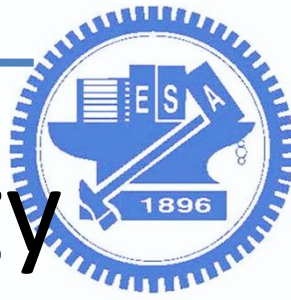
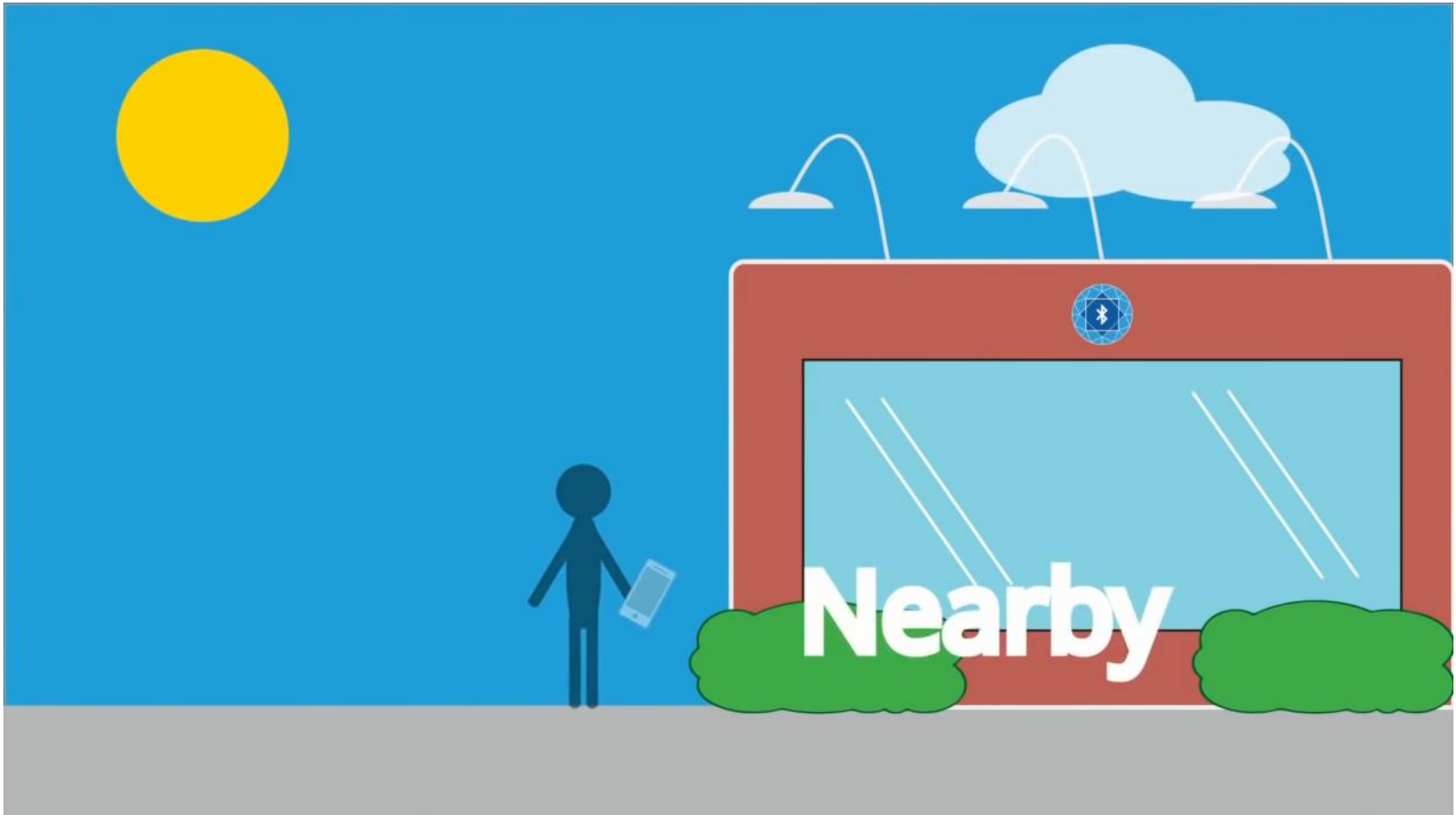


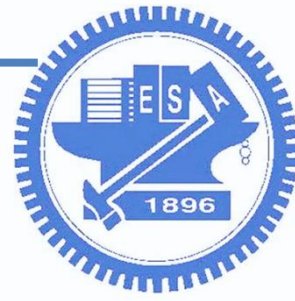
# Outline

- 嵌入式應用: BLE beacon
  - Beacon applications
  - Eddystone, iBeacon protocol



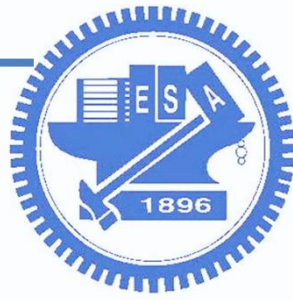
# What Is Beacon Technology





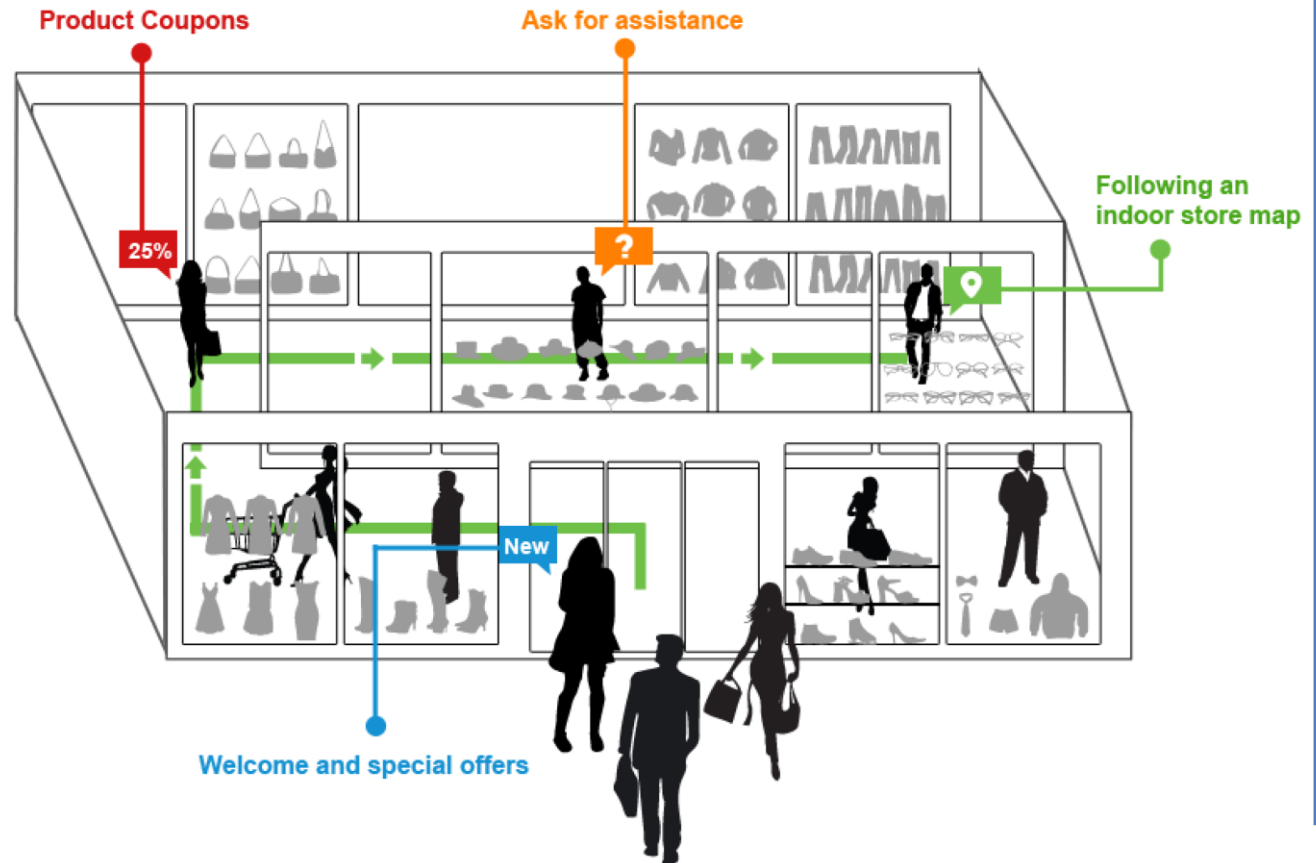
# Beacon Technology in Real Estate Industry





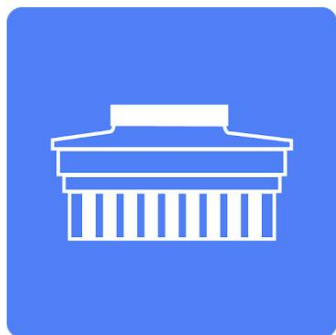
# BLE 的應用

- 微型定位服務
- 推播訊息





# Beacon x 台北車站



## 台北車站通

ASKEY Computer Corporation 地圖與導航

★★★★★ 176 人

3+

含廣告內容

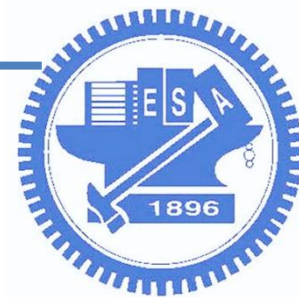
這個應用程式與你的部分裝置相容。

加入願望清單

安裝

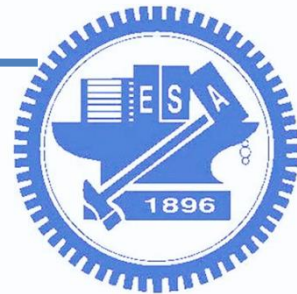






# Line Beacon x 台北捷運



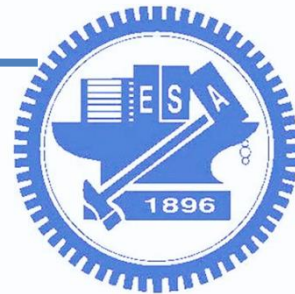


# Line Beacon x 台北捷運

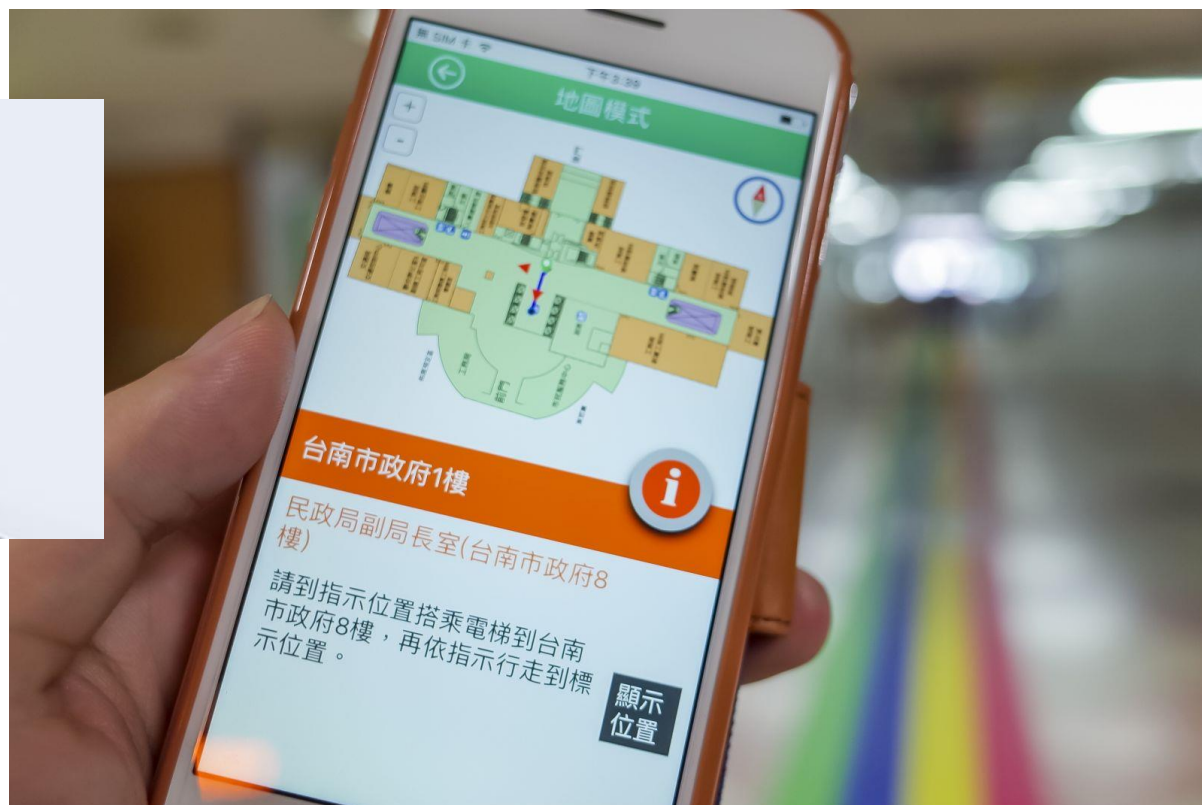
**LINE Beacon**是一個藍牙發射裝置，可以將優惠、特價資訊，或是特別情報發到您的手機中。對您來說，只要走到**LINE Beacon**的發送範圍，並且開啟手機藍牙，就可以收到**LINE Beacon**發給你的訊號囉！**LINE Beacon**可以結合許多時髦有趣的手機應用💖，在台灣人常去的日本，可是一點也不陌生！

偷偷預告一下，**LINE**即將要在台北捷運玩一個超狂的踩點遊戲！（當然是有獎品的那種）屆時會透過**LINE Beacon**跟大家玩，所以現在我們要先做暖身練習，這樣到時候才不會漏接**LINE Beacon**發給你的訊號喔！能在連外國旅客都說讚的台北捷運玩，讓大台北捷運族優先試行，可是破天荒第一次啊！（**LINE Beacon**本人也表示感動🥰）





# Beacon x 台南市政府



要到臺南市政府永華行政中心洽公的市民，現在透過洽公智慧導航系統的幫助，如要向市府申請補助，可以先下載「臺南洽公小幫手」的App，就可以搜尋衛生醫療、補助資訊、教育與求職相關的便民服務，這裡提供了洽辦單位的聯絡電話，並顯示了在行政大樓內的位置，還能透過室內導航，引導民眾直接前往。



# Research

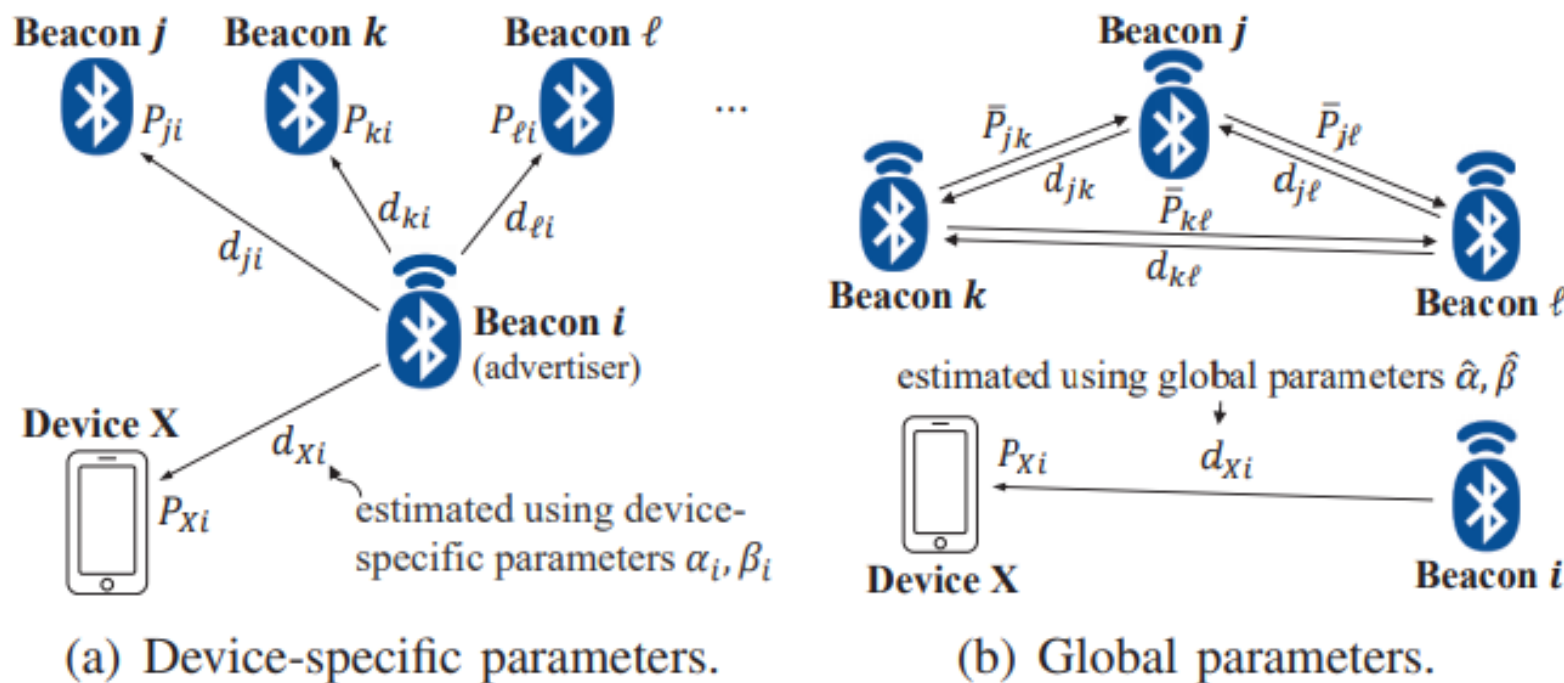
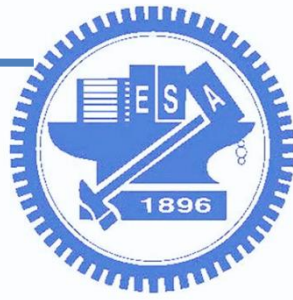


Fig. 2. Two types of regression parameters for adaptive ranging.

J.-W. Qiu, C.-P. Lin, and Y.-C. Tseng, "BLE-based Collaborative Indoor Localization with Adaptive Multi-lateration and Mobile Encountering", IEEE Wireless Communications and Networking Conference (WCNC), 2016.



# Bluetooth (藍牙)

- 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



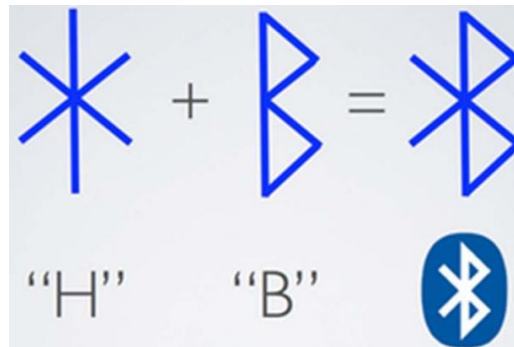
<https://zh.wikipedia.org/zh-tw/%E8%97%8D%E7%89%99>

# 藍牙起源

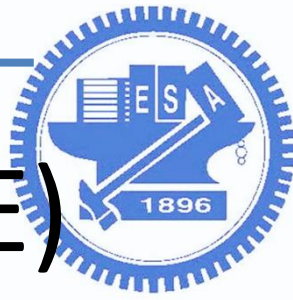


## □ 歷史

- 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！



# 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
Throughput	2 ~ 3 Mbps	0.2 Mbps
Range	50 ~ 300 m	10 ~ 30 m
Power consumption	1 W	0.01 ~ 0.5 W
Connection time	5 s	0.1 s





# Bluetooth on PI

- ❑ Does your BT device support BLE?
  - ❑ `hciconfig -a hci0 features` (“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 tools

- ❑ 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



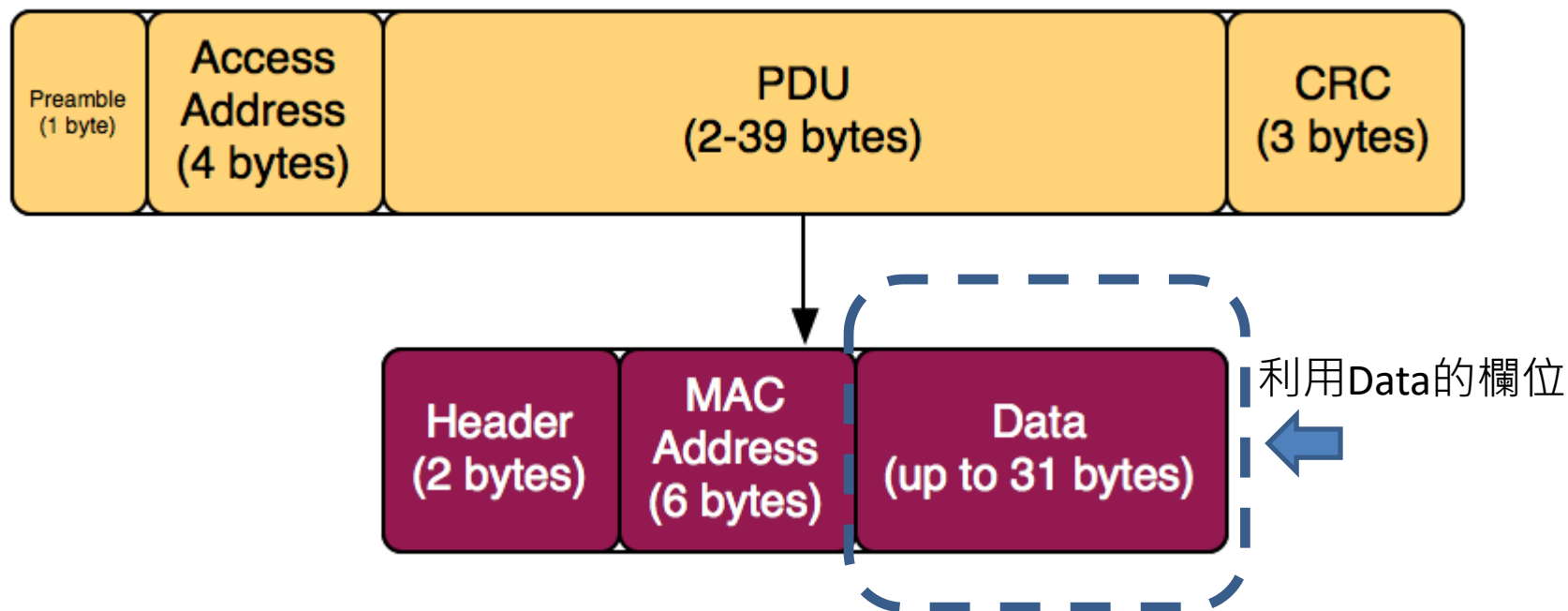
# BLE supported platform

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



# BLE frame format

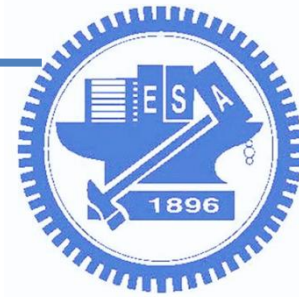
- 1 byte preamble
- 4 byte access address
- 2-39 bytes advertising channel PDU
- 3 bytes CRC



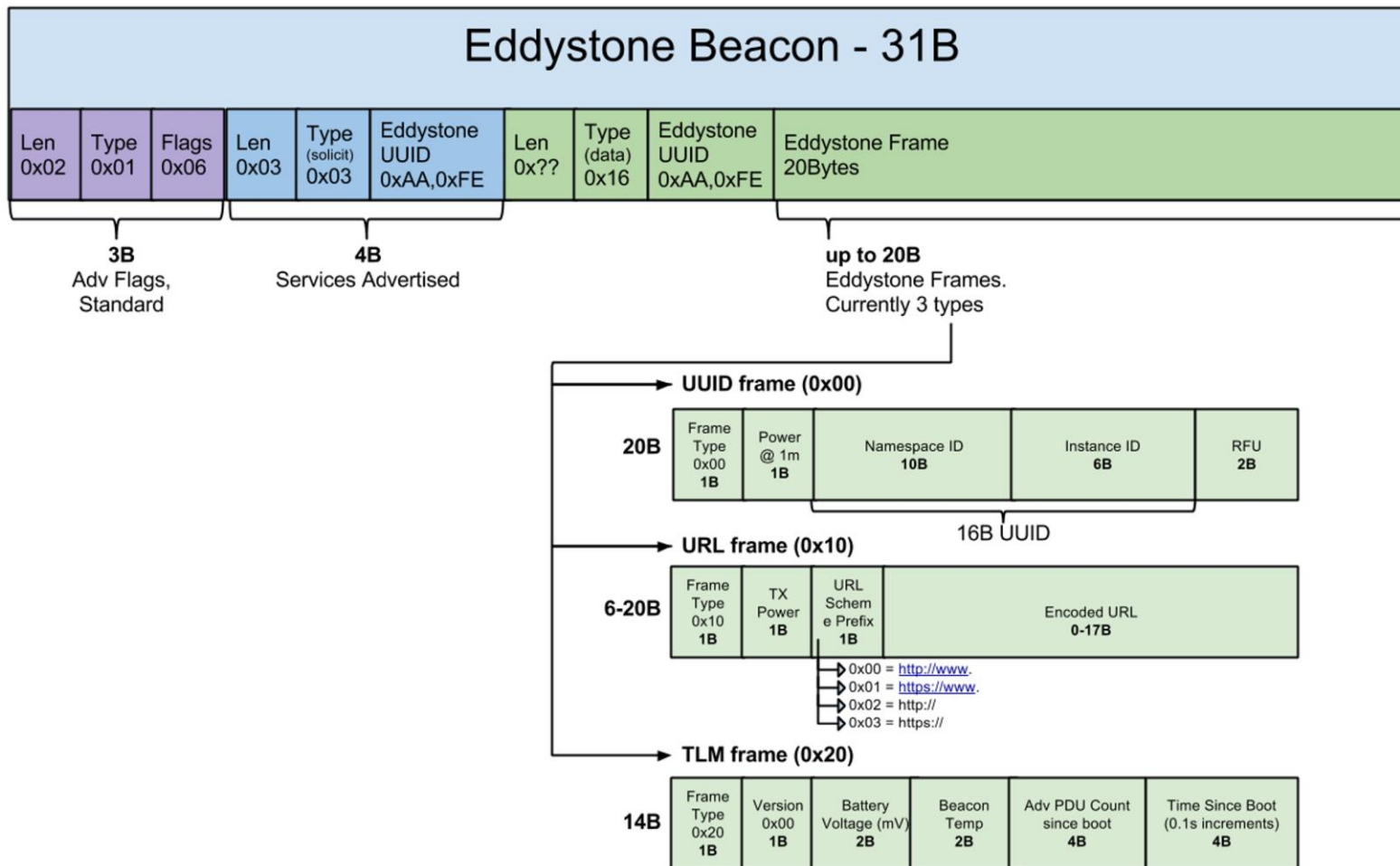


# Eddystone

- 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

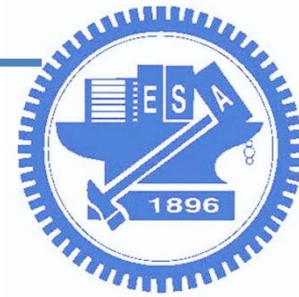


# Eddystone Frame format

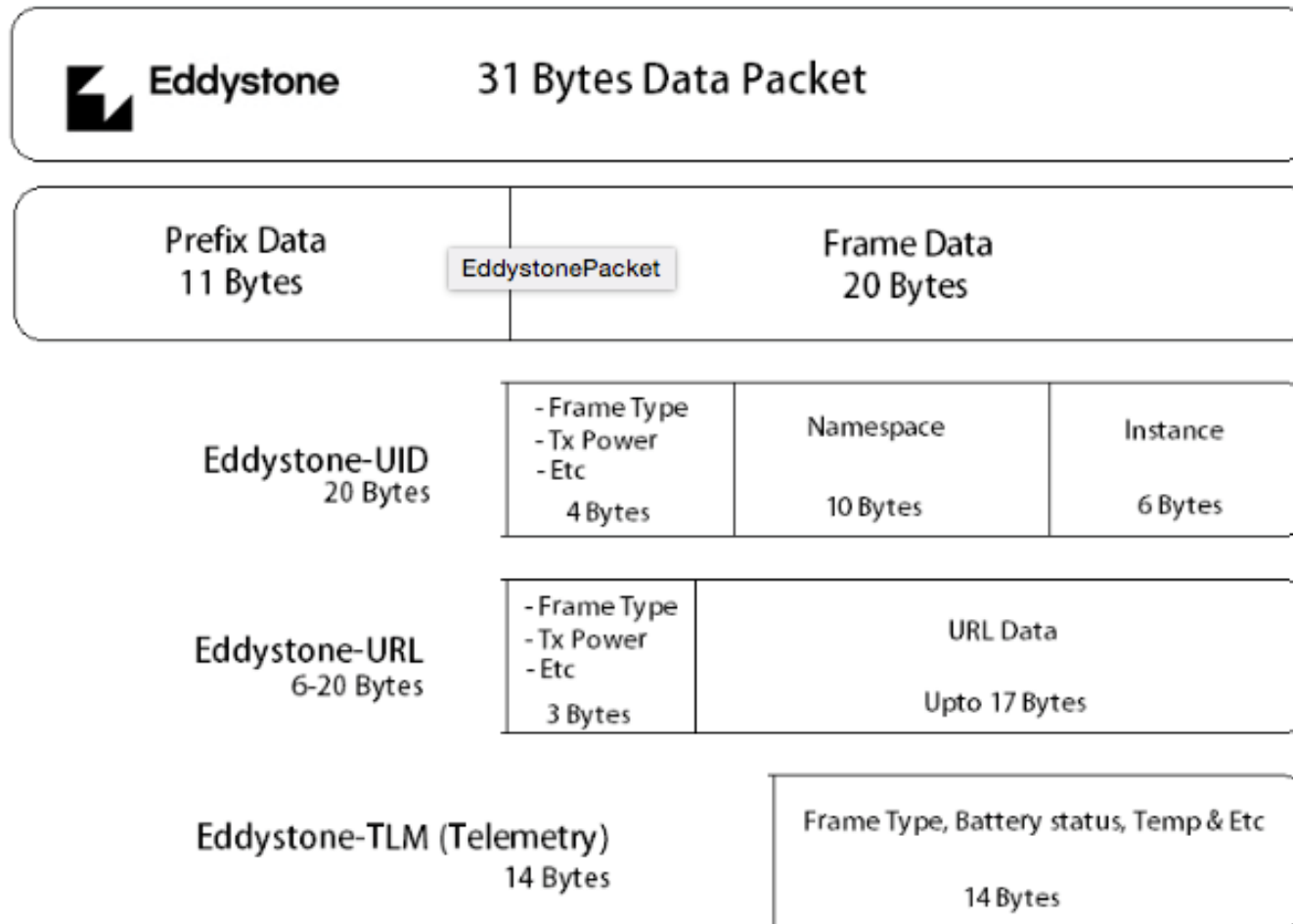


[https://developer.mbed.org/teams/Bluetooth-Low-Energy/code/BLE\\_EddystoneBeacon\\_Service/file/dfb7fb5a971b/Eddystone.h](https://developer.mbed.org/teams/Bluetooth-Low-Energy/code/BLE_EddystoneBeacon_Service/file/dfb7fb5a971b/Eddystone.h)





# Eddystone Frame format

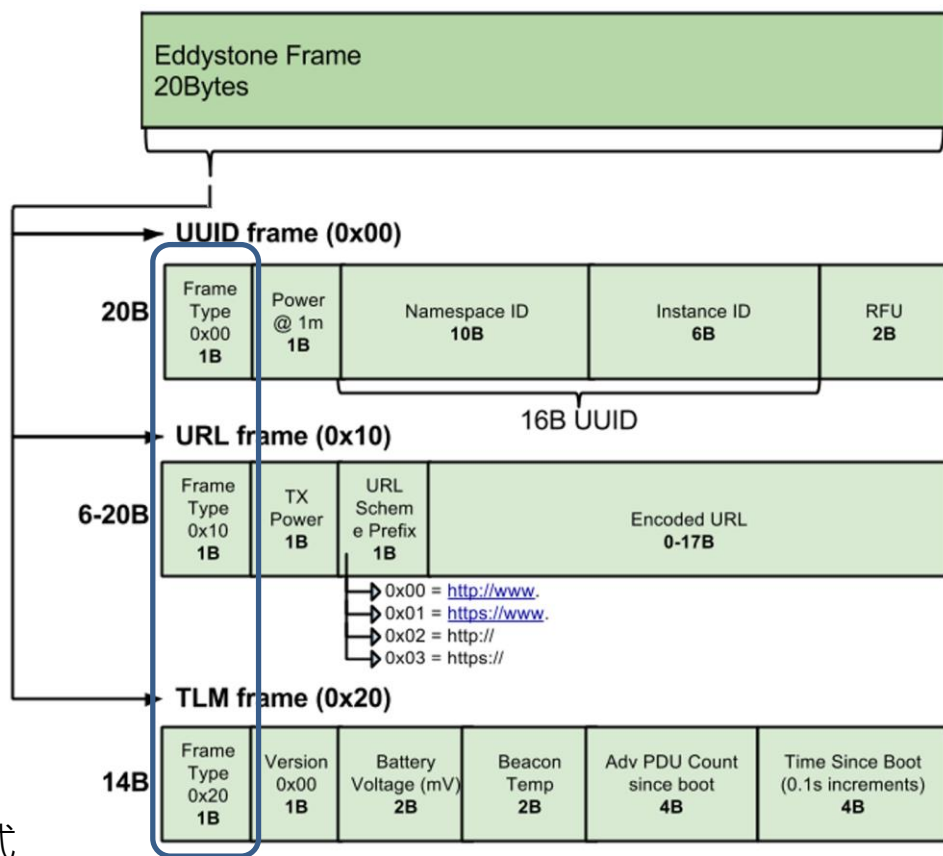




# Eddystone Frame format

## □ 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



ps. 這張圖沒有畫出Eddystone-EID frame的格式



# Eddystone

- Source: <https://github.com/google/eddystone>
- Download tool
  - `wget`  
<https://raw.githubusercontent.com/google/eddystone/master/eddystone-url/implementations/linux/advertise-url>
  - `chmod +x advertise-url`
  - `sudo ./advertise-url -u http://ptt.cc` // adversary URL
  - `sudo ./advertise-url -s` // stop



# Eddystone

## □ 手機端可安裝app查看Eddystone訊息



iBeacon & Eddystone Scanner

flurp laboratories 工具

★★★★★ 132

這個應用程式與您的部分裝置相容。

已安裝

**Beacon Scanner**

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

**Beacon detail**

<b>RSSI</b>	<b>Distance</b>
<b>-50 dBm</b>	<b>0.15 m</b>
	Immediate
<b>TX</b>	<b>Bluetooth</b>
<b>-60 dBm</b>	No name found
	00:1A:7D:DA:71:13

**Beacon Scanner**

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

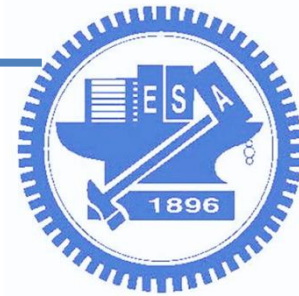
RSSI	Far	TX	UUID	
-87 dBm	-70 dBm	Distance	Major	Minor
iBeacon	2.91 m	10	231	
RSSI	Far	TX	UUID	
-90 dBm	-70 dBm	Distance	Major	Minor
iBeacon	3.03 m	10	236	
RSSI	Far	TX	UUID	
-88 dBm	-70 dBm	Distance	Major	Minor
iBeacon	3.16 m	10	237	
RSSI	Far	TX	UUID	
-92 dBm	-70 dBm	Distance	Major	Minor
iBeacon	3.16 m	10	232	
RSSI	Far	TX	UUID	
-94 dBm	-70 dBm	Distance	Major	Minor
iBeacon	3.16 m	10	232	

**Beacon detail**

<b>RSSI</b>	<b>Distance</b>
<b>-50 dBm</b>	<b>0.15 m</b>
	Immediate
<b>TX</b>	<b>Bluetooth</b>
<b>-60 dBm</b>	No name found
	00:1A:7D:DA:71:13

100  
80  
60  
40  
20  
0

URL  
http://ptt.cc



# Eddystone

- `sudo ./advertise-url -u http://hk.3345678`

The terminal window shows the command `sudo ./advertise-url -u http://hk.3345678` being executed on a Raspberry Pi. The output is `Advertising: http://hk.3345678`.

The Beacon Scanner app shows the following data:

RSSI	TX	URL
3 分鐘前	-60 dBm	http://hk
-67 dBm	Distance	.3345678
Eddystone-URL	1.15 m	

- `sudo ./advertise-url -s`

The terminal window shows the command `sudo ./advertise-url -s` being executed on a Raspberry Pi. The output is `Stopping advertising`.



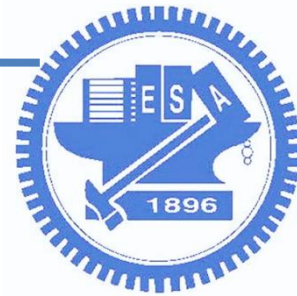


# Eddystone

- Translate URL to Eddystone message
  - Ex: `http://ptt.cc`
  - ASCII table `https://zh.wikipedia.org/wiki/ASCII`

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

- 也可以使用bluetooth工具傳送網址廣播

```
sudo hciconfig hci0 leadv 3 // 啟用藍牙的低耗能廣告(LE advertising)模式
sudo hciconfig hci0 noscan // 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 00 //傳送Eddystone frame
```

 <http://ptt.cc>

```
sudo hciconfig hci0 noadv //停止廣告
```

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



# Eddystone by hcitool

```
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 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
- 00 00 00 00 00 00 00 00 00 00 00 00: 共 10 byte

12 byte



# iBeacon

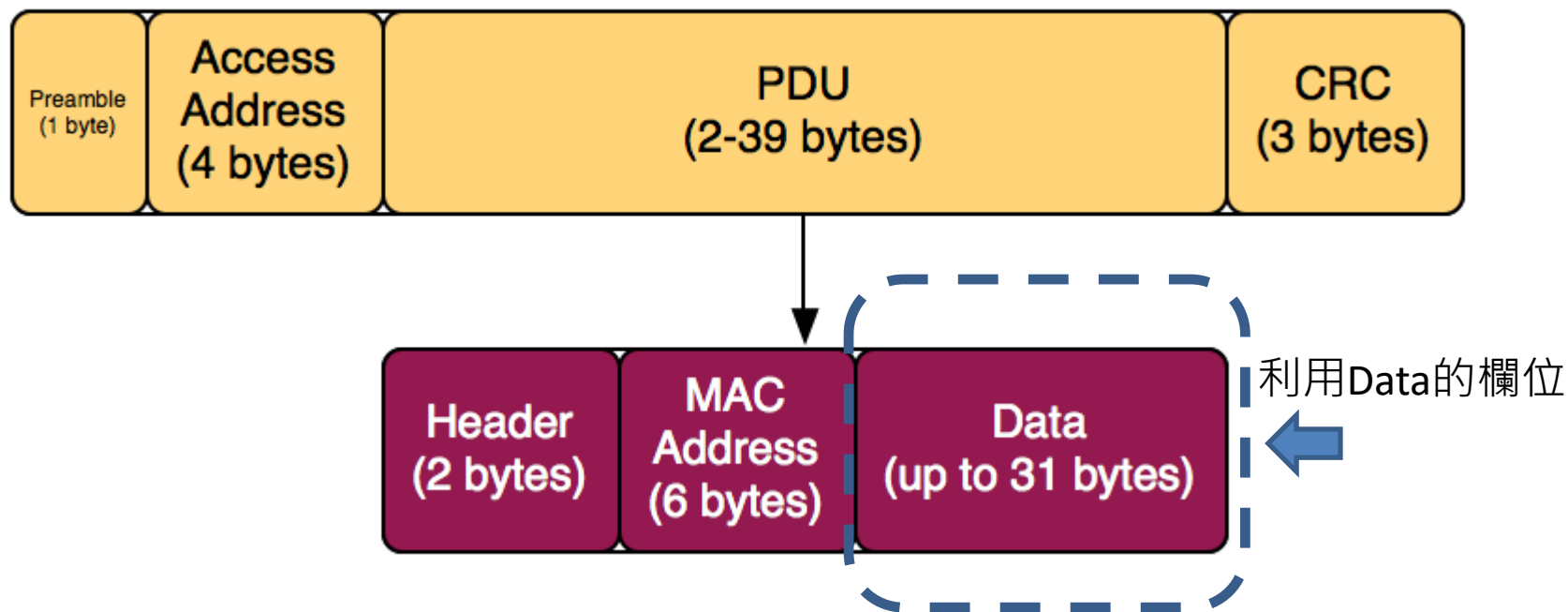
From welcoming people as they arrive at a sporting event to providing information about a nearby museum exhibit, iBeacon opens a new world of possibilities for location awareness, and countless opportunities for interactivity between iOS devices and iBeacon hardware.

<https://developer.apple.com/ibeacon/>

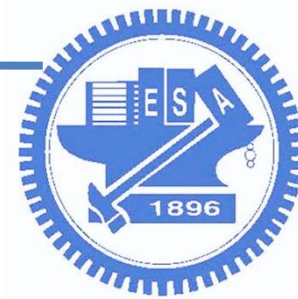


# BLE frame format

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

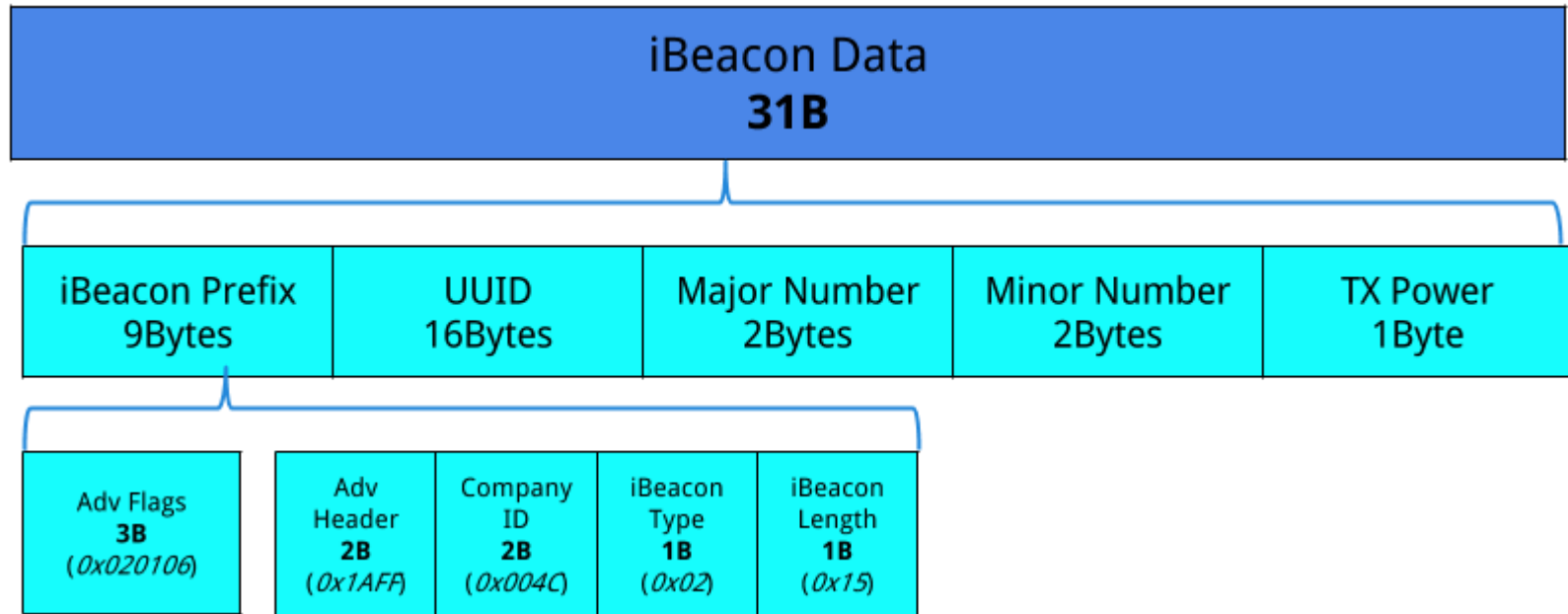






iBeacon

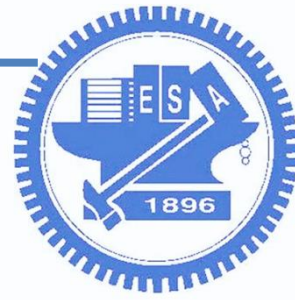
# iBeacon format





# iBeacon tool

- ❑ Dependencies
  - ❑ `sudo apt-get install bluetooth bluez-utils blueman`
- ❑ `git clone https://github.com/dburr/linux-ibeacon`
- ❑ `cd linux-ibeacon/`
- ❑ `chmod +x ibeacon`
- ❑ `sudo ./ibeacon -u your_uuid -M your_majorID -m your_minorID`
- ❑ `sudo ./ibeacon -z`



# iBeacon tool

- What is UUID?
  - UUID stands for Universally Unique Identifier. It contains 32 hexadecimal digits, split into 5 groups, separated by hyphens and should look something like this:  
**f7826da6-4fa2-4e98-8024-bc5b71e0893e**
- Each of the 5 groups must contain the following number of characters per section:
  - First section: 8
  - Second section: 4
  - Third section: 4
  - Fourth section: 4
  - Fifth section: 12



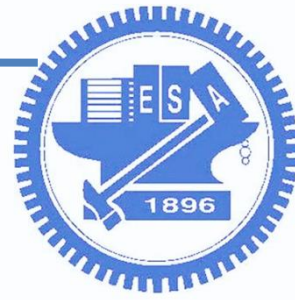
# Start advertising

- `sudo ./ibeacon -M 5566 -m 7788`
  - Major ID = 5566; Minor ID = 7788

```
(COM8) [80x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
pi@raspberrypi:~/linux-ibeacon$ sudo ./ibeacon -M 5566 -m 7788
Advertising on hci0 with:
    uuid: 0xE20A39F473F54BC4A12F17D1AD07A961
major/minor: 5566/7788 (0x15BE/0x1E6C)
    power: 200 (0xC8)
```

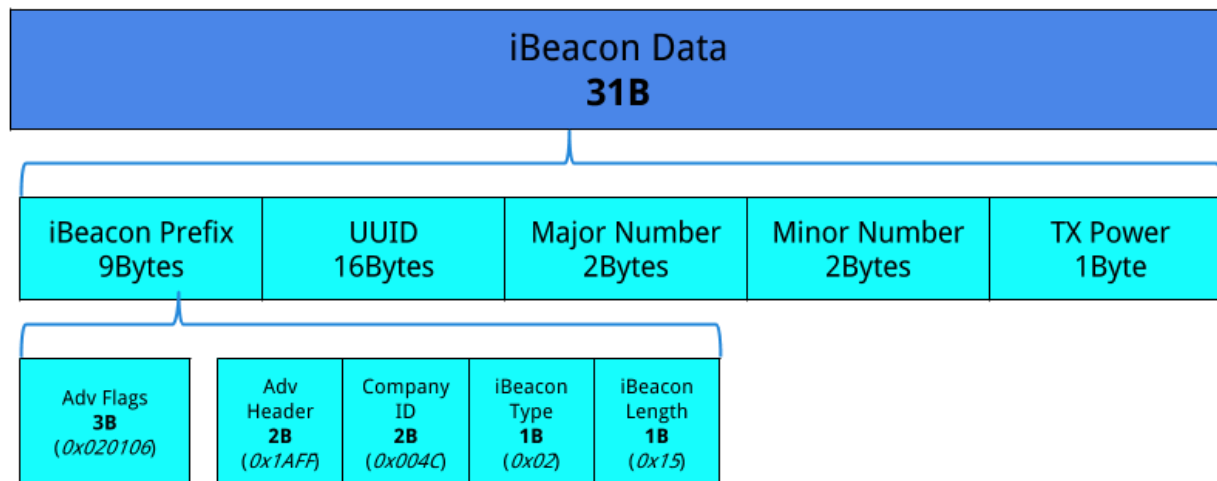
- Stop: `sudo ./ibeacon -z`

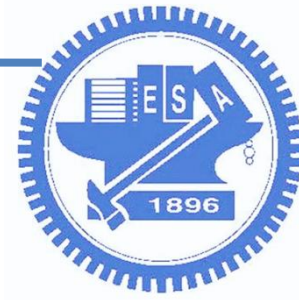
```
(COM8) [80x24]
連線(C) 編輯(E) 檢視(V) 視窗(W) 選項(O) 說明(H)
pi@raspberrypi:~/linux-ibeacon$ sudo ./ibeacon -z
Downing iBeacon on hci0
```



# Advertising by hciconfig

- ❑ `sudo hciconfig hci0 up`
- ❑ `sudo hciconfig hci0 leadv 3`
- ❑ `sudo hciconfig hci0 noscan`
- ❑ `sudo hcidtool -i hci0 cmd 0x08 0x0008 1E 02 01 06 1A FF 00 4C 02 15 E2 0A 39 F4 73 F5 4B C4 A1 2F 17 D1 AD 07 A9 61 00 00 00 00 C8 00`





# iBeacon by hcitool

- ❑ `sudo hcitool -i hci0 cmd 0x08 0x0008 1E 02 01 06 1A FF 00 4C 02 15 E2 0A 39 F4 73 F5 4B C4 A1 2F 17 D1 AD 07 A9 61 00 00 00 00 C8`
- ❑ 0x08 0x0008: set the ad package
  - ❑ #OGF = Operation Group Field = Bluetooth Command Group = 0x08
  - ❑ #OCF = Operation Command Field = HCI\_LE\_Set\_Advertising\_Data = 0x0008
- ❑ 1E // the ENTIRE following data packet in bytes (31 byte)
- ❑ 02 01 06 // set the flags for General Discoverable and BR/EDR not supported
- ❑ 1A FF // the length of the Manufacturer specific data field will be 26 bytes
- ❑ 00 4C // Company ID
- ❑ 02 // iBeacon type, ID
- ❑ 15 // length of remaining data in bytes  
(16B UUID+ 2B major, 2B minor, 1B Txpower)
- ❑ **E2 0A 39 F4 73 F5 4B C4 A1 2F 17 D1 AD 07 A9 61** // UUID
- ❑ **00 00** // Major ID
- ❑ **00 00** // Minor ID
- ❑ **C8** // Tx power