<docnum>: 2A Decrypt Z-Wave RF Frames using the Zniffer

This hands-on exercise will demonstrate how to decrypt Z-Wave RF frames using the Z-Wave Zniffer tool.

This exercise is part of the series ‘Z-Wave 1-Day Course’.

- 1 Include using SmartStart
- **2 Decrypt Z-Wave RF Frames using the Zniffer**
- 3A Compile Switch On/Off and Enable Debug
- 3B Modify Switch On/Off
- 4 Understand FLiRS devices

KEY FEATURES

- Decrypt Z-Wave RF Frames
- Learn to use Z-Wave Zniffer tool
- Introduction to Z-Wave Command Classes.

1 Introduction

In this exercise, we will use the Z-Wave Zniffer tool to decrypt the RF traffic when knowing the security keys for the network.

We will decrypt Z-Wave frames and get a basic understand of the Z-Wave Command Classes.

1.1 Hardware Requirements

- 1 WSTK Main Development Board
- 1 Z-Wave Radio Development Board: ZGM130S SiP Module
- 1 UZB Controller
- 1 USB Zniffer

1.2 Software Requirements

- Simplicity Studio v4
- Z-Wave 7 SDK
- Z-Wave PC Controller
- Z-Wave Zniffer

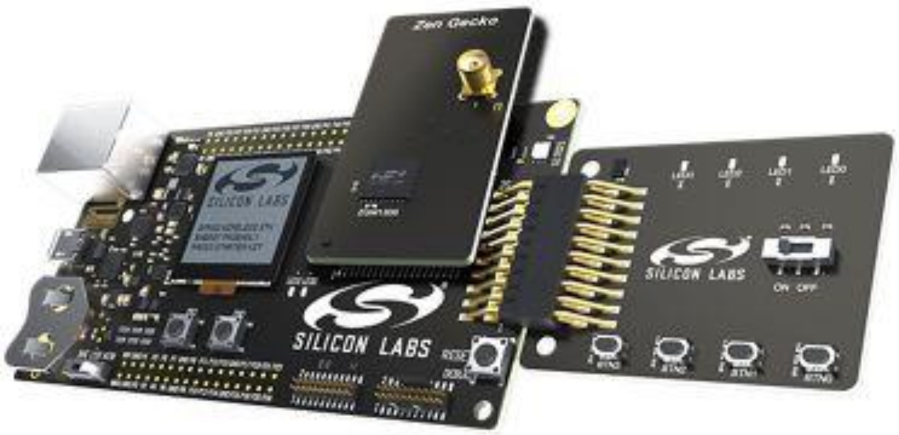


Figure 1: Main development board with Z-Wave SiP module

1.3 Pre-requisites

You need to have setup a Z-Wave network with a Controller and a Switch On / Off slave device.

For instructions in how to setup the network, refer to the previous exercise “1 Include using SmartStart”.

2 Capture RF packages using the Zniffer

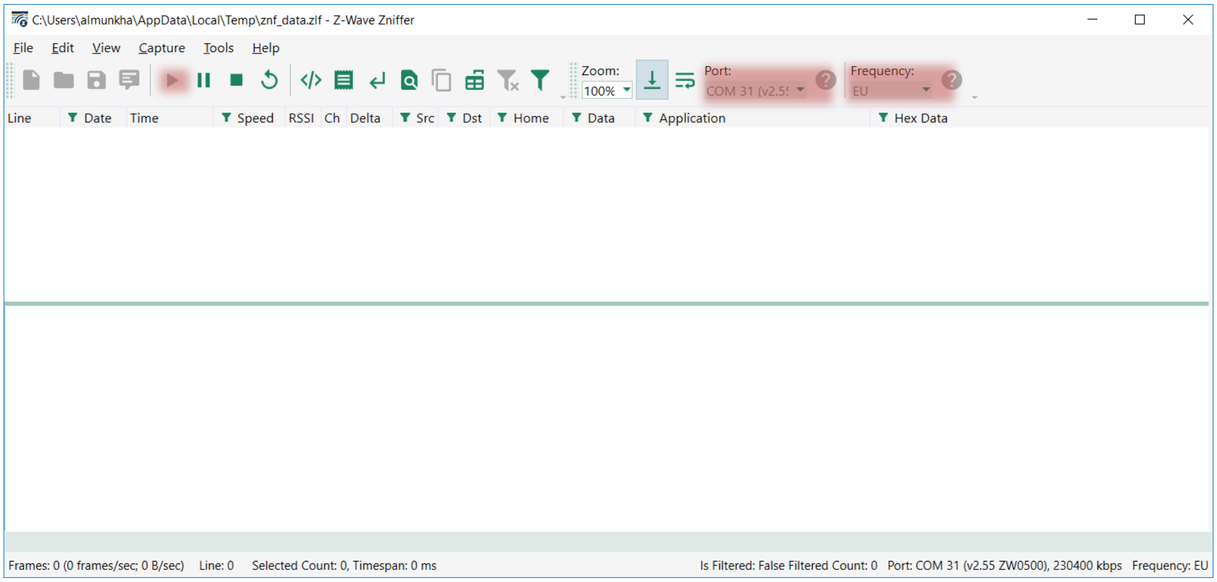
In the previous exercise "1 Include using SmartStart", we learned how to include a device using SmartStart and we tested the basic functionality using the PC Controller.

2.1 Setup Zniffer

Now, let's use the Zniffer to see which frames are being sent to turn on and off the LED.

- Make sure your Zniffer is plugged into your PC and open the Z-Wave Zniffer tool from Simplicity Studio Tools menu.
- Select the COM port by clicking on the icon ? next to Port. This will search for connected Zniffers.
- Select the COM port in the drop down menu.
- Select the Frequency by clicking on the icon ? next to Frequency.
- Select the Frequency that matches the frequency you programmed your device with. These exercises uses "EU".
- Start a new Trace ▶.

The Zniffer tool is now ready and listening for Z-Wave RF Traffic.

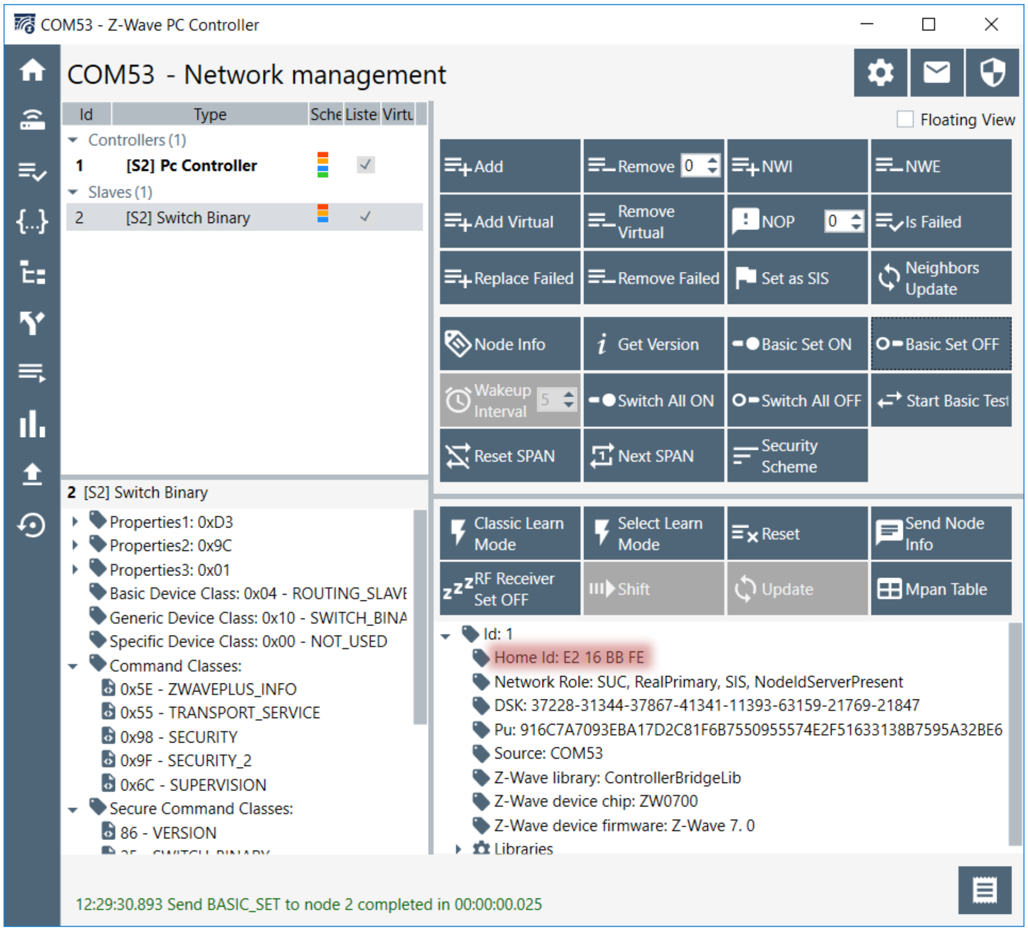


Frames: 0 (0 frames/sec; 0 B/sec) Line: 0 Selected Count: 0, Timespan: 0 ms Is Filtered: False Filtered Count: 0 Port: COM 31 (v2.55 ZW0500), 230400 kbps Frequency: EU

Figure 2: Zniffer setup and listening for Z-Wave traffic

You might see other traffic, despite you are not sending any to your device. Currently, the Zniffer is configured for listening for any traffic in the selected region. We need to filter the trace by "Home ID" to only show traffic from your network.

- From the PC Controller, find the "Home ID" in the "Network Management" tab.
  - In Figure 3, the example HomeID is E2 16 BB FE.
- Knowing the Home ID, click the small icon ▼ next to "Home" in the Zniffer. Refer to Figure 4.
- Write the Home ID in this field and click OK.
- The green icon now turns red ▼ symbolizing the Zniffer is filtering on Home Id.



- Controllers (1)
  - 1 [S2] Pc Controller ✓
- Slaves (1)
  - 2 [S2] Switch Binary ✓

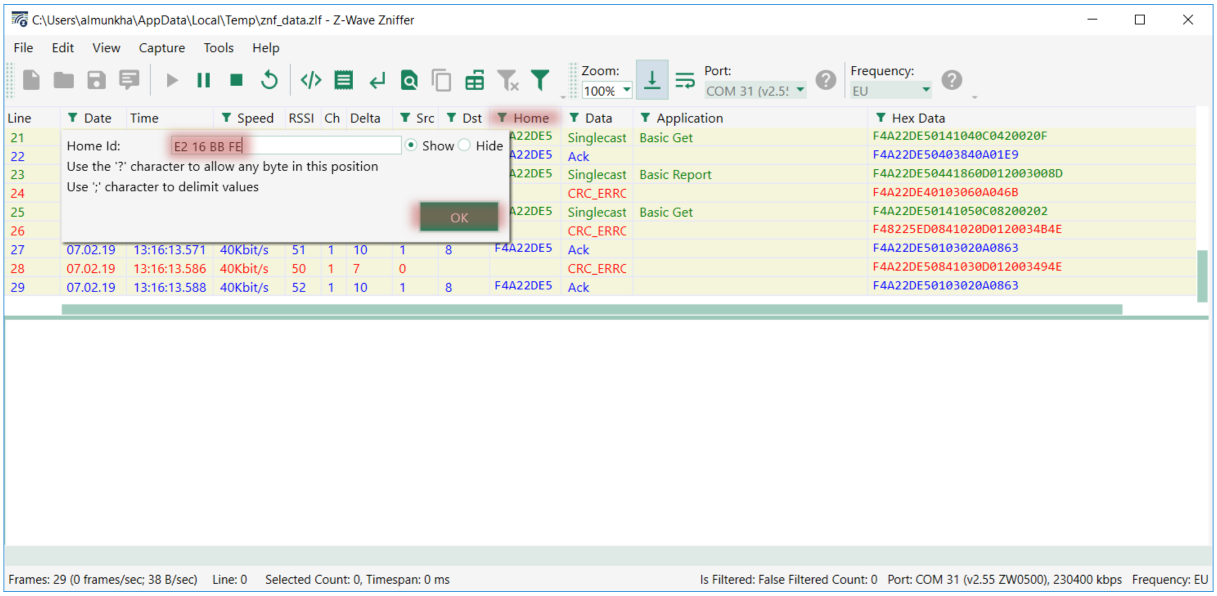
2 [S2] Switch Binary

- Properties1: 0xD3
- Properties2: 0x9C
- Properties3: 0x01
- Basic Device Class: 0x04 - ROUTING_SLAVE
- Generic Device Class: 0x10 - SWITCH_BINA
- Specific Device Class: 0x00 - NOT_USED
- Command Classes:
  - 0x5E - ZWAVEPLUS_INFO
  - 0x55 - TRANSPORT_SERVICE
  - 0x98 - SECURITY
  - 0x9F - SECURITY_2
  - 0x6C - SUPERVISION
- Secure Command Classes:
  - 86 - VERSION

- Id: 1
  - Home Id: E2 16 BB FE
  - Network Role: SUC, RealPrimary, SIS, NodeIdServerPresent
  - DSK: 37228-31344-37867-41341-11393-63159-21769-21847
  - Pu: 916C7A7093EBA17D2C81F6B7550955574E2F51633138B7595A32BE6
  - Source: COM53
  - Z-Wave library: ControllerBridgeLib
  - Z-Wave device chip: ZW0700
  - Z-Wave device firmware: Z-Wave 7. 0
  - Libraries

12:29:30.893 Send BASIC_SET to node 2 completed in 00:00:00.025

Figure 3: Home ID from PC Controller



Home Id: E2 16 BB FE ● Show ○ Hide
Use the '?' character to allow any byte in this position
Use ';' character to delimit values

Line	Date	Time	Speed	RSSI	Ch	Delta	Src	Dst	Home	Data	Application	Hex Data
21									A22DE5	Singlecast	Basic Get	F4A22DE50141040C0420020F
22									A22DE5	Ack		F4A22DE50403840A01E9
23									A22DE5	Singlecast	Basic Report	F4A22DE50441860D012003008D
24										CRC_ERRC		F4A22DE40103060A046B
25									A22DE5	Singlecast	Basic Get	F4A22DE50141050C08200202
26										CRC_ERRC		F48225ED0841020D0120034B4E
27	07.02.19	13:16:13.571	40Kbit/s	51	1	10	1	8	F4A22DE5	Ack		F4A22DE50103020A0863
28	07.02.19	13:16:13.586	40Kbit/s	50	1	7	0			CRC_ERRC		F4A22DE50841030D012003494E
29	07.02.19	13:16:13.588	40Kbit/s	52	1	10	1	8	F4A22DE5	Ack		F4A22DE50103020A0863

Frames: 29 (0 frames/sec; 38 B/sec) Line: 0 Selected Count: 0, Timespan: 0 ms Is Filtered: False Filtered Count: 0 Port: COM 31 (v2.55 ZW0500), 230400 kbps Frequency: EU

Figure 4: Insert Home ID in Zniffer to filter trace

Hint If you press on 'Enter' on the keyboard, instead of clicking OK in the pop-up box, the filter is not applied. This means, the symbol will not turn red. Turn on the filter by clicking on Toggle Filter in the menu bar.

2.2 Update Zniffer Nonce and SPAN Table

Nonce is only exchanged once during inclusion and is used to calculate subsequent SPANs in order to prevent replay attacks.

SPAN becomes out of sync if the message did not reach the destination. A new Nonce must then be requested to update the SPAN table.

As such; In order to decrypt a Z-Wave RF frame you need two things:

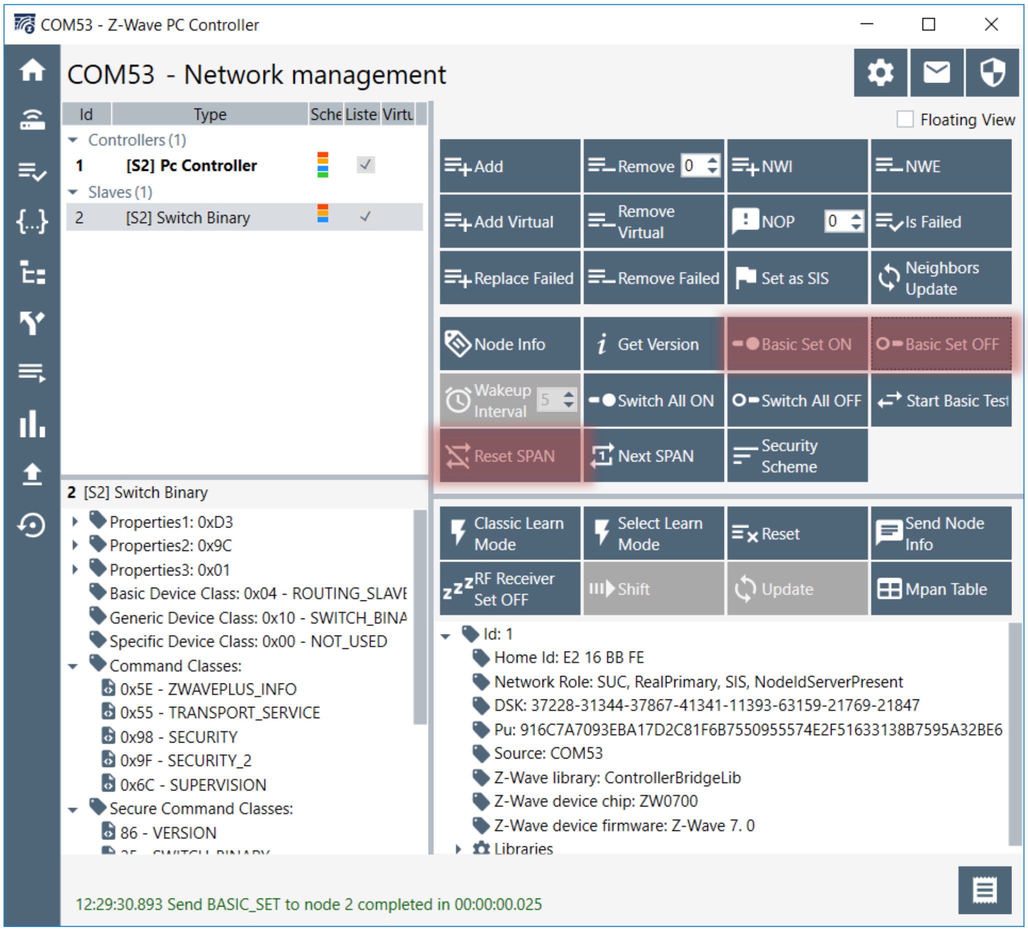
- The security keys for the network
- The Nonce key / SPAN table

This section will introduce how to add this information to the Zniffer so it can decrypt the individual frames.

> ***Hint*** More information on the key exchange can be found the Knowledge Base:
>
> Secure S2 key exchange methods during inclusion

If a trace was started during inclusion, the trace will already contain the Nonce key and thus be able to calculate the SPANs. However, in this exercise we have not the inclusion process in our Zniffer trace and therefore we must provide the Nonce key to the Zniffer.

- Make sure the Zniffer is still tracing as instructed in section 2.1.
- In the PC Controller, click on Reset SPAN.
- In the PC Controller, click on Basic Set ON. This will send a command to the device, which then triggers a reset of SPAN.
- In the PC Controller, click on Basic Set OFF to turn off the LED again.



2 [S2] Switch Binary

Properties1: 0xD3
Properties2: 0x9C
Properties3: 0x01
Basic Device Class: 0x04 - ROUTING_SLAVE
Generic Device Class: 0x10 - SWITCH_BINA
Specific Device Class: 0x00 - NOT_USED
Command Classes:
0x5E - ZWAVEPLUS_INFO
0x55 - TRANSPORT_SERVICE
0x98 - SECURITY
0x9F - SECURITY_2
0x6C - SUPERVISION
Secure Command Classes:
86 - VERSION

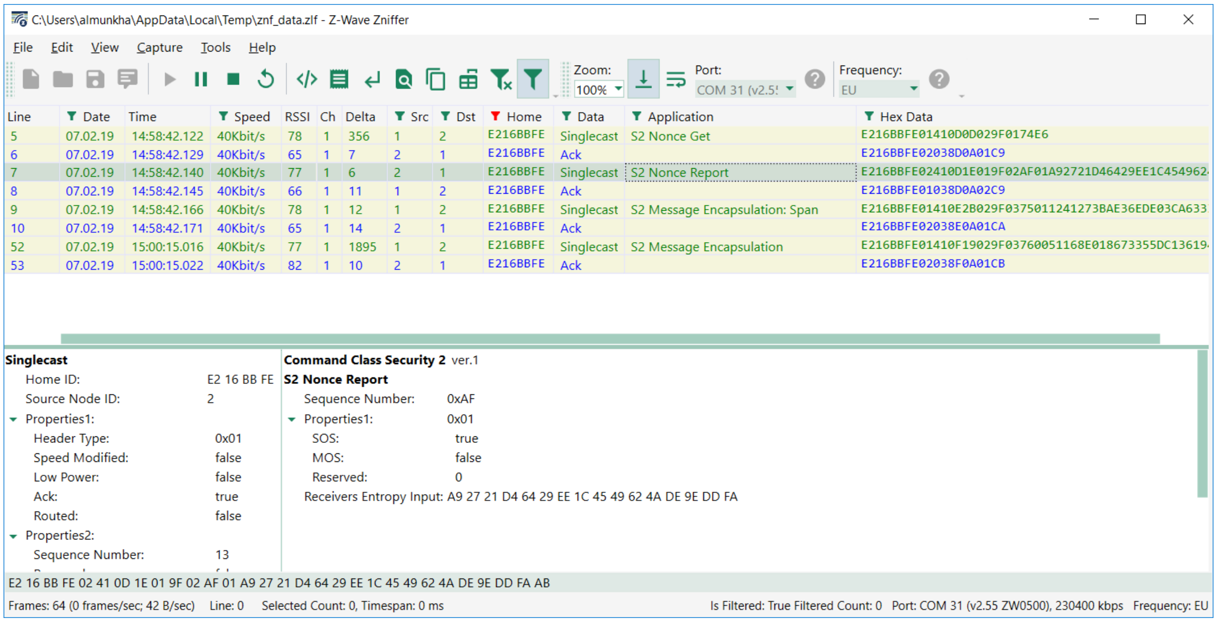
Id: 1
Home Id: E2 16 BB FE
Network Role: SUC, RealPrimary, SIS, NodeIdServerPresent
DSK: 37228-31344-37867-41341-11393-63159-21769-21847
Pu: 916C7A7093EBA17D2C81F6B7550955574E2F51633138B7595A32BE6
Source: COM53
Z-Wave library: ControllerBridgeLib
Z-Wave device chip: ZW0700
Z-Wave device firmware: Z-Wave 7. 0
Libraries

12:29:30.893 Send BASIC_SET to node 2 completed in 00:00:00.025

Figure 5: Reset SPAN in PC Controller

Return to the Zniffer tool and notice the following:

- A 'Nonce Get' and a response 'Nonce Report' is shown
- Some encrypted S2 Messages that we cannot yet decrypt.



C:\Users\almunkha\AppData\Local\Temp\znf_data.zlf - Z-Wave Zniffer

Line	Date	Time	Speed	RSSI	Ch	Delta	Src	Dst	Home	Data	Application	Hex Data
5	07.02.19	14:58:42.122	40Kbit/s	78	1	356	1	2	E216BBFE	Singlecast	S2 Nonce Get	E216BBFE01410D0D029F0174E6
6	07.02.19	14:58:42.129	40Kbit/s	65	1	7	2	1	E216BBFE	Ack		E216BBFE02038D0A01C9
7	07.02.19	14:58:42.140	40Kbit/s	77	1	6	2	1	E216BBFE	Singlecast	S2 Nonce Report	E216BBFE02410D1E019F02AF01A92721D46429EE1C454962
8	07.02.19	14:58:42.145	40Kbit/s	66	1	11	1	2	E216BBFE	Ack		E216BBFE01038D0A02C9
9	07.02.19	14:58:42.166	40Kbit/s	78	1	12	1	2	E216BBFE	Singlecast	S2 Message Encapsulation: Span	E216BBFE01410E2B029F0375011241273BAE36EDE03CA633
10	07.02.19	14:58:42.171	40Kbit/s	65	1	14	2	1	E216BBFE	Ack		E216BBFE02038E0A01CA
52	07.02.19	15:00:15.016	40Kbit/s	77	1	1895	1	2	E216BBFE	Singlecast	S2 Message Encapsulation	E216BBFE01410F19029F03760051168E018673355DC13619
53	07.02.19	15:00:15.022	40Kbit/s	82	1	10	2	1	E216BBFE	Ack		E216BBFE02038F0A01CB

```
Singlecast                                Command Class Security 2  ver.1
  Home ID:               E2 16 BB FE      S2 Nonce Report
  Source Node ID:        2                  Sequence Number:   0xAF
▾ Properties1:                            ▾ Properties1:       0x01
    Header Type:           0x01               SOS:               true
    Speed Modified:        false              MOS:               false
    Low Power:             false              Reserved:          0
    Ack:                   true             Receivers Entropy Input: A9 27 21 D4 64 29 EE 1C 45 49 62 4A DE 9E DD FA
    Routed:                false
▾ Properties2:
    Sequence Number:       13
```

```
E2 16 BB FE 02 41 0D 1E 01 9F 02 AF 01 A9 27 21 D4 64 29 EE 1C 45 49 62 4A DE 9E DD FA AB
```

Frames: 64 (0 frames/sec; 42 B/sec)   Line: 0   Selected Count: 0, Timespan: 0 ms   Is Filtered: True Filtered Count: 0   Port: COM 31 (v2.55 ZW0500), 230400 kbps   Frequency: EU

Figure 6: SPAN reset and encrypted S2 messages

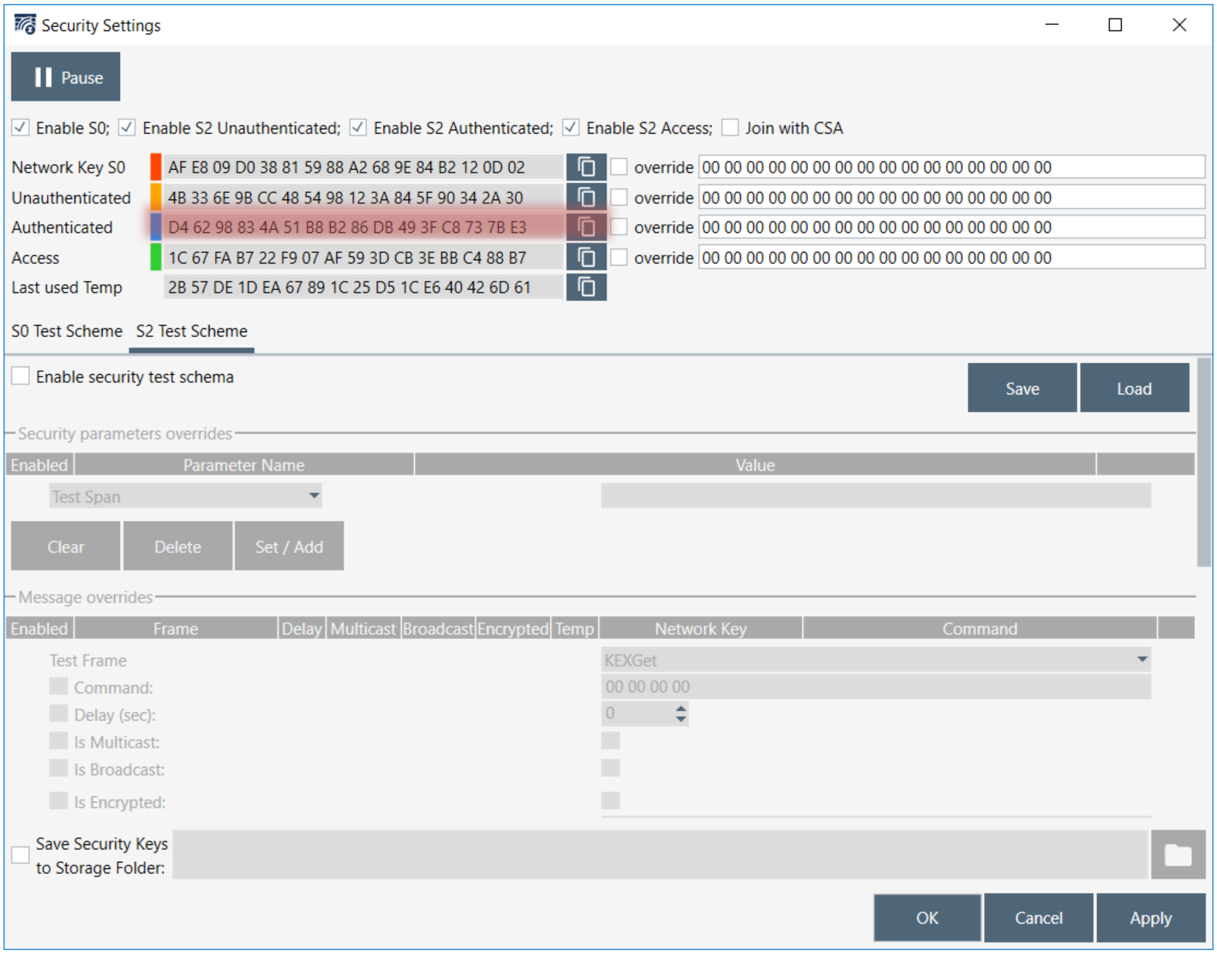
The frames we see in the Zniffer are still encrypted. We are still missing the network keys. Return to the PC Controller to find the needed network key.

- You can find the keys in the PC Controller by clicking on the icon 🛡 in the upper right corner.
- Network keys for all security groups are shown in the pop-up window, refer to Figure 7.
  - S0
  - S2 Unauthenticated
  - S2 Authenticated
  - S2 Access
- Since our device is included as S2 Authenticated using the DSK, we will be needed in S2 Authenticated key.
  - In Figure 7, the example key is: D4 62 98 83 4A 51 B8 B2 86 DB 49 3F C8 73 7B E3
- Click on the "Copy to Clipboard" ⧉.

Hint More information on the security groups can be found the Knowledge Bases:

[Is S2-AccessControl more secure than S2-Authenticated?]

[Why use S2-Unauthentucated?]



Security Settings

☑ Enable S0; ☑ Enable S2 Unauthenticated; ☑ Enable S2 Authenticated; ☑ Enable S2 Access; □ Join with CSA

Network Key S0	AF E8 09 D0 38 81 59 88 A2 68 9E 84 B2 12 0D 02	□ override	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Unauthenticated	4B 33 6E 9B CC 48 54 98 12 3A 84 5F 90 34 2A 30	□ override	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Authenticated	D4 62 98 83 4A 51 B8 B2 86 DB 49 3F C8 73 7B E3	□ override	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Access	1C 67 FA B7 22 F9 07 AF 59 3D CB 3E BB C4 88 B7	□ override	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Last used Temp	2B 57 DE 1D EA 67 89 1C 25 D5 1C E6 40 42 6D 61		

□ Enable security test schema

Security parameters overrides

Enabled	Parameter Name	Value
	Test Span	

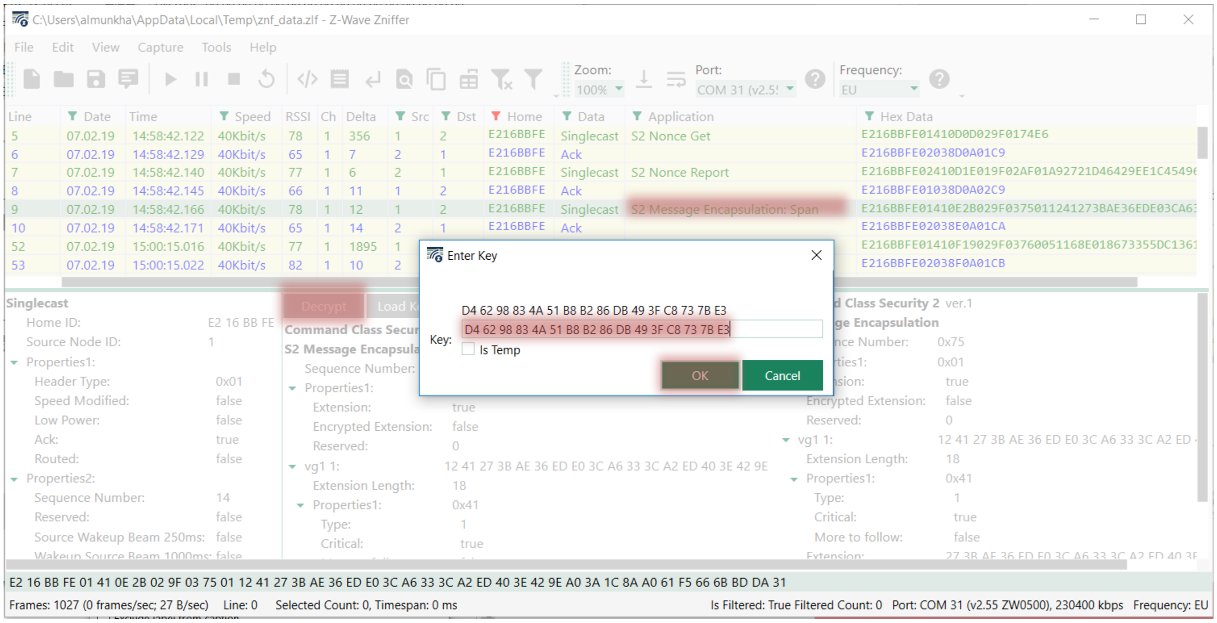
Message overrides

Enabled	Frame	Delay	Multicast	Broadcast	Encrypted	Temp	Network Key	Command

Test Frame	KEXGet
□ Command:	00 00 00 00
□ Delay (sec):	0
□ Is Multicast:	□
□ Is Broadcast:	□
□ Is Encrypted:	□

□ Save Security Keys to Storage Folder:

Figure 7: Network settings found in PC Controller



C:\Users\almunkha\AppData\Local\Temp\znf_data.zlf - Z-Wave Zniffer

Zoom: 100%   Port: COM 31 (v2.5!   Frequency: EU

Line	Date	Time	Speed	RSSI	Ch	Delta	Src	Dst	Home	Data	Application	Hex Data
5	07.02.19	14:58:42.122	40Kbit/s	78	1	356	1	2	E216BBFE	Singlecast	S2 Nonce Get	E216BBFE01410D0D029F0174E6
6	07.02.19	14:58:42.129	40Kbit/s	65	1	7	2	1	E216BBFE	Ack		E216BBFE02038D0A01C9
7	07.02.19	14:58:42.140	40Kbit/s	77	1	6	2	1	E216BBFE	Singlecast	S2 Nonce Report	E216BBFE02410D1E019F02AF01A92721D46429EE1C4549
8	07.02.19	14:58:42.145	40Kbit/s	66	1	11	1	2	E216BBFE	Ack		E216BBFE01038D0A02C9
9	07.02.19	14:58:42.166	40Kbit/s	78	1	12	1	2	E216BBFE	Singlecast	S2 Message Encapsulation: Span	E216BBFE01410E2B029F0375011241273BAE36EDE03CA6
10	07.02.19	14:58:42.171	40Kbit/s	65	1	14	2	1	E216BBFE	Ack		E216BBFE02038E0A01CA
52	07.02.19	15:00:15.016	40Kbit/s	77	1	1895	1					E216BBFE01410F19029F03760051168E018673355DC136
53	07.02.19	15:00:15.022	40Kbit/s	82	1	10	2					E216BBFE02038F0A01CB

Singlecast

Home ID:	E2 16 BB FE
Source Node ID:	1
Properties1:	
Header Type:	0x01
Speed Modified:	false
Low Power:	false
Ack:	true
Routed:	false
Properties2:	
Sequence Number:	14
Reserved:	false
Source Wakeup Beam 250ms:	false
Wakeup Source Beam 1000ms:	false

Command Class Secur

S2 Message Encapsula

Sequence Number:	
Properties1:	
Extension:	true
Encrypted Extension:	false
Reserved:	0
vg1 1:	12 41 27 3B AE 36 ED E0 3C A6 33 3C A2 ED 40 3E 42 9E
Extension Length:	18
Properties1:	0x41
Type:	1
Critical:	true

d Class Security 2 ver.1

ge Encapsulation

nce Number:	0x75
rties1:	0x01
nsion:	true
Encrypted Extension:	false
Reserved:	0
vg1 1:	12 41 27 3B AE 36 ED E0 3C A6 33 3C A2 ED
Extension Length:	18
Properties1:	0x41
Type:	1
Critical:	true
More to follow:	false
Extension:	27 3B AE 36 ED E0 3C A6 33 3C A2 ED 40 3E

Enter Key

D4 62 98 83 4A 51 B8 B2 86 DB 49 3F C8 73 7B E3

Key: D4 62 98 83 4A 51 B8 B2 86 DB 49 3F C8 73 7B E3

□ Is Temp

E2 16 BB FE 01 41 0E 2B 02 9F 03 75 01 12 41 27 3B AE 36 ED E0 3C A6 33 3C A2 ED 40 3E 42 9E A0 3A 1C 8A A0 61 F5 66 6B BD DA 31

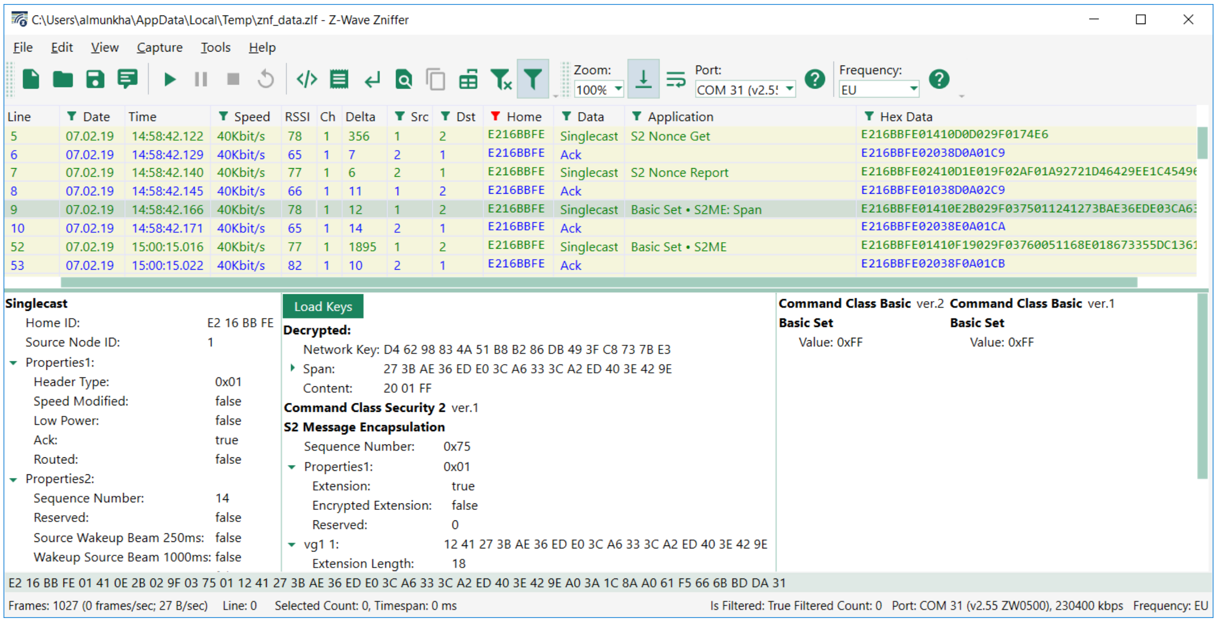
Frames: 1027 (0 frames/sec; 27 B/sec)   Line: 0   Selected Count: 0, Timespan: 0 ms   Is Filtered: True Filtered Count: 0   Port: COM 31 (v2.55 ZW0500), 230400 kbps   Frequency: EU

Figure 8: Enter network key in Zniffer

When the key is known, it is time to decrypt the traffic using the Zniffer.

- Click on a S2 Message, refer to Figure 8.
- Click on "Decrypt"
- Paste the network key.
- Click "OK"

With the SPAN synchronization and the network key, the Zniffer can now decrypt the S2 messages.



Line	Date	Time	Speed	RSSI	Ch	Delta	Src	Dst	Home	Data	Application	Hex Data
5	07.02.19	14:58:42.122	40Kbit/s	78	1	356	1	2	E216BBFE	Singlecast	S2 Nonce Get	E216BBFE01410D0D029F0174E6
6	07.02.19	14:58:42.129	40Kbit/s	65	1	7	2	1	E216BBFE	Ack		E216BBFE02038D0A01C9
7	07.02.19	14:58:42.140	40Kbit/s	77	1	6	2	1	E216BBFE	Singlecast	S2 Nonce Report	E216BBFE02410D1E019F02AF01A92721D46429EE1C4549
8	07.02.19	14:58:42.145	40Kbit/s	66	1	11	1	2	E216BBFE	Ack		E216BBFE01038D0A02C9
9	07.02.19	14:58:42.166	40Kbit/s	78	1	12	1	2	E216BBFE	Singlecast	Basic Set • S2ME: Span	E216BBFE01410E2B029F0375011241273BAE36EDE03CA6
10	07.02.19	14:58:42.171	40Kbit/s	65	1	14	2	1	E216BBFE	Ack		E216BBFE02038E0A01CA
52	07.02.19	15:00:15.016	40Kbit/s	77	1	1895	1	2	E216BBFE	Singlecast	Basic Set • S2ME	E216BBFE01410F19029F03760051168E018673355DC136
53	07.02.19	15:00:15.022	40Kbit/s	82	1	10	2	1	E216BBFE	Ack		E216BBFE02038F0A01CB

```
Singlecast
   Home ID:                      E2 16 BB FE
   Source Node ID:               1
 ▾ Properties1:
     Header Type:                0x01
     Speed Modified:             false
     Low Power:                  false
     Ack:                        true
     Routed:                     false
 ▾ Properties2:
     Sequence Number:            14
     Reserved:                   false
     Source Wakeup Beam 250ms:   false
     Wakeup Source Beam 1000ms:  false
```

```
Decrypted:
   Network Key: D4 62 98 83 4A 51 B8 B2 86 DB 49 3F C8 73 7B E3
 ▸ Span:        27 3B AE 36 ED E0 3C A6 33 3C A2 ED 40 3E 42 9E
   Content:     20 01 FF
Command Class Security 2 ver.1
S2 Message Encapsulation
   Sequence Number:      0x75
 ▾ Properties1:          0x01
     Extension:           true
     Encrypted Extension: false
     Reserved:            0
 ▾ vg1 1:                12 41 27 3B AE 36 ED E0 3C A6 33 3C A2 ED 40 3E 42 9E
     Extension Length:    18
```

```
Command Class Basic ver.2   Command Class Basic ver.1
Basic Set                   Basic Set
   Value: 0xFF                 Value: 0xFF
```

```
E2 16 BB FE 01 41 0E 2B 02 9F 03 75 01 12 41 27 3B AE 36 ED E0 3C A6 33 3C A2 ED 40 3E 42 9E A0 3A 1C 8A A0 61 F5 66 6B BD DA 31
```

```
Frames: 1027 (0 frames/sec; 27 B/sec)   Line: 0   Selected Count: 0, Timespan: 0 ms   Is Filtered: True Filtered Count: 0   Port: COM 31 (v2.55 ZW0500), 230400 kbps   Frequency: EU
```

Figure 9: Messages are now decrypted using the Zniffer

Notice how the 2 frames contains a Command Class called "Basic", with command "Basic Set" and values "0xFF" (ON) and "0x00" (OFF).

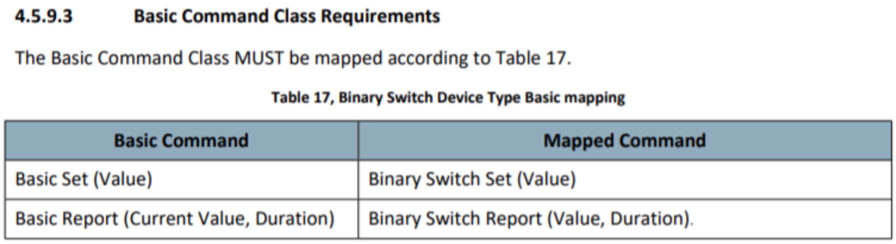
Hint More information on the decrypting Z-Wave frames using the Zniffer be found the Knowledge Base:

Decrypt S2 frames in Zniffer trace

2.3 Using Command Class Binary Switch

When you send a Basic Set Command to the Switch On / Off, it is being mapped to the Binary Switch Command Class by the device. This is a requirement in the Z-Wave Specification for a Device Type of type “Binary Switch”.

Refer to Z-Wave specification SDS14224 Z-Wave Plus v2 Device Type Specification.



4.5.9.3 Basic Command Class Requirements

The Basic Command Class MUST be mapped according to Table 17.

Table 17, Binary Switch Device Type Basic mapping

Basic Command	Mapped Command
Basic Set (Value)	Binary Switch Set (Value)
Basic Report (Current Value, Duration)	Binary Switch Report (Value, Duration).

Figure 10: Basic mapping for device type Binary Switch

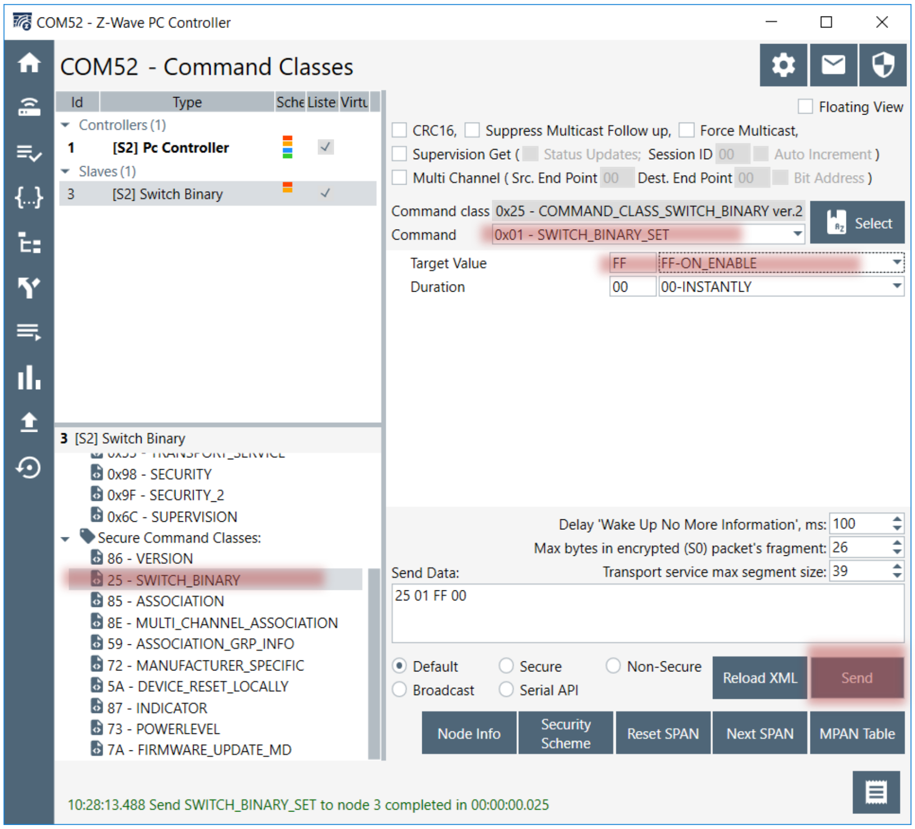
The reason for this requirement is to ensure all Z-Wave controllers can do basic communication with all Z-Wave devices.

In this section, we will try to turn the LED ON and OFF using the Binary Switch command class.

- In the PC Controller, double click on “25 – SWITCH_BINARY” under secure Command Classes in the lower left corner.
- This opens the “Command Classes” view in the PC Controller and selects the Switch Binary Command class.

- Set the Command to “0x01 – SWITCH_BINARY_SET”
- Set the “Target Value” to “FF-ON_ENABLE”
- Click “Send”.

- Set the “Target Value” to “00-OFF_DISABLE”
- Click “Send”.



COM52 - Z-Wave PC Controller

COM52 - Command Classes

Id	Type	Sche	Liste	Virtu
Controllers (1)				
1	[S2] Pc Controller		✓	
Slaves (1)				
3	[S2] Switch Binary		✓	

3 [S2] Switch Binary

- 0x98 - SECURITY
- 0x9F - SECURITY_2
- 0x6C - SUPERVISION
- Secure Command Classes:
  - 86 - VERSION
  - 25 - SWITCH_BINARY
  - 85 - ASSOCIATION
  - 8E - MULTI_CHANNEL_ASSOCIATION
  - 59 - ASSOCIATION_GRP_INFO
  - 72 - MANUFACTURER_SPECIFIC
  - 5A - DEVICE_RESET_LOCALLY
  - 87 - INDICATOR
  - 73 - POWERLEVEL
  - 7A - FIRMWARE_UPDATE_MD

□ Floating View

□ CRC16, □ Suppress Multicast Follow up, □ Force Multicast,
□ Supervision Get (□ Status Updates; Session ID 00 □ Auto Increment)
□ Multi Channel (Src. End Point 00 Dest. End Point 00 □ Bit Address)

Command class 0x25 - COMMAND_CLASS_SWITCH_BINARY ver.2
Command 0x01 - SWITCH_BINARY_SET
Target Value FF FF-ON_ENABLE
Duration 00 00-INSTANTLY

Delay 'Wake Up No More Information', ms: 100
Max bytes in encrypted (S0) packet's fragment: 26
Transport service max segment size: 39

Send Data:
25 01 FF 00

● Default ○ Secure ○ Non-Secure
○ Broadcast ○ Serial API

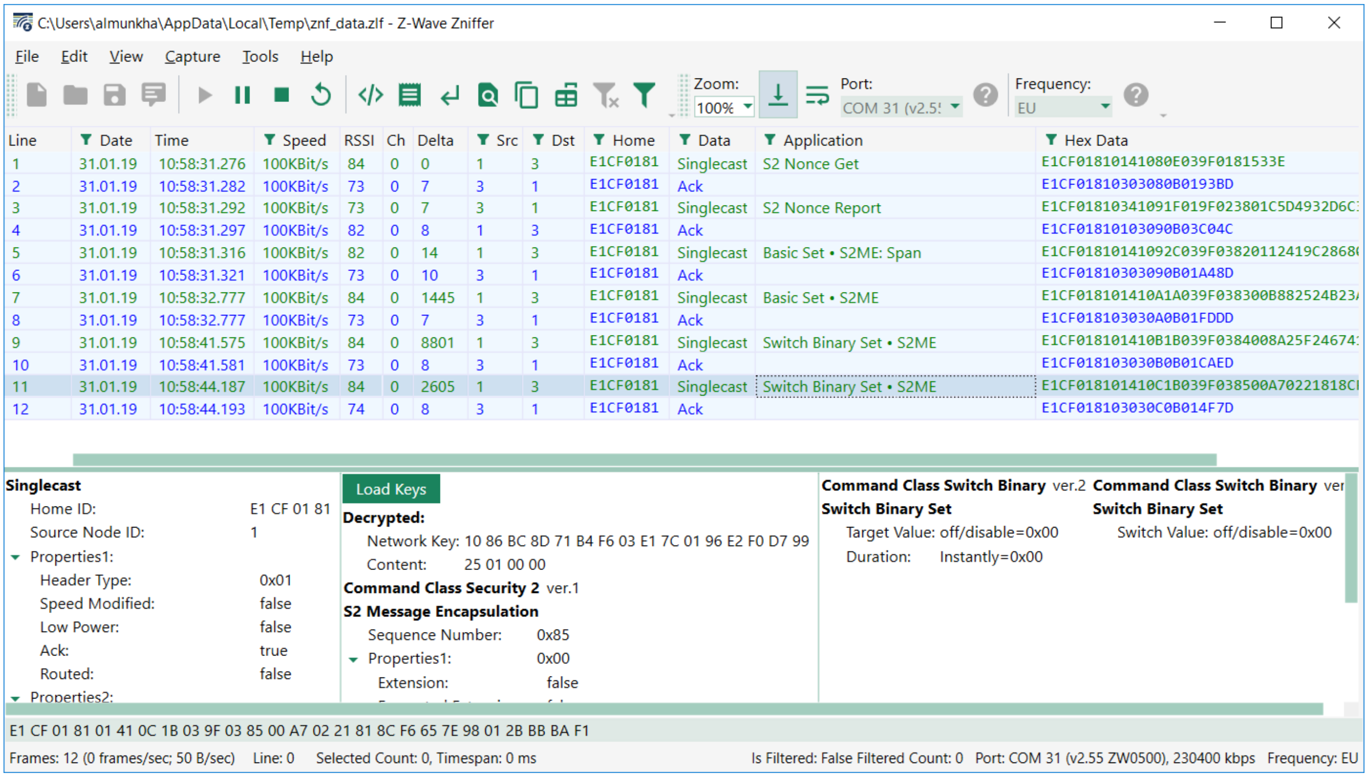
10:28:13.488 Send SWITCH_BINARY_SET to node 3 completed in 00:00:00.025

Figure 11: Command Class View in PC Controller

2.4 Capture RF packages using the Zniffer: Binary Switch Set

Now that we have learned how to send a Binary Switch Set, let's trace the RF communication again to understand which frames are being sent.

- Return to Z-Wave Zniffer tool, which should have been running in the background.
- The trace now contains a Nonce resync, 2 Basic Set frames and 2 Binary Switch Set frames.



Line	Date	Time	Speed	RSSI	Ch	Delta	Src	Dst	Home	Data	Application	Hex Data
1	31.01.19	10:58:31.276	100KBit/s	84	0	0	1	3	E1CF0181	Singlecast	S2 Nonce Get	E1CF01810141080E039F0181533E
2	31.01.19	10:58:31.282	100KBit/s	73	0	7	3	1	E1CF0181	Ack		E1CF01810303080B0193BD
3	31.01.19	10:58:31.292	100KBit/s	73	0	7	3	1	E1CF0181	Singlecast	S2 Nonce Report	E1CF01810341091F019F023801C5D4932D6C
4	31.01.19	10:58:31.297	100KBit/s	82	0	8	1	3	E1CF0181	Ack		E1CF01810103090B03C04C
5	31.01.19	10:58:31.316	100KBit/s	82	0	14	1	3	E1CF0181	Singlecast	Basic Set • S2ME: Span	E1CF01810141092C039F03820112419C2868
6	31.01.19	10:58:31.321	100KBit/s	73	0	10	3	1	E1CF0181	Ack		E1CF01810303090B01A48D
7	31.01.19	10:58:32.777	100KBit/s	84	0	1445	1	3	E1CF0181	Singlecast	Basic Set • S2ME	E1CF018101410A1A039F038300B882524B23
8	31.01.19	10:58:32.777	100KBit/s	73	0	7	3	1	E1CF0181	Ack		E1CF018103030A0B01FDDD
9	31.01.19	10:58:41.575	100KBit/s	84	0	8801	1	3	E1CF0181	Singlecast	Switch Binary Set • S2ME	E1CF018101410B1B039F0384008A25F24674
10	31.01.19	10:58:41.581	100KBit/s	73	0	8	3	1	E1CF0181	Ack		E1CF018103030B0B01CAED
11	31.01.19	10:58:44.187	100KBit/s	84	0	2605	1	3	E1CF0181	Singlecast	Switch Binary Set • S2ME	E1CF018101410C1B039F038500A70221818C
12	31.01.19	10:58:44.193	100KBit/s	74	0	8	3	1	E1CF0181	Ack		E1CF018103030C0B014F7D

Singlecast

Home ID:	E1 CF 01 81
Source Node ID:	1
Properties1:	
Header Type:	0x01
Speed Modified:	false
Low Power:	false
Ack:	true
Routed:	false
Properties2:	

Decrypted:

Network Key: 10 86 BC 8D 71 B4 F6 03 E1 7C 01 96 E2 F0 D7 99

Content: 25 01 00 00

Command Class Security 2 ver.1

S2 Message Encapsulation

Sequence Number:	0x85
Properties1:	0x00
Extension:	false

Command Class Switch Binary ver.2

Switch Binary Set

Target Value: off/disable=0x00

Duration: Instantly=0x00

Command Class Switch Binary ver

Switch Binary Set

Switch Value: off/disable=0x00

E1 CF 01 81 01 41 0C 1B 03 9F 03 85 00 A7 02 21 81 8C F6 65 7E 98 01 2B BB BA F1

Frames: 12 (0 frames/sec; 50 B/sec) Line: 0 Selected Count: 0, Timespan: 0 ms Is Filtered: False Filtered Count: 0 Port: COM 31 (v2.55 ZW0500), 230400 kbps Frequency: EU

Figure 12: Zniffer trace containing Basic Set and Binary Switch Set command class

Notice how to Zniffer shows the command class used to transfer data between the PC Controller and the device.

Now try to send a "Switch Binary Get" from the PC Controller, and see the response in the Zniffer.

- What does the response show?

This concludes the tutorial in how to trace and decrypt Z-Wave RF traffic using the Zniffer tool.