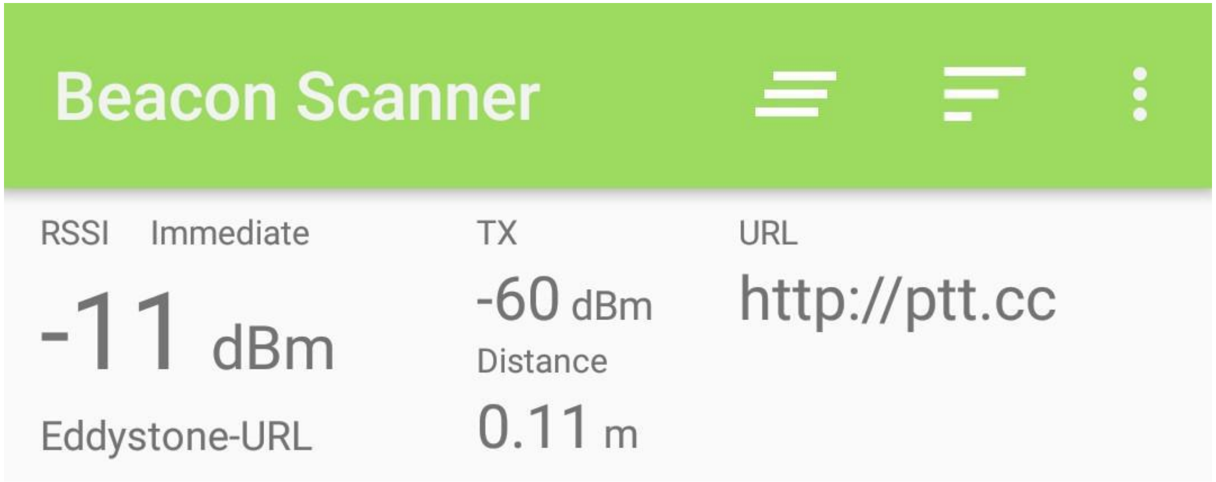
Wireless Ad Hoc Networks
Lab 5

Bluetooth

Outline

- BLE實驗
  - 藍牙BLE介紹
  - BLE廣播封包實作

Bluetooth®



Beacon Scanner

RSSI Immediate

-11 dBm

Eddystone-URL

TX

-60 dBm

Distance

0.11 m

URL

http://ptt.cc

藍牙 Bluetooth

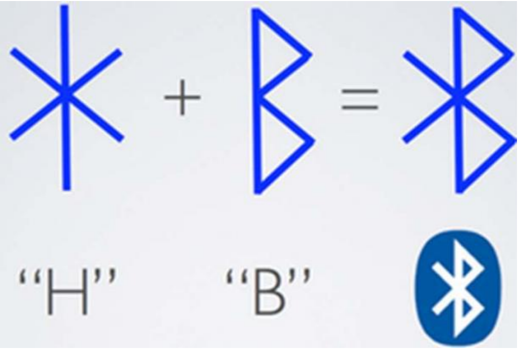
- 目的
  - 為了解決電腦與電器設備之間的傳輸問題
- 特色
  - 短距離無線技術 (10 - 100m)
  - 使用 2.4 至 2.485 GHz 的 ISM 頻段
- Bluetooth Classic: 802.15
- Bluetooth 4.0 Low Energy (BLE): 802.15.1
- Bluetooth 5.0: Faster, Further, for IoT

https://zh.wikipedia.org/zh-tw/%E8%97%8D%E7%89%99

藍牙起源

- 歷史
  - 十世紀國王的名字 (Harald Blåtand)
    - 統一了因宗教戰爭和領土爭議而分裂的挪威與丹麥而聞名於世
    - 喜歡吃藍莓，因此牙齒都變成藍色 (Blue tooth)
    - 另一說，他的牙齒很差，看起來像藍色(blue, dark, black)
    - 他喜歡穿藍色的服飾，當時的藍色有昂貴、尊爵、不凡的意思
  - 由 Ericsson 在 1994 年創製 ,希望為裝置間的通訊創造一組統一規則（標準化協定），以解決用戶間互不相容的移動電子裝置

不要寫成藍**芽**喔!



https://zh.wikipedia.org/zh-tw/%E8%97%8D%E7%89%99
https://en.wikipedia.org/wiki/Harald_Bluetooth

Bluetooth Low Energy (BLE)

- 一種無線個人區域網路 (Wireless PAN) 的技術
- 出現目的 : 低成本 , 低耗電 (CR2032 電池可用 1 年)
- BT4 分 Classic(BR/EDR), High Speed(HS), Low Energy

	Classic	BLE
Data Rate	1~3 Mbps	1 Mbps
Range	10 ~ 100 m	10 ~ 30 m
Power consumption	1 W	0.01 ~ 0.5 W
Connection time	5 s	0.1 s

Bluetooth™ 4.0 Low Energy

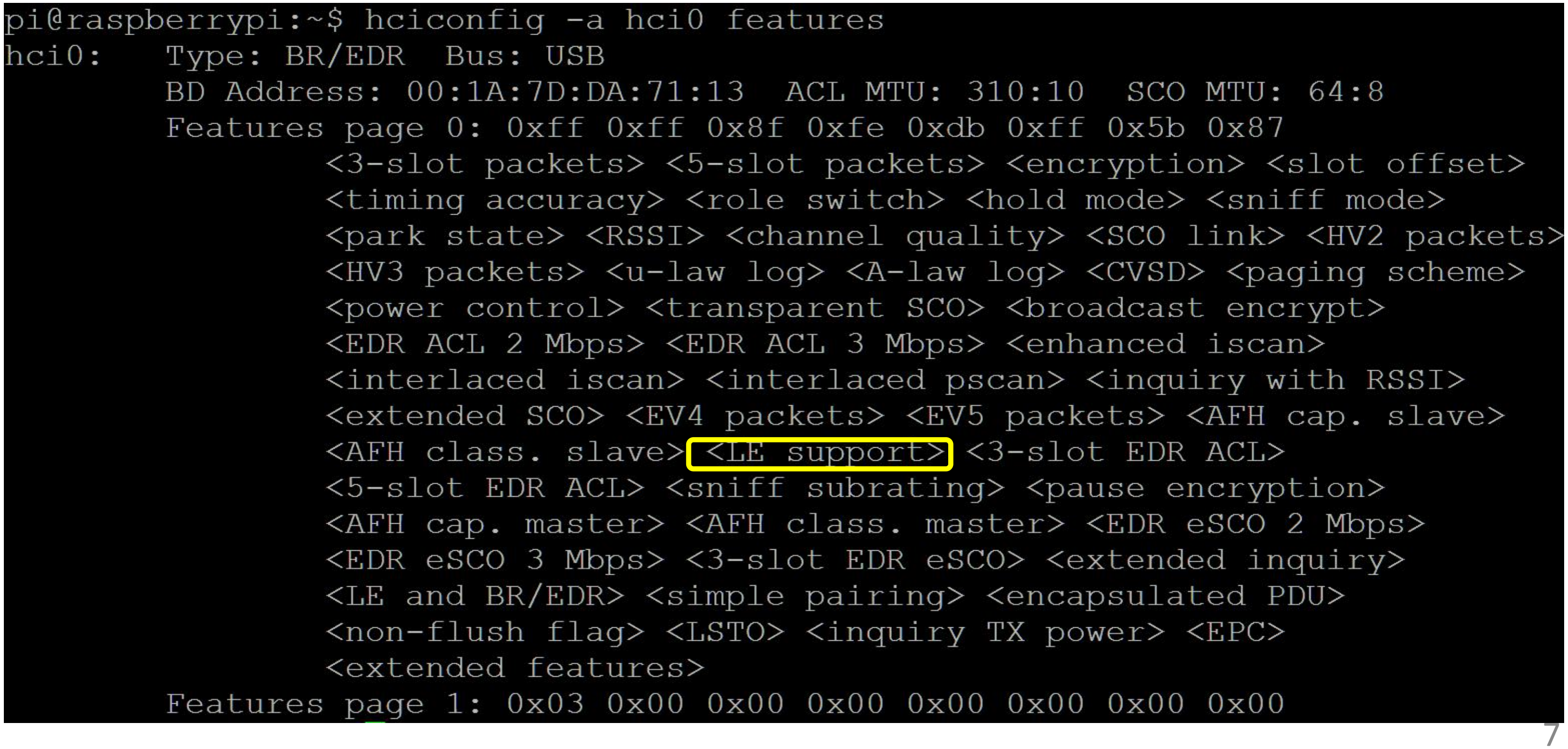
Bluetooth 5.0

- Mesh Networking: 一對一>>>多對多
- 出現目的 : IoT
- 室內導航、安全、抗干擾(New Algorithm)

	4.2	5.0
Data Rate	1 Mbps	2 Mbps
Range	1x	4x
Bandwidth	1x	8x

藍牙 + BLE

- 確認藍牙裝置是否有支援BLE功能
  - hciconfig -a hci0 features (尋找 **LE support**)



```
pi@raspberrypi:~$ hciconfig -a hci0 features
hci0:   Type: BR/EDR  Bus: USB
        BD Address: 00:1A:7D:DA:71:13  ACL MTU: 310:10  SCO MTU: 64:8
        Features page 0: 0xff 0xff 0x8f 0xfe 0xdb 0xff 0x5b 0x87
                <3-slot packets> <5-slot packets> <encryption> <slot offset>
                <timing accuracy> <role switch> <hold mode> <sniff mode>
                <park state> <RSSI> <channel quality> <SCO link> <HV2 packets>
                <HV3 packets> <u-law log> <A-law log> <CVSD> <paging scheme>
                <power control> <transparent SCO> <broadcast encrypt>
                <EDR ACL 2 Mbps> <EDR ACL 3 Mbps> <enhanced iscan>
                <interlaced iscan> <interlaced pscan> <inquiry with RSSI>
                <extended SCO> <EV4 packets> <EV5 packets> <AFH cap. slave>
                <AFH class. slave> <LE support> <3-slot EDR ACL>
                <5-slot EDR ACL> <sniff subrating> <pause encryption>
                <AFH cap. master> <AFH class. master> <EDR eSCO 2 Mbps>
                <EDR eSCO 3 Mbps> <3-slot EDR eSCO> <extended inquiry>
                <LE and BR/EDR> <simple pairing> <encapsulated PDU>
                <non-flush flag> <LSTO> <inquiry TX power> <EPC>
                <extended features>
        Features page 1: 0x03 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

Bluetooth 常用工具

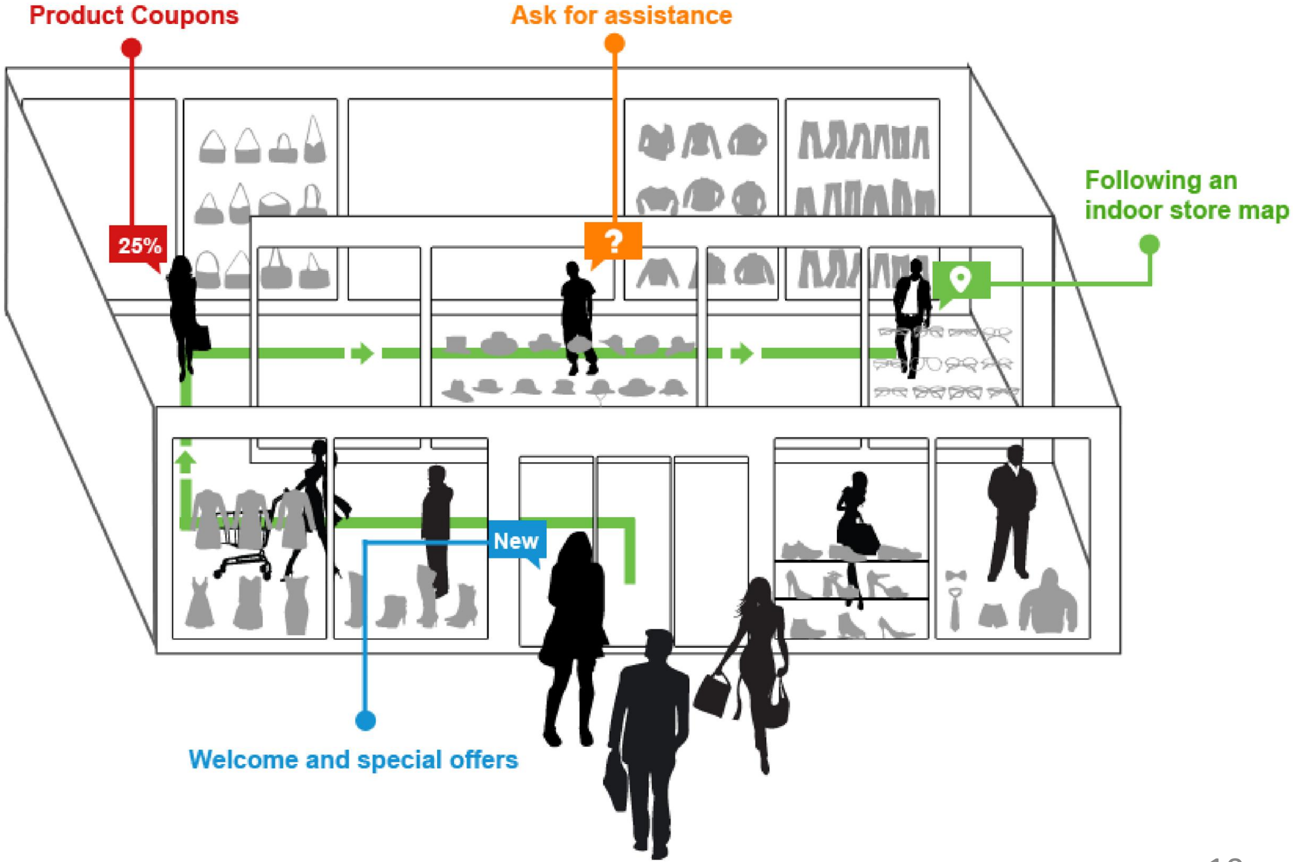
- bluetoothctl - bluetooth control tool
- hciconfig - configure Bluetooth devices
- hcitool - configure Bluetooth connections
- l2ping - Send L2CAP echo request and receive answer
- btmon - Bluetooth monitor
- gatttool - GATT tool

支援 BLE 的平台

- iOS5+ (iOS7+ preferred)
- Android 4.3+ (numerous bug fixes in 4.4+)
- Apple OS X 10.6+
- Windows 10/8 (XP, Vista and 7 only support Bluetooth 2.1)
- GNU/Linux Vanilla BlueZ 4.93+

BLE 的應用

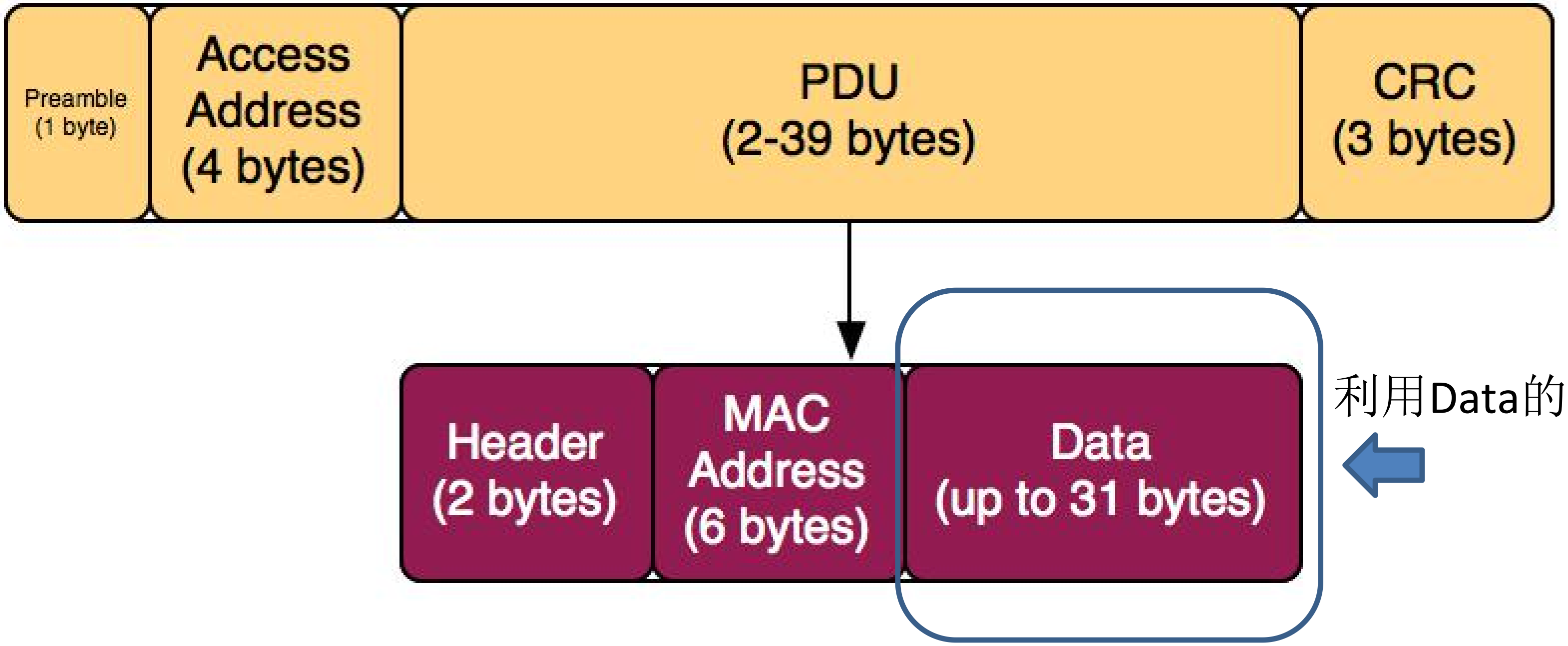
- □ 微型定位服務
- □ 推播訊息



https://learn.adafruit.com/pibeacon-ibeacon-with-a-raspberry-pi/overview

BLE frame format

- 1 byte preamble
- 4 byte access address
- 2-39 bytes advertising channel PDU
- 3 bytes CRC



利用Data的欄位

http://www.warski.org/blog/2014/01/how-ibeacons-work/

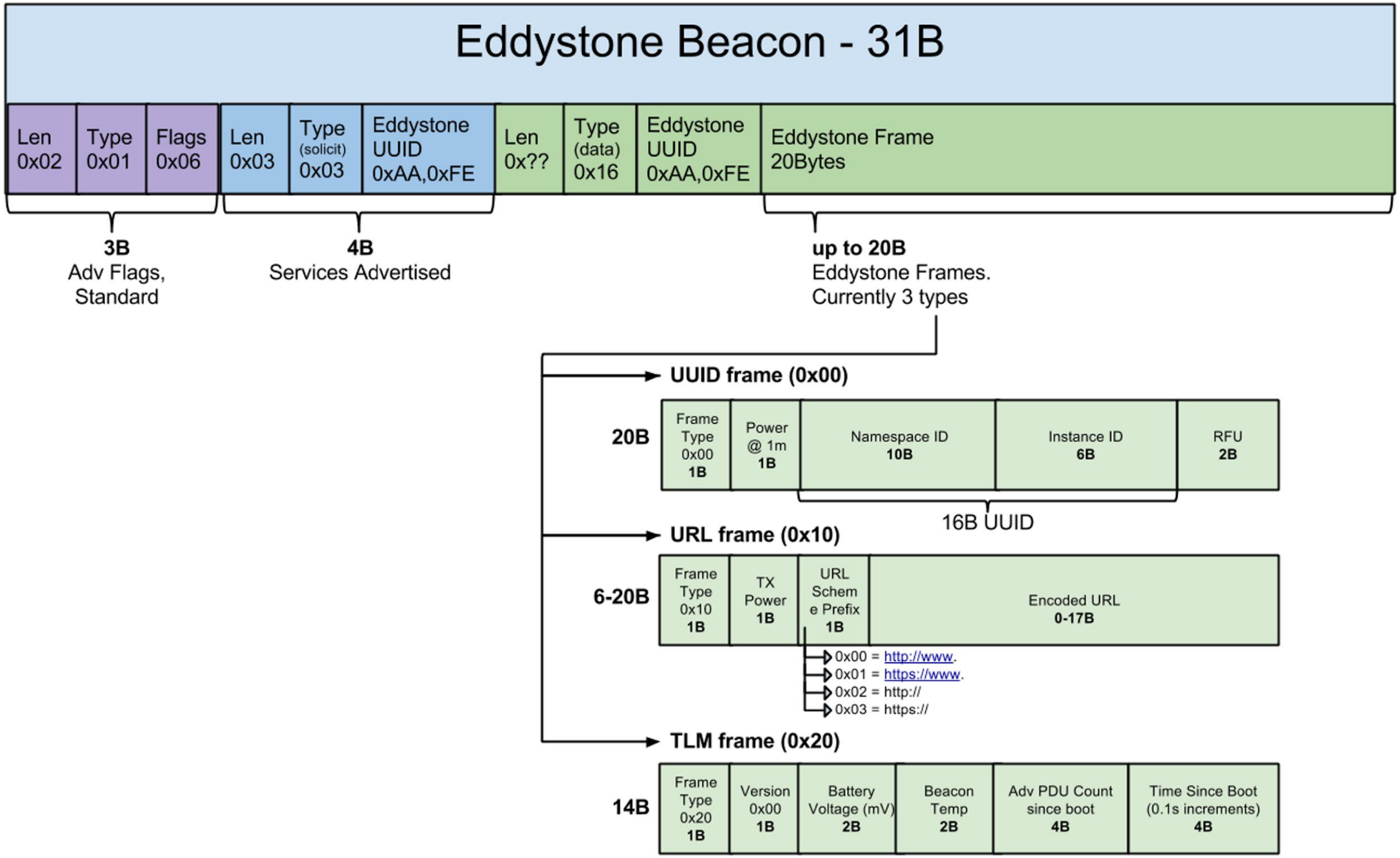
BLE 的應用 (Eddystone)

- Eddystone is a protocol specification that defines a Bluetooth low energy (BLE) message format for proximity beacon messages.

- Design Goals
  - Works well with Android and iOS Bluetooth developer APIs
  - Straightforward implementation on a wide range of existing BLE devices
  - Flexible architecture permitting development of new frame types
  - Fully compliant with the Bluetooth Core Specification

https://github.com/google/eddystone

Eddystone Frame format



Eddystone Beacon - 31B

Len 0x02	Type 0x01	Flags 0x06	Len 0x03	Type (solicit) 0x03	Eddystone UUID 0xAA,0xFE	Len 0x??	Type (data) 0x16	Eddystone UUID 0xAA,0xFE	Eddystone Frame 20Bytes

3B
Adv Flags,
Standard

4B
Services Advertised

up to 20B
Eddystone Frames.
Currently 3 types

UUID frame (0x00)

20B

Frame Type 0x00 **1B**	Power @ 1m **1B**	Namespace ID **10B**	Instance ID **6B**	RFU **2B**

16B UUID

URL frame (0x10)

6-20B

Frame Type 0x10 **1B**	TX Power **1B**	URL Schem e Prefix **1B**	Encoded URL **0-17B**

0x00 = http://www.
0x01 = https://www.
0x02 = http://
0x03 = https://

TLM frame (0x20)

14B

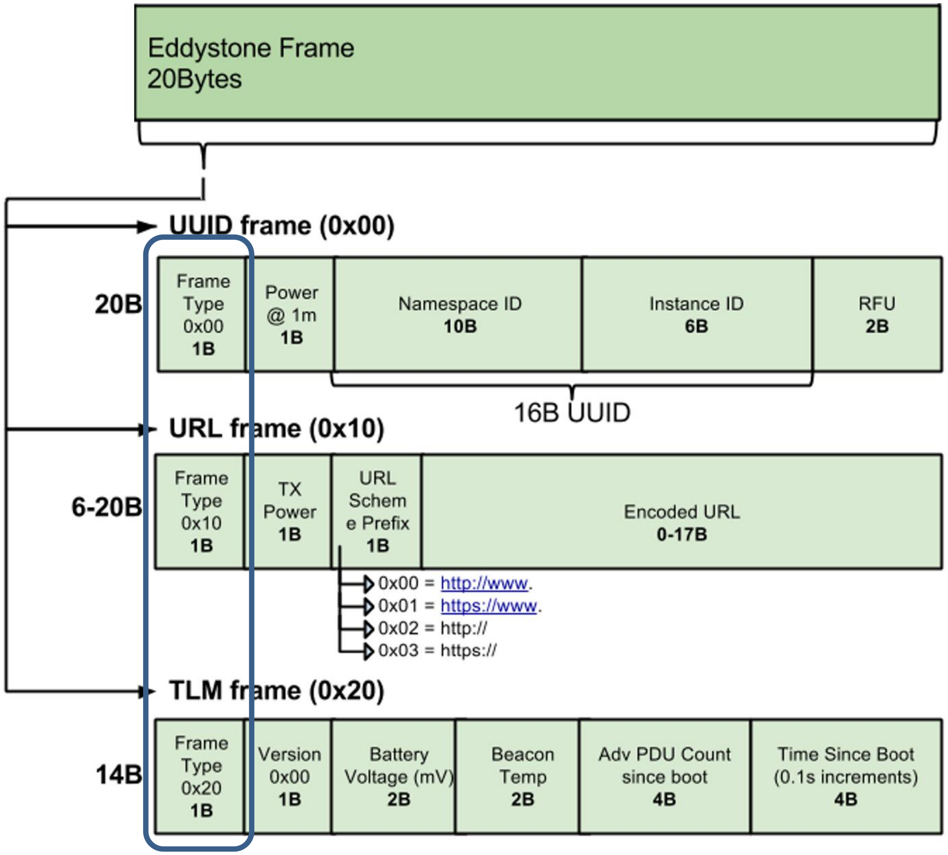
Frame Type 0x20 **1B**	Version 0x00 **1B**	Battery Voltage (mV) **2B**	Beacon Temp **2B**	Adv PDU Count since boot **4B**	Time Since Boot (0.1s increments) **4B**

https://developer.mbed.org/teams/Bluetooth-Low-Energy/code/BLE_EddystoneBeacon_Service/file/dfb7fb5a971b/Eddystone.h

Eddystone Frame format

- Eddystone Protocol Specification

Frame Type	High-Order 4 bits	Byte Value
UID	0000	0x00
URL	0001	0x10
TLM	0010	0x20
EID	0011	0x30
RESERVED	0100	0x40



Eddystone Frame
20Bytes

UUID frame (0x00)

20B

Frame Type 0x00 1B	Power @ 1m 1B	Namespace ID 10B	Instance ID 6B	RFU 2B

16B UUID

URL frame (0x10)

6-20B

Frame Type 0x10 1B	TX Power 1B	URL Scheme Prefix 1B	Encoded URL 0-17B

0x00 = http://www.
0x01 = https://www.
0x02 = http://
0x03 = https://

TLM frame (0x20)

14B

Frame Type 0x20 1B	Version 0x00 1B	Battery Voltage (mV) 2B	Beacon Temp 2B	Adv PDU Count since boot 4B	Time Since Boot (0.1s increments) 4B

https://github.com/google/eddystone/blob/master/protocol-specification.md

Eddystone訊息

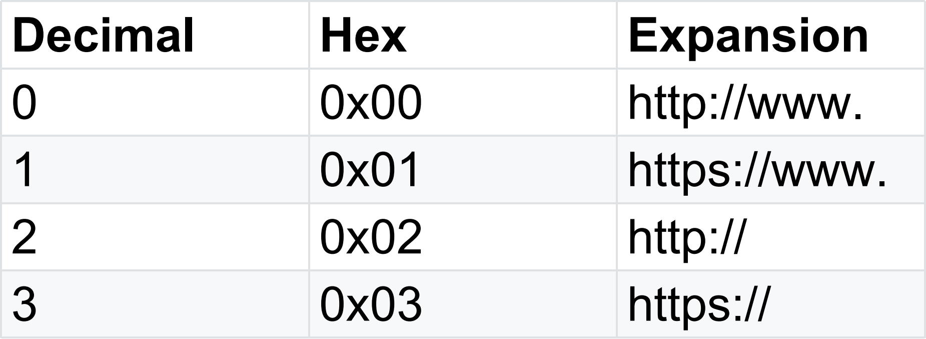
- Goal:
  - 利用PI的BLE, 產生Eddystone的廣告訊息
  - 依照網址建立一個符合Eddystone格式的frame

  - Eddystone網址格式
    - https://github.com/google/eddystone/tree/master/eddystone-url
  - ACSII table
    - https://zh.wikipedia.org/wiki/ASCII

Eddystone訊息

- 將網址轉換為Eddystone格式
  - Ex: http://ptt.cc
  - 利用ASCII table查詢數值

數值 (16進位)	網址
02	http://
70	p
74	t
74	t
2e	.
63	c
63	c



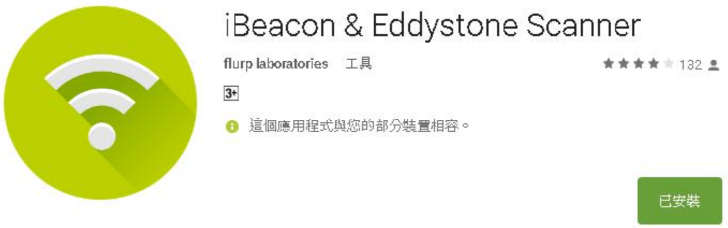
Decimal	Hex	Expansion
0	0x00	http://www.
1	0x01	https://www.
2	0x02	http://
3	0x03	https://

Eddystone訊息

- 使用 advertise-url 來傳送網址廣播
  - Source code
    - https://github.com/google/eddystone/blob/master/eddystone-url/implementations/linux/advertise-url
    - wget https://raw.githubusercontent.com/google/eddystone/master/eddystone-url/implementations/linux/advertise-url
  - 下載後
    - chmod +x advertise-url (新增執行權限)
    - sudo ./advertise-url -u http://ptt.cc (開始廣播)
    - sudo ./advertise-url -s (停止廣播)

Eddystone訊息

- 手機端可安裝BLE scanner app查看Eddystone訊息



iBeacon & Eddystone Scanner

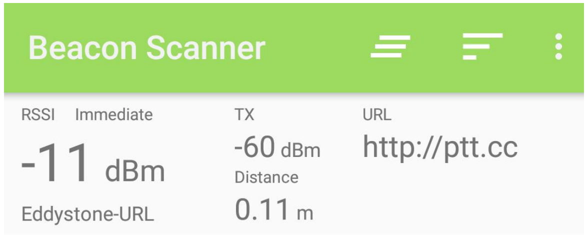
flurp laboratories 工具

★★★★★ 132

3+

這個應用程式與您的部分裝置相容。

已安裝

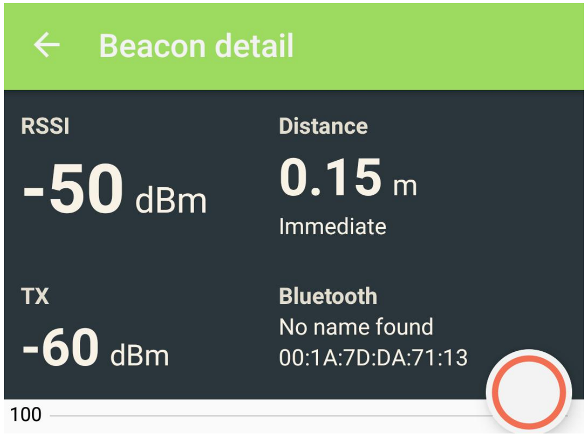


Beacon Scanner

RSSI Immediate
-11 dBm
Eddystone-URL

TX
-60 dBm
Distance
0.11 m

URL
http://ptt.cc



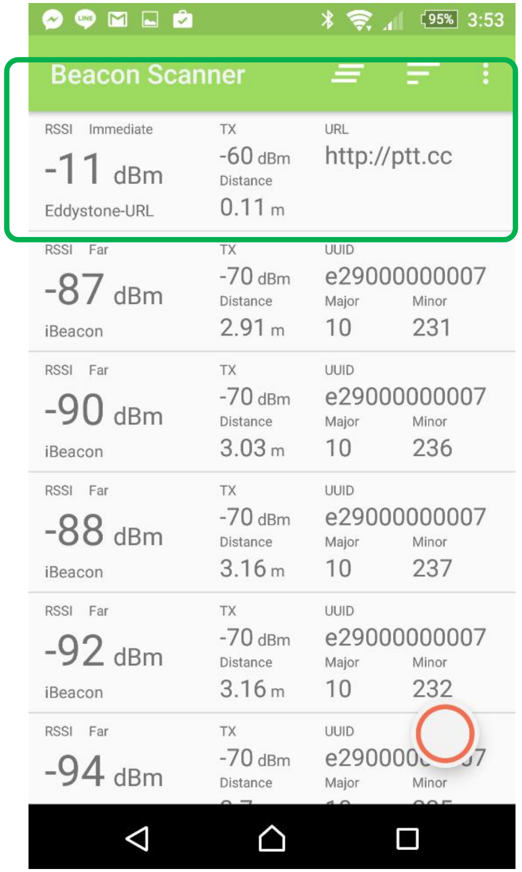
Beacon detail

RSSI
-50 dBm

Distance
0.15 m
Immediate

TX
-60 dBm

Bluetooth
No name found
00:1A:7D:DA:71:13



Beacon Scanner

RSSI Immediate
-11 dBm
Eddystone-URL
TX -60 dBm
Distance 0.11 m
URL http://ptt.cc

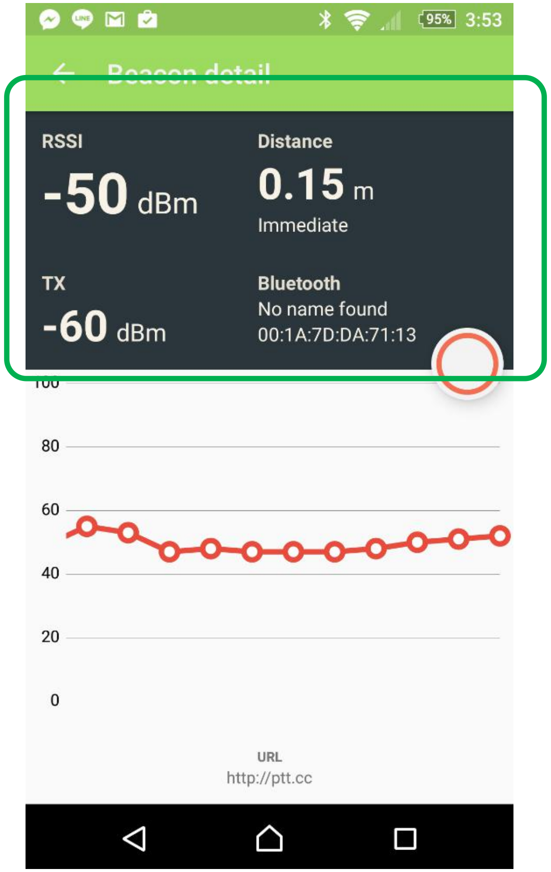
RSSI Far
-87 dBm
iBeacon
TX -70 dBm
Distance 2.91 m
UUID e29000000007
Major 10
Minor 231

RSSI Far
-90 dBm
iBeacon
TX -70 dBm
Distance 3.03 m
UUID e29000000007
Major 10
Minor 236

RSSI Far
-88 dBm
iBeacon
TX -70 dBm
Distance 3.16 m
UUID e29000000007
Major 10
Minor 237

RSSI Far
-92 dBm
iBeacon
TX -70 dBm
Distance 3.16 m
UUID e29000000007
Major 10
Minor 232

RSSI Far
-94 dBm
TX -70 dBm
Distance
UUID e290000 07
Major
Minor



Beacon detail

RSSI
-50 dBm

Distance
0.15 m
Immediate

TX
-60 dBm

Bluetooth
No name found
00:1A:7D:DA:71:13

URL
http://ptt.cc

Eddystone訊息

- 也可以使用bluetooth工具傳送網址廣播

```
sudo hciconfig hci0 leadv3
sudo hciconfig hci0 noscan
```

啟用藍牙的低耗能廣告(LE advertising)模式，並關閉掃描功能

```
sudo hcitool -i hci0 cmd 0x08 0x0008 14 02 01 1a 03 03 aa fe 0c 16
aa fe 10 ed 02 70 74 74 2e 63 63 00 00 00 00 00 00 00 00 00 00 00
```

↑ http://ptt.cc

傳送Eddystone frame

```
sudo hciconfig hci0 noleadv
```

停止廣告

Eddystone訊息

```
sudo hcitool -i hci0 cmd 0x08 0x0008 14 02 01 1a 03 03 aa fe 0c 16 aa fe 10 ed
02 70 74 74 2e 63 63 00 00 00 00 00 00 00 00 00 00 00
```

- 0x08 0x0008: set the ad package
  - #OGF = Operation Group Field = Bluetooth Command Group = 0x08
  - #OCF = Operation Command Field = HCI_LE_Set_Advertising_Data = 0x0008
- 14: the ENTIRE following data packet in bytes (16進位的14 = 20 byte)

20 byte

- 02 01 1a: Eddystone Adv Flags
  - 0x06 - The device is BLE only. The full Bluetooth stack is not supported.
  - 0x1A - The device can be used as BLE as well as full Bluetooth Controller/Host simultaneously.
- 03 03 aa fe: Eddystone service adv
- 0c: length (12 byte)
- 16: type (data)
- aa fe: Eddystone UUID
- 10: URL frame type
- ed: TX power
- 02 70 74 74 2e 63 63: http://ptt.cc,共 7 byte

12 byte

- 00 00 00 00 00 00 00 00 00 00 00: 共 11 byte

Eddystone訊息

- Q1：
  - 使用advertise-url，產生Eddystone的廣告訊息
    - 網址 http://bun.cm.nctu/xxx
  - 手機抓取Eddystone截圖
- Q2：
  - 使用hcitool傳送

    https://www.nycu/學號
  - 手機抓取Eddystone截圖
  - 說明數值意義

數值 (16進位)	網址
???	???
???	???
???	???
???	???
???	???
???	???
???	???

Reference

- □ Raspberry Pi IoT無線傳輸技術介紹 – Bluetooth
  - https://www.slideshare.net/raspberrypi-tw/raspberry-pi-iot-bluetooth
- □ Eddystone
  - https://github.com/google/eddystone
- □ Eddystone Protocol Specification
  - https://github.com/google/eddystone/blob/master/protocol-specification.md
- □ Eddystone-URL Beacon Implementations
  - https://github.com/google/eddystone/tree/master/eddystone-url/implementations/