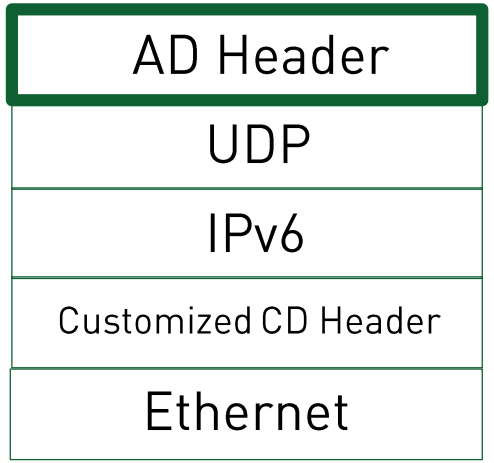
- Adjacency Discovery phase on port 4936

```
      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.

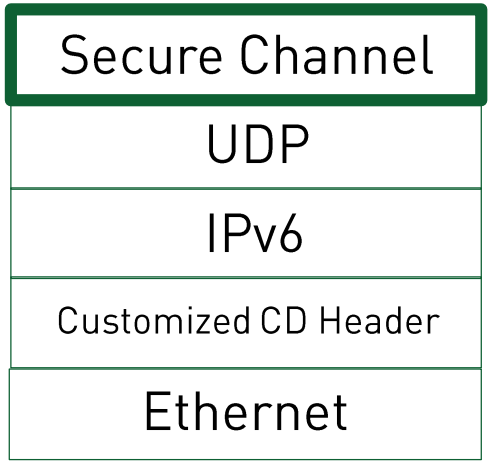


AN Protocol Analysis

- Adjacency Discovery phase on port 4936

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

ERNW
providing security.



AN Protocol Analysis

- Secure Channel phase
- DIKE, Data-Internet Key Exchange V2, port 5000
- IPSEC, IP Secure, port 500

ERNW
providing security.

Secure Channel
UDP
IPv6
Customized CD Header
Ethernet

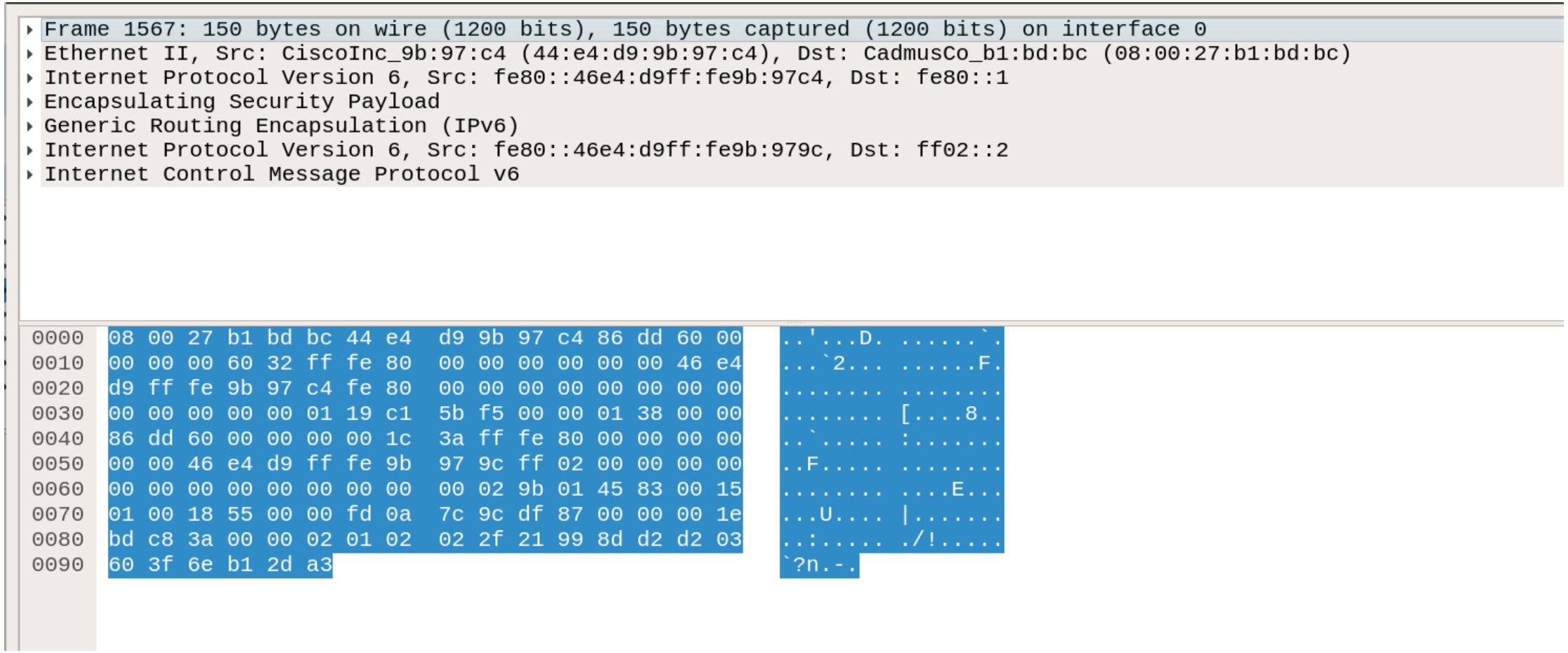
AN Protocol Analysis

- Secure Channel phase

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

ME 3600X-24CX-M

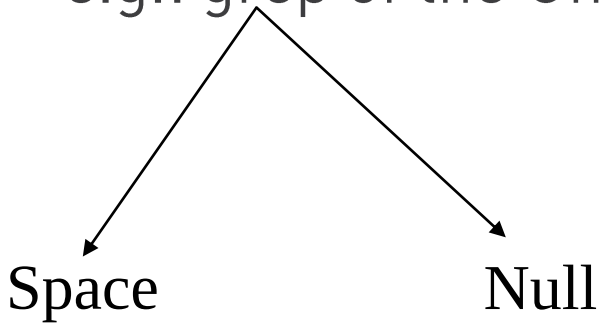
ERNW
providing security.



AN Protocol Testing

- Whitelist
- Malicious user tries to get unauthorized access or hinder the network performance
- What search function is used to search in the list? e.g.: grep of the Unix systems

```
Registrar#more flash:whitelist.txt
PID:ISR4321/K9 SN:FDO2018A0M9
PID:ISR4321/K9 SN:FDO2018A0M8
PID:ISR4321/K9 SN:FDO1845A00F
```



Live Demo

ERNW
providing security.

Demo Results

- Autonomic Network registrars can not handle neither space nor null as an enrollee UDI
- CVE-2017-3849
- CSCvc42717: Cisco IOS and IOS XE Software Autonomic Networking Infrastructure Registrar Denial of Service Vulnerability

ERNW
providing security.

AN Protocol Testing

- Adjacency Discovery packets specifically crafted
- Unexpected types within the packets
- Unexpected values assigned to the types

Live Demo

ERNW
providing security.

Demo Results

- Specifically crafted Adjacency Discovery packets can cause the ISR4321 to reload

- Details will be published in couple of days on insinuator.net

ERNW
providing security.

AN Protocol Testing

- No need for autonomic services to be running on the device

- You only need a reachable IPv6 address to crash the routers, that's all!

By World IPv6 Day (Internet Society)

Live Demo

ERNW
providing security.

Demo Results

- There is no need for autonomic services to be enabled to crash ISR4321
- All what is needed is just the IPv6 address regardless of being link-local or global
- CVE-2017-3050
- CSCvc42729: Cisco IOS and IOS XE Software IPv6 Denial of Service Vulnerability

ERNW
providing security.

Conclusion

- Smart network where nodes can manage themselves
- Channel Discovery, Adjacency Discovery, Secure Channel
- Vulnerable to null/space as UDIs
- Vulnerable to unexpected fields within the packets
- Denali 16.2.1 and 16.3.1 operating systems (IOS XE) can be crashed using only their IPv6 address

ERNW
providing security.

Finally…

- There are **more vulnerabilities** to announce and disclose, everything will be there on insinuator.net
- 3-part series about Autonomic Network on insinuator.net
  - Introduction
  - Analysis
  - Vulnerabilities
- I would like to thank Marc Heuse for his contributions with protocol analysis

oeissa@ernw.de

www.ernw.de

@Insinuator

www.insinuator.net