Howdy y'all,

This is a slide deck intended for performance in front of a live audience. It is not--and cannot be--appropriate for reading at the same time. Only Dan Geer is good enough for that, and we can't yet preach as well as he does.

So if you want to learn these techniques, please read the fucking papers that we cite. Read PoC||GTFO, read WOOT, and read our technical reports. Looking at a slide show just ain't enough.

73 from Austin,
--Travis

PHY 802.15.4

TRAVIS GOODSPEED, SERGEY BRATUS

DEMISTIPHY 802.15.4

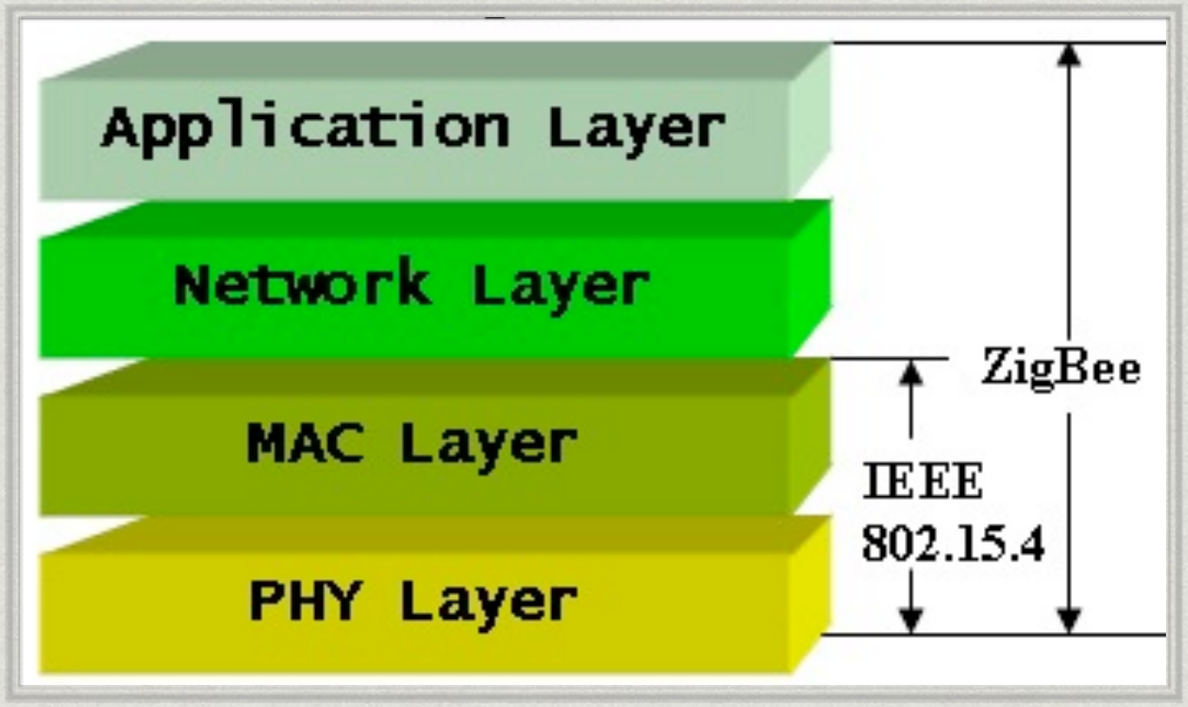
TRAVIS GOODSPEED, SERGEY BRATUS

KNOWING THE PHY
WELCOME TO BABYLON

Wright's Principle

"Security won't get better until tools for **practical exploration of the attack surface** are made available"

--Joshua Wright, 2011
Toorcon KillerBee talk



Scapy dot15d4

Octets: 2	1	4/10	0/5/6/10/14	2	variable	variable	variable	2
Frame Control	Sequence Number	Addressing fields	Auxiliary Security Header	Superframe Specification	GTS fields (Figure 45)	Pending address fields (Figure 46)	Beacon Payload	FCS
MHR				MAC Payload				MFR

Scapy dot15d4

Bit: 0–2	3–4	5–7
Security Level	Key Identifier Mode	Reserved

Bits: 0–3	4-7	8-11	12	13	14	15
Beacon Order	Superframe Order	Final CAP Slot	Battery Life Extension (BLE	Reserved	PAN Coordinator	Association Permit

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	Ack. Request	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

Octets: 1	4	0/1/5/9
Security Control	Frame Counter	Key Identifier

Octets: 2	1	4/10	0/5/6/10/14	2	variable	variable	variable	2
Frame Control	Sequence Number	Addressing fields	Auxiliary Security Header	Superframe Specification	GTS fields (Figure 45)	Pending address fields (Figure 46)	Beacon Payload	FCS
				MAC Payload				MFR

0/2	0/2/8	0/2	0/2/8
Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address

Octets: 1	0/1	variable
GTS Specification	GTS Directions	GTS List

Octets: 1	variable
Pending Address Specification	Address List

Bits: 0-2	3-6	7
GTS Descriptor Count	Reserved	GTS Permit

Bits: 0-6	7
GTS Directions Mask	Reserved

Bits: 0-15	16-19	20-23
Device Short Address	GTS Starting Slot	GTS Length

Bits: 0-2	3	4-6	7
Number of Short Addresses Pending	Reserved	Number of Extended Addresses Pending	Reserved

Scapy dot15d4

Bit: 0–2	3–4	5–7
Security Level	Key Identifier Mode	Reserved

Bits: 0–3	4-7	8-11	12	13	14	15
Beacon Order	Superframe Order	Final CAP Slot	Battery Life Extension (BLE)	Reserved	PAN Coordinator	Association Permit

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	Ack. Request	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

Octets: 1	4	0/1/5/9
Security Control	Frame Counter	Key Identifier

Octets: 2	1	4/10	0/2/6/10/14	2	variable	variable	variable	2
Frame Control	Sequence Number	Addressing fields	Auxiliary Security Header	Superframe Specification	GTS fields (Figure 45)	Pending address fields (Figure 46)	Beacon Payload	FCS
				MAC Payload				MFR

0/2	0/2/8	0/2	0/2/8
Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address

Octets: 1	0/1	variable
GTS Specification	GTS Directions	GTS List

Octets: 1	variable
Pending Address Specification	Address List

Bits: 0-2	3-6	7
GTS Descriptor Count	Reserved	GTS Permit

Bits: 0-6	7
GTS Directions Mask	Reserved

Bits: 0-15	16-19	20-23
Device Short Address	GTS Starting Slot	GTS Length

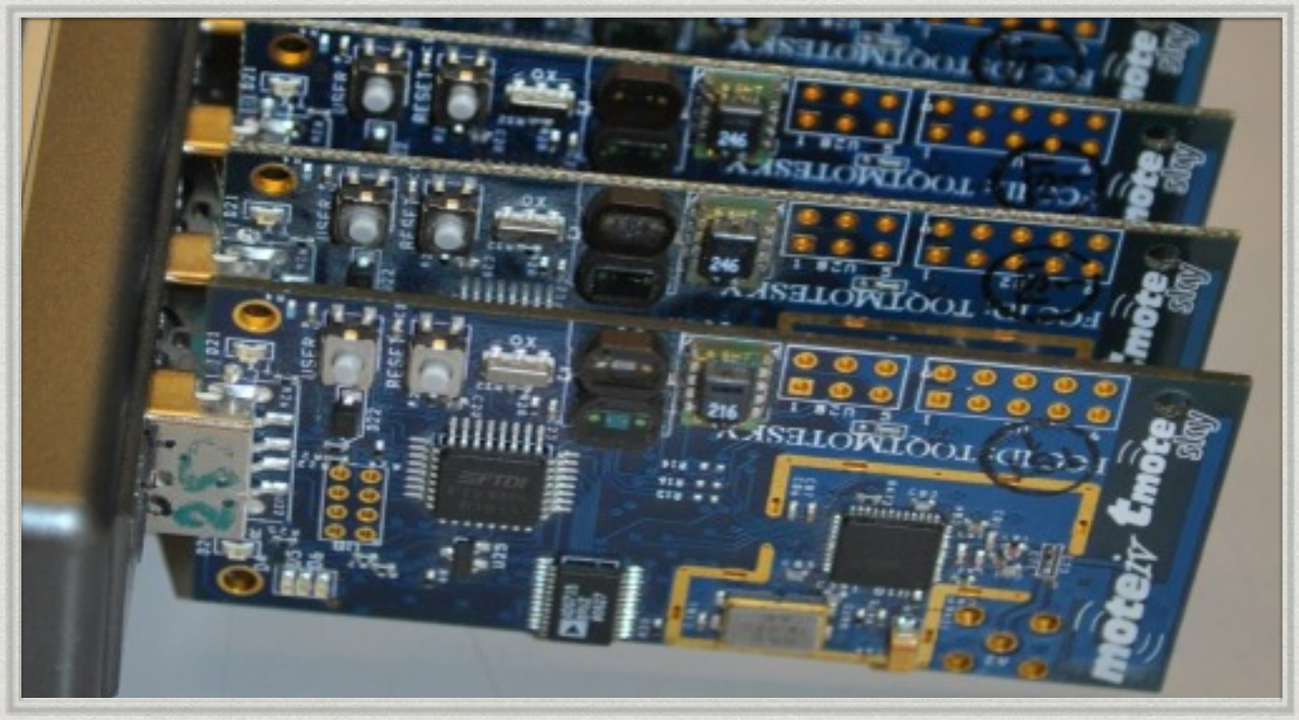
Bits: 0-2	3	4-6	7
Number of Short Addresses Pending	Reserved	Number of Extended Addresses Pending	Reserved

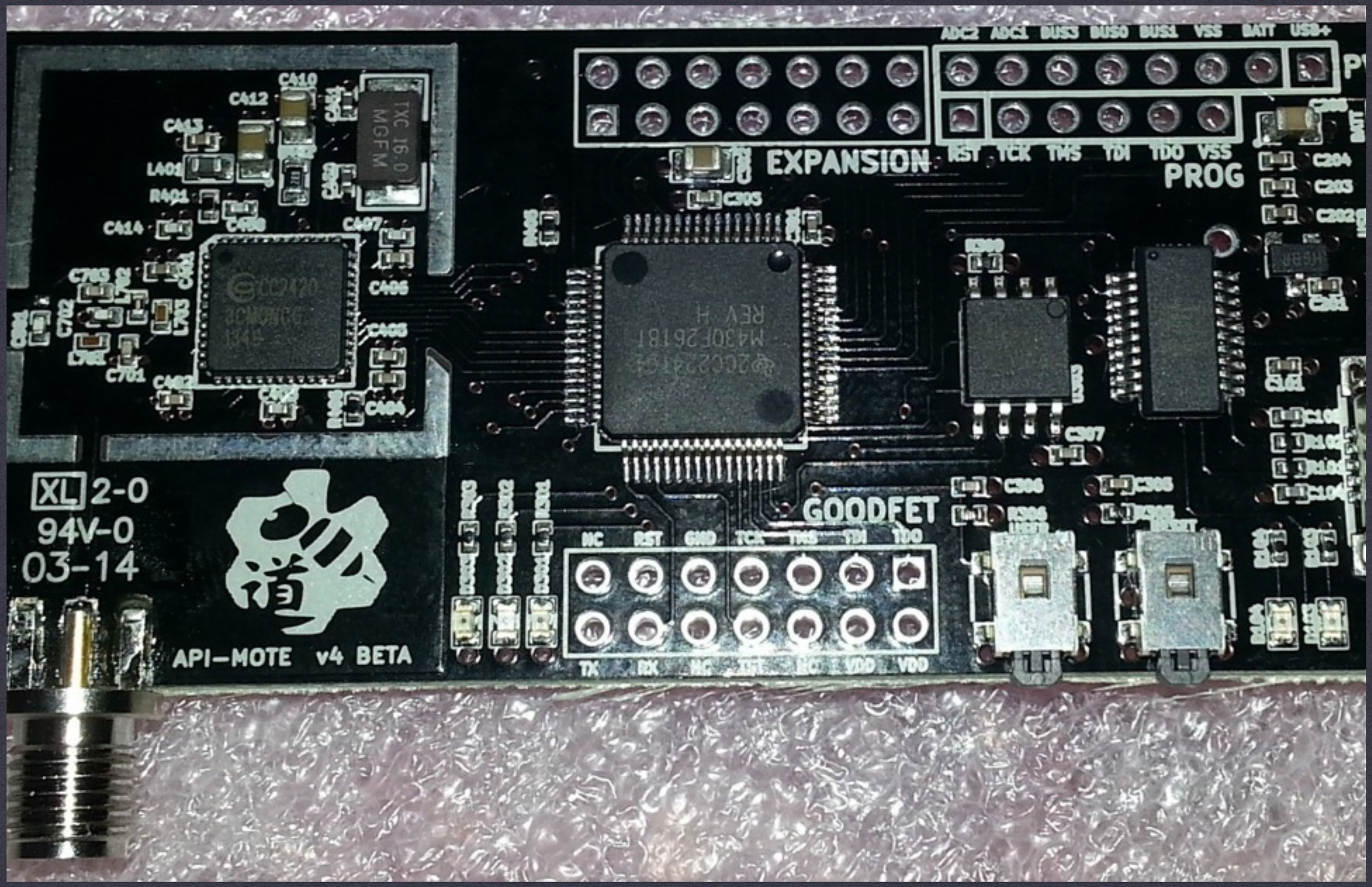
Hardware:

- existing hardware
  - **Atmel RZUSBTICK**
  - **Freakduino Chibi**
  - Zena Packet Analyzer
  - Sewio Open Sniffer
  - **Tmote Sky/TelosB**
  - ~~SDRs: USRP/etc~~

Hardware:

- existing hardware
  - **Atmel RZUSBTICK**
  - **Freakduino Chibi**
  - Zena Packet Analyzer
  - Sewio Open Sniffer
  - **Tmote Sky/TelosB**
  - ~~SDRs: USRP/etc~~



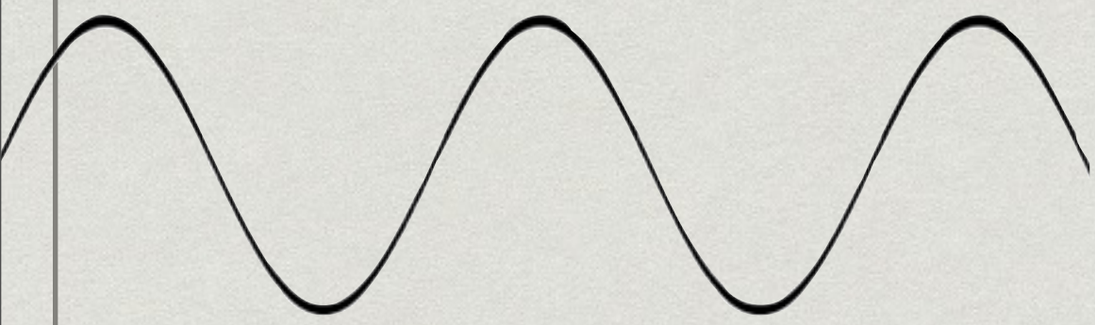


APIMOTE V4 BETA

PCB FRONT

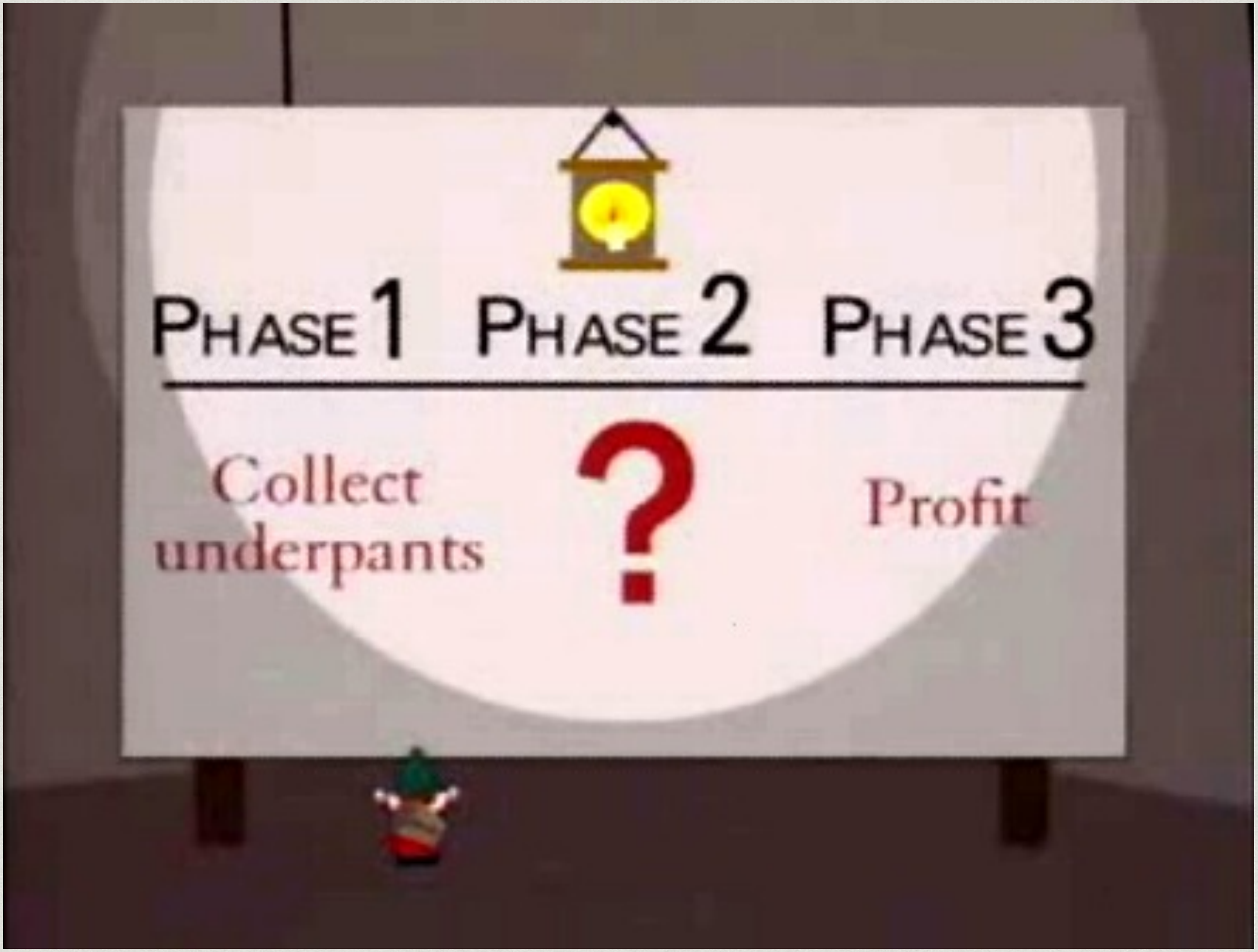
RIVER LOOP SECURITY

Fairy tales of PHY

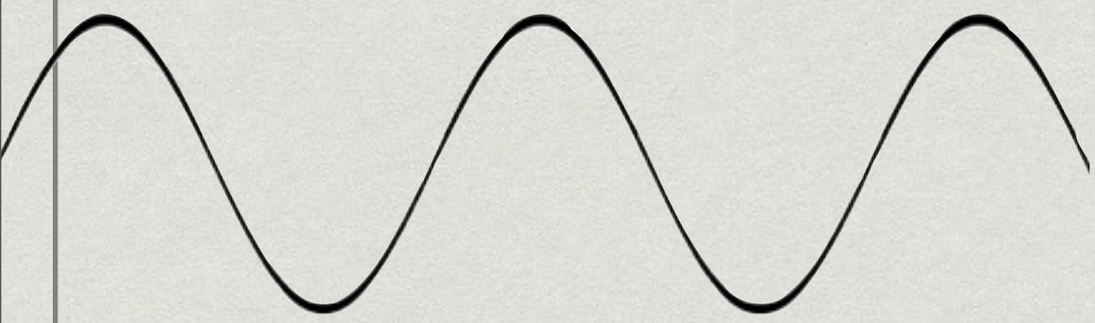


Bytes: 2	1	0 to 20	n	2
Frame Control Field (FCF)	Data Sequence Number	Address Information	Frame payload	Frame Check Sequence (FCS)

1. Receive RF waves
2. ...
3. Get an LNK Frame!


PHASE 1
PHASE 2
PHASE 3
Collect underpants
?
Profit

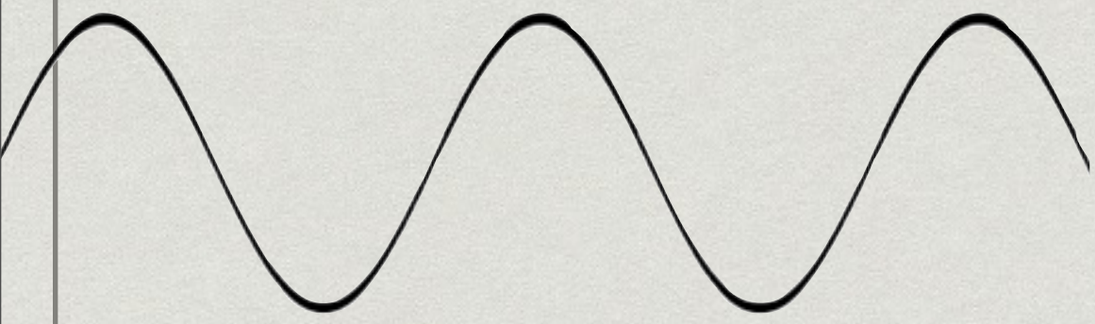
Fairy tales of PHY



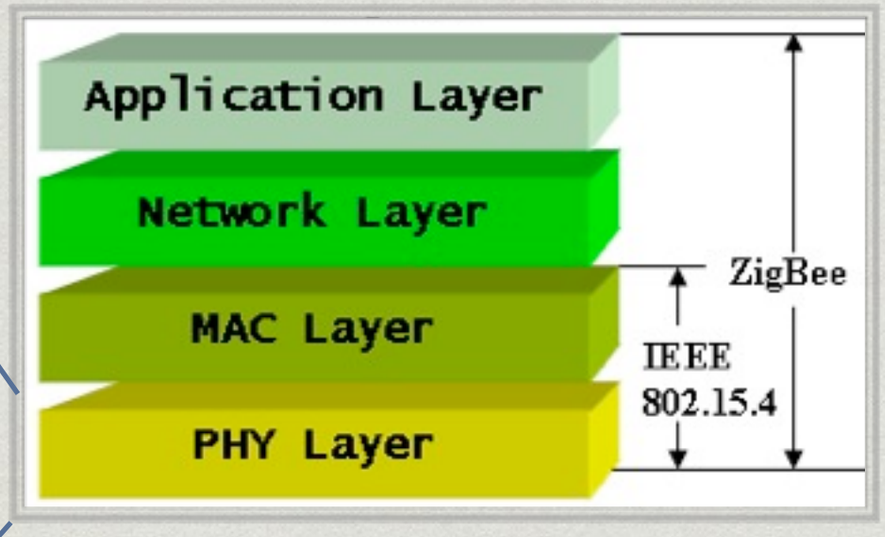
FC	Seq.No	Addr Info	$$$	FCS

1. Receive RF waves
2. ...
3. Get an LNK Frame!

Fairy tales of PHY



The Layer Cake is a PHY!



802.15.4 frame (PHY+LNK)

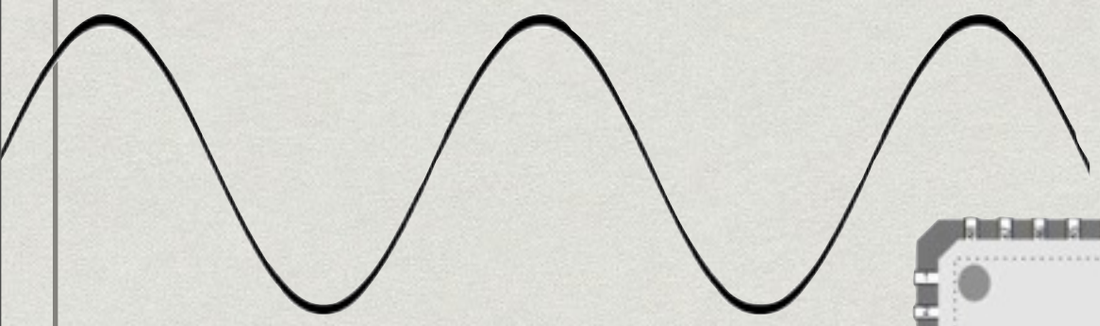
Length

```
00 00 00 00 a7 0f 01 08 82 ff ff ff ff ...
```

Preamble Sync Body

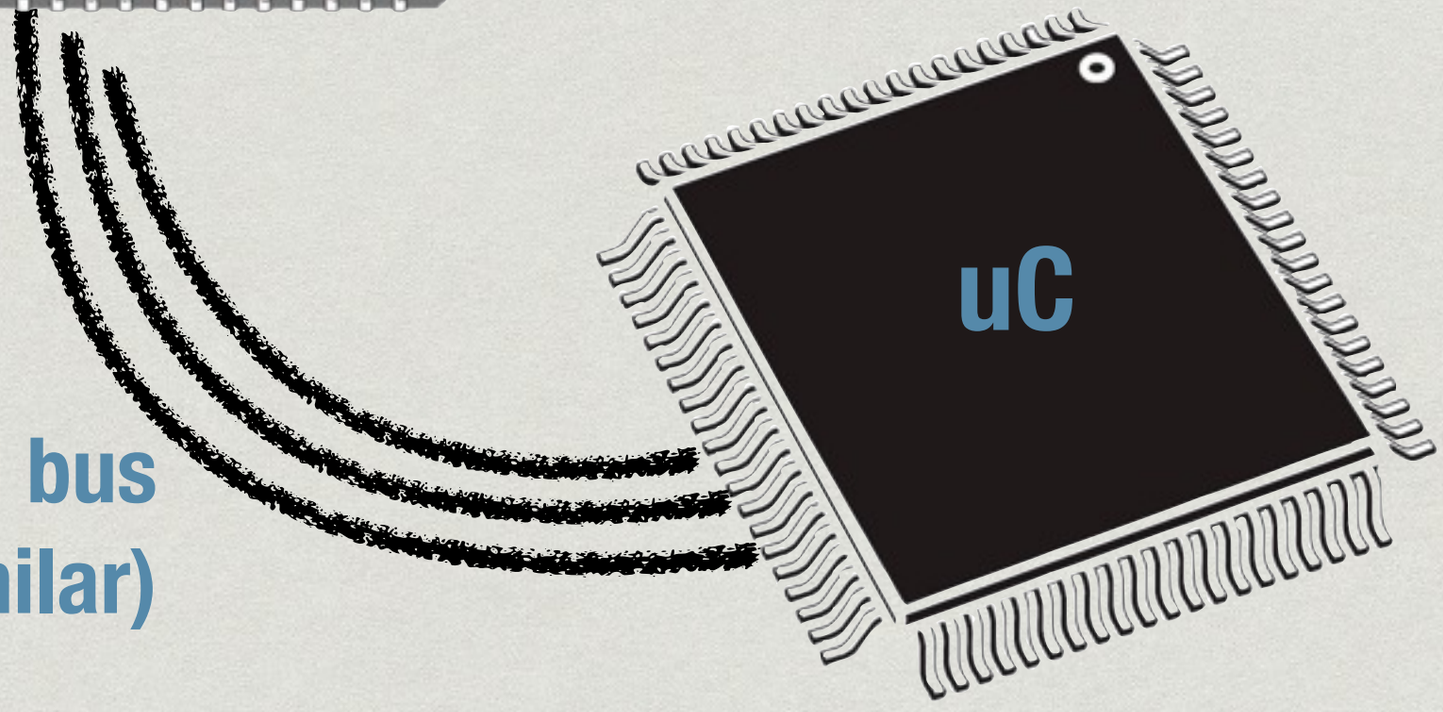
Octets: 2	1	(see 7.2.2.4.1)	1	variable	2
Frame control	Sequence number	Addressing fields	Command frame identifier	Command payload	FCS
MHR			MAC payload		MFR

how a frame is received



symbols
2.4 GHz
(or 868/915/etc MHz)

bytes or frames



SPI bus
(or similar)

diving into the PHY layer

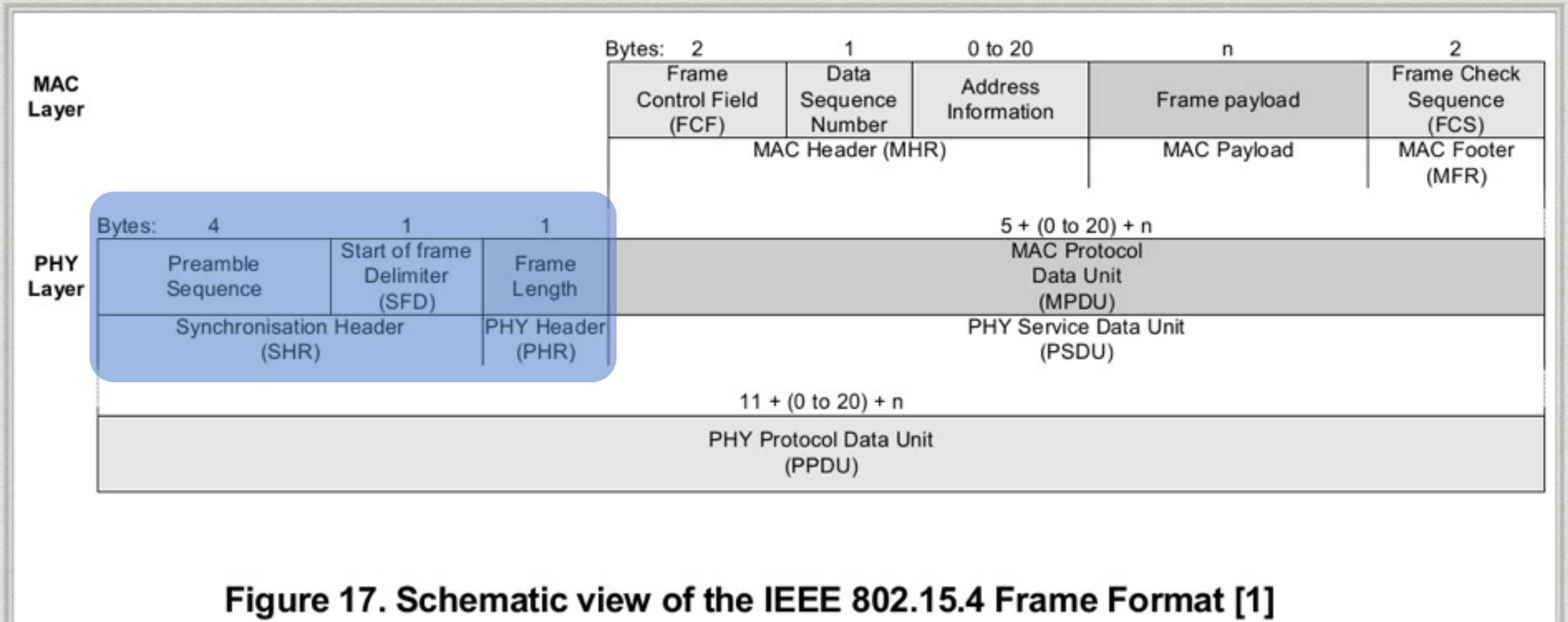
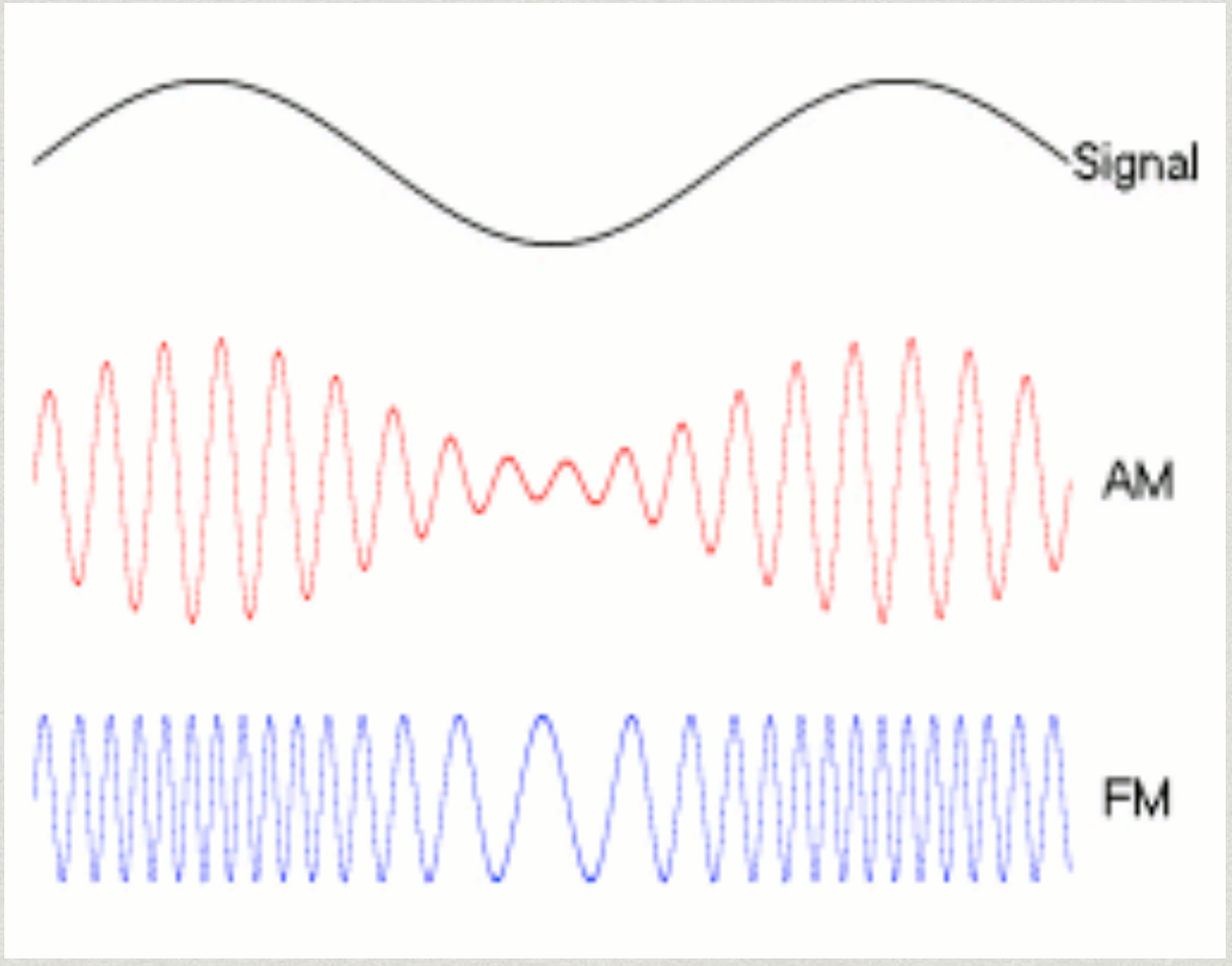
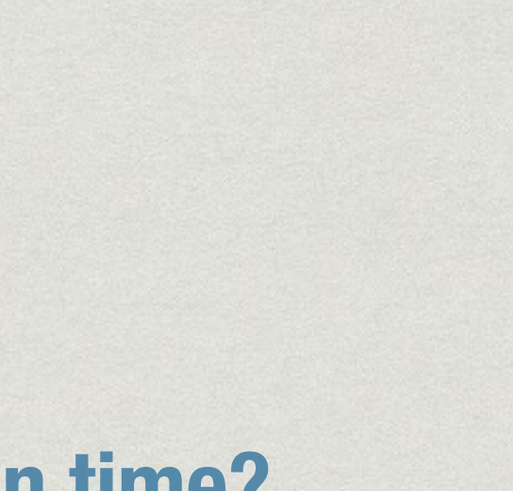


Figure 17. Schematic view of the IEEE 802.15.4 Frame Format [1]

Why Preamble?

Forget sending data -- can you even agree on time?

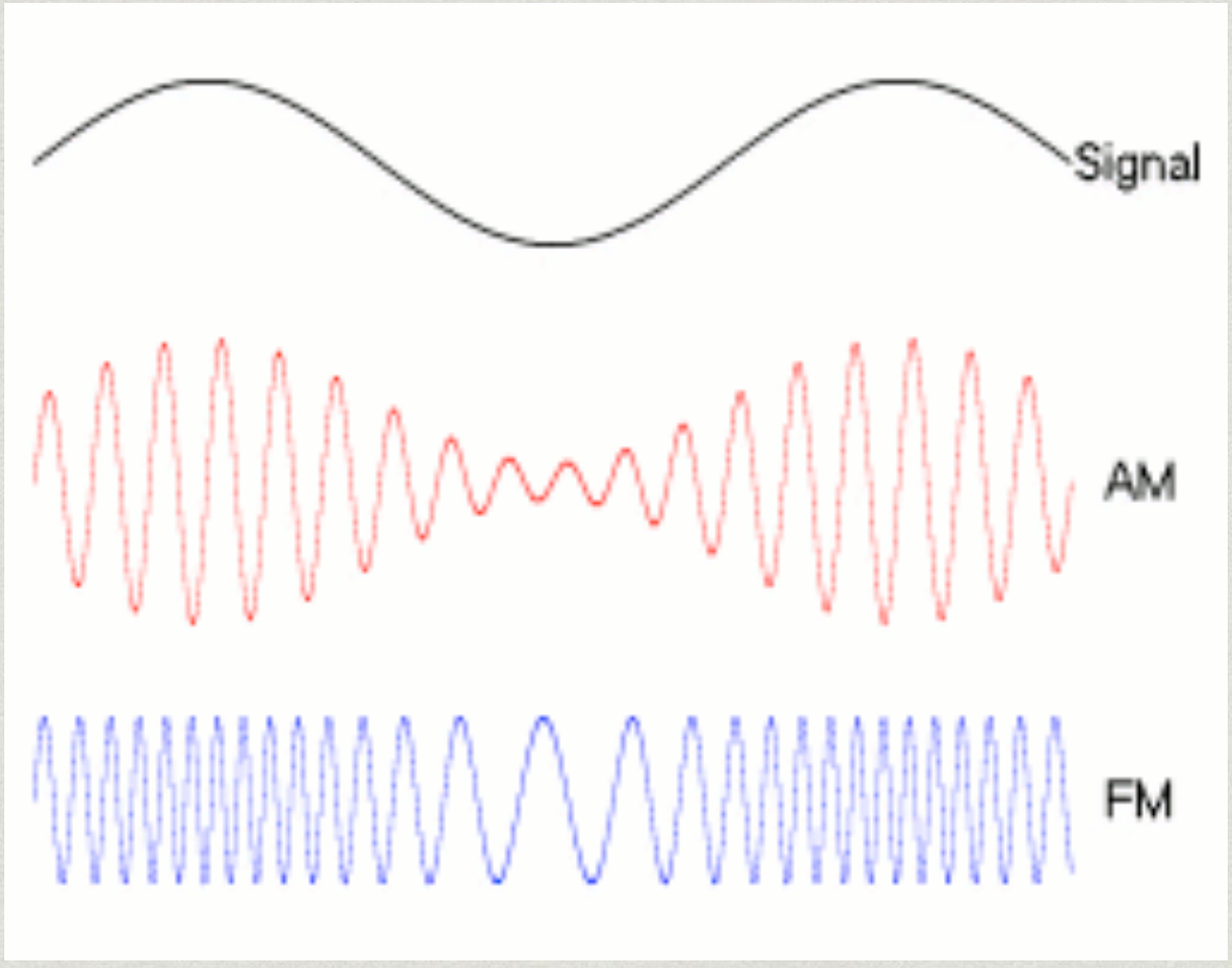


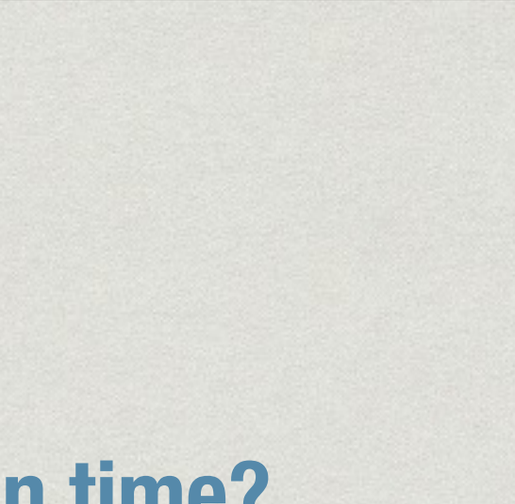


Why Preamble?

Forget sending data -- can you even agree on time?

Clock drift

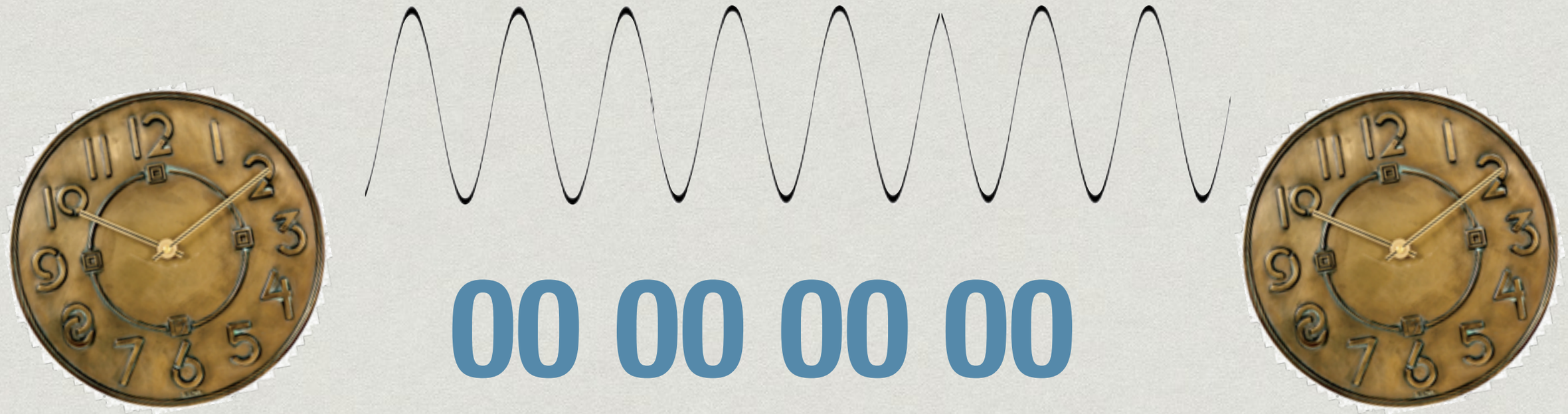




Clock drift

Why Preamble?

Forget sending data -- can you even agree on time?



00 00 00 00

Synchronized

How much preamble is really needed?

802.15.4 standard says 8 symbols: 00 00 00 00

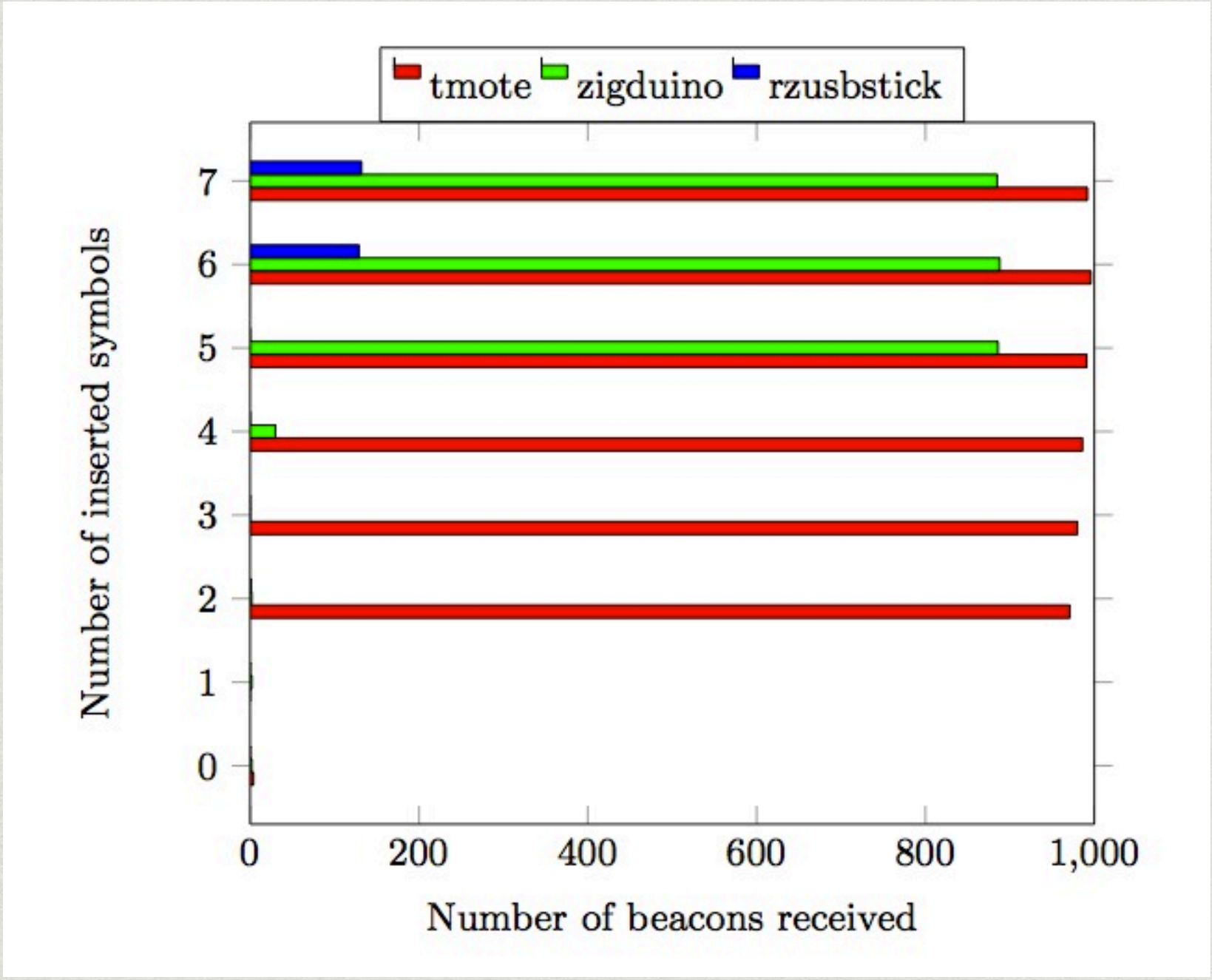
has a register to set preamble length:

00 00 00 00 00 00 <none>

Depends on clocks, temperature

Fingerprinting with variable preamble

Variable Preamble	SFD	Length	Payload



Why SFD?

`00 00 00 00 a7 0f 01 08 82 ff ff ff ff ...`

Preamble Sync Body

Shift Register

Out-of-frame

Why SFD?

`00 00 00 00 a7 0f 01 08 82 ff ff ff ff ...`

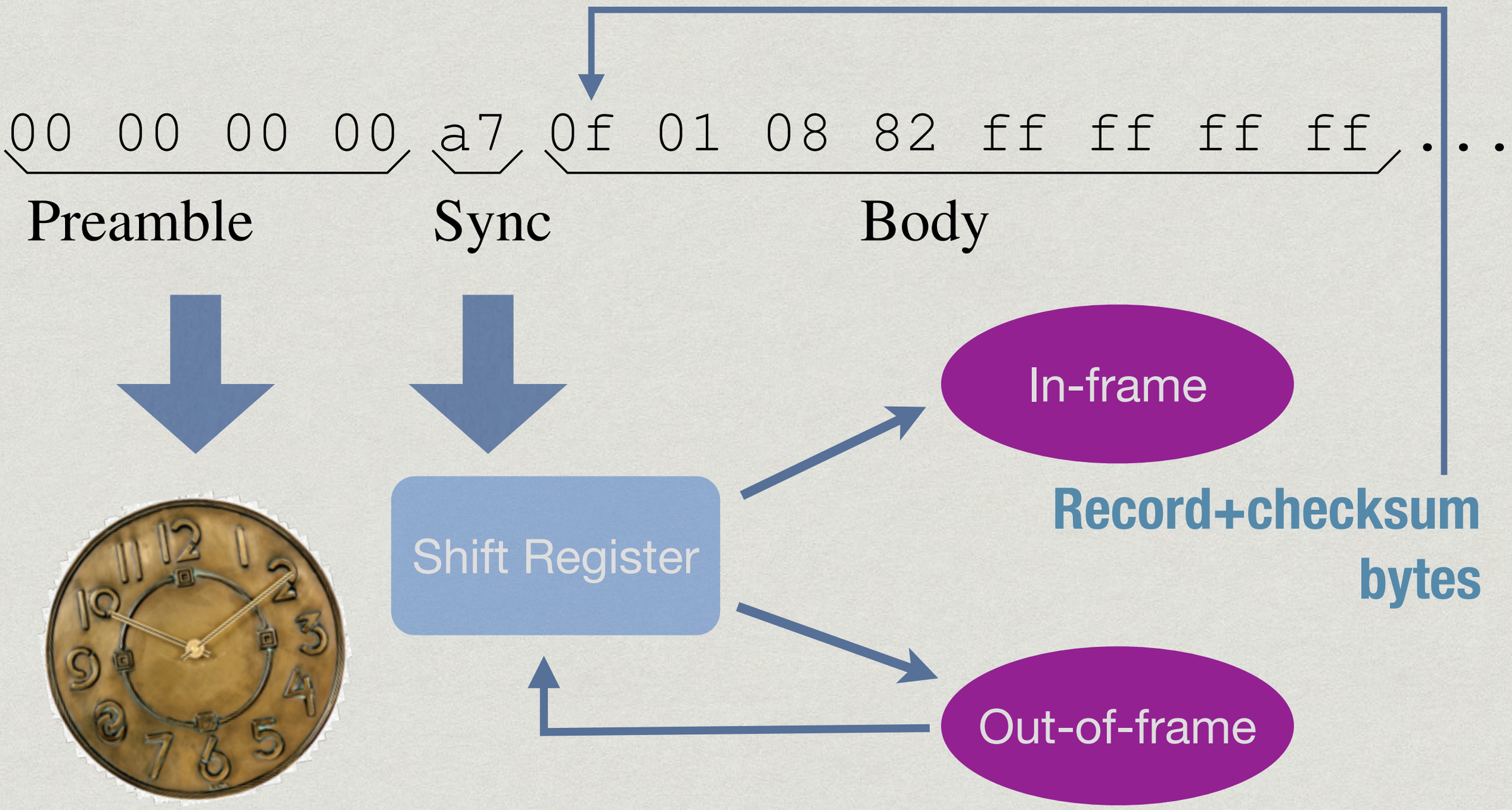
Preamble Sync Body

Shift Register

In-frame

Out-of-frame

Why SFD?


00 00 00 00 a7 0f 01 08 82 ff ff ff ff ...
Preamble
Sync
Body
In-frame
Record+checksum bytes
Shift Register
Out-of-frame

Is SFD in the symbol set?

Yes

No

802.15.4

802.11b/g*

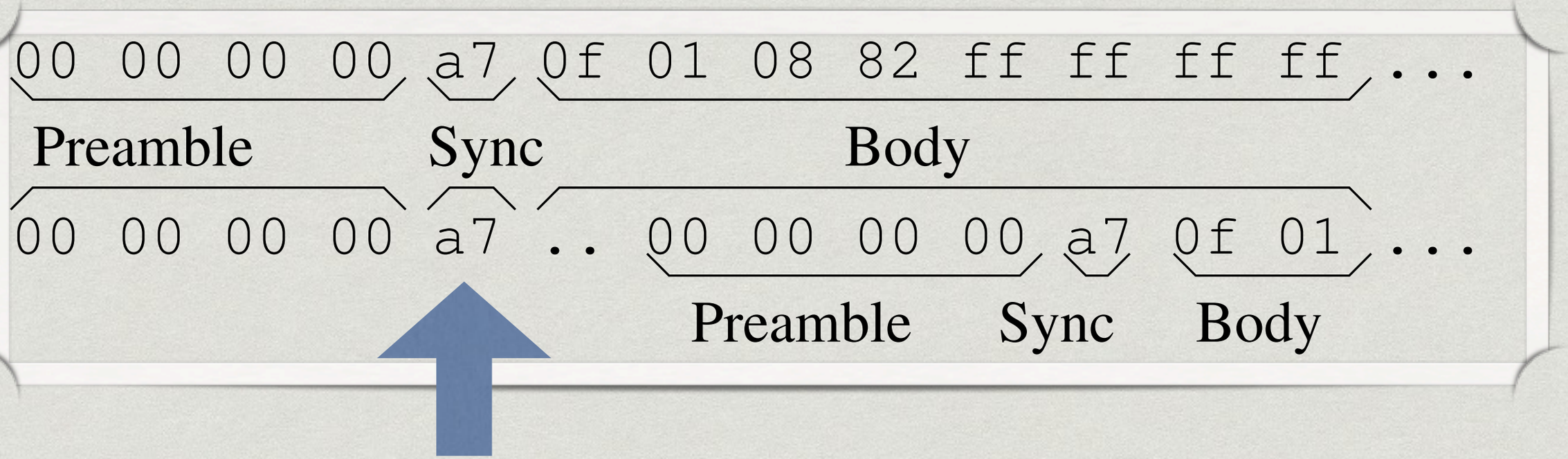
(*) kind of..

PCI Express

AX.25 packet radio

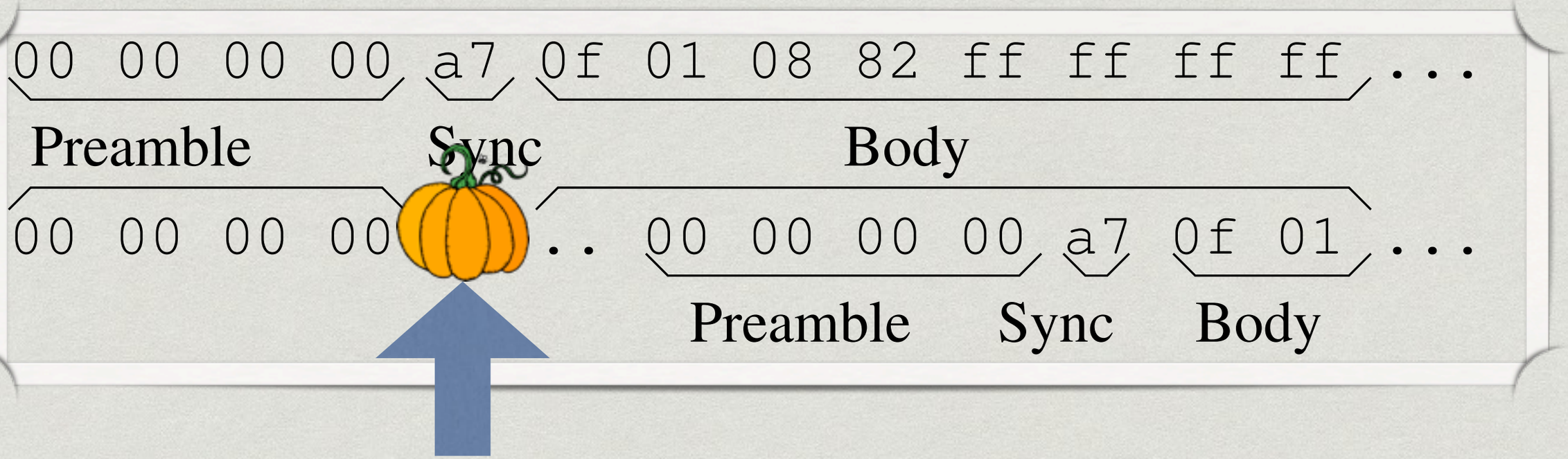
802.3

Packet-in-packet



What if this gets damaged by noise?

Packet-in-packet



What if this gets damaged by noise?

Packet-in-packet in Hex

Outer	Hex	Inner
Preamble	00 00 00 00	
Sync	a7	
Body	19	
	01 08 82	
	ca fe ba be	
	00 00 00 00	Preamble
	a7	Sync
	0a 01 08 82 ff ff ff ff c9 d1	Body
	15 e8	

You too can send a PHY frame without a radio! *)

(*) If you can control application layer bytes and there's noise **)

(**) There's always noise

Read the Fscking Paper

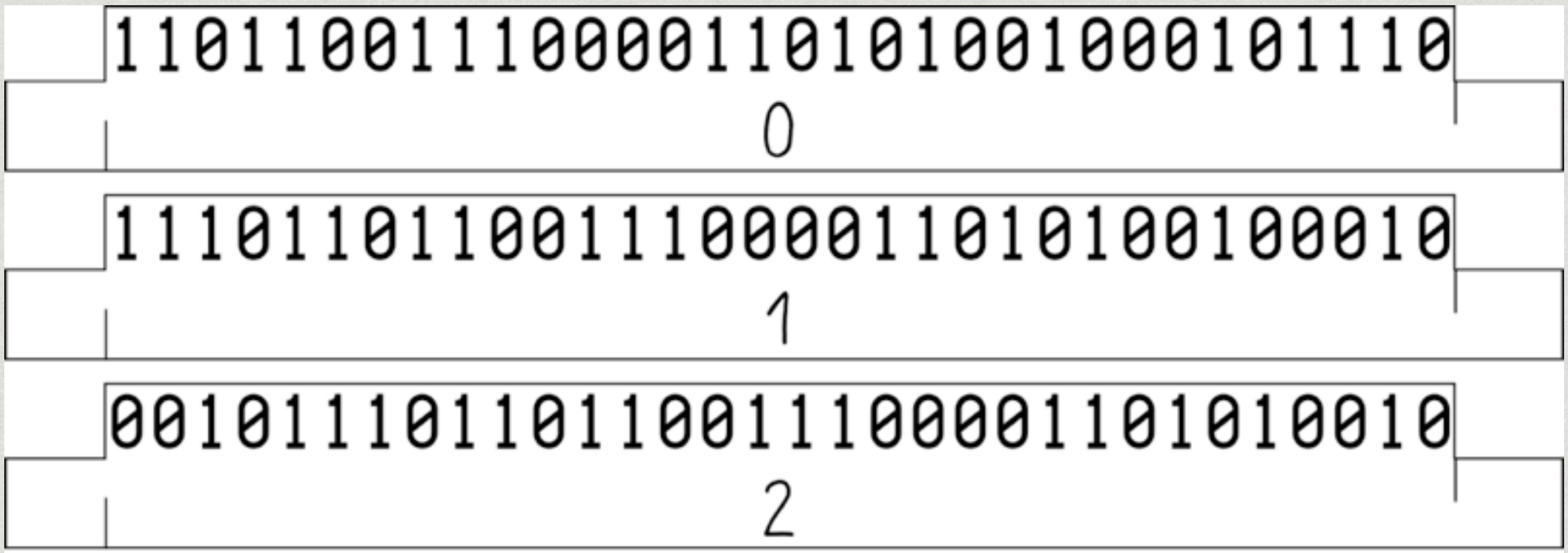
“Packets in Packets: Orson Welles’ In-Band Signaling Attacks for Modern Radios”, WOOT 2011

So how to send a symbol?

1101100111000011010100100010111 0	1000110010010110000001110111011 8
1110110110011100001101010010001 1	1011100011001001011000001110111 9
0010111011011001110000110101001 2	0111101110001100100101100000111 A
0010001011101101100111000011010 3	0111011110111000110010010110000 B
0101001000101110110110011100001 4	0000011101111011100011001001011 C
0011010100100010111011011001110 5	0110000001110111101110001100100 D
1100001101010010001011101101100 6	1001011000000111011111011100011 E
1001110000110101001000101110110 7	1100100101100000011101111011100 F

Chips!

Error correction



Some of these chips are going to arrive flipped.
Receiver will take symbol with the _closest code_
by Hamming distance *)
This is entirely transparent to _all_ layers above,
__including SFD matching___

Error ~~correction~~ connection

Symbol codes rotate into each other:

```
0                                 11011001110000110101001000101110
1                                111011011001110000110101001000010
2                              001011101101100111000011010100010
3                            00100010111011011001110000110101
4                         0101001000101110110110011110000011
5                      00110101001000101110110110011100
6                   11000011010100100010111011011001
7  10011100001101010010001011101101

8                                  10001100100101100000011101111011
9                                 10111000110010010110000001110111
A                               01111011100011001001011000000111
B                            01110111101110001100100101100000
C                         00000111011110111000110010010110
D                      01100000011101111011100011001001
E                   10010110000001110111101110001100
F  11001001011000000111011110111000
```

Error ~~correction~~ connection

Symbol codes rotate into each other (now in hex):

0	D9C3522E
1	ED9C3522
2	2ED9C352
3	22ED9C35
4	522ED9C3
5	3522ED9C
6	C3522ED9
7	9C3522ED

8	8C96077B
9	B8C96077
A	7B8C9607
B	77B8C960
C	077B8C96
D	6077B8C9
E	96077B8C
F	C96077B8

1/8 of a nybble (symbol)

Stream of symbols is actually a stream of chips

Boundaries between symbols are _imaginary_

Can my radio receive a frame that wasn't sent?

0	0	0	0	0	0	0	0
D9C3522E	D9C3522E	D9C3522E	D9C3522E	D9C3522E	D9C3522E	D9C3522E	D9C3522E
1	1	1	1	1	1	1	1
ED9C3522	ED9C3522	ED9C3522	ED9C3522	ED9C3522	ED9C3522	ED9C3522	ED9C3522

Hamming distance at most 4

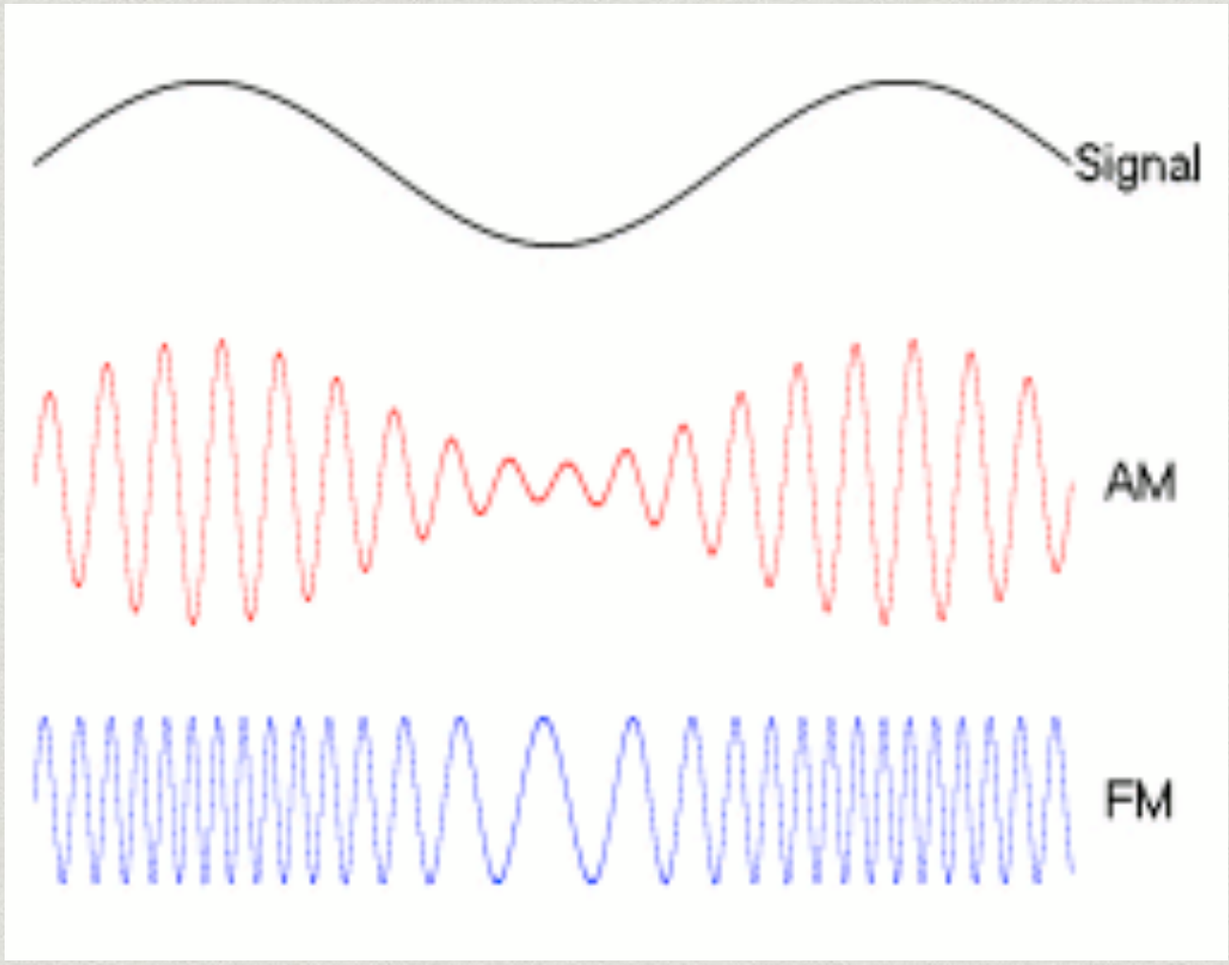
"I'll be SFD now"

```
BO  --  77B8C960D9C3522E
        ||||||||
A7  --  7B8C96079C3522ED
```

Your radio can receive frames that share no symbol with sent frames *)

(*) If you can cause misalignment by 1/8 of a nybble

Modulation of chips

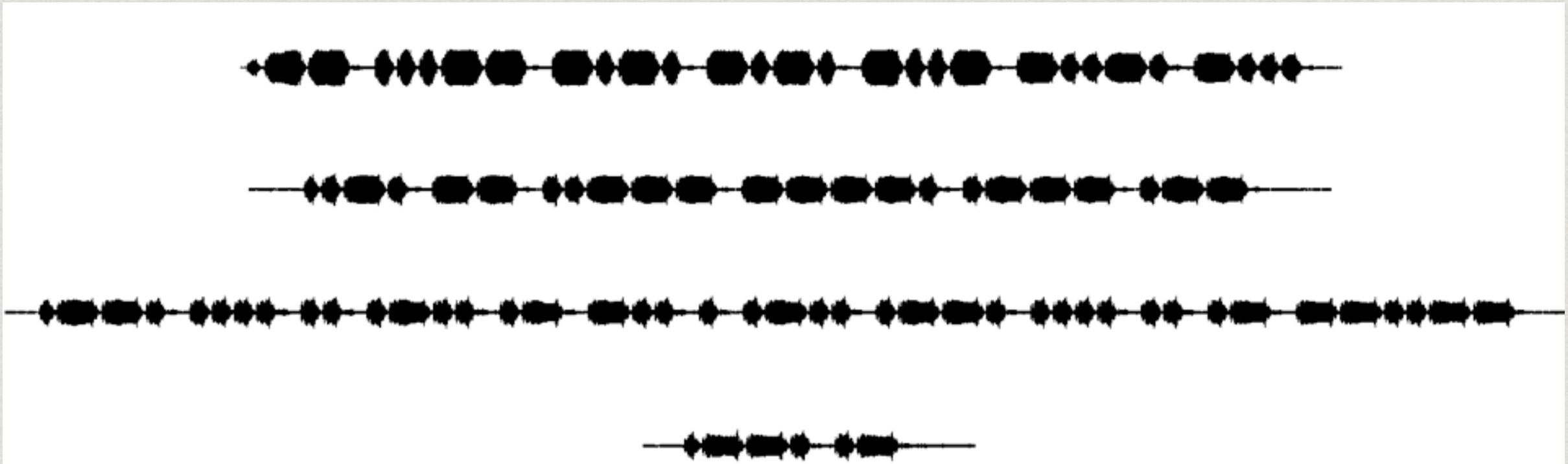


OOK, kinda like AM

FSK, kinda like FM

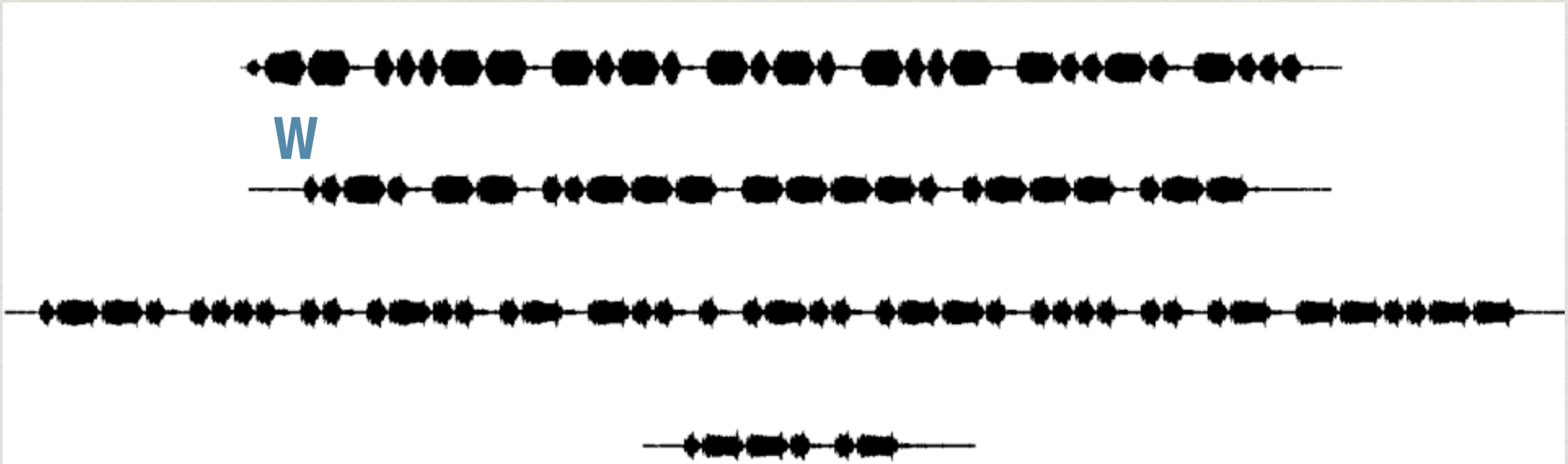
PSK, kinda like PSK

OOK



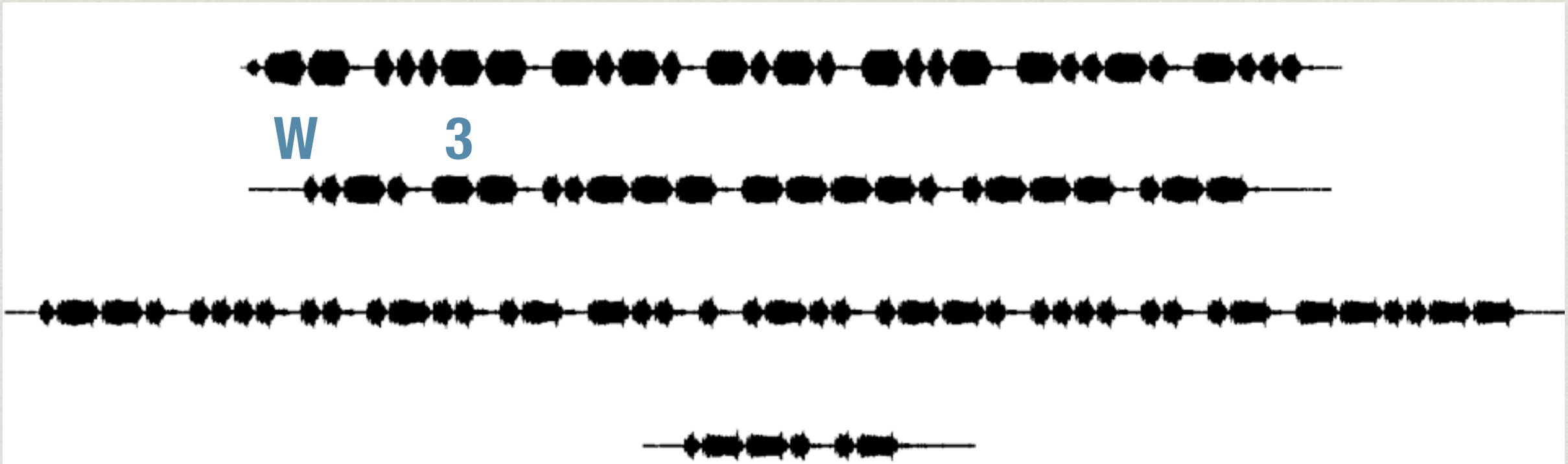
- On-Off Keying
- First used for Morse Code (CW)!

OOK



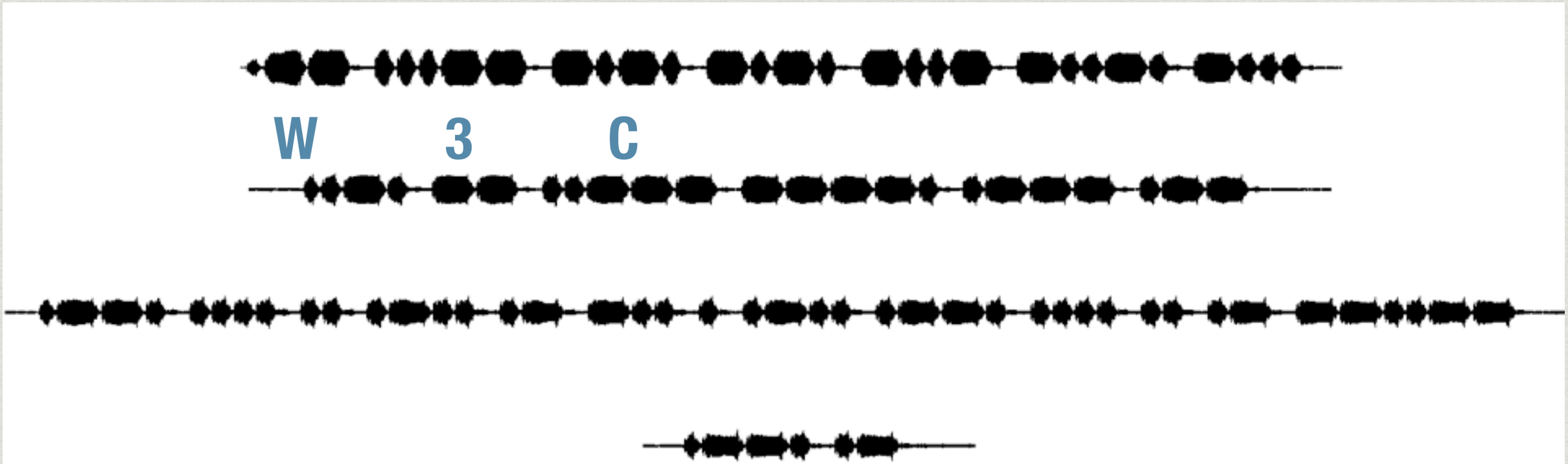
- On-Off Keying
- First used for Morse Code (CW)!

OOK



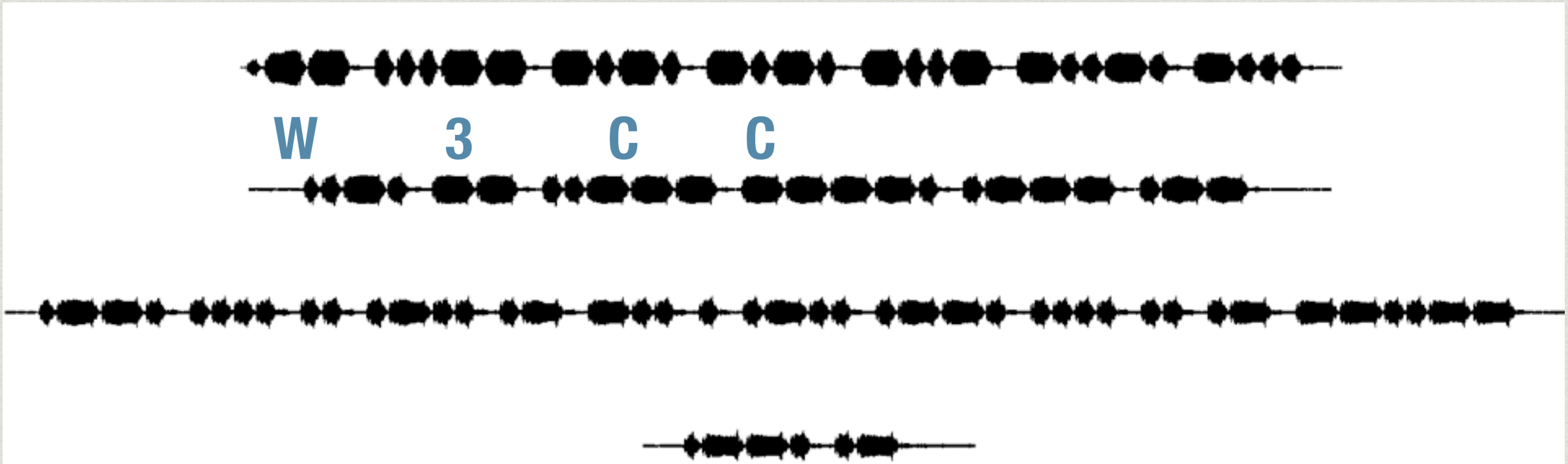
- On-Off Keying
- First used for Morse Code (CW)!

OOK



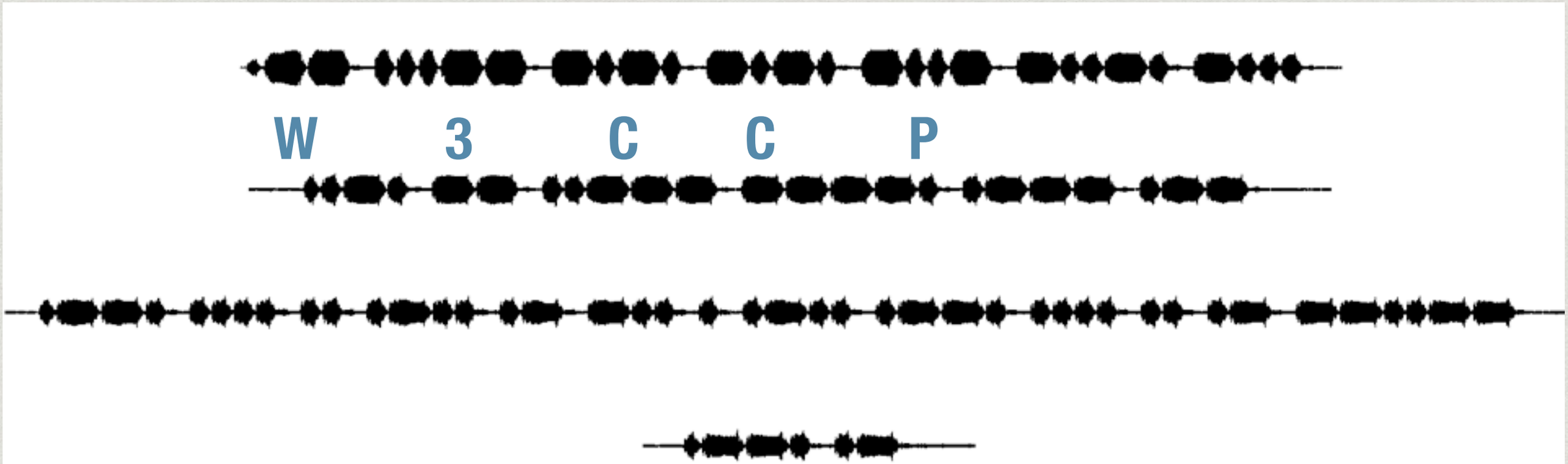
- On-Off Keying
- First used for Morse Code (CW)!

OOK



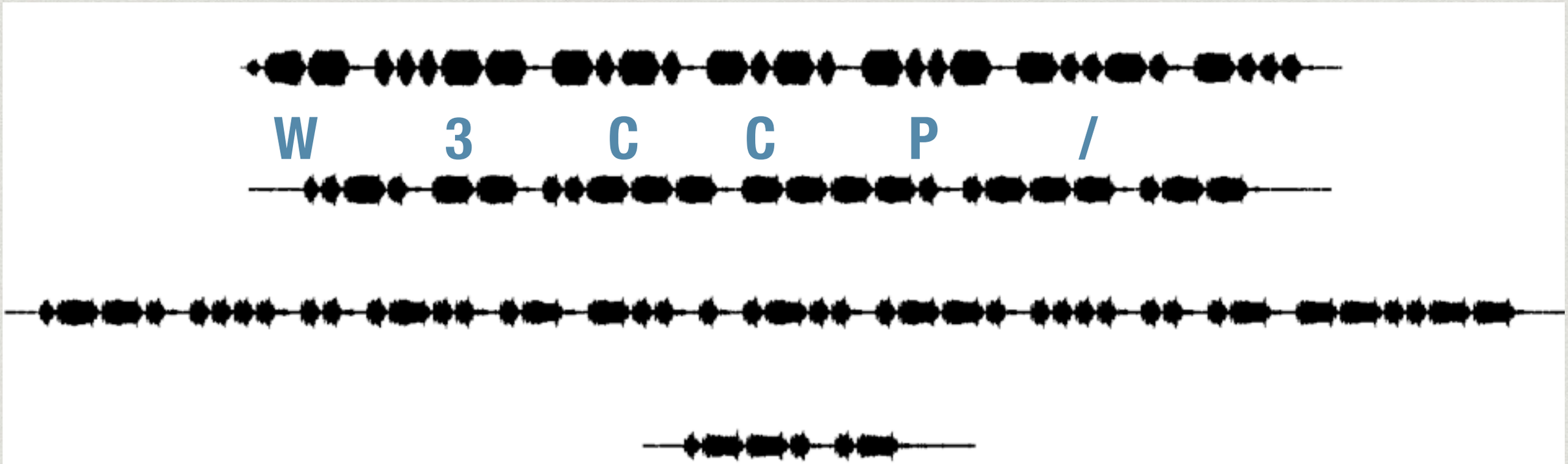
- On-Off Keying
- First used for Morse Code (CW)!

OOK



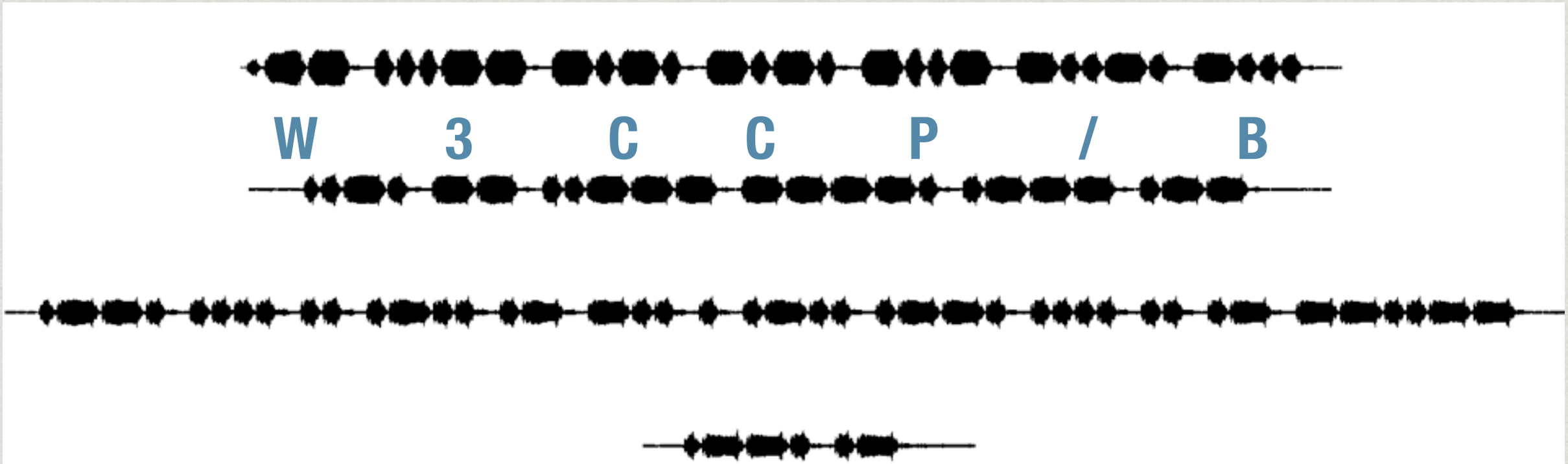
- On-Off Keying
- First used for Morse Code (CW)!

OOK



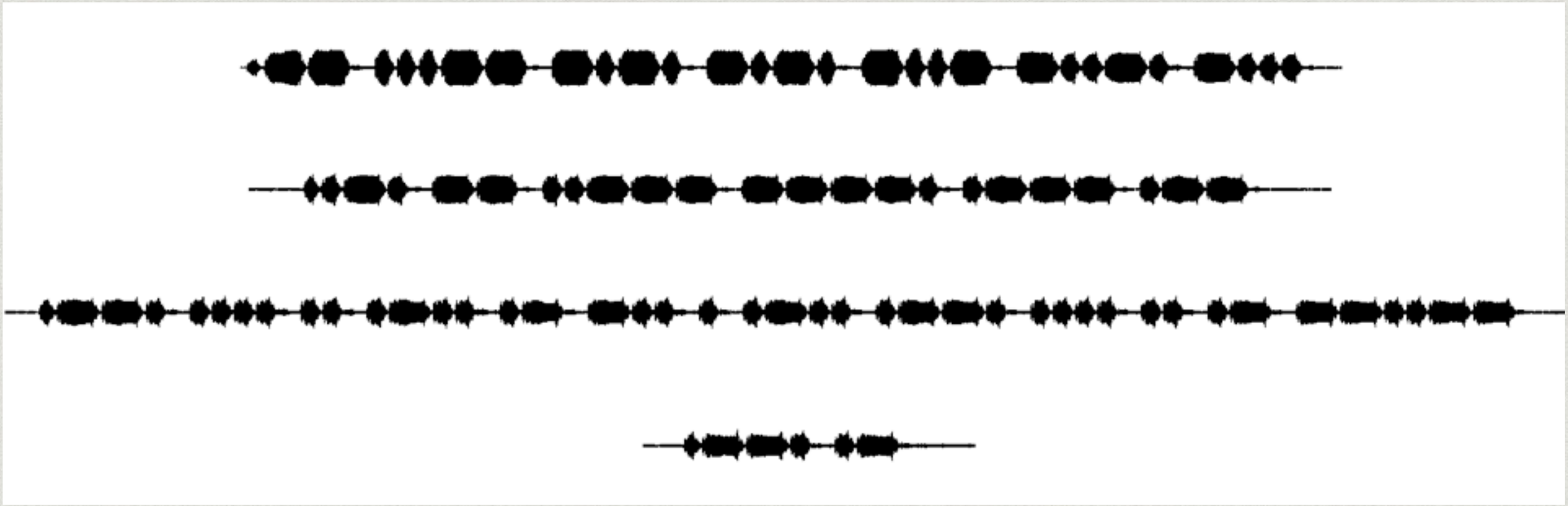
- On-Off Keying
- First used for Morse Code (CW)!

OOK



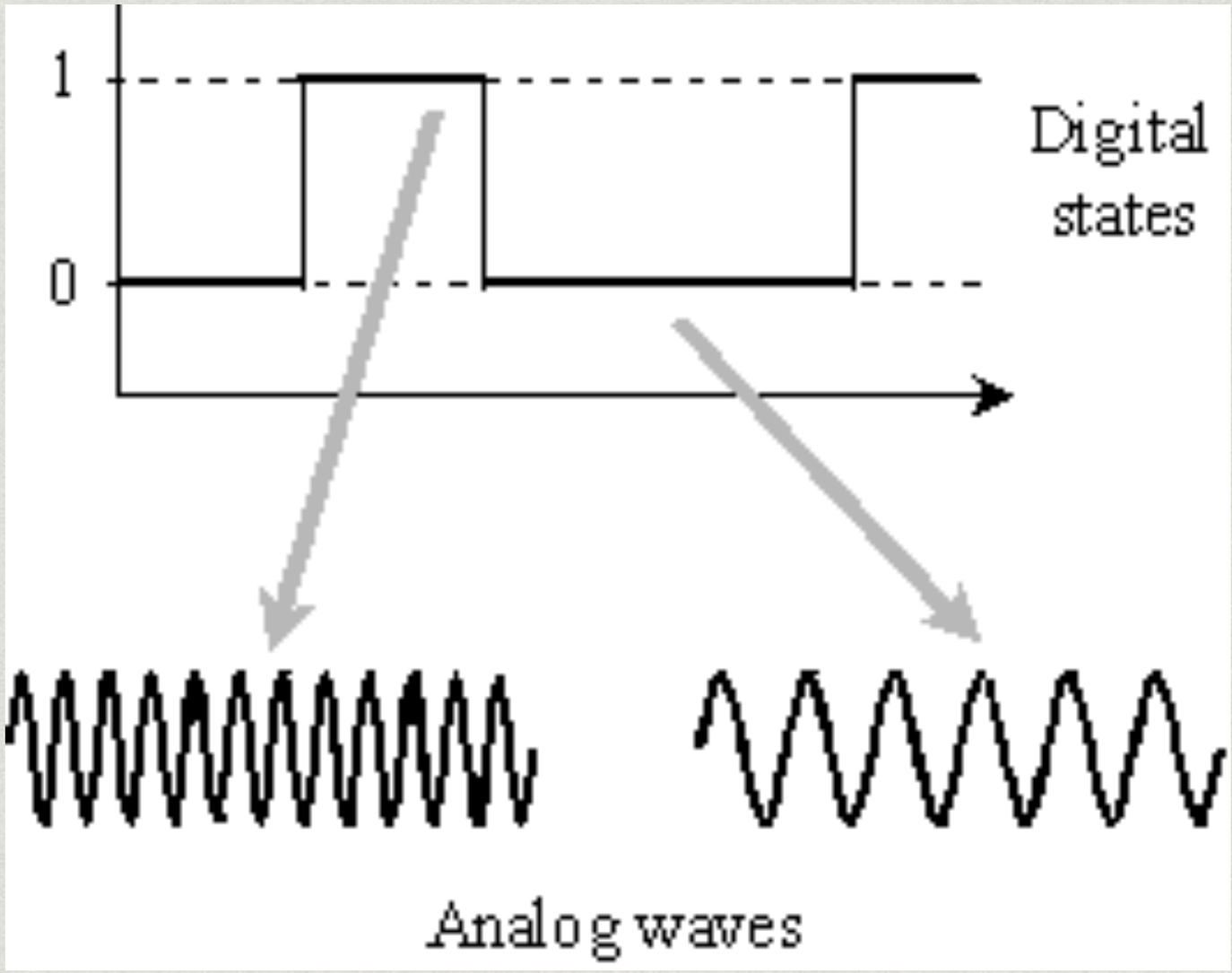
- On-Off Keying
- First used for Morse Code (CW)!

Wifi to Morse



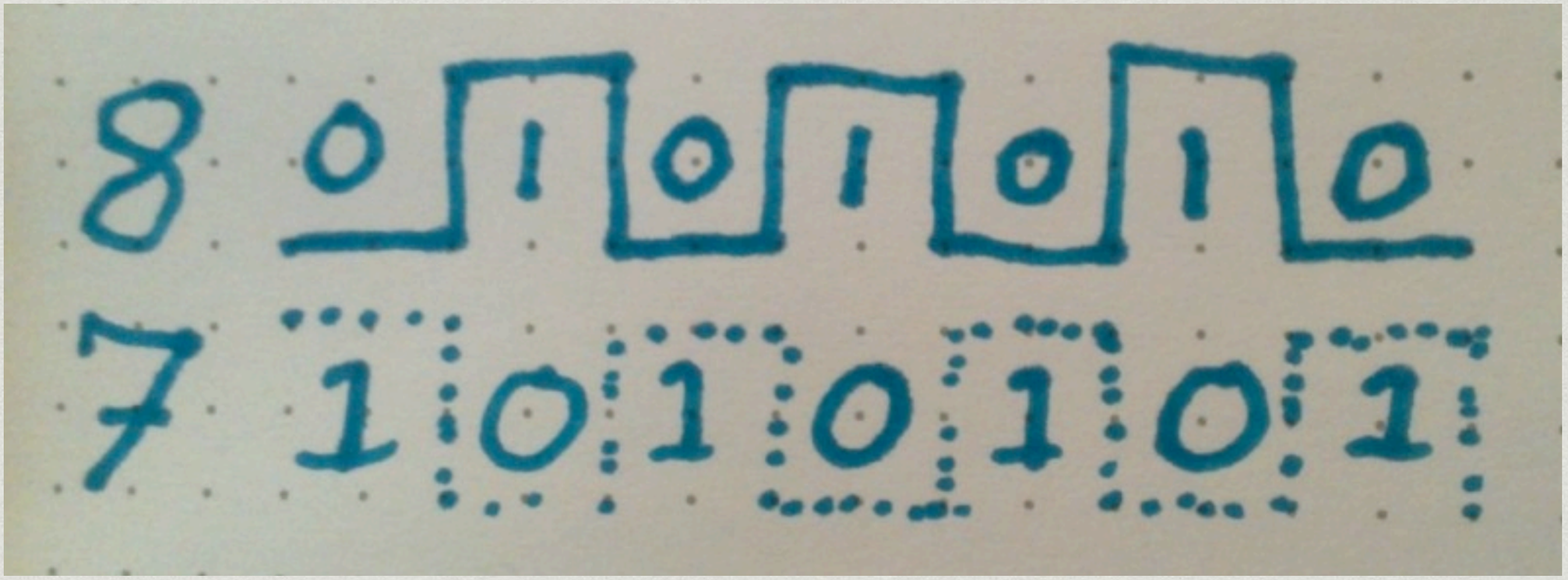
- Suppose you MITM an SSL session, but don’t know key.
- Enable and disable line to inject Morse code.
- Sniff at 2.4GHz with extreme range!

FSK



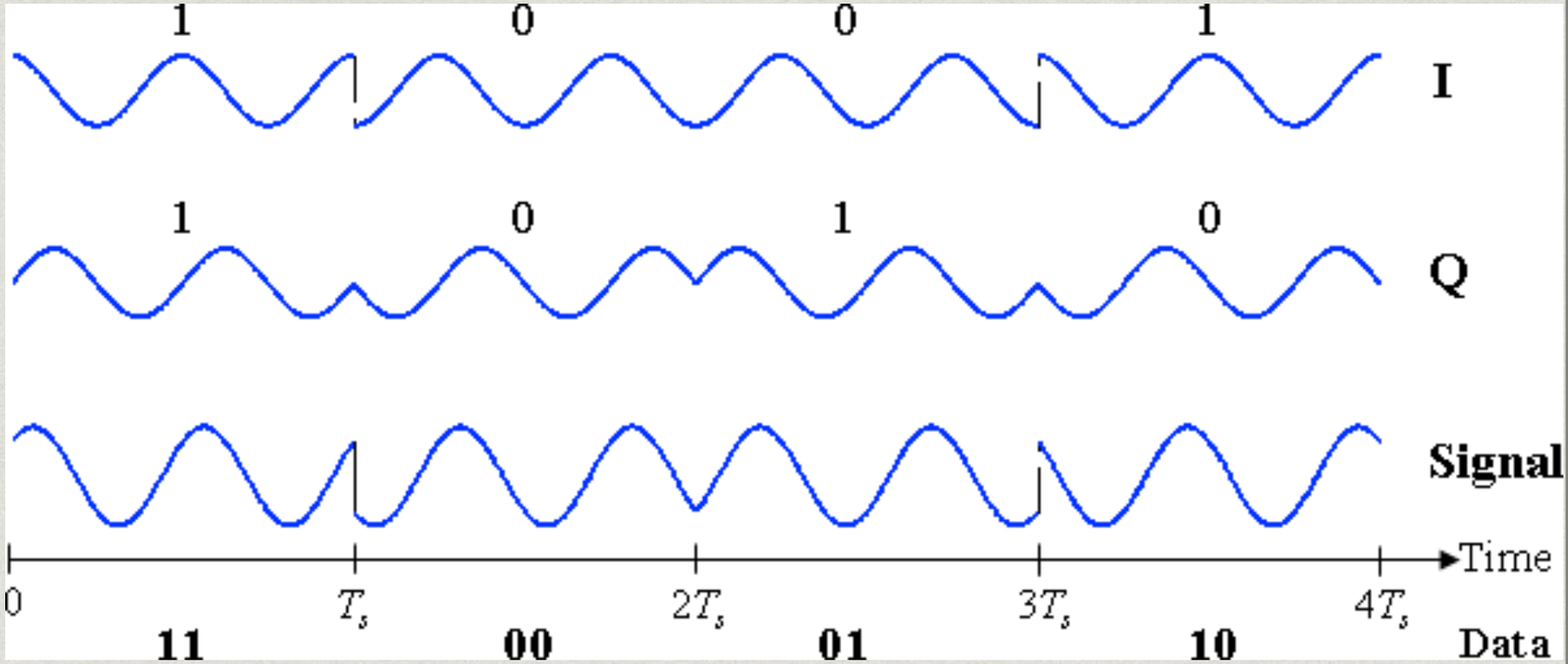
- Frequency Shift Keying
- Kinda like FM, but finite shifts.
- Used for Bluetooth.

FSK Ghosts



- Transmit on Channel 8.
- Flipped bits are received on Channel 7.

PSK



- Phase Shift Keying
- Phase varies to mark bits.
- BPSK--2 phases
  QPSK--4 phases 802.15.4

A zero is a zero and a one is a one, except when they aren’t.

Do radios have dialects?

- We can send **arbitrary symbol streams** with CC2420 (including preambles, SFDs, “inner” PIP packets, “packet-out-of-packet”, etc.)
- Active fingerprinting to find out what corruptions work.
  http://www.cs.dartmouth.edu/reports/abstracts/TR2014-749/
- Profit: capability to send packets that some radios see, and others don’t!
  (**Separate** from signal strength, range, etc.)

Do radios have dialects?

- We can send **arbitrary symbol streams** with CC2420 (including preambles, SFDs, “inner” PIP packets, “packet-out-of-packet”, etc.)
- Active fingerprinting to find out what corruptions work.
  http://www.cs.dartmouth.edu/reports/abstracts/TR2014-749/
- Profit: capability to send packets that some radios see, and others don’t!
  (**Separate** from signal strength, range, etc.)

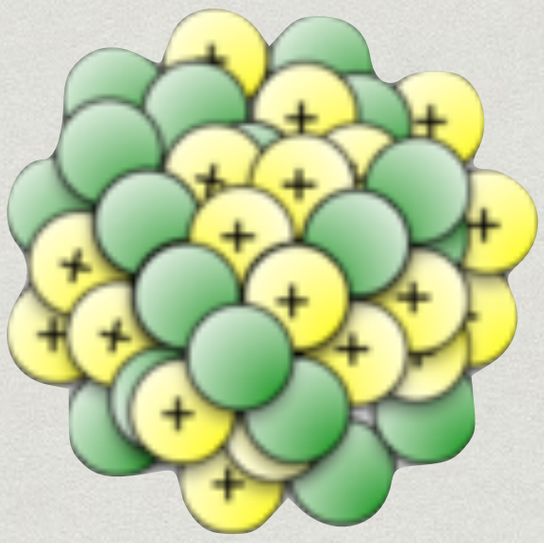
That’s a 802.15.4 WIDS evasion!

Isotope: Fingerprinting FTW!

- Fingerprinting: meh?
- “[Digital radio] chip makes are all different”- Captain Obvious

Isotope: Fingerprinting FTW!

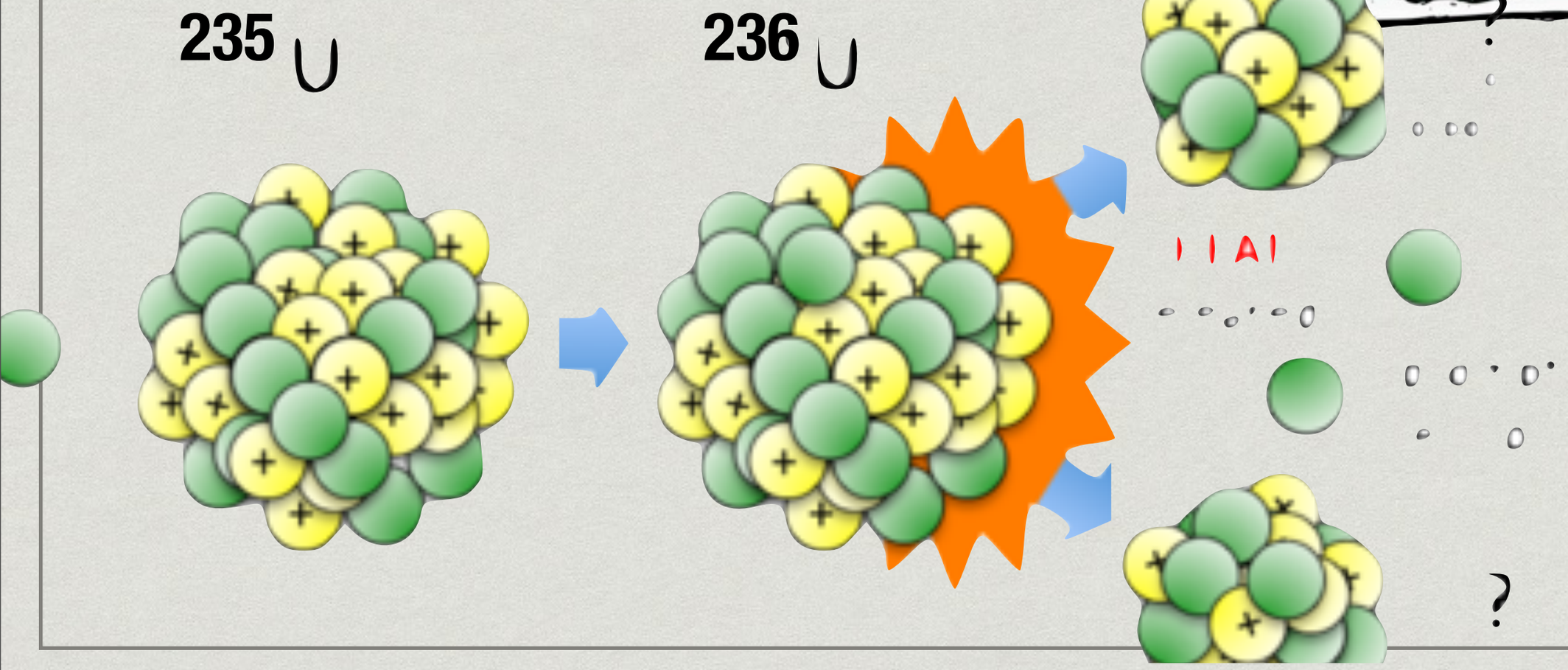
- Fingerprinting: meh?
- “[Digital radio] chip makes are all different”- Captain Obvious



- “Some nuclei aren’t like the others”
- Like **U** 238 v. **U** 235 ?

Isotope: Fingerprinting FTW!

- Fingerprinting: meh?
- “[Digital radio] chip makes are all different”- Captain Obvious



Cumberland Gap

Normal Frame:

Symbols: 8	2	2		variable
Preamble	SFD	Frame length (7 bits)	Reserved	PSDU
00 00 00 00	HR A7	PHR		PHY payload

What we send:

Preamble	SFD (bad)	0xFs	Preamble	SFD	Length	Payload

(..drink a little whiskey, take a little nap...)

Franconia Notch

Normal Frame:

Symbols: 8	2	2		variable
Preamble	SFD	Frame length (7 bits)	Reserved	PSDU
00 00 00 00 SHR	A7	PHR		PHY payload

What we send:

0x0s	0xFs	SFD	Length	Payload

(..drink a little whiskey, take a little nap...)

Franconia Bridge

Normal Frame:

Symbols: 8	2	2		variable
Preamble	SFD	Frame length (7 bits)	Reserved	PSDU
00 00 00 00 SHR	A7	PHR		PHY payload

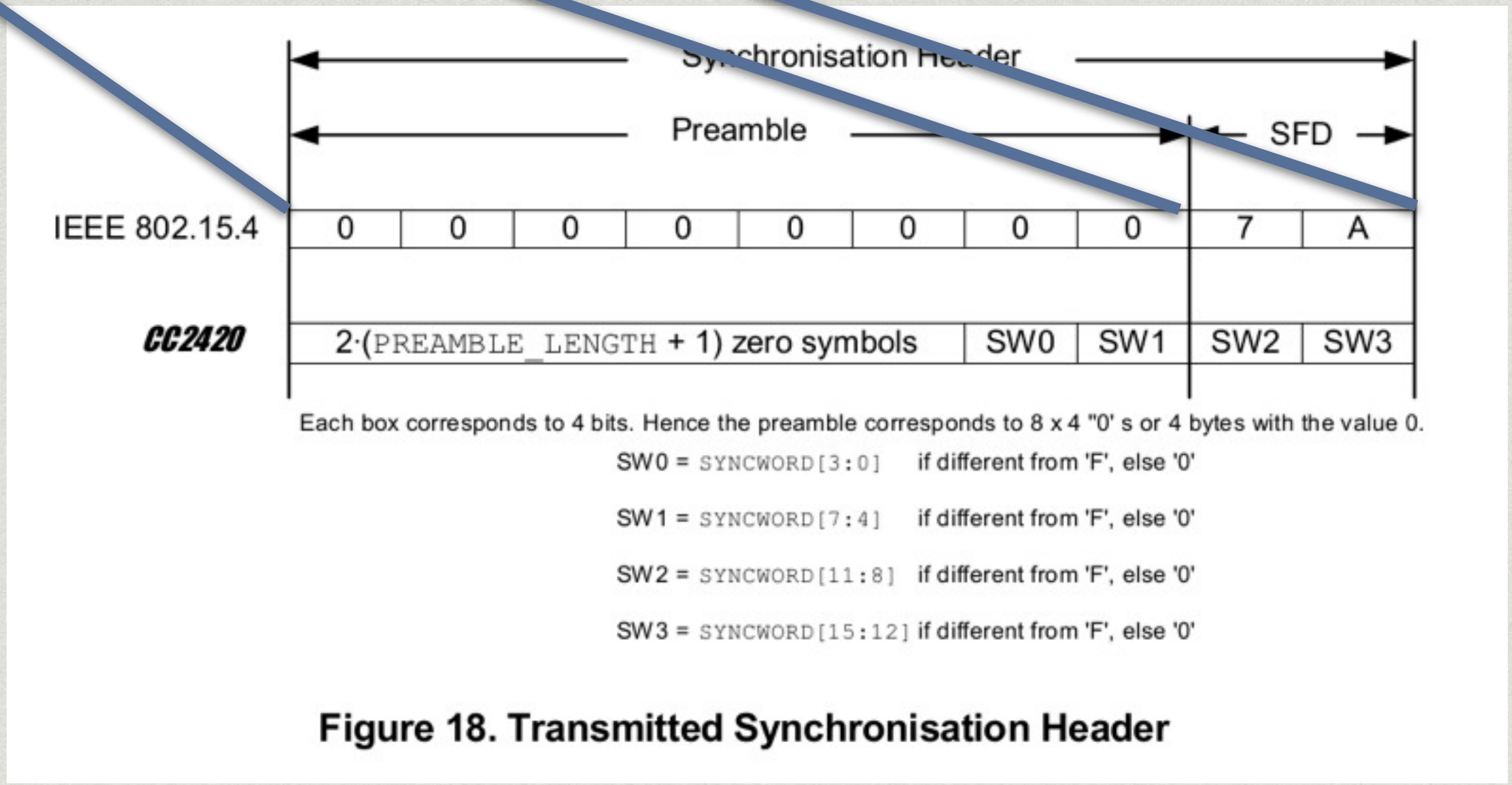
What we send:

Preamble	0xFs	SFD	Length	Payload

(..drink a little whiskey, take a little nap...)

Franconia notch

0x0s	0xFs	SFD	Length	Payload



Each box corresponds to 4 bits. Hence the preamble corresponds to 8 x 4 "0' s or 4 bytes with the value 0.

SW0 = SYNCWORD[3:0] if different from 'F', else '0'

SW1 = SYNCWORD[7:4] if different from 'F', else '0'

SW2 = SYNCWORD[11:8] if different from 'F', else '0'

SW3 = SYNCWORD[15:12] if different from 'F', else '0'

Figure 18. Transmitted Synchronisation Header

Franconia notch

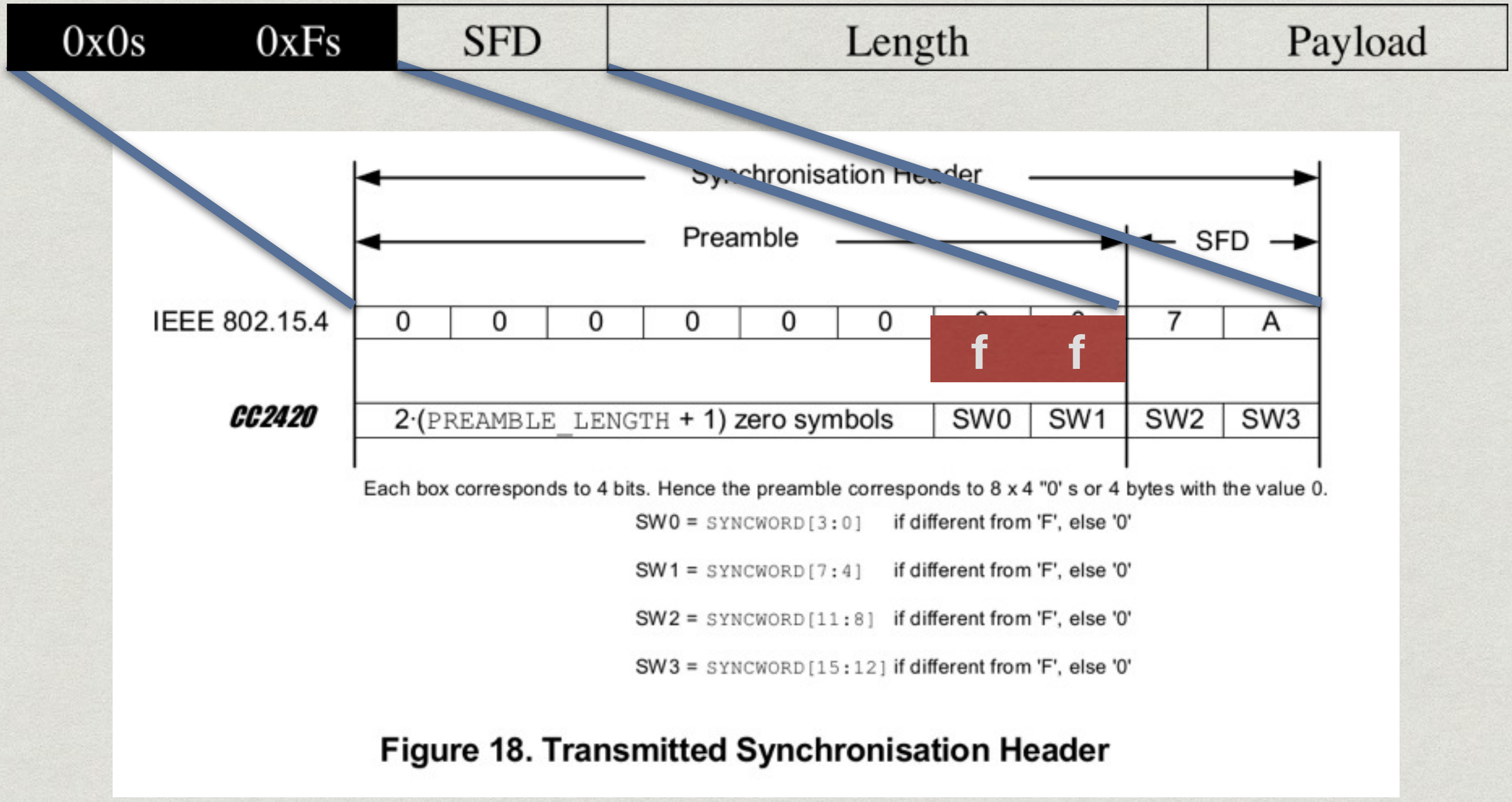


Figure 18. Transmitted Synchronisation Header

Franconia notch

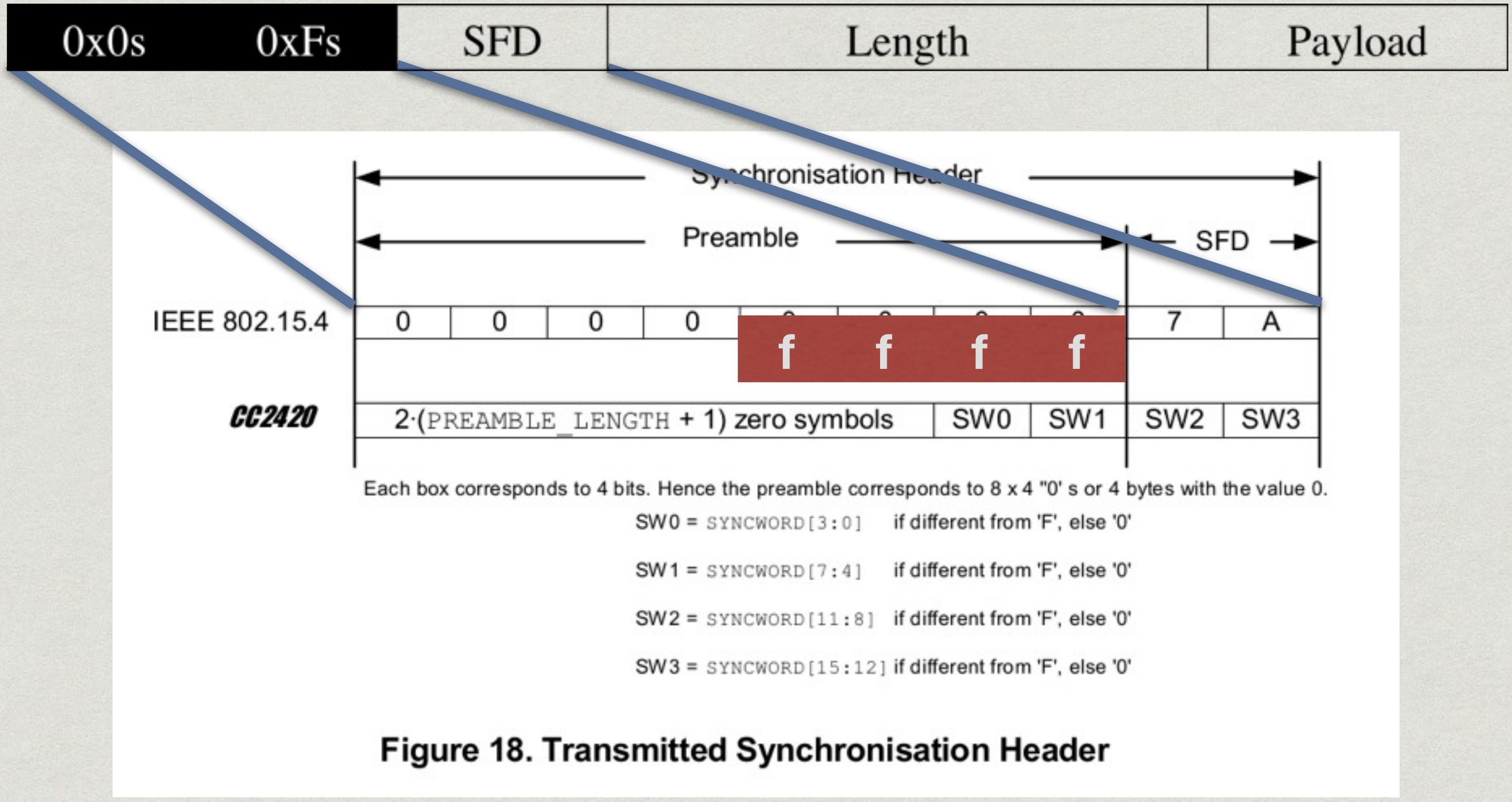


Figure 18. Transmitted Synchronisation Header

Franconia notch

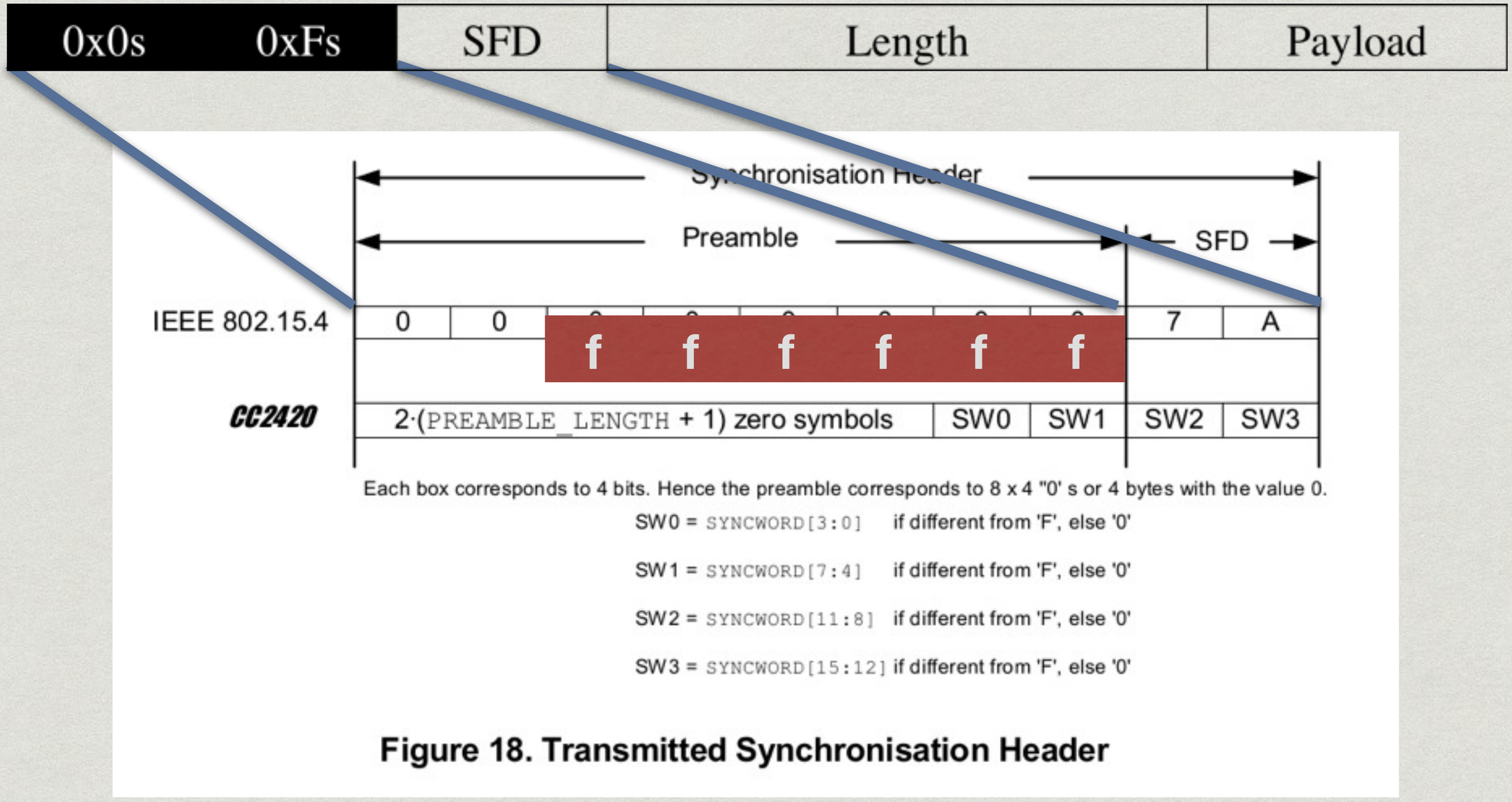


Figure 18. Transmitted Synchronisation Header

Franconia notch

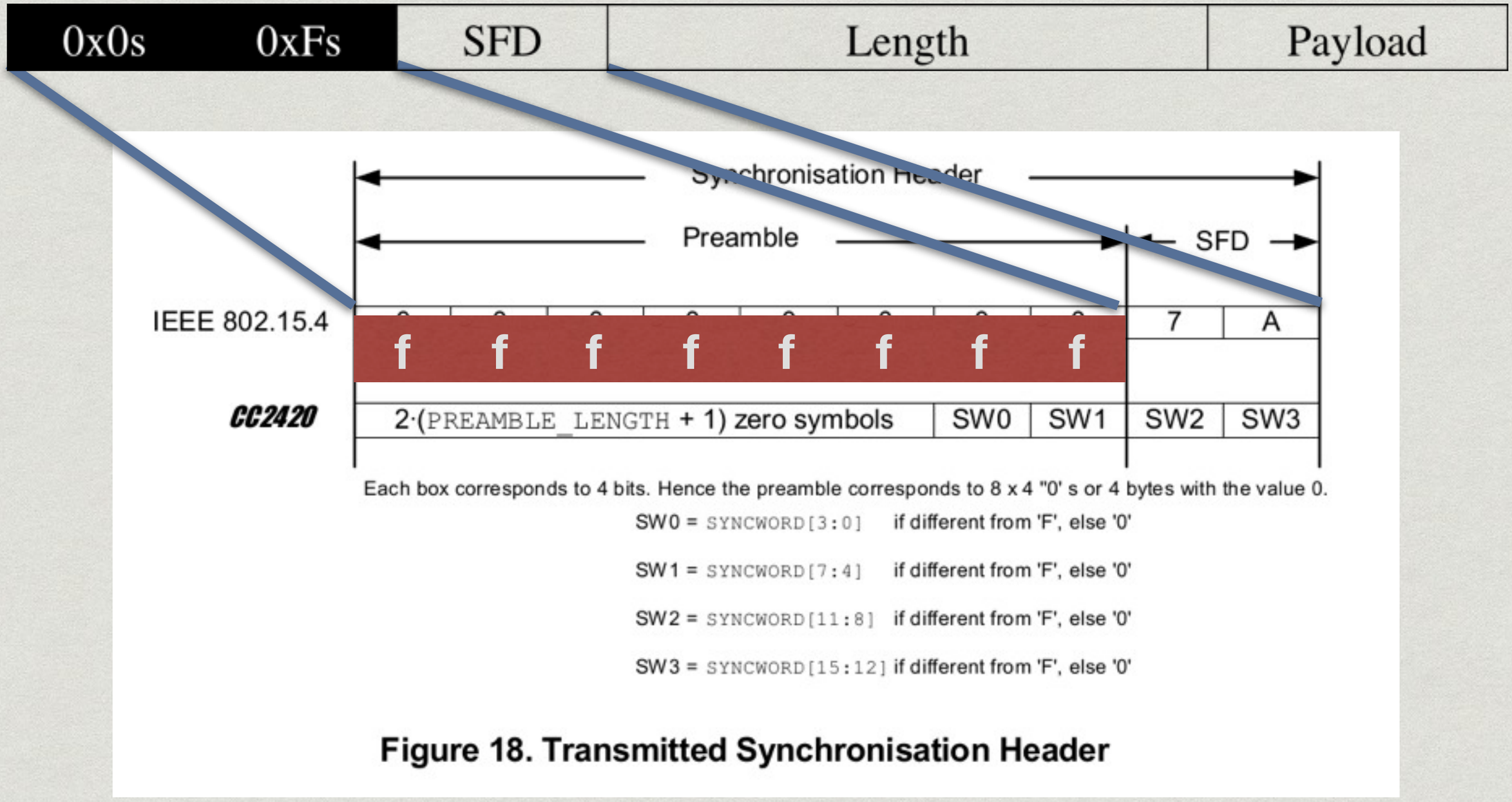
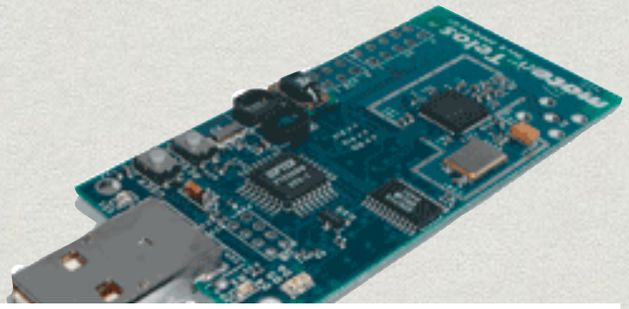
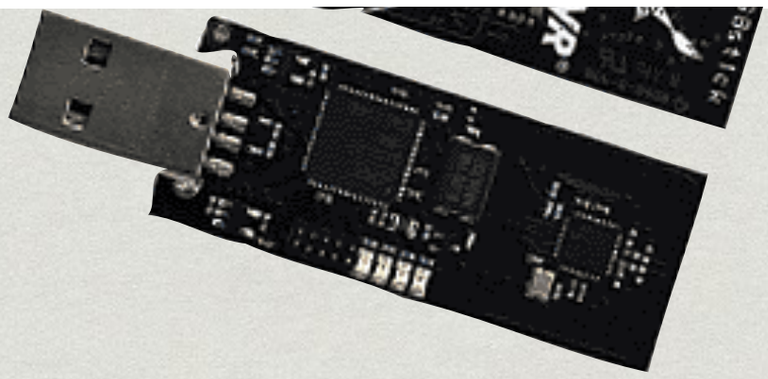


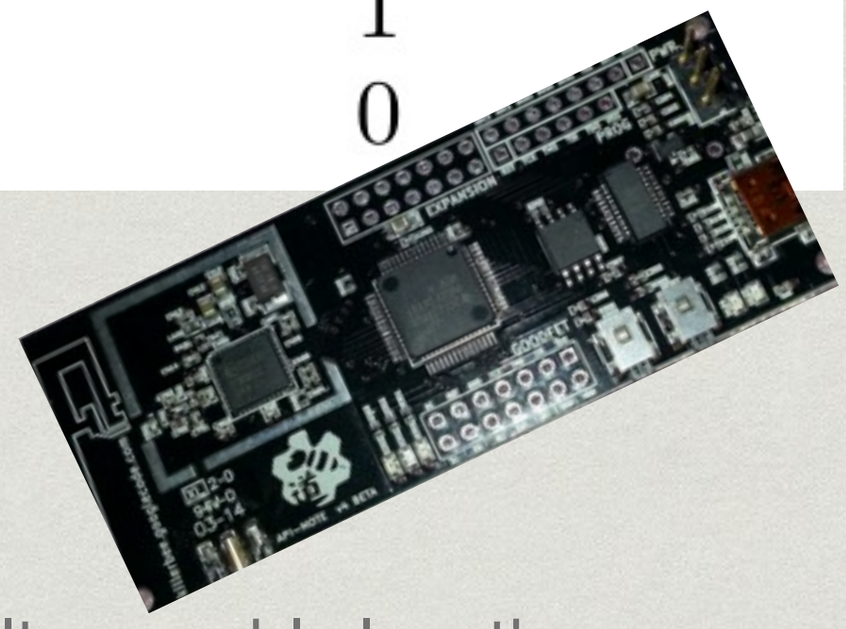
Figure 18. Transmitted Synchronisation Header

Local Dialect as a Shaped Charge



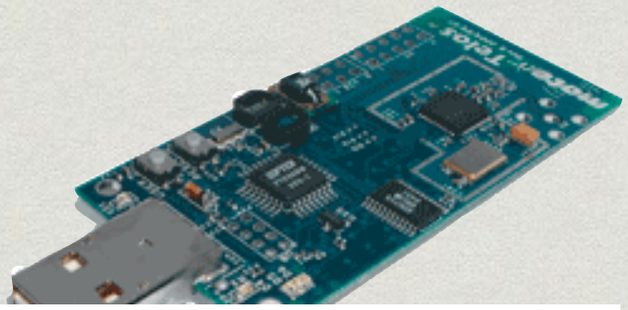
Preamble	RZUSB Observed	ApiMote Observed
00 00 00 00	672	1000
00 00 00 ff	991	0
00 00 ff ff	990	0
00 ff ff ff	855	1
ff ff ff ff	4	0



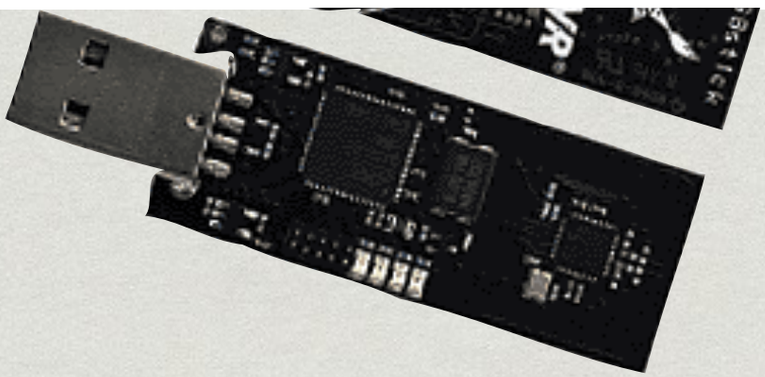


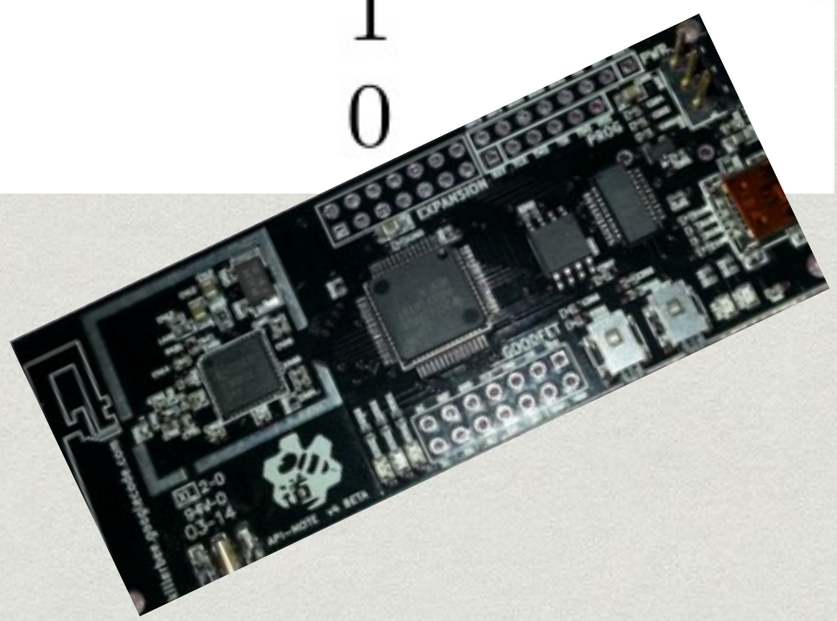
ApiMote's CC2420 RF chip was configured to default preamble length and SFD. Address and checksum verification was disabled.

Local Dialect as a Shaped Charge



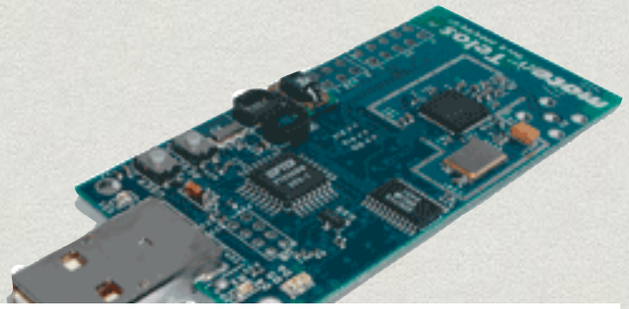
Preamble	RZUSB Observed	ApiMote Observed
00 00 00 00	672	1000
00 00 00 ff	991	0
00 00 ff ff	990	0
00 ff ff ff	855	1
ff ff ff ff	4	0



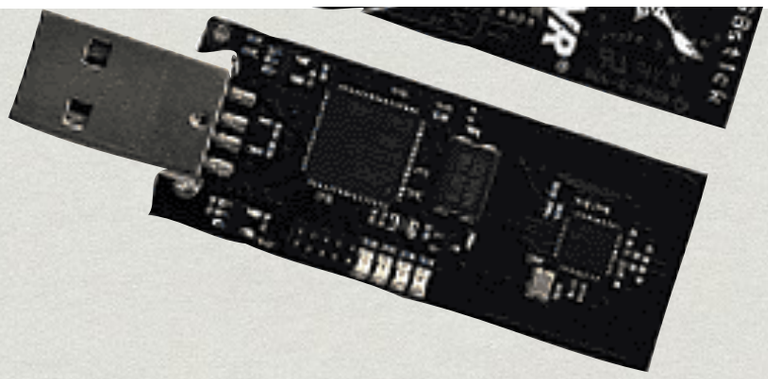


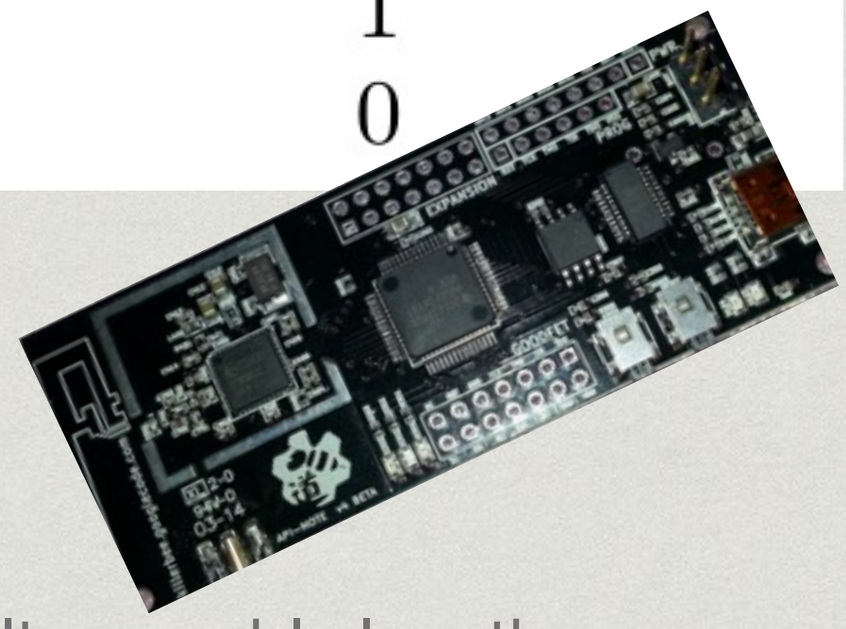
ApiMote's CC2420 RF chip was configured to default preamble length and SFD. Address and checksum verification was disabled.

Local Dialect as a Shaped Charge



Preamble	RZUSB Observed	ApiMote Observed
00 00 00 00	672	1000
00 00 00 ff	991	0
00 00 ff ff	990	0
00 ff ff ff	855	1
ff ff ff ff	4	0





ApiMote's CC2420 RF chip was configured to default preamble length and SFD. Address and checksum verification was disabled.

RZUSBSTICK PCAP

No.	Time	Source	Destination	Preamble	Protocol	Length	Sequence Number	Epoch Time	Info
6	5.000083	Broadcast	Broadcast	00 00 00 00	IEEE 802	10	1	1394396580.000099000	Beacon Request
7	9.999989	Broadcast	Broadcast	00 00 ff ff	IEEE 802	10	3	1394396585.000005000	Beacon Request
8	11.999992	Broadcast	Broadcast	00 ff ff ff	IEEE 802	10	4	1394396587.000008000	Beacon Request
9	15.999997	Broadcast	Broadcast	00 00 00 00	IEEE 802	10	6	1394396591.000013000	Beacon Request
10	17.999999	Broadcast	Broadcast	00 00 00 ff	IEEE 802	10	7	1394396593.000015000	Beacon Request
11	20.000002	Broadcast	Broadcast	00 00 ff ff	IEEE 802	10	8	1394396595.000018000	Beacon Request
12	22.000005	Broadcast	Broadcast	00 ff ff ff	IEEE 802	10	9	1394396597.000021000	Beacon Request
13	26.000011	Broadcast	Broadcast	00 00 00 00	IEEE 802	10	11	1394396601.000027000	Beacon Request
14	28.000013	Broadcast	Broadcast	00 00 00 ff	IEEE 802	10	12	1394396603.000029000	Beacon Request
15	30.000016	Broadcast	Broadcast	00 00 ff ff	IEEE 802	10	13	1394396605.000032000	Beacon Request
16	32.000018	Broadcast	Broadcast	00 ff ff ff	IEEE 802	10	14	1394396607.000034000	Beacon Request
17	36.000023	Broadcast	Broadcast	00 00 00 00	IEEE 802	10	16	1394396611.000039000	Beacon Request
18	38.000027	Broadcast	Broadcast	…	IEEE 802	10	17	1394396613.000043000	Beacon Request
19	40.000030	Broadcast	Broadcast		IEEE 802	10	18	1394396615.000046000	Beacon Request
20	46.000040	Broadcast	Broadcast		IEEE 802	10	21	1394396621.000056000	Beacon Request
21	48.000043	Broadcast	Broadcast		IEEE 802	10	22	1394396623.000059000	Beacon Request
22	50.000046	Broadcast	Broadcast		IEEE 802	10	23	1394396625.000062000	Beacon Request
23	55.999991	Broadcast	Broadcast		IEEE 802	10	26	1394396631.000007000	Beacon Request
24	58.000056	Broadcast	Broadcast		IEEE 802	10	27	1394396633.000072000	Beacon Request
25	60.000059	Broadcast	Broadcast		IEEE 802	10	28	1394396635.000075000	Beacon Request
26	62.000062	Broadcast	Broadcast		IEEE 802	10	29	1394396637.000078000	Beacon Request
27	66.000067	Broadcast	Broadcast		IEEE 802	10	31	1394396641.000083000	Beacon Request
28	68.000071	Broadcast	Broadcast		IEEE 802	10	32	1394396643.000087000	Beacon Request
29	69.999993	Broadcast	Broadcast		IEEE 802	10	33	1394396645.000009000	Beacon Request
30	72.000077	Broadcast	Broadcast		IEEE 802	10	34	1394396647.000093000	Beacon Request
31	76.000082	Broadcast	Broadcast		IEEE 802	10	36	1394396651.000098000	Beacon Request
32	78.999984	Broadcast	Broadcast		IEEE 802	10	37	1394396654.000000000	Beacon Request
33	80.999987	Broadcast	Broadcast		IEEE 802	10	38	1394396656.000003000	Beacon Request
34	86.999996	Broadcast	Broadcast		IEEE 802	10	41	1394396662.000012000	Beacon Request
35	88.999998	Broadcast	Broadcast		IEEE 802	10	42	1394396664.000014000	Beacon Request
36	91.000000	Broadcast	Broadcast		IEEE 802	10	43	1394396666.000016000	Beacon Request
37	93.000003	Broadcast	Broadcast		IEEE 802	10	44	1394396668.000019000	Beacon Request
38	101.000017	Broadcast	Broadcast		IEEE 802	10	48	1394396676.000033000	Beacon Request

RZUSBSTICK PCAP

No.	Time	Source	Destination	Preamble	Protocol	Length	Sequence Number	Epoch Time	Info
6	5.000083			00 00 00 00	IEEE 802	10	1	1394396580.000099000	Beacon Request
7	9.999989			00 00 ff ff	IEEE 802	10	3	1394396585.000005000	Beacon Request
8	11.999992			00 ff ff ff	IEEE 802	10	4	1394396587.000008000	Beacon Request
9	15.999997			00 00 00 00	IEEE 802	10	6	1394396591.000013000	Beacon Request
10	17.999999			00 00 00 ff	IEEE 802	10	7	1394396593.000015000	Beacon Request
11	20.000002			00 00 ff ff	IEEE 802	10	8	1394396595.000018000	Beacon Request
12	22.000005			00 ff ff ff	IEEE 802	10	9	1394396597.000021000	Beacon Request
13	26.000011			00 00 00 00	IEEE 802	10	11	1394396601.000027000	Beacon Request
14	28.000013			00 00 00 ff	IEEE 802	10	12	1394396603.000029000	Beacon Request
15	30.000016			00 00 ff ff	IEEE 802	10	13	1394396605.000032000	Beacon Request
16	32.000018			00 ff ff ff	IEEE 802	10	14	1394396607.000034000	Beacon Request
17	36.000023			00 00 00 00	IEEE 802	10	16	1394396611.000039000	Beacon Request
18	38.000027			...	IEEE 802	10	17	1394396613.000043000	Beacon Request
19	40.000030				IEEE 802	10	18	1394396615.000046000	Beacon Request
20	46.000040				IEEE 802	10	21	1394396621.000056000	Beacon Request
21	48.000043				IEEE 802	10	22	1394396623.000059000	Beacon Request

RZUSBSTICK PCAP

No.	Time	Source	Preamble	Destination	Protocol	Length	Sequence Number	Epoch Time	Info
6	5.000083		00 00 00 00		IEEE 802	10	1	1394396580.000099000	Beacon Request
7	9.999989		00 00 ff ff		IEEE 802	10	3	1394396585.000005000	Beacon Request
8	11.999992		00 ff ff ff		IEEE 802	10	4	1394396587.000008000	Beacon Request
9	15.999997		00 00 00 00		IEEE 802	10	6	1394396591.000013000	Beacon Request
10	17.999999		00 00 00 ff		IEEE 802	10	7	1394396593.000015000	Beacon Request
11	20.000002		00 00 ff ff		IEEE 802	10	8	1394396595.000018000	Beacon Request
12	22.000005		00 ff ff ff		IEEE 802	10	9	1394396597.000021000	Beacon Request
13	26.000011		00 00 00 00		IEEE 802	10	11	1394396601.000027000	Beacon Request
14	28.000013		00 00 00 ff		IEEE 802	10	12	1394396603.000029000	Beacon Request
15	30.000016		00 00 ff ff		IEEE 802	10	13	1394396605.000032000	Beacon Request
16	32.000018		00 ff ff ff		IEEE 802	10	14	1394396607.000034000	Beacon Request
17	36.000023		00 00 00 00		IEEE 802	10	16	1394396611.000039000	Beacon Request
18	38.000027		...		IEEE 802	10	17	1394396613.000043000	Beacon Request
19	40.000030				IEEE 802	10	18	1394396615.000046000	Beacon Request
20	46.000040				IEEE 802	10	21	1394396621.000056000	Beacon Request
21	48.000043				IEEE 802	10	22	1394396623.000059000	Beacon Request

ApiMote PCAP

No.	Time	Source	Preamble	Destination	Protocol	Length	Sequence Number	Epoch Time	Info
6	5.999984		00 00 00 00		IEEE 802	10	1	1394396581.000000000	Beacon Request
7	15.999997		00 00 00 00		IEEE 802	10	6	1394396591.000013000	Beacon Request
8	26.000011		00 00 00 00		IEEE 802	10	11	1394396601.000027000	Beacon Request
9	35.999988		00 00 00 00		IEEE 802	10	16	1394396611.000004000	Beacon Request
10	46.000040		00 00 00 00		IEEE 802	10	21	1394396621.000056000	Beacon Request
11	55.999991		00 00 00 00		IEEE 802	10	26	1394396631.000007000	Beacon Request
12	66.000068		00 00 00 00		IEEE 802	10	31	1394396641.000084000	Beacon Request
13	76.000083		00 00 00 00		IEEE 802	10	36	1394396651.000099000	Beacon Request
14	86.999996		00 00 00 00		IEEE 802	10	41	1394396662.000012000	Beacon Request
15	97.000012		00 00 00 00		IEEE 802	10	46	1394396672.000028000	Beacon Request

RZUSBSTICK PCAP

No.	Time	Source	Preamble	Destination	Protocol	Length	Sequence Number	Epoch Time	Info
6	5.000083		00 00 00 00		IEEE 802	10	1	1394396580.000099000	Beacon Request
7	9.999989		00 00 ff ff		IEEE 802	10	3	1394396585.000005000	Beacon Request
8	11.999992		00 ff ff ff		IEEE 802	10	4	1394396587.000008000	Beacon Request
9	15.999997		00 00 00 00		IEEE 802	10	6	1394396591.000013000	Beacon Request
10	17.999999		00 00 00 ff		IEEE 802	10	7	1394396593.000015000	Beacon Request
11	20.000002		00 00 ff ff		IEEE 802	10	8	1394396595.000018000	Beacon Request
12	22.000005		00 ff ff ff		IEEE 802	10	9	1394396597.000021000	Beacon Request
13	26.000011		00 00 00 00		IEEE 802	10	11	1394396601.000027000	Beacon Request
14	28.000013		00 00 00 ff		IEEE 802	10	12	1394396603.000029000	Beacon Request
15	30.000016		00 00 ff ff		IEEE 802	10	13	1394396605.000032000	Beacon Request
16	32.000018		00 ff ff ff		IEEE 802	10	14	1394396607.000034000	Beacon Request
17	36.000023		00 00 00 00		IEEE 802	10	16	1394396611.000039000	Beacon Request
18	38.000027		…		IEEE 802	10	17	1394396613.000043000	Beacon Request
19	40.000030				IEEE 802	10	18	1394396615.000046000	Beacon Request
20	46.000040				IEEE 802	10	21	1394396621.000056000	Beacon Request
21	48.000043				IEEE 802	10	22	1394396623.000059000	Beacon Request

ApiMote PCAP

No.	Time	Source	Preamble	Destination	Protocol	Length	Sequence Number	Epoch Time	Info
6	5.999984		00 00 00 00		IEEE 802	10	1	1394396581.000000000	Beacon Request
7	15.999997		00 00 00 00		IEEE 802	10	6	1394396591.000013000	Beacon Request
8	26.000011		00 00 00 00		IEEE 802	10	11	1394396601.000027000	Beacon Request
9	35.999988		00 00 00 00		IEEE 802	10	16	1394396611.000004000	Beacon Request
10	46.000040		00 00 00 00		IEEE 802	10	21	1394396621.000056000	Beacon Request
11	55.999991		00 00 00 00		IEEE 802	10	26	1394396631.000007000	Beacon Request
12	66.000068		00 00 00 00		IEEE 802	10	31	1394396641.000084000	Beacon Request
13	76.000083		00 00 00 00		IEEE 802	10	36	1394396651.000099000	Beacon Request
14	86.999996		00 00 00 00		IEEE 802	10	41	1394396662.000012000	Beacon Request
15	97.000012		00 00 00 00		IEEE 802	10	46	1394396672.000028000	Beacon Request

There be pwnage in PHY!

~~Know your PHY!~~ Thou shalt know thy PHY!

Byte (even symbol) boundaries are imaginary

The deeper a layer, the simpler are its machines; they know nothing of sender's intent

Layers of abstraction become boundaries of competence.

ENJOY BABYLON!