Bluetooth Low Energy

Robin Heydon
Senior Director, Technology, Qualcomm

Starting Premise

If we are going to connect Everything to the Internet,
we have to give everything wireless connectivity

These must be powered somehow
(RFID, Wireless Power, Coin Cell Batteries, Nuclear Power Stations)

If they are battery powered
you can't change batteries every week/month/year

50 devices in a home, their batteries last a year
how often do you have to change their batteries?

IETF RFC 1925

(7) Good, Fast, Cheap: Pick any two (you can't have all three).

(8) It is more complicated than you think.

(10) One size never fits all.

Wi-Fi	Good / Fast / !Cheap
Bluetooth	Good / !Fast / Cheap

(12) In protocol design, perfection has been reached not when there is nothing left to add, but when there is nothing left to take away.

https://tools.ietf.org/html/rfc1925

Design Goals

1) Good and Cheap
   does not need to be fast

2) Design around the single biggest constraint
   Coin Cell Batteries

3) Design around major use cases, ignore everything else
   no audio, no streaming, no connection-oriented data

Basic Concepts

Optimize ***EVERYTHING*** for lowest power consumption

from the physics to the users

Why?

button cells will be main power source for peripherals

~15 mA peak current

~19 µA average current

Basic Concepts

Receiving more expensive, Transmitting cheap

- best optimize to reduce Rx time as much possible

Advertising Channels – discovery / connections

- just use 3 channels – reduces time to find devices
- smallest battery device advertises
  - “Peripheral”

Basic Concepts

Memory is expensive

- memory requires silicon area – costs money
- memory increases leakage current – costs battery life

Reduce dynamic memory footprint for specs

- keep packets short – less buffer memory
- keep protocol simple – less state information
- keep services simple – one protocol / defined behavior

Basic Concepts

Keep packets short

- when Tx – short packets don't need constant re-calibration
  - reduces peak current during Tx
- when Rx – radio on for less time
  - reduces total current usage

Optimized for low power consumption

Basic Concepts

Peripherals are simple – very resource constrained

- optimize peripherals first

Central devices are complex – lots of memory & battery

- not as critical to optimize here

Asymmetry is Good

Basic Concepts

Design for Success

- able to discover thousands of devices in local area
- unlimited number of slaves connected to a master
- unlimited number of masters
- state of the art encryption
- security including privacy / authentication / authorization
- class leading robustness, data integrity
- future proof

Basic Concepts

Everything has **STATE**

- devices expose their state
- these are servers

Clients can use the state exposed on servers

- read it – get current temperature
- write it – increase set point temperature for room

Servers can tell clients when state updates

- notify it – temperature up to set point

Basic Concepts

Client Server Architecture

- proven architecture for web-infrastructure

Gateways allow interconnect of internet & low energy

- weighing scales send reports to doctor
- home security web site shows all windows closed
- assisted living for your parents allows low cost monitoring
- sports data immediately uploaded via cellular phone

New Connection Models

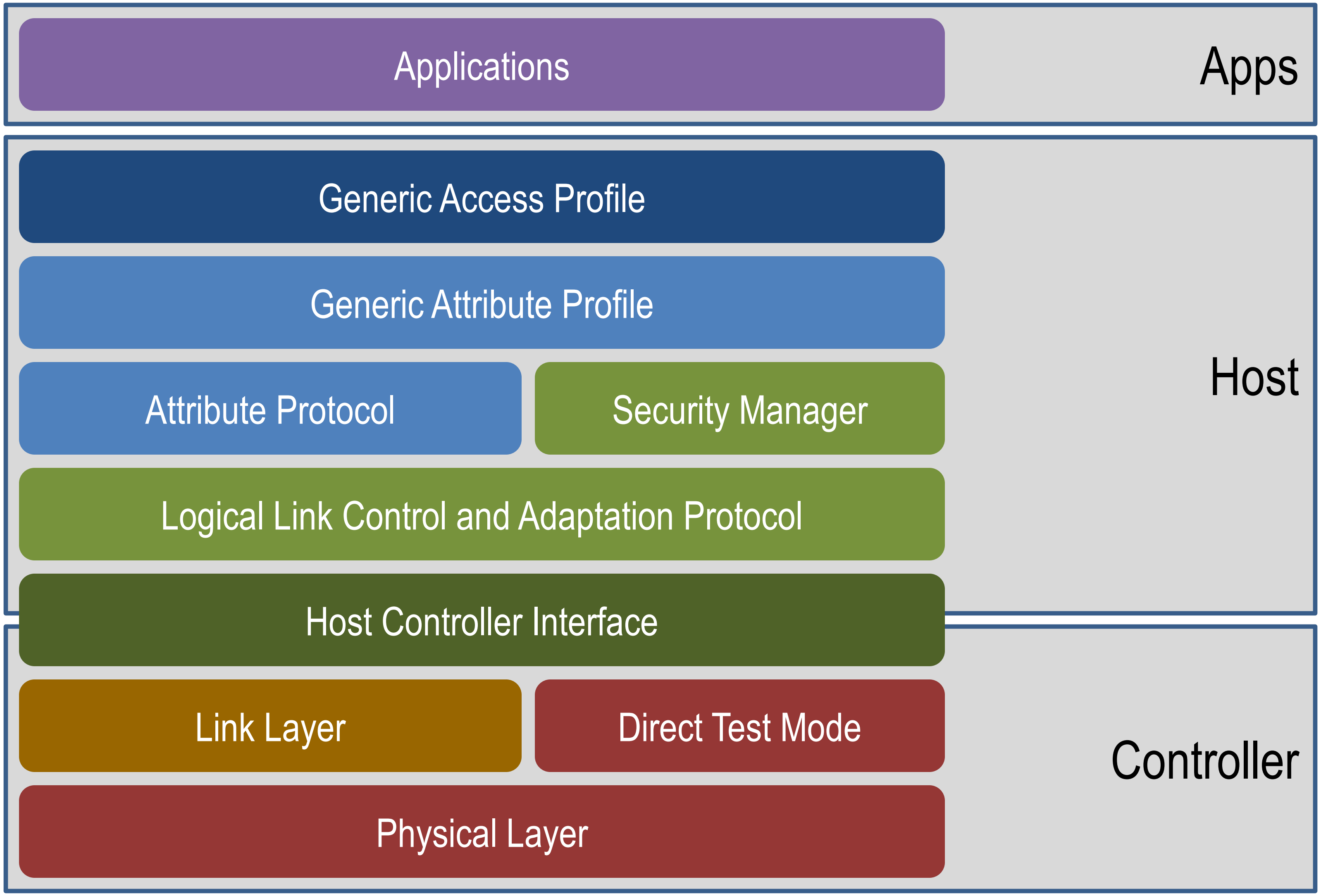
Classic Bluetooth is largely cable replacement:

- Headset Cables
- Mouse Cables
- Keyboard Cables

Bluetooth low energy is application enabling:

- Accessories for smartphone apps
- Internet connected devices
- New billion unit markets

Stack Architecture



Physical Layer

Uses 2.4 GHz ISM Band

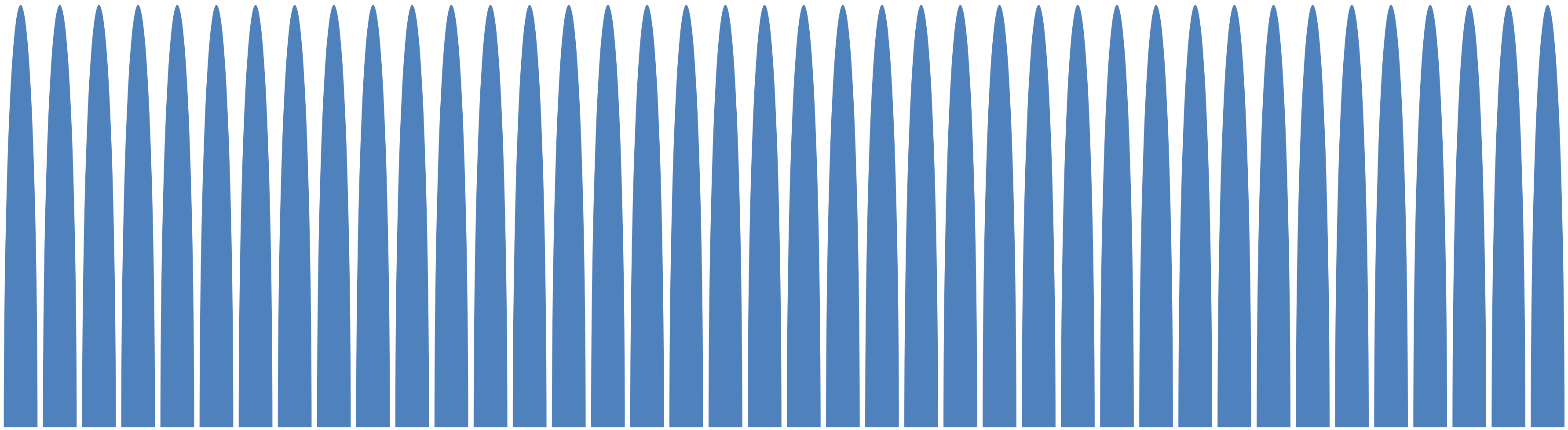
- Industrial Scientific Medical band
- License Free – with certain rules
- 2400 MHz to 2483.5 MHz

Used by many other standards

- IEEE 802.11, IEEE 802.15
- and many proprietary radios

40 Physical Channels

$$f = 2402 + 2 \cdot k \text{ MHz}$$



RF	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	33	34	35	36	37	38	39
Frequency	2402 MHz	2404 MHz	2406 MHz	2408 MHz	2410 MHz	2412 MHz	2414 MHz	2416 MHz	2418 MHz	2420 MHz	2422 MHz	2424 MHz	2426 MHz	2428 MHz	2430 MHz	2432 MHz	2434 MHz	2436 MHz	2438 MHz	2440 MHz	2442 MHz	2444 MHz	2446 MHz	2448 MHz	2450 MHz	2452 MHz	2454 MHz	2456 MHz	2458 MHz	2460 MHz	2462 MHz	2464 MHz	2466 MHz	2468 MHz	2470 MHz	2472 MHz	2474 MHz	2476 MHz	2478 MHz	2480 MHz

Modulation

GFSK Modulation

bit period product BT = 0.5

modulation index = 0.5 ± 0.05

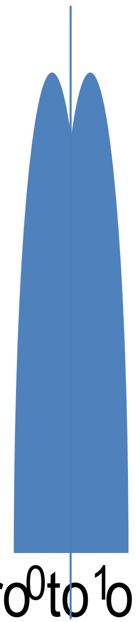
PHY Bandwidth = 1 million bits / seconds

Why GFSK?

"pulse shaping"

Gaussian filter smoothes transitions from zero to one

reduces spectral width



Link Layer (LL)

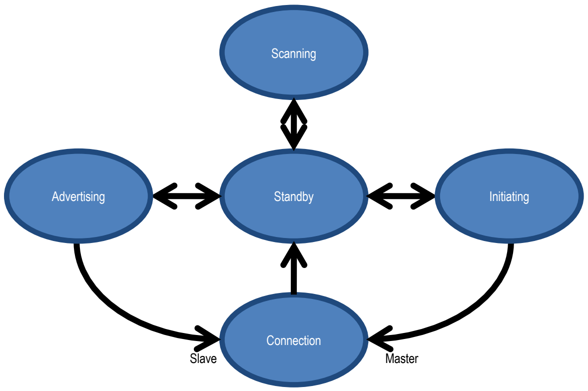
Link Layer State Machine

- can have multiple state machines active in device

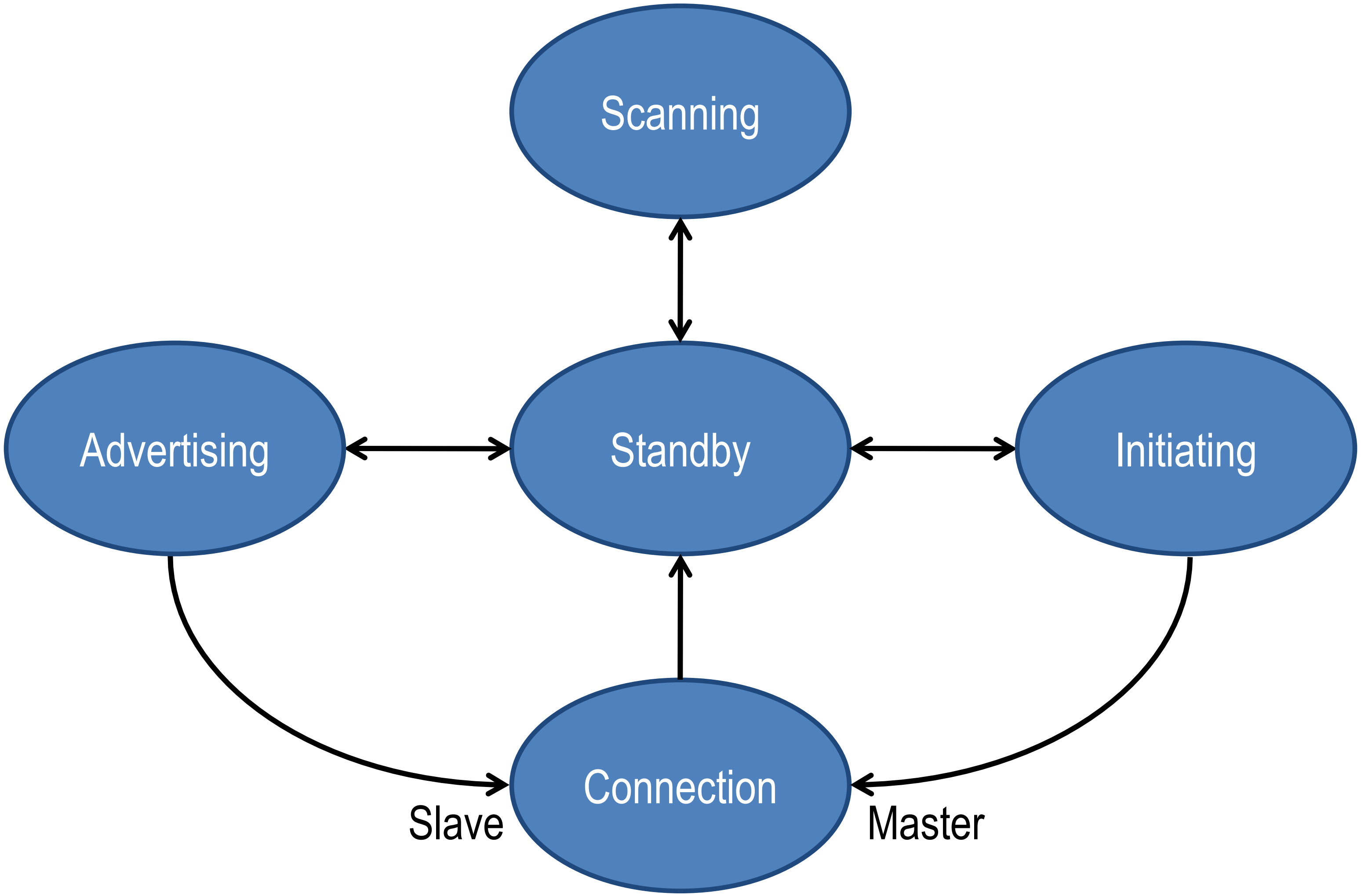
Link Layer Channels

- Advertising Channels & Data Channels
- Advertising Packets & Data Packets

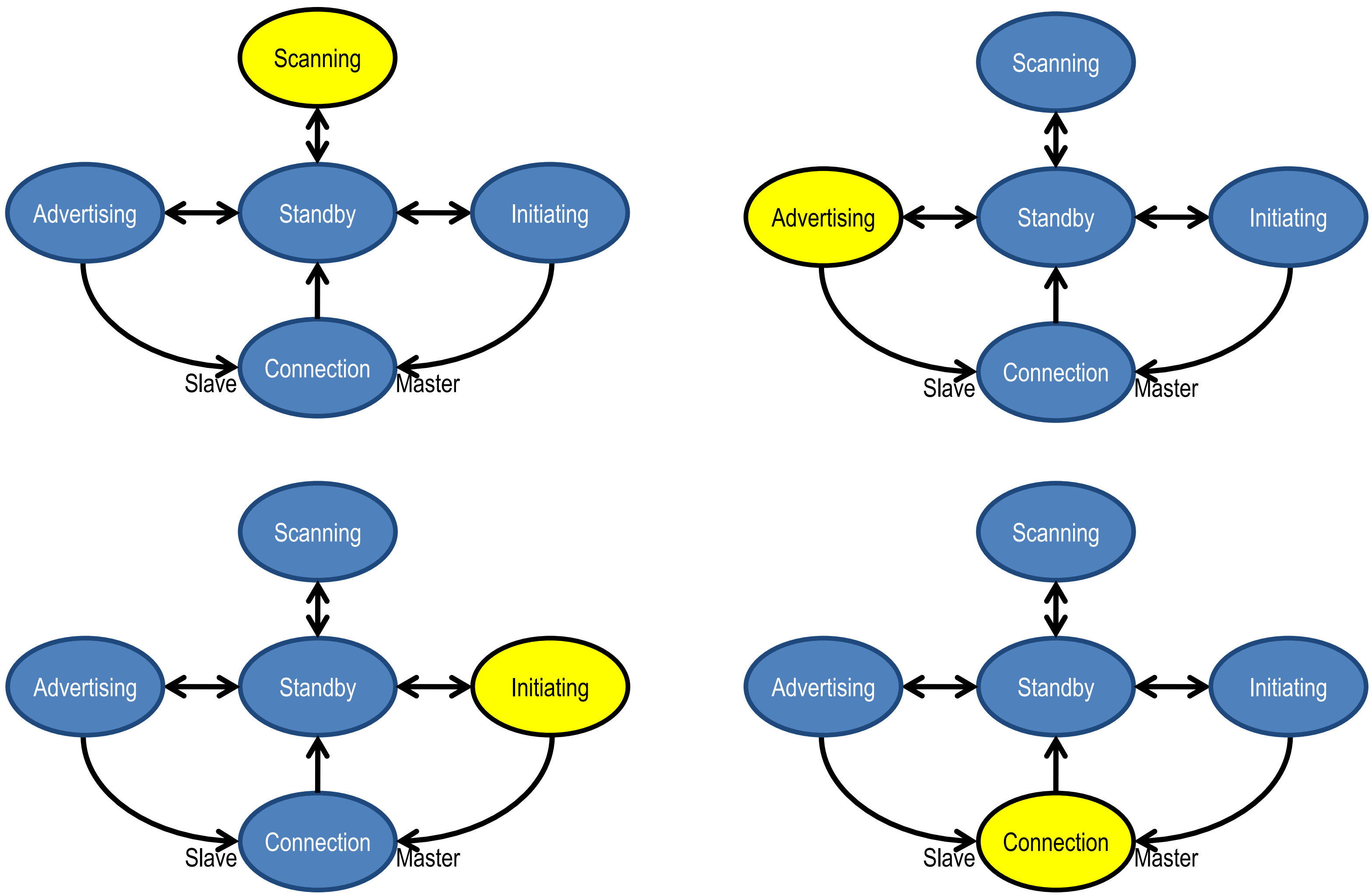
Link Layer Control Procedures



Link Layer State Machine

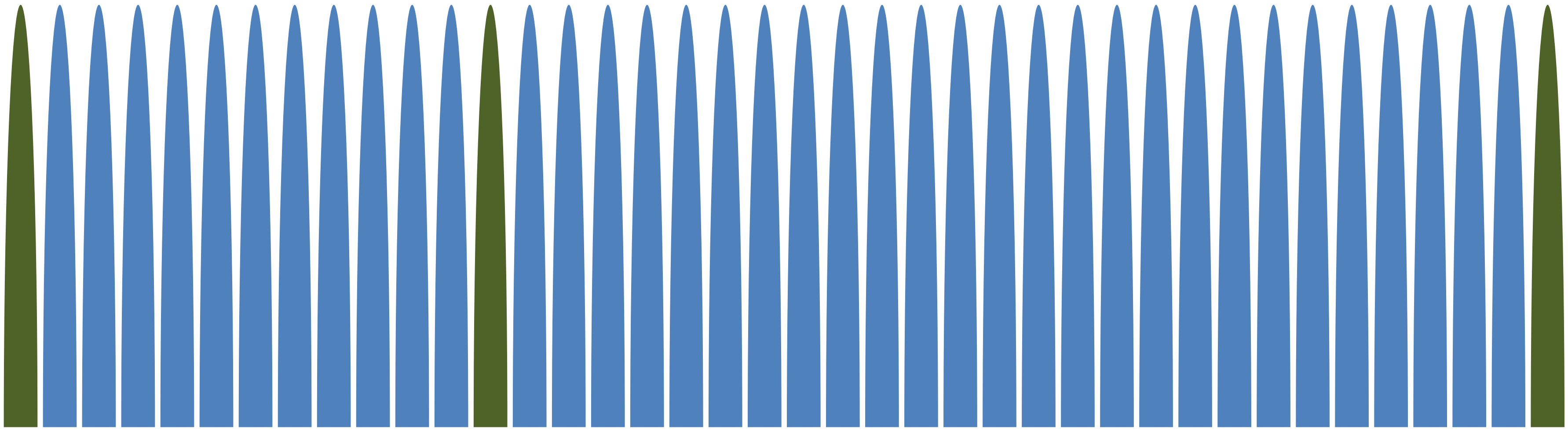


Link Layer State Machine(s)



Link Layer Channels

3 Advertising Channels and 37 Data Channels



LL	Frequency
37	2402 MHz
0	2404 MHz
1	2406 MHz
2	2408 MHz
3	2410 MHz
4	2412 MHz
5	2414 MHz
6	2416 MHz
7	2418 MHz
8	2420 MHz
9	2422 MHz
10	2424 MHz
38	2426 MHz
11	2428 MHz
12	2430 MHz
13	2432 MHz
14	2434 MHz
15	2436 MHz
16	2438 MHz
17	2440 MHz
18	2442 MHz
19	2444 MHz
20	2446 MHz
21	2448 MHz
22	2450 MHz
23	2452 MHz
24	2454 MHz
25	2456 MHz
26	2458 MHz
27	2460 MHz
28	2462 MHz
29	2464 MHz
30	2466 MHz
31	2468 MHz
32	2470 MHz
33	2472 MHz
34	2474 MHz
35	2476 MHz
36	2478 MHz
39	2480 MHz

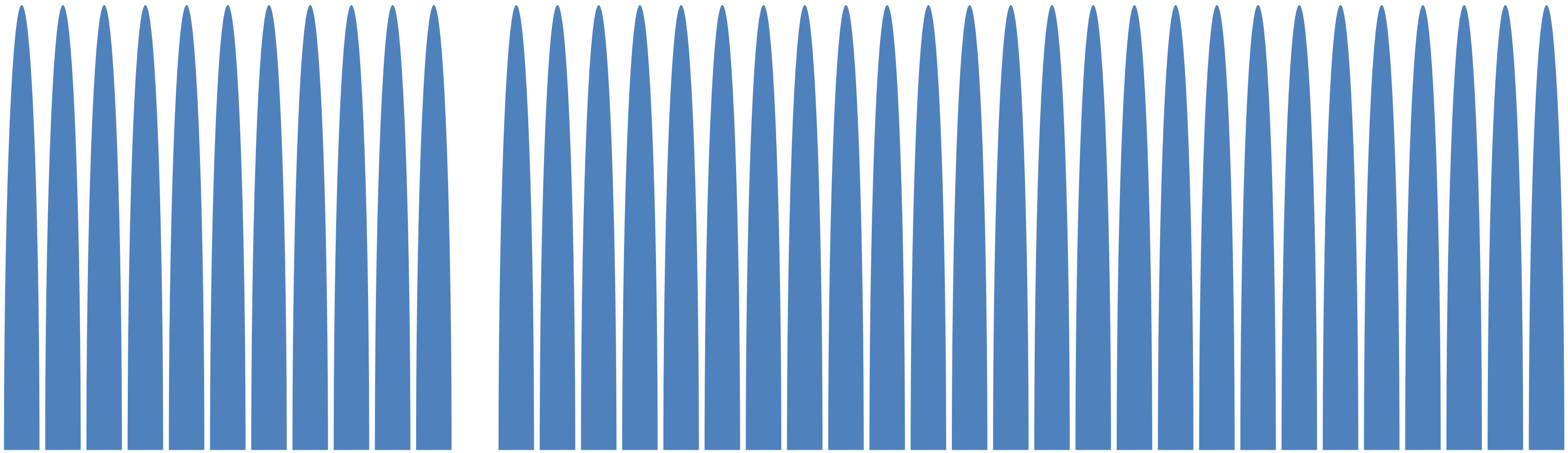
Link Layer Channels

3 Advertising Channels

LL	Frequency
37	**2402 MHz**
0	2404 MHz
1	2406 MHz
2	2408 MHz
3	2410 MHz
4	2412 MHz
5	2414 MHz
6	2416 MHz
7	2418 MHz
8	2420 MHz
9	2422 MHz
10	2424 MHz
38	**2426 MHz**
11	2428 MHz
12	2430 MHz
13	2432 MHz
14	2434 MHz
15	2436 MHz
16	2438 MHz
17	2440 MHz
18	2442 MHz
19	2444 MHz
20	2446 MHz
21	2448 MHz
22	2450 MHz
23	2452 MHz
24	2454 MHz
25	2456 MHz
26	2458 MHz
27	2460 MHz
28	2462 MHz
29	2464 MHz
30	2466 MHz
31	2468 MHz
32	2470 MHz
33	2472 MHz
34	2474 MHz
35	2476 MHz
36	2478 MHz
39	**2480 MHz**

Link Layer Channels

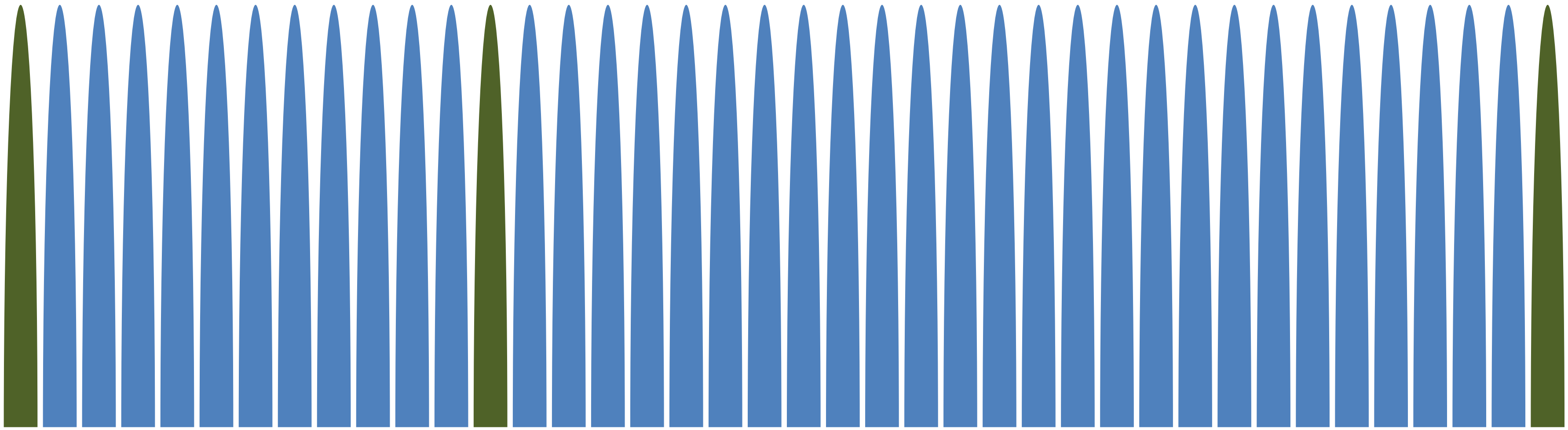
37 Data Channels



LL	Frequency
37	2402 MHz
0	2404 MHz
1	2406 MHz
2	2408 MHz
3	2410 MHz
4	2412 MHz
5	2414 MHz
6	2416 MHz
7	2418 MHz
8	2420 MHz
9	2422 MHz
10	2424 MHz
38	2426 MHz
11	2428 MHz
12	2430 MHz
13	2432 MHz
14	2434 MHz
15	2436 MHz
16	2438 MHz
17	2440 MHz
18	2442 MHz
19	2444 MHz
20	2446 MHz
21	2448 MHz
22	2450 MHz
23	2452 MHz
24	2454 MHz
25	2456 MHz
26	2458 MHz
27	2460 MHz
28	2462 MHz
29	2464 MHz
30	2466 MHz
31	2468 MHz
32	2470 MHz
33	2472 MHz
34	2474 MHz
35	2476 MHz
36	2478 MHz
39	2480 MHz

Link Layer Channels

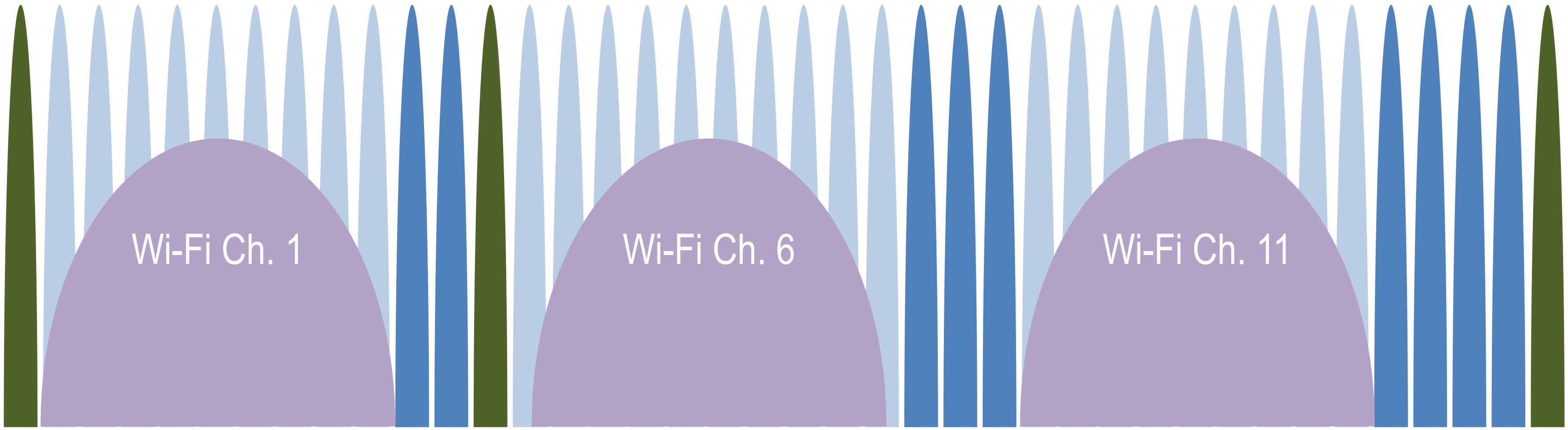
3 Advertising Channels and 37 Data Channels



LL	Frequency
37	2402 MHz
0	2404 MHz
1	2406 MHz
2	2408 MHz
3	2410 MHz
4	2412 MHz
5	2414 MHz
6	2416 MHz
7	2418 MHz
8	2420 MHz
9	2422 MHz
10	2424 MHz
38	2426 MHz
11	2428 MHz
12	2430 MHz
13	2432 MHz
14	2434 MHz
15	2436 MHz
16	2438 MHz
17	2440 MHz
18	2442 MHz
19	2444 MHz
20	2446 MHz
21	2448 MHz
22	2450 MHz
23	2452 MHz
24	2454 MHz
25	2456 MHz
26	2458 MHz
27	2460 MHz
28	2462 MHz
29	2464 MHz
30	2466 MHz
31	2468 MHz
32	2470 MHz
33	2472 MHz
34	2474 MHz
35	2476 MHz
36	2478 MHz
39	2480 MHz

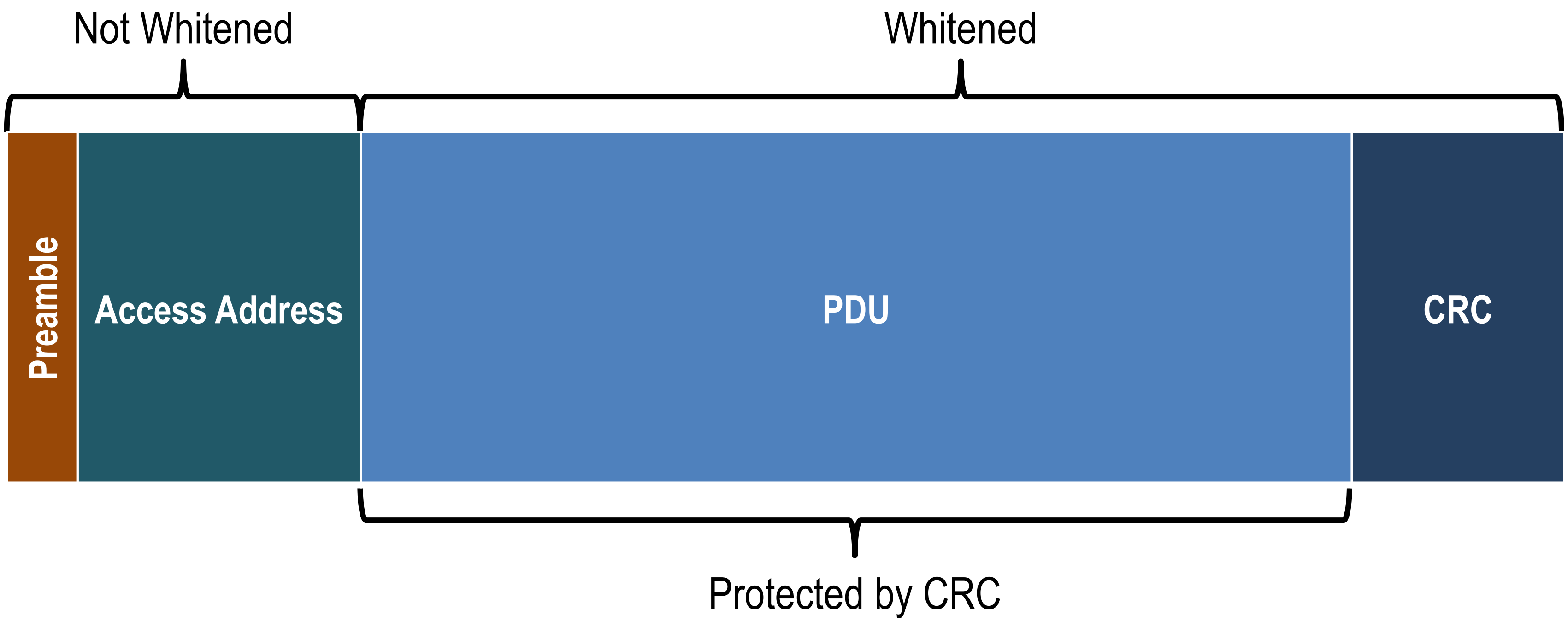
Link Layer Channels

9 LL Data Channels still available

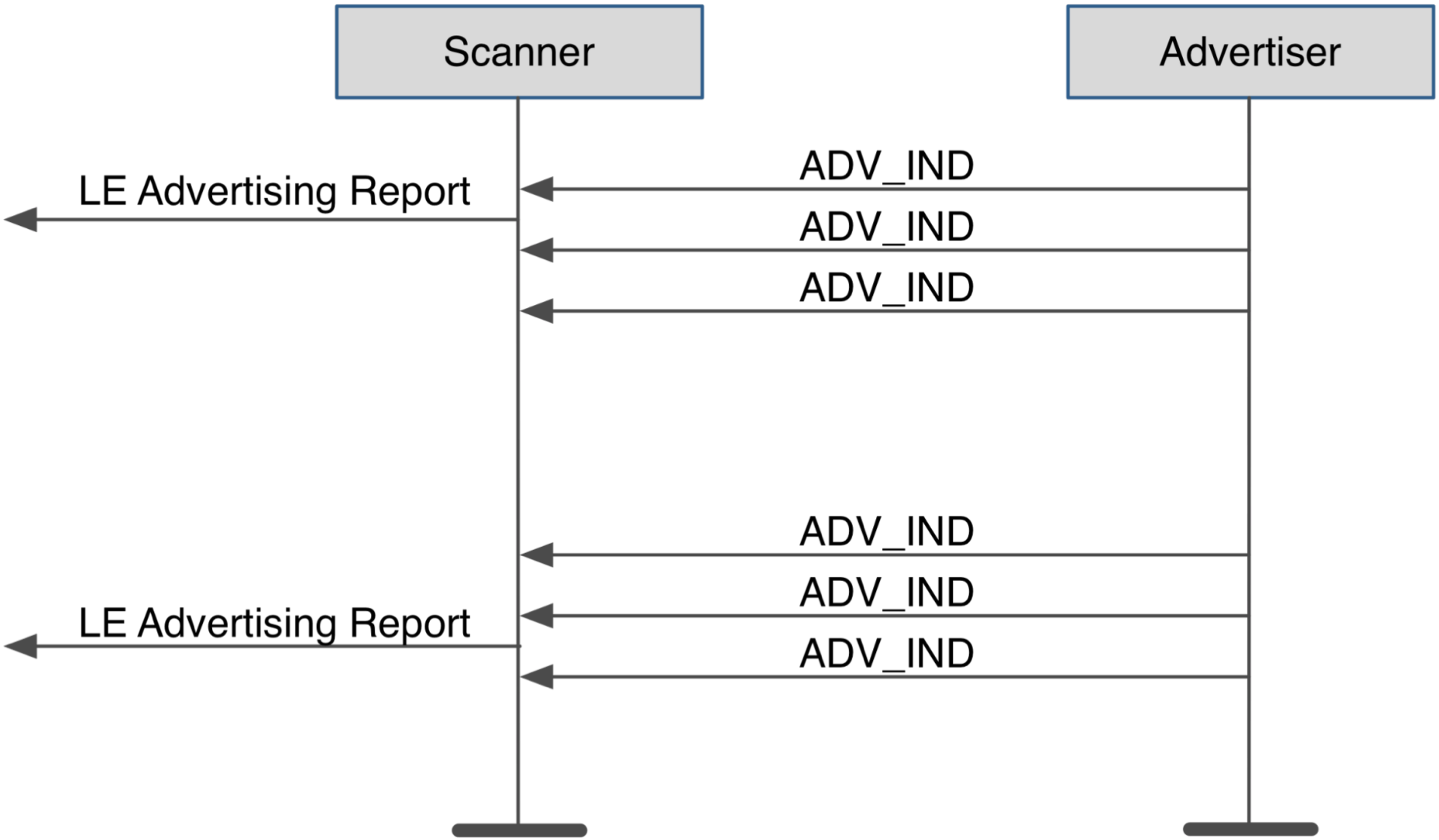


LL	Frequency
37	2402 MHz
0	2404 MHz
1	2406 MHz
2	2408 MHz
3	2410 MHz
4	2412 MHz
5	2414 MHz
6	2416 MHz
7	2418 MHz
8	2420 MHz
9	2422 MHz
10	2424 MHz
38	2426 MHz
11	2428 MHz
12	2430 MHz
13	2432 MHz
14	2434 MHz
15	2436 MHz
16	2438 MHz
17	2440 MHz
18	2442 MHz
19	2444 MHz
20	2446 MHz
21	2448 MHz
22	2450 MHz
23	2452 MHz
24	2454 MHz
25	2456 MHz
26	2458 MHz
27	2460 MHz
28	2462 MHz
29	2464 MHz
30	2466 MHz
31	2468 MHz
32	2470 MHz
33	2472 MHz
34	2474 MHz
35	2476 MHz
36	2478 MHz
39	2480 MHz

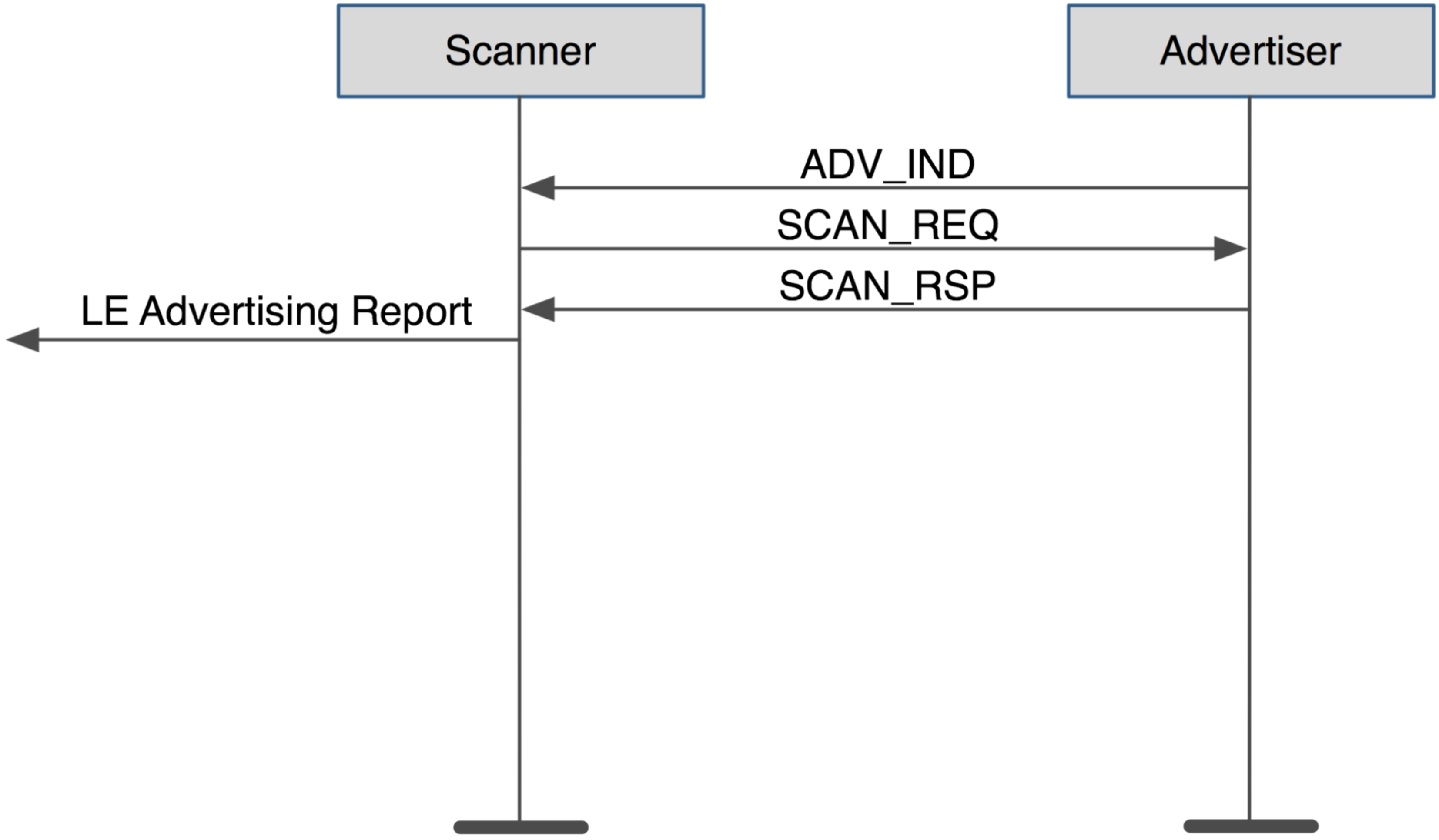
One Packet Format



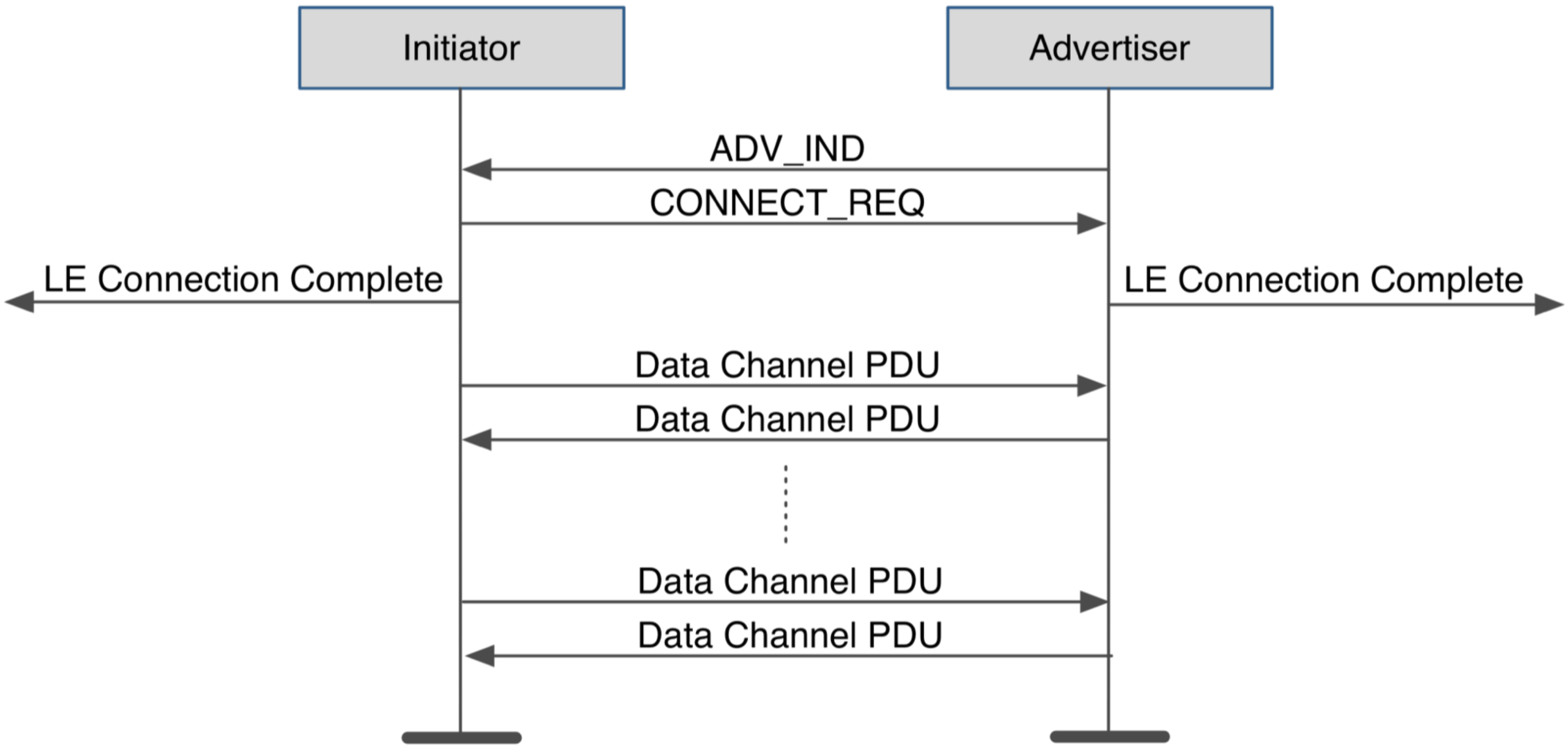
Passive Scanning



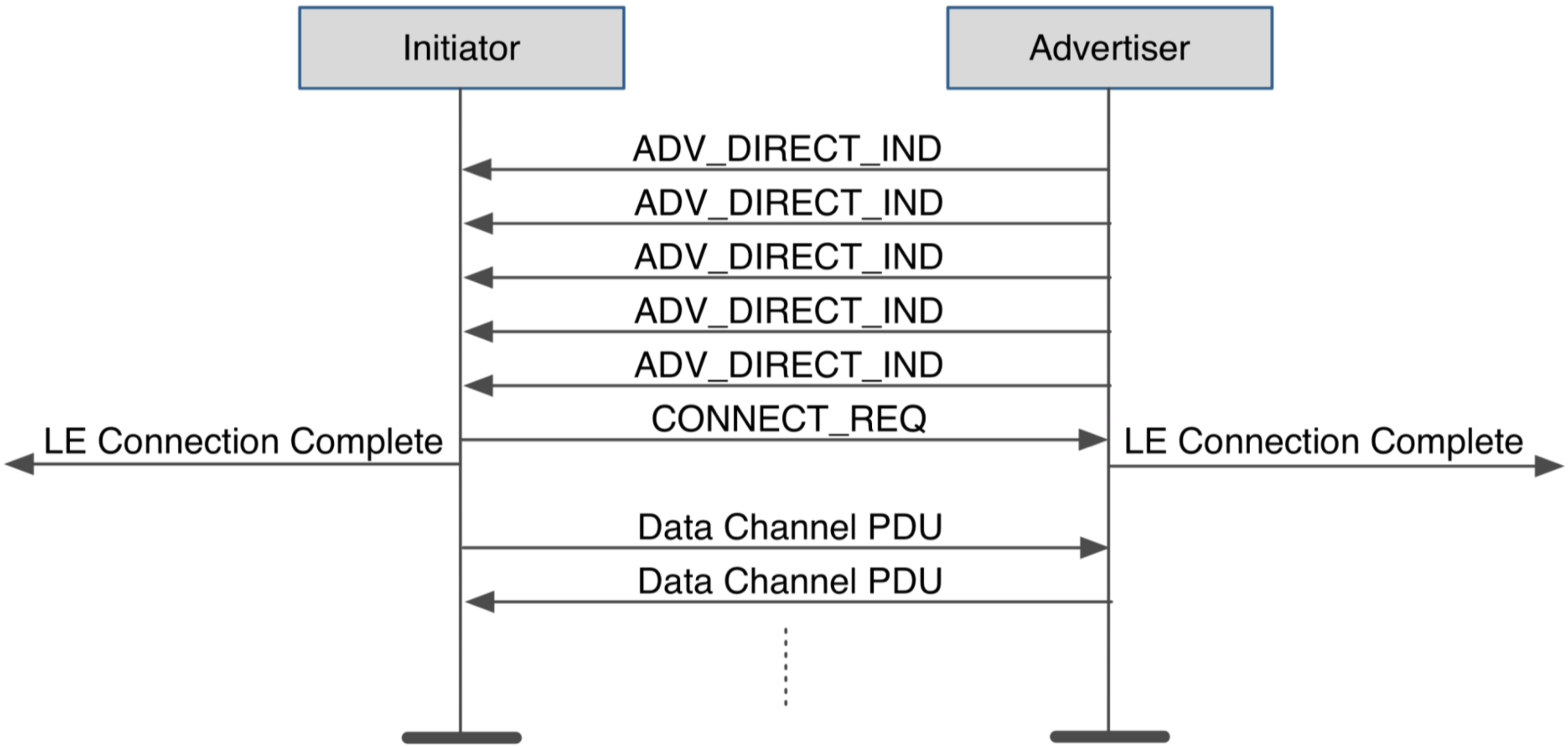
Active Scanning



Initiating Connections

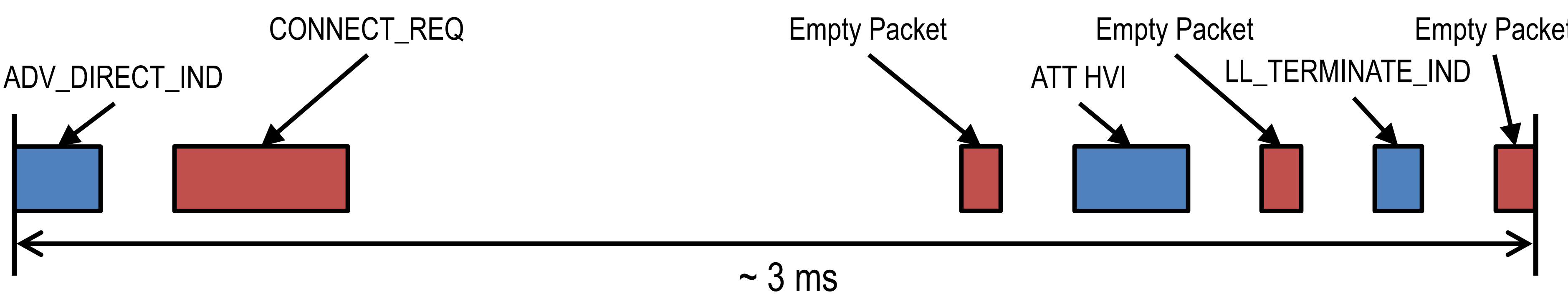


Directed Connections

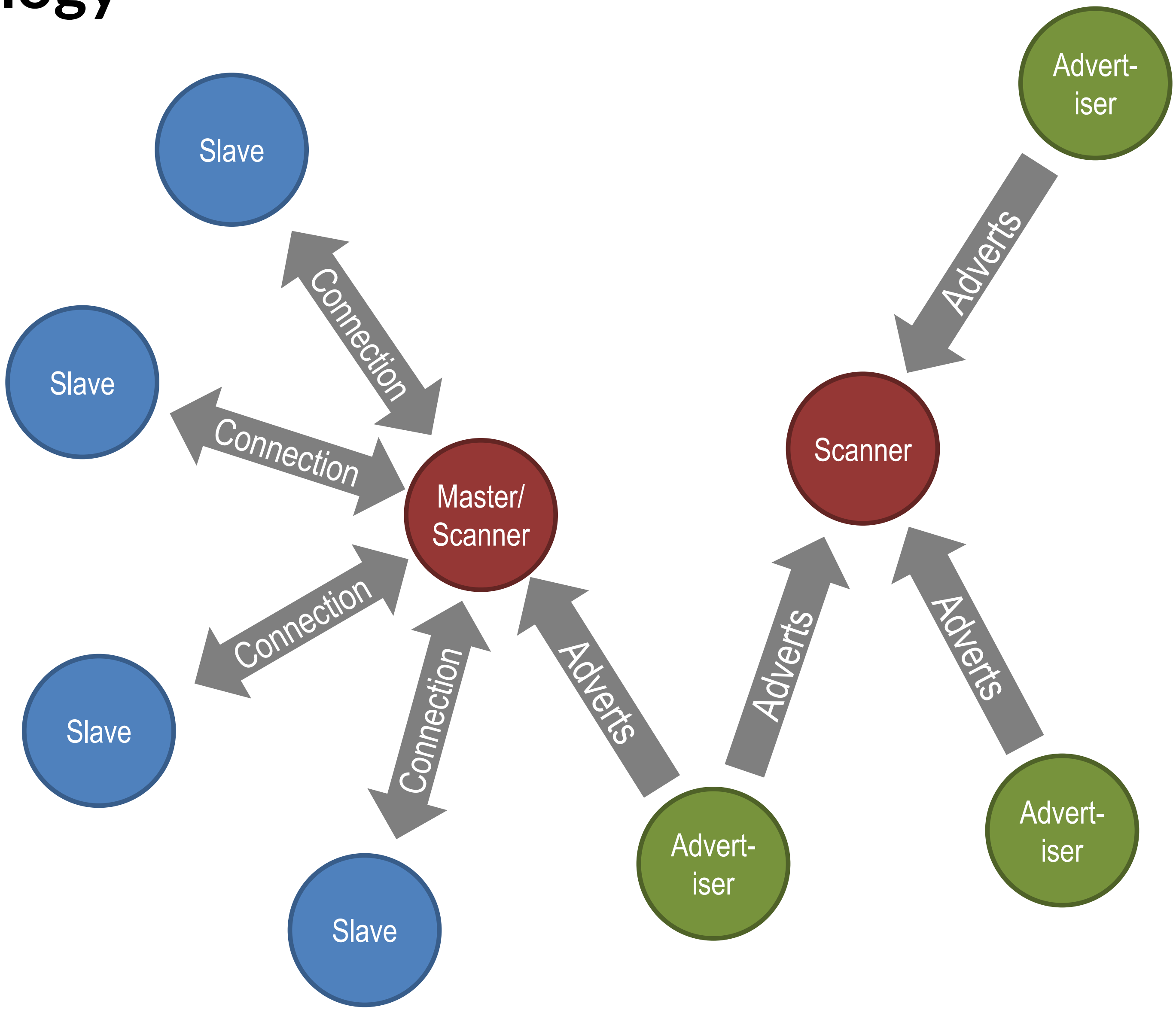


Time From Disconnected To Data ~ 3ms (Radio Active ~ 1ms)

Time (us)	Master Tx	Radio Active (us)	Slave Tx
0		176	ADV_DIRECT_IND
326	CONNECT_REQ	352	
1928	Empty Packet	80	
2158		144	Attribute Protocol Handle Value Indication
2452	Empty Packet (Acknowledgement)	80	
2682		96	LL_TERMINATE_IND
2928	Empty Packet (Acknowledgement)	80	

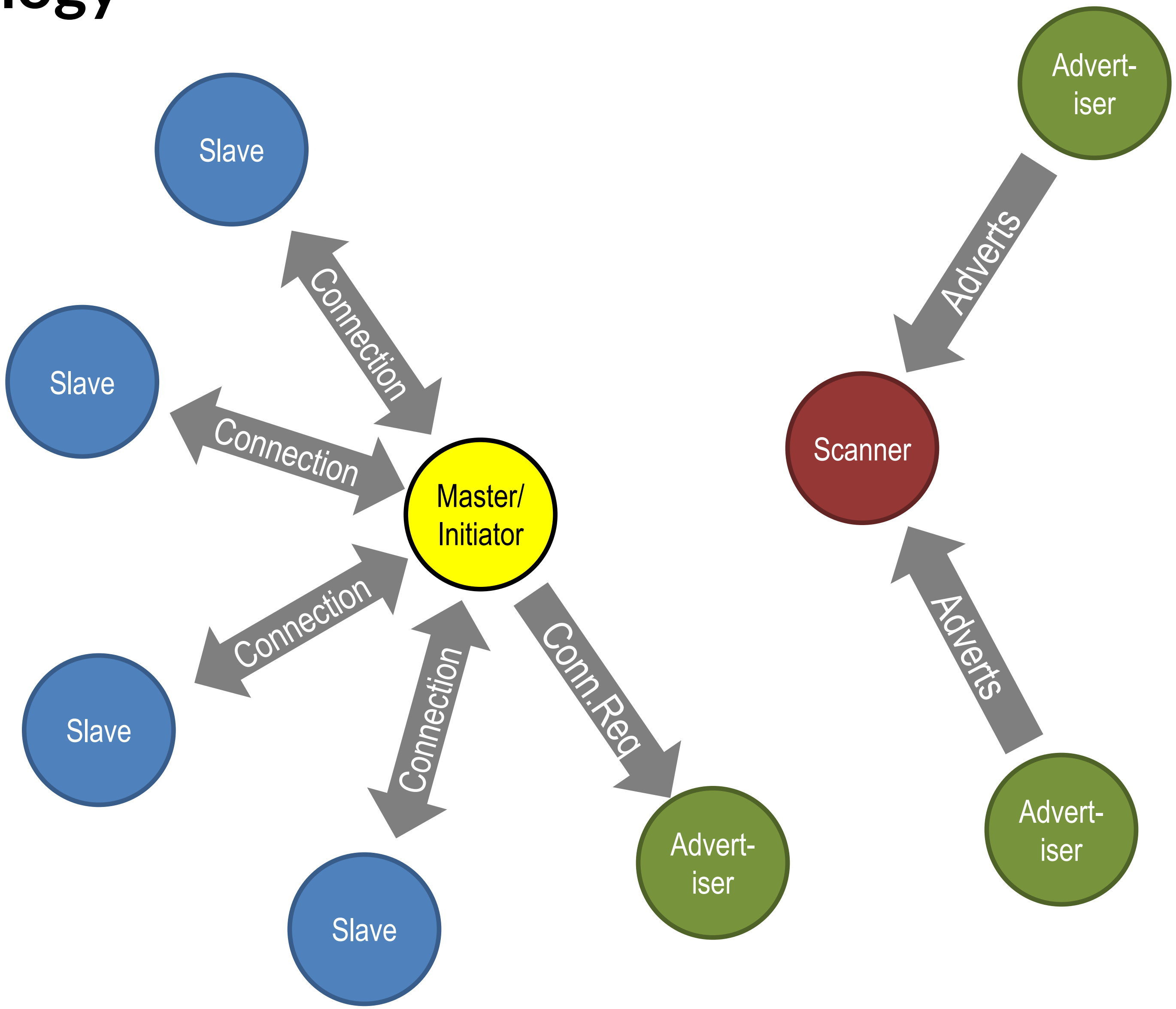


Topology



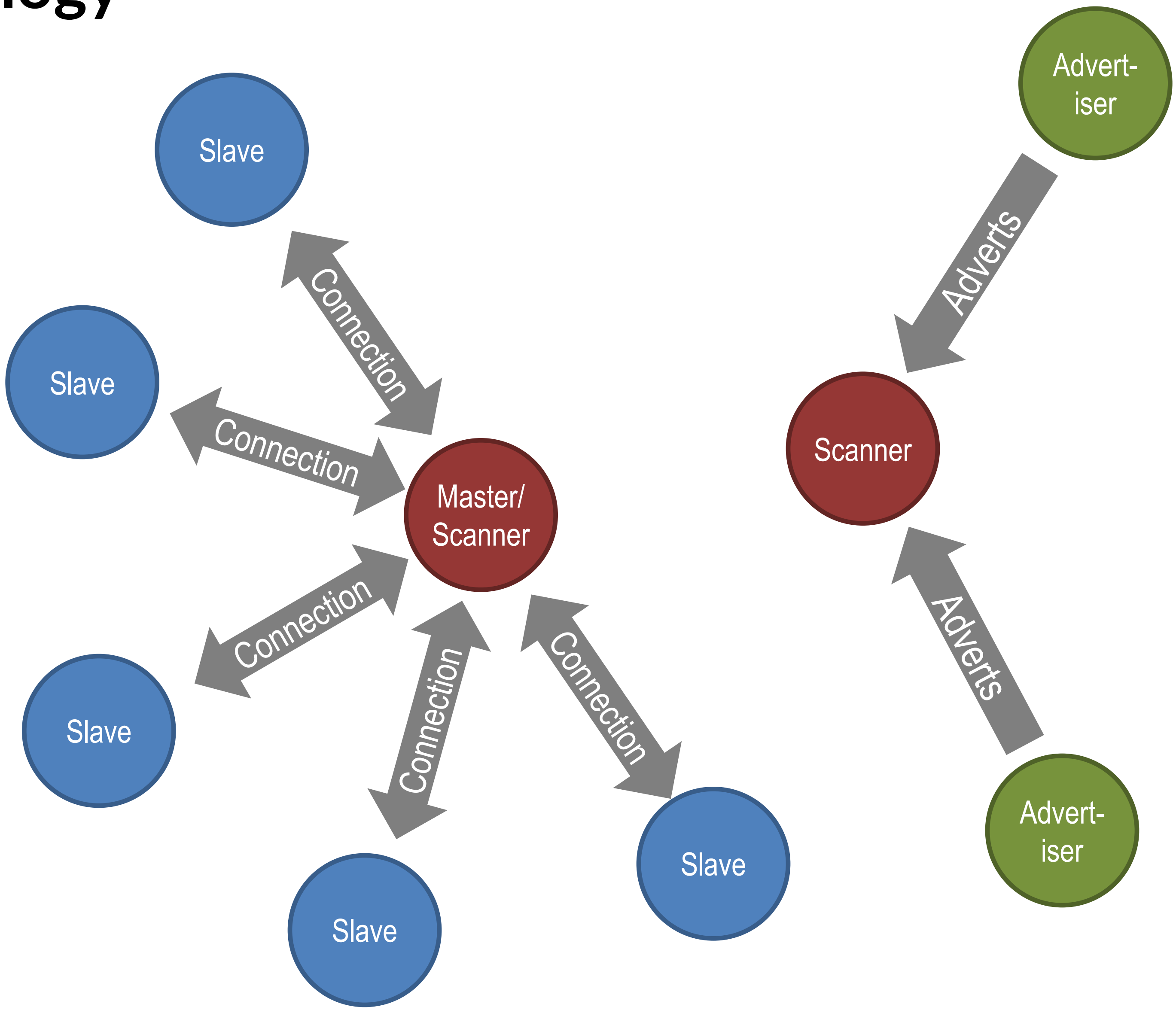
Slave
Slave
Slave
Slave
Connection
Connection
Connection
Connection
Master/
Scanner
Scanner
Advert-
iser
Advert-
iser
Advert-
iser
Adverts
Adverts
Adverts
Adverts

Topology



Slave
Slave
Slave
Slave
Connection
Connection
Connection
Connection
Master/ Initiator
Conn.Req
Advert-iser
Scanner
Adverts
Adverts
Advert-iser
Advert-iser

Topology


Slave
Slave
Slave
Slave
Slave
Connection
Connection
Connection
Connection
Connection
Master/
Scanner
Advert-
iser
Adverts
Scanner
Adverts
Advert-
iser

Limits

A single master can address ~2^{31} slaves

- ~ 2 billion addressable slaves per master

Max Connection Interval = 4.0 seconds

Can address a slave every ~ 5 ms (assuming 250 ppm clocks)

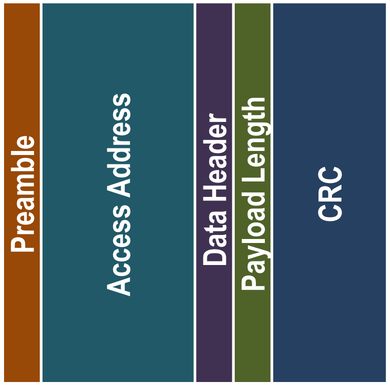
- ~ 800 active slaves per master

Connections

Used to send application data
- reliably, robustly

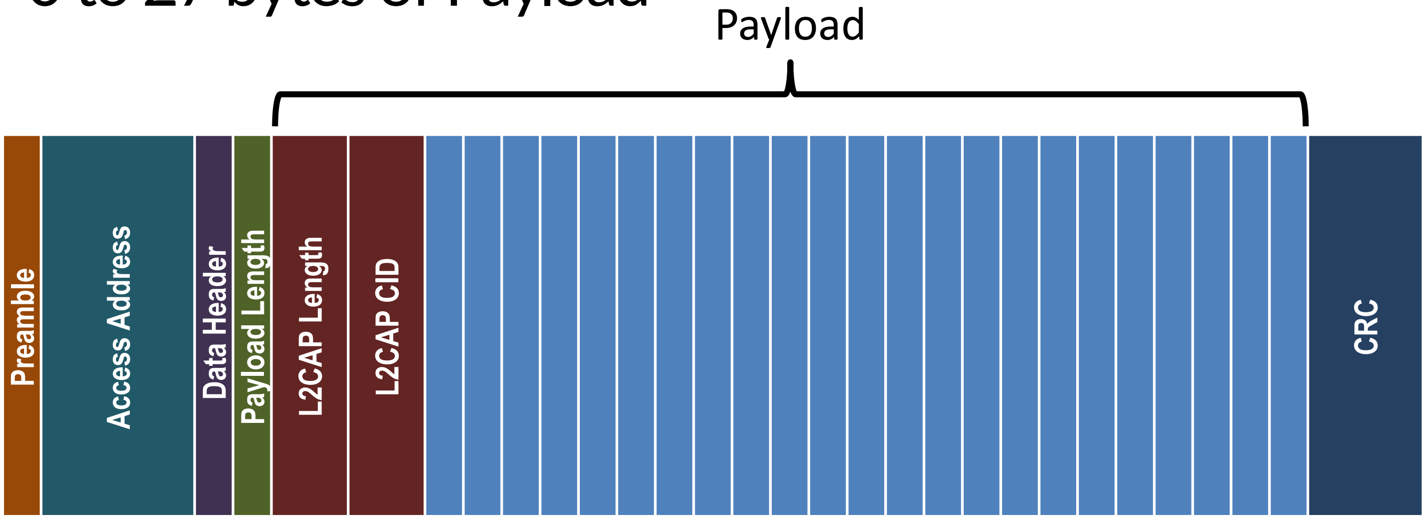
Includes
- ultra low power connection mode
- adaptive frequency hopping
- connection supervision timeout

Data Packet



Empty Packet

0 to 27 bytes of Payload

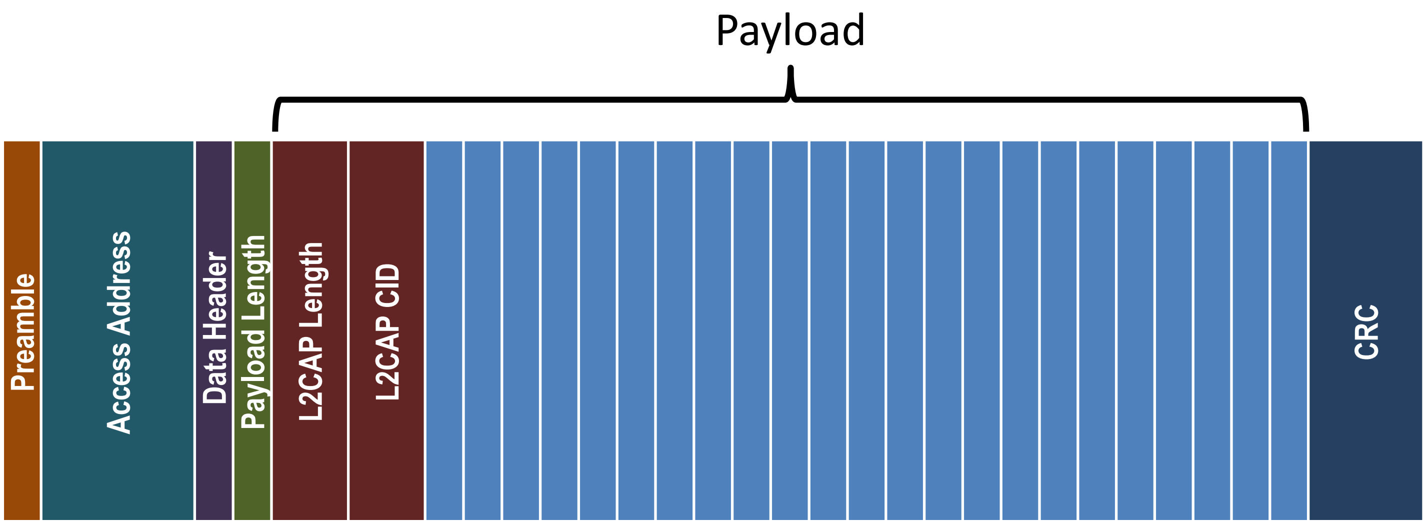


Data Packet

0 to 27 bytes of Payload (unencrypted)

CRC protects

- Data Header
- Payload Length
- Payload

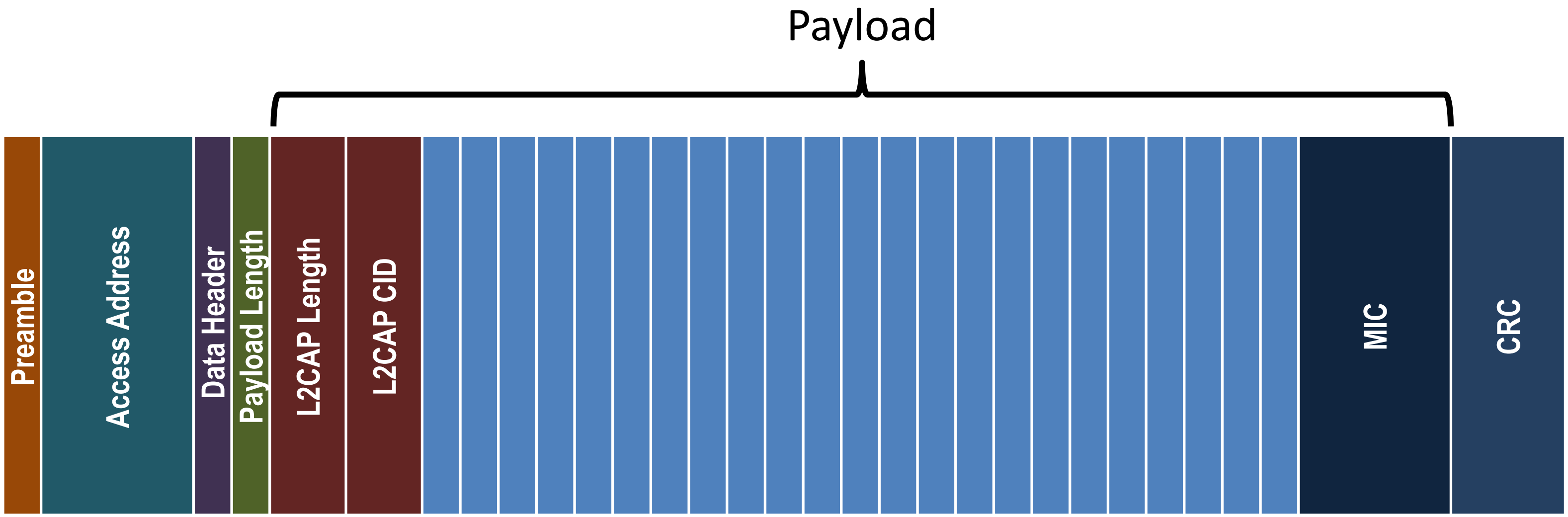


Encrypted Data Packet

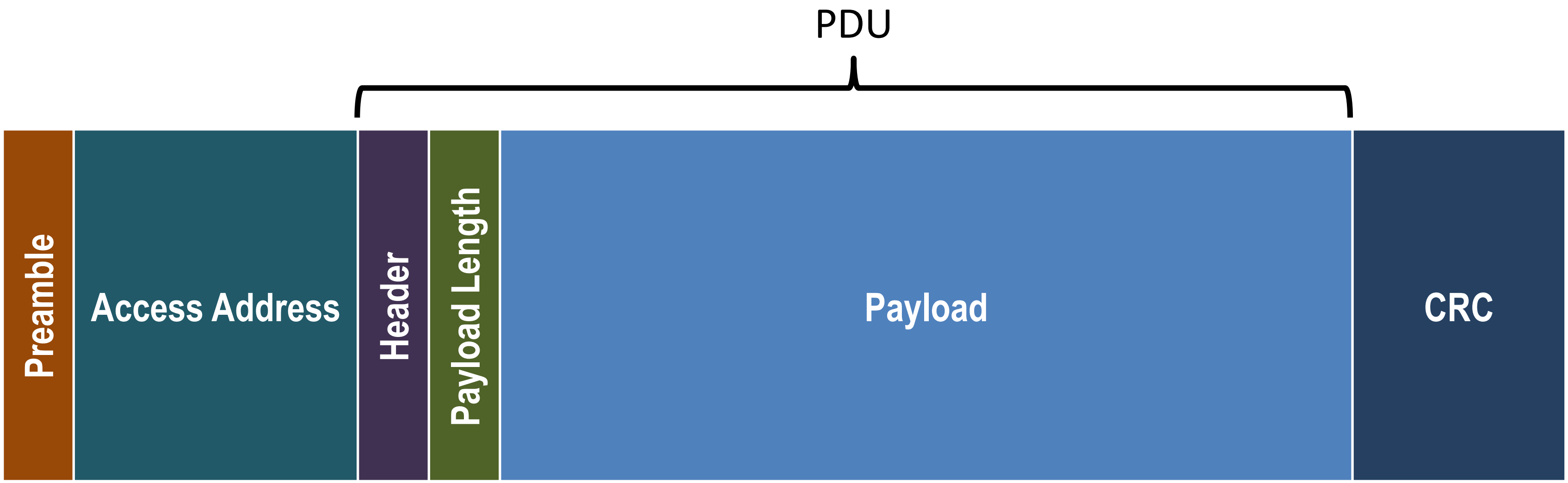
4 to 31 bytes of payload length

MIC is part of “Payload”, CRC protects it

MIC can be computed / checked in background



PDU Headers



Data channel PDU Header / Payload Length

LLID	NESN	SN	MD	RFU
Length (0 – 31)				RFU

Logical Link Identifier

LLID	Description
00	Reserved
01	LL Data PDU - Continuation of an L2CAP message or an Empty PDU
10	LL Data PDU - Start of an L2CAP message or a Complete L2CAP message
11	LL Control PDU

Sequence Numbers

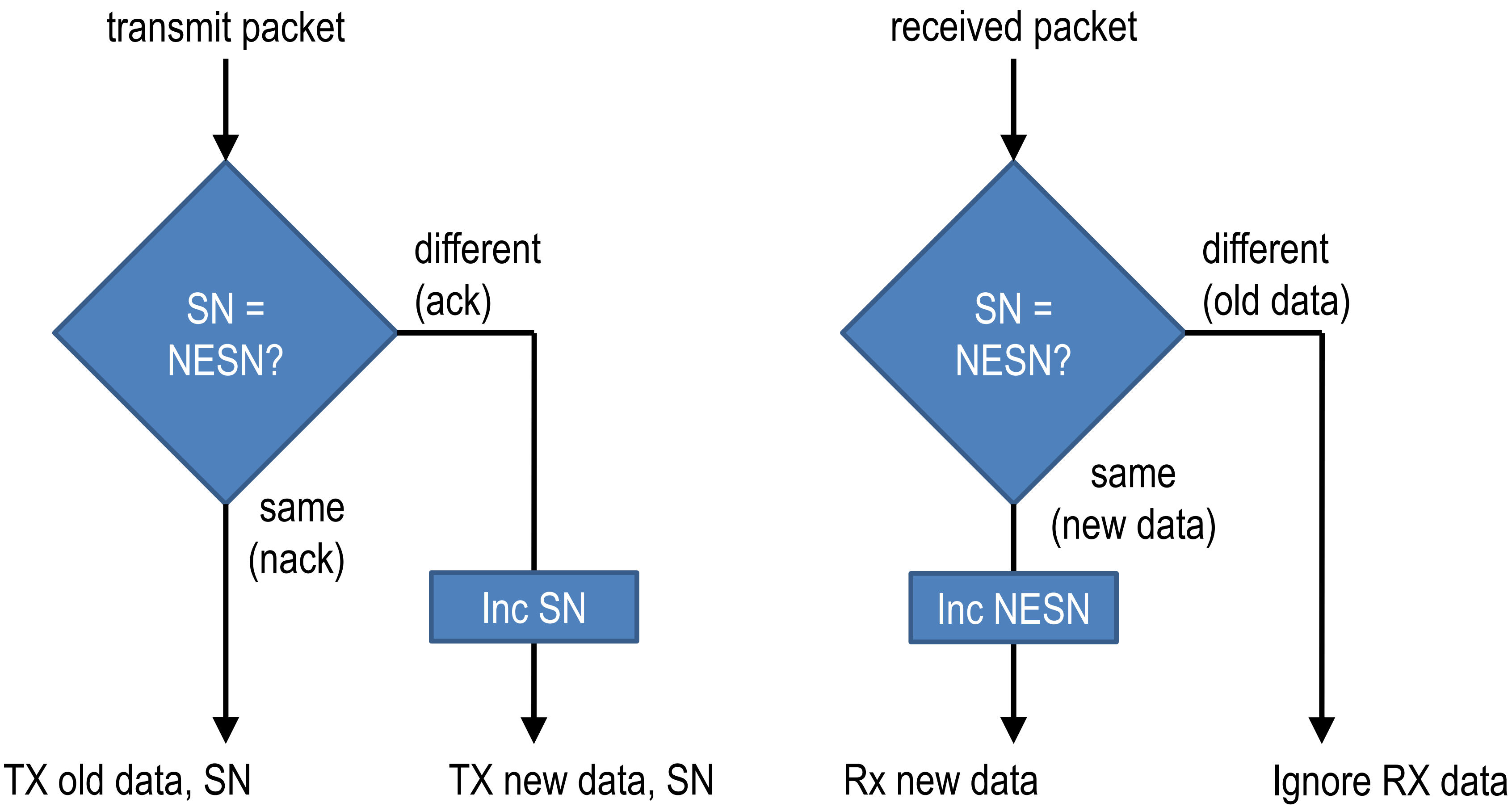
SN = Sequence Number

NESN = Next Expected Sequence Number

Sliding Window Algorithm

- window size of 1
- lazy acknowledgement possible – saves power

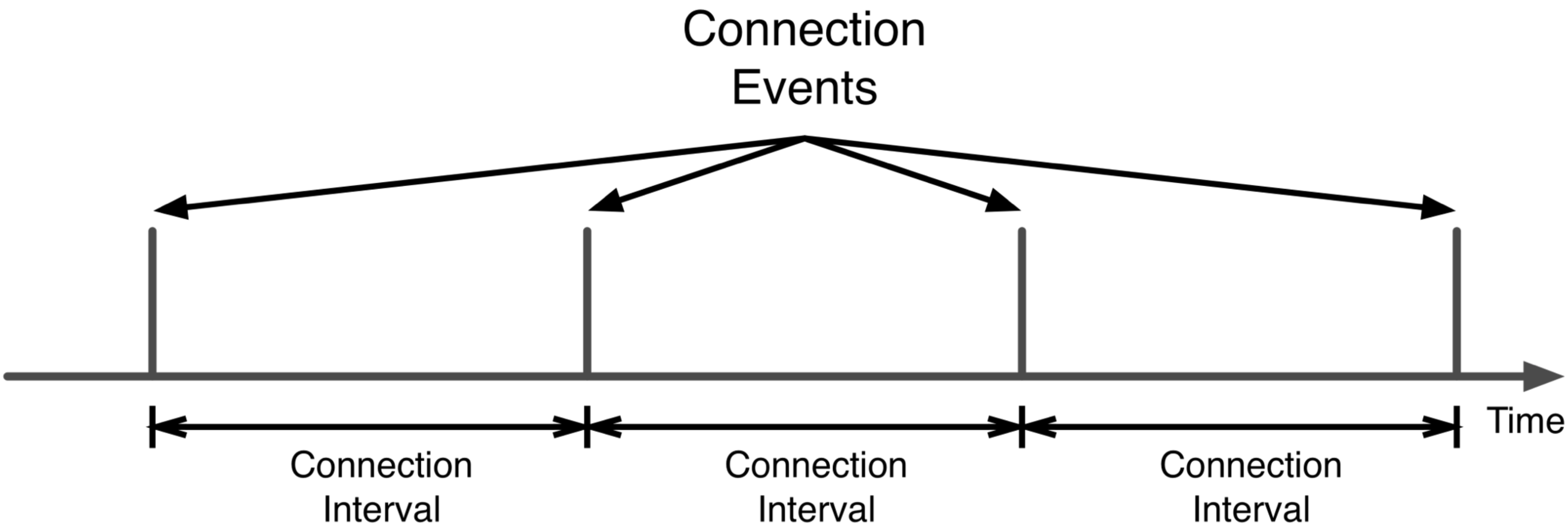
Transmitting Data



Connection Events

Masters transmits periodically at a connection events

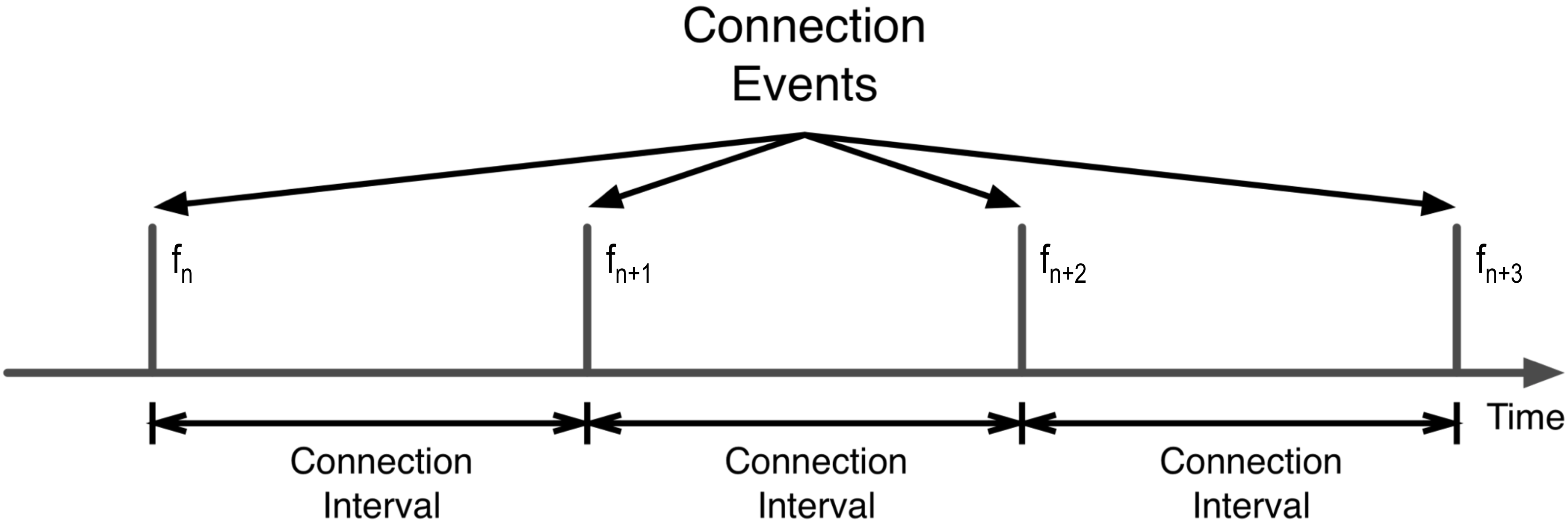
- Connection Interval sent in CONNECT_REQ
- Connection events continue until MD = 0



Connection Events

Each connection event uses a different channel

$f_{n+1} = (f_n + hop) \bmod 37$



Latency

Master Latency

how often the master will transmit to slave

Slave Latency

how often the slave will listen to master

The two latencies don't have to be the same

Master Latency = Connection Interval (7.5 ms to 4.0 s)

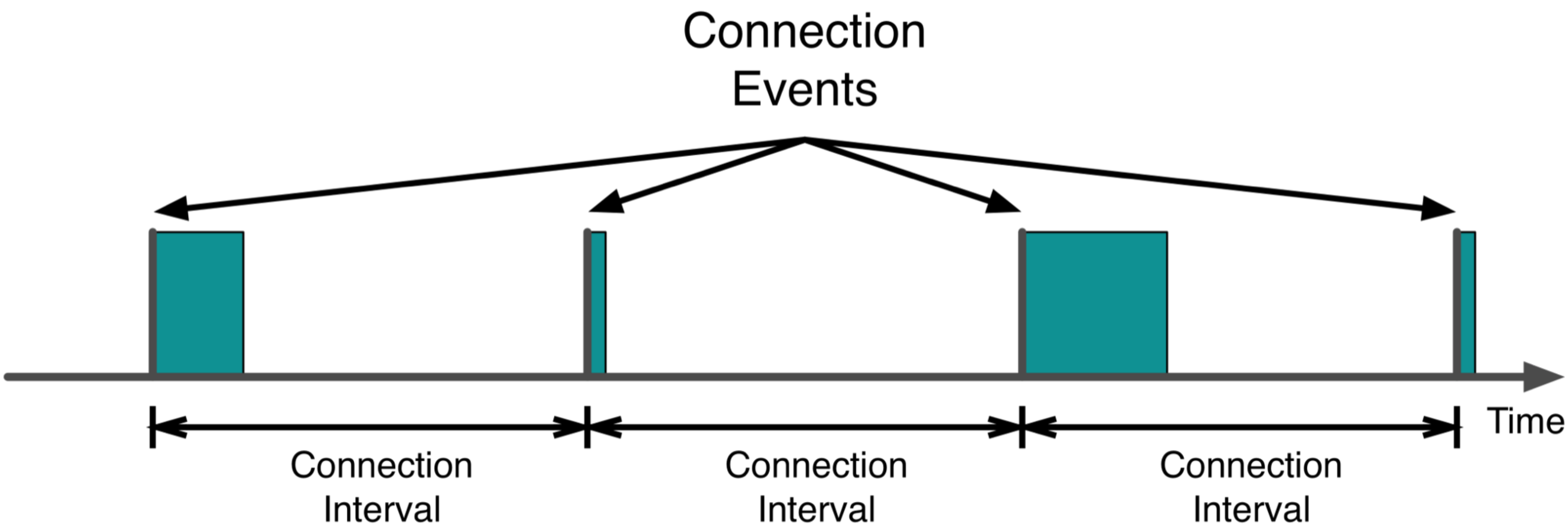
Slave Latency = Connection Interval * Slave Latency

More Data

		Master	
		MD = 0	MD = 1
Slave	MD = 0	Neither device has more data to send. Connection event closed	Master has more data, Slave has no more data. Master may continue, Slave should listen
	MD = 1	Slave has more data, Master has no more data. Master may continue, Slave should listen	Both devices have more data. Master may continue, Slave should listen.

Connection Events

More Data bit automatically extends connection events



Packet Timings

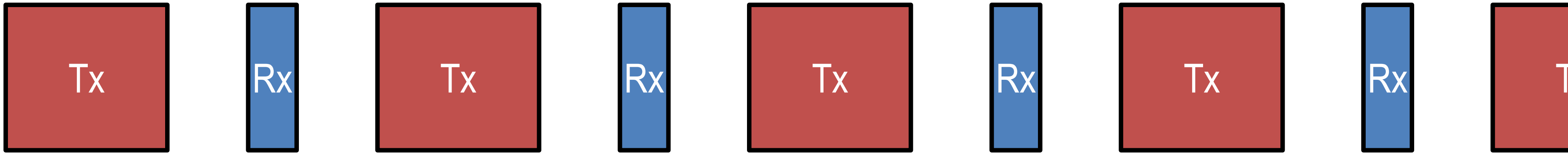
Peer device transmits 150 µs after last packet

Minimum size packet = 80 µs

(Preamble + Access Address + Header + CRC)

Maximum size packet = 328 µs

(Preamble + Access Address + Header + Payload + MIC + CRC)

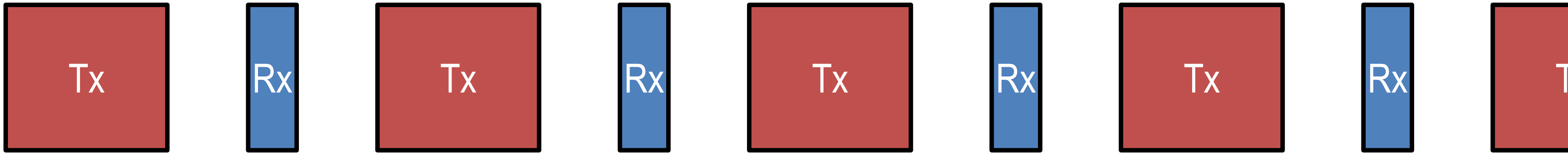


Maximum Data Rate

Asymmetric Tx/Rx Packet Sequence

- 328 + 150 + 80 + 150 = 708 µs
- Transmitting 27 octets of application data

~305.1 kbps



Doubling the Symbol Rate?

LE = 1 MS/s

1,000,000 symbols per second

LE2 = 2 MS/s

2,000,000 symbols per second

PHY data rate has doubled

What about the application data rate?

2 Mbits/second data rate

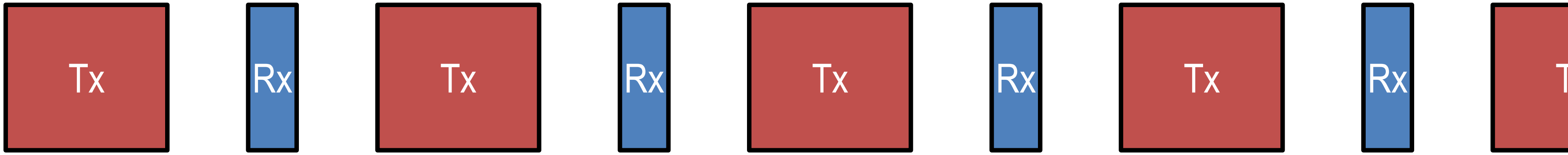
Asymmetric Tx/Rx Packet Sequence

168 + 150 + 44 + 150 = 512 μs

Transmitting 27 octets of application data

2M Symbols/second

~412.9 kbps



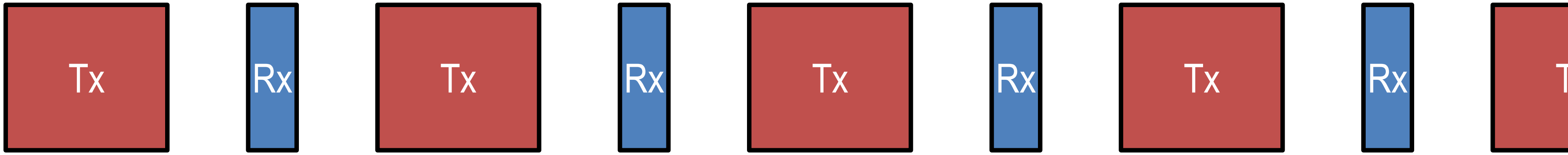
Extending Payload Length

Asymmetric Tx/Rx Packet Sequence

- 2200 + 150 + 80 + 150 = 2500 µs
- Transmitting 251 octets of application data

Data Length Extensions

~803.2 kbps



Extending Payload Length at 2 MS/s

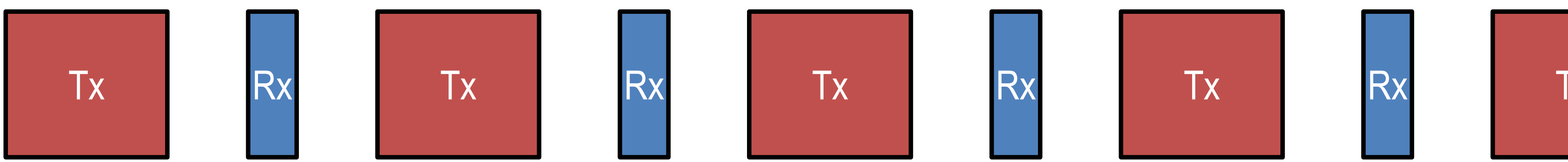
Asymmetric Tx/Rx Packet Sequence

1108 + 150 + 80 + 150 = 1408 µs

Transmitting 251 octets of application data

Data Length Extensions with 2M Symbols/second

~1426.1 kbps



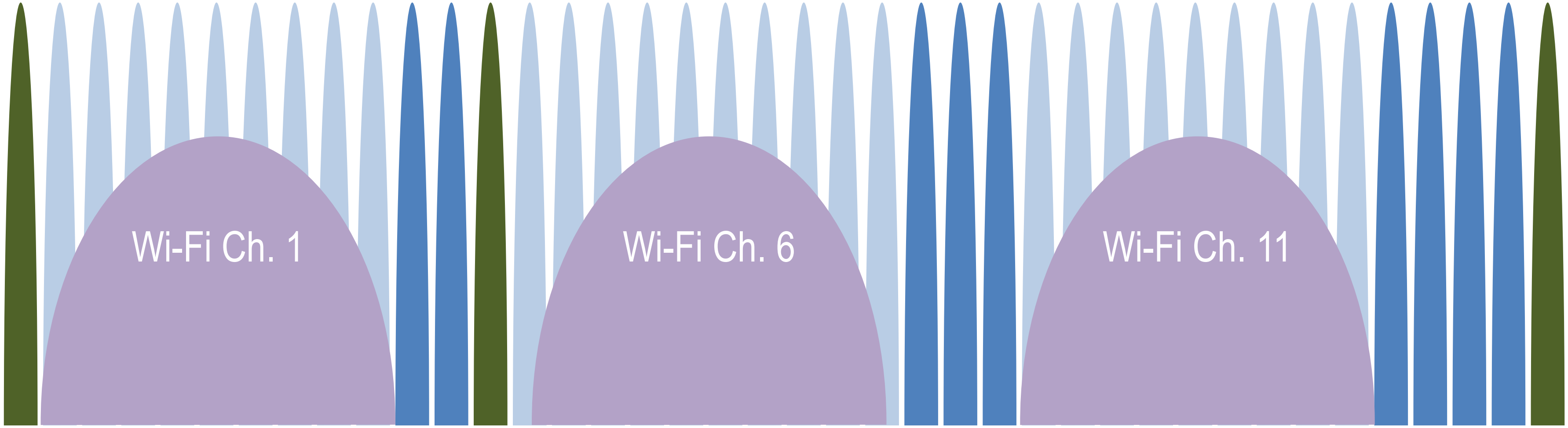
Adaptive Frequency Hopping

Frequency Hopping algorithm is very simple

$$f_{n+1} = (f_n + hop) \bmod 37$$

If f_n is a “used” channel, use as is

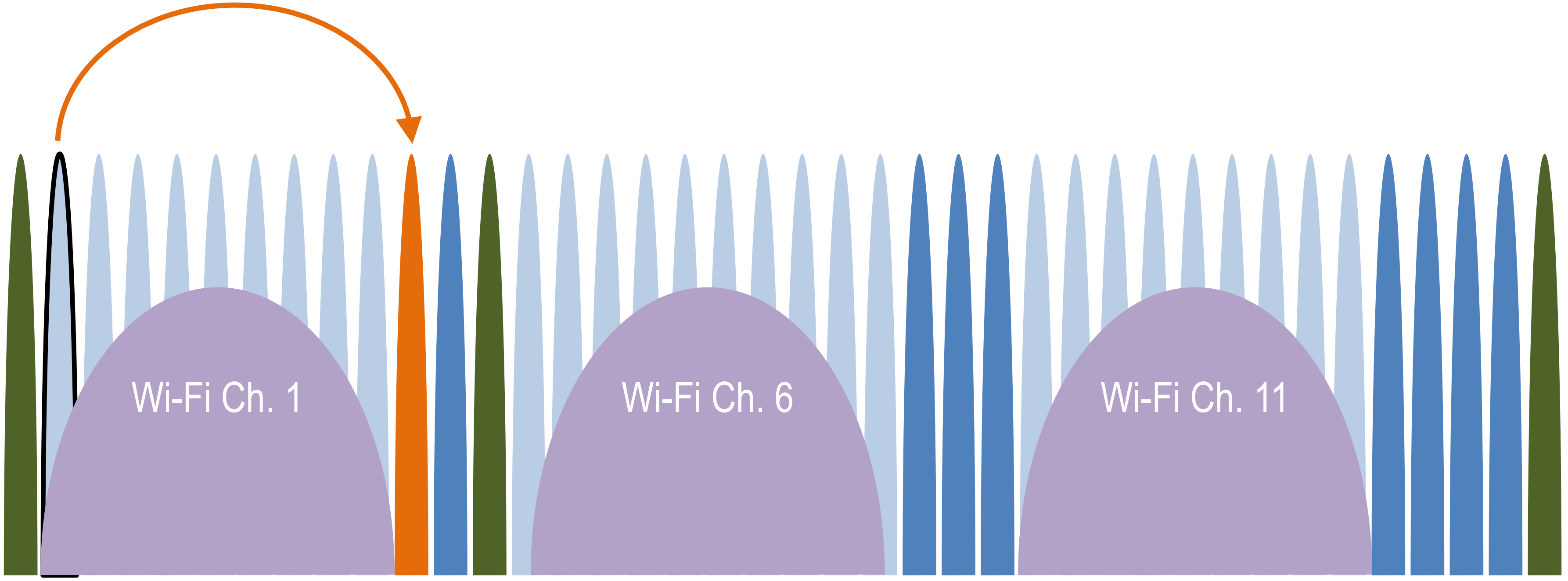
If f_n is an “unused” channel, remap to set of good channels



Adaptive Frequency Hopping (hop = 7)

f_n = 0, used = [9, 10, 21, 22, 23, 33, 34, 35, 36]

"unused"; 0 mod 9 → 0; used[0] → 9

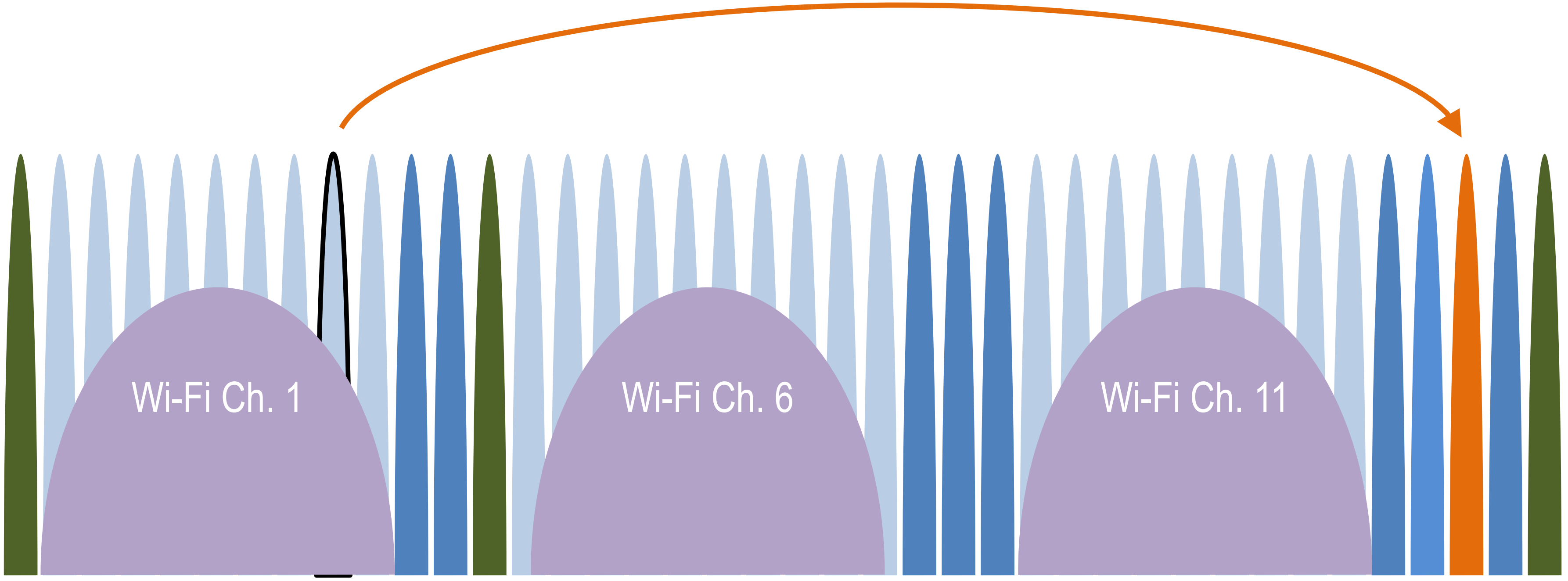


Adaptive Frequency Hopping (hop = 7)

$f_n = f_{n-1} + 7 \bmod 37 = 7 \bmod 37 \rightarrow 7$

$f_n = 7$, used = [9, 10, 21, 22, 23, 33, 34, 35, 36]

"unused"; $7 \bmod 9 \rightarrow 7$; used[7] $\rightarrow 35$

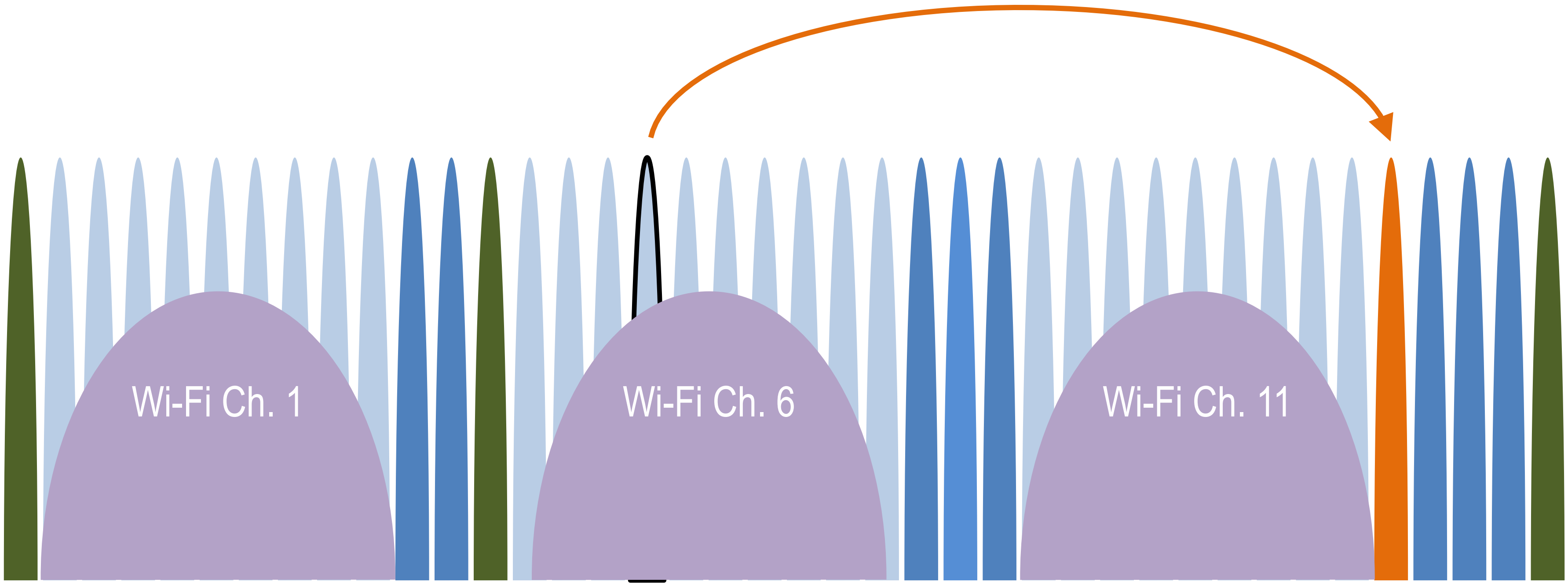


Adaptive Frequency Hopping

$f_n = f_{n-1} + 7 \bmod 37 = 14 \bmod 37 \rightarrow 14$

$f_n = 14$, used = [9, 10, 21, 22, 23, 33, 34, 35, 36]

"unused"; 14 mod 9 → 5; used[5] → 33

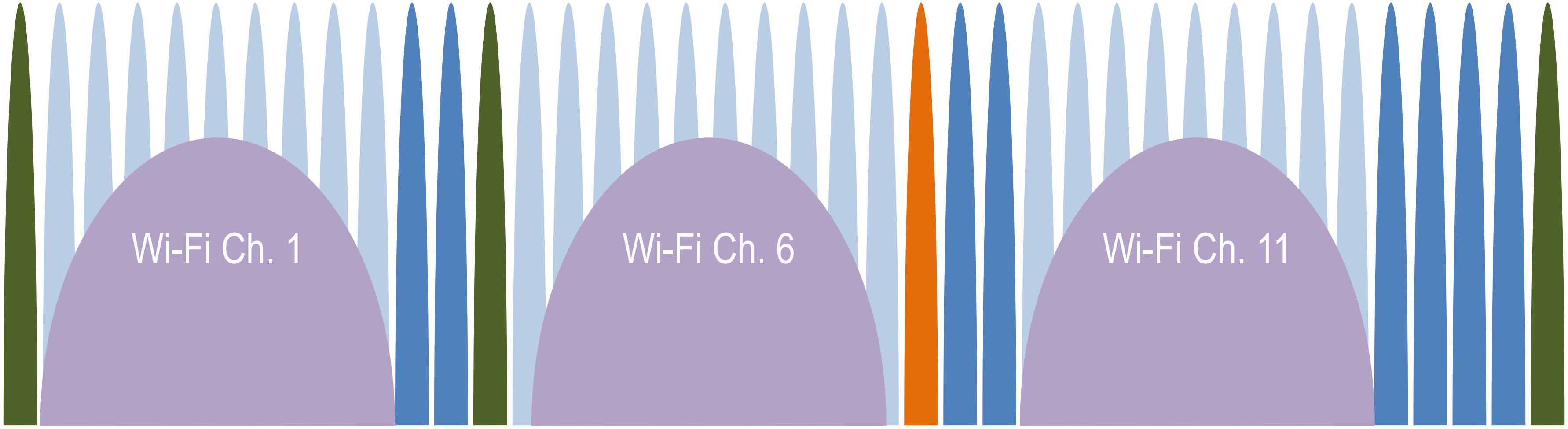


Adaptive Frequency Hopping

$f_n = f_{n-1} + 7 \bmod 37 = 21 \bmod 37 \rightarrow 21$

$f_n = 21$, used = [9, 10, 21, 22, 23, 33, 34, 35, 36]

“used”



Limits

Maximum 2^{39} packets per LTK per direction

- Each packet can contain up to 251 octets data
- Max 125.5 Terabytes of data per connection
- ~3 years at maximum data rate

Then you have to change the encryption key

- use “Restart Encryption Procedure”

Link Layer Summary

Low Complexity

- 1 packet format
- 2 PDU types – depending on Advertising / Data Channel
- 7 Advertising PDU Types
- 7 Link Layer Control Procedures

Useful Features

- Adaptive Frequency Hopping
- Low Power Acknowledgement
- Very Fast Connections

And there is more…

Not even covered Attribute Protocol or Generic Attribute Profile

- and how it enables Services and Characteristics, reading, writing, notifications…

Not even covered Security Manager (SM)

- and how it enables a secure bond between devices

Not even covered Application APIs

- and how to create smart phone apps to talk with devices

Interesting new use cases using LE Advertising

- iBeacon / Mesh / Tracking / Marketing / Finding etc…

thank you