

IDENTIFICACIÓN DE DISPOSITIVOS BLUETOOTH



Alberto Moreno Tablado

1. Introducción

Cuando realizamos algún escaneo de dispositivos Bluetooth con ayuda de herramientas o simplemente con el asistente de conexiones Bluetooth de Windows, observamos que los dispositivos detectados son mostrados mediante iconos representativos de su naturaleza, ya sean PCs, PDAs, teléfonos móviles, manos libres, etc.



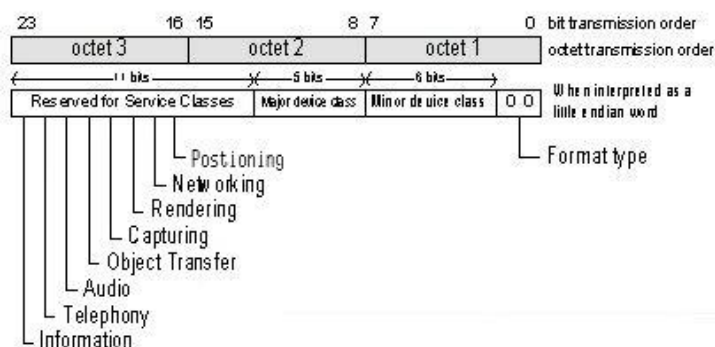
Nos preguntamos, ¿cómo será posible conocer el tipo de dispositivo del que se trata? La respuesta es, a través de los **DIACs (The General- and Device-Specific Inquiry Access Codes)**

2. Campo Class of Device/Service

Cada dispositivo Bluetooth incorpora en la cabecera de nivel de Banda Base (Baseband 1.1) de sus paquetes un campo **Class of Device/Service**. Este campo se compone de 3 octetos organizados con el siguiente formato (en *little endian*):

- 11 últimos bits reservados para las **Service Classes**.
- 11 siguientes bits reservados para las **Device Classes**.
 - 6 últimos bits reservados para las **Major Device Classes**.
 - 5 siguientes bits reservados para las **Minor Device Classes**.
- 2 primeros bits para el campo Format Type, por defecto a 0.

El siguiente esquema resume lo explicado:



Con el fin de poder obtener información del campo **Class of Device/Service**, los 3 octetos se traducen a un string binario de 24 bits cuya ordenación de 1s y 0s permite identificar los servicios ofrecidos por el dispositivo, así como la naturaleza del mismo.

3. Service Classes (Clases de servicios)

El campo reservado para las Service Classes permite identificar los servicios soportados por el dispositivo. Este campo se compone de 11 bits, del 13 al 23. Cada servicio Bluetooth está asociado a un bit en concreto, de forma que si un determinado bit del campo está a 1, entonces el dispositivo soporta ese servicio Bluetooth. La correspondencia entre nº de bit y servicio se recoge en la siguiente tabla:

Bit	Major Service Class
13	Limited Discoverable Mode [Ref #1]
14	(reserved)
15	(reserved)
16	Positioning (Location identification)
17	Networking (LAN, Ad hoc, ...)
18	Rendering (Printing, Speaker, ...)
19	Capturing (Scanner, Microphone, ...)
20	Object Transfer (v-Inbox, v-Folder, ...)
21	Audio (Speaker, Microphone, Headset service, ...)
22	Telephony (Cordless telephony, Modem, Headset service, ...)
23	Information (WEB-server, WAP-server, ...)

4. Device Classes (Clases de Dispositivos)

El campo reservado para las Device Classes permite identificar la naturaleza del dispositivo. Este campo se compone 2 subcampos: **Major Device Classes** y **Minor Device Classes**

4.1. Major Device Classes

El campo reservado para las Major Device Classes permite identificar el tipo genérico de dispositivo. Este campo se compone de 5 bits, del 8 al 12. Cada tipo genérico de dispositivo está asociado a una representación concreta de bits dentro del campo. La correspondencia entre bits y tipos genéricos de dispositivos se recoge en la siguiente tabla:

12	11	10	9	8	Major Device Class
0	0	0	0	0	Miscellaneous
0	0	0	0	1	Computer (desktop, notebook, PDA, organizers,)
0	0	0	1	0	Phone (cellular, cordless, payphone, modem, ...)
0	0	0	1	1	LAN /Network Access point
0	0	1	0	0	Audio/Video (headset, speaker, stereo, display, ...)
0	0	1	0	1	Peripheral (mouse, joystick, keyboards, ...)
0	0	1	1	0	Imaging (printing, scanner, camera, display, ...)
0	0	1	1	1	Wearable (complemento que puedes llevar puesto)
0	1	0	0	0	Toy (Juguete)
1	1	1	1	1	Uncategorized, specific device code not specified
X	X	X	X	X	All other values reserved

4.2. Minor Device Classes

El campo reservado para las Minor Device Classes permite identificar el tipo específico de dispositivo. Este campo se compone de 6 bits, del 7 al 2. Cada tipo específico de dispositivo está asociado a una representación concreta de bits dentro del campo. La correspondencia entre bits y tipos específicos de dispositivos, dentro de cada tipo genérico, se recoge en las siguientes tablas:

Computer Major Class

7	6	5	4	3	2	Minor Device Class
0	0	0	0	0	0	Uncategorized, code for device not assigned
0	0	0	0	0	1	Desktop workstation
0	0	0	0	1	0	Server-class computer
0	0	0	0	1	1	Laptop
0	0	0	1	0	0	Handheld PC/PDA (clam shell)
0	0	0	1	0	1	Palm sized PC/PDA
0	0	0	1	1	0	Wearable computer (Watch sized)
X	X	X	X	X	X	All other values reserved

Phone Major Class

7	6	5	4	3	2	Minor Device Class
0	0	0	0	0	0	Uncategorized, code for device not assigned
0	0	0	0	0	1	Cellular
0	0	0	0	1	0	Cordless
0	0	0	0	1	1	Smart phone
0	0	0	1	0	0	Wired modem or voice gateway
0	0	0	1	0	1	Common ISDN Access
X	X	X	X	X	X	All other values reserved

Audio/Video Major Class

7	6	5	4	3	2	Minor Device Class
0	0	0	0	0	0	Uncategorized, code for device not assigned
0	0	0	0	0	1	Wearable Headset Device
0	0	0	0	1	0	Hands-free Device
0	0	0	0	1	1	(Reserved)
0	0	0	1	0	0	Microphone
0	0	0	1	0	1	Loudspeaker
0	0	0	1	1	0	Headphones
0	0	0	1	1	1	Portable Audio
0	0	1	0	0	0	Car audio
0	0	1	0	0	1	Set-top box
0	0	1	0	1	0	HiFi Audio Device
0	0	1	0	1	1	VCR
0	0	1	1	0	0	Video Camera
0	0	1	1	0	1	Camcorder
0	0	1	1	1	0	Video Monitor
0	0	1	1	1	1	Video Display and Loudspeaker
0	1	0	0	0	0	Video Conferencing
0	1	0	0	0	1	(Reserved)
0	1	0	0	1	0	Gaming/Toy
X	X	X	X	X	X	All other values reserved

Peripheral Major Class

7	6	Minor Device Class	
0	0	Other (Joystick, Gamepad, Remote control, ...)	
0	1	Keyboard	
1	0	Pointing device	
1	1	Combo keyboard/pointing device	

Imaging Major Class

7	6	5	4	Minor Device Class	
X	X	X	1	Display	
X	X	1	X	Camera	
X	1	X	X	Scanner	
1	X	X	X	Printer	
X	X	X	X	All other values reserved	

Wearable Major Class

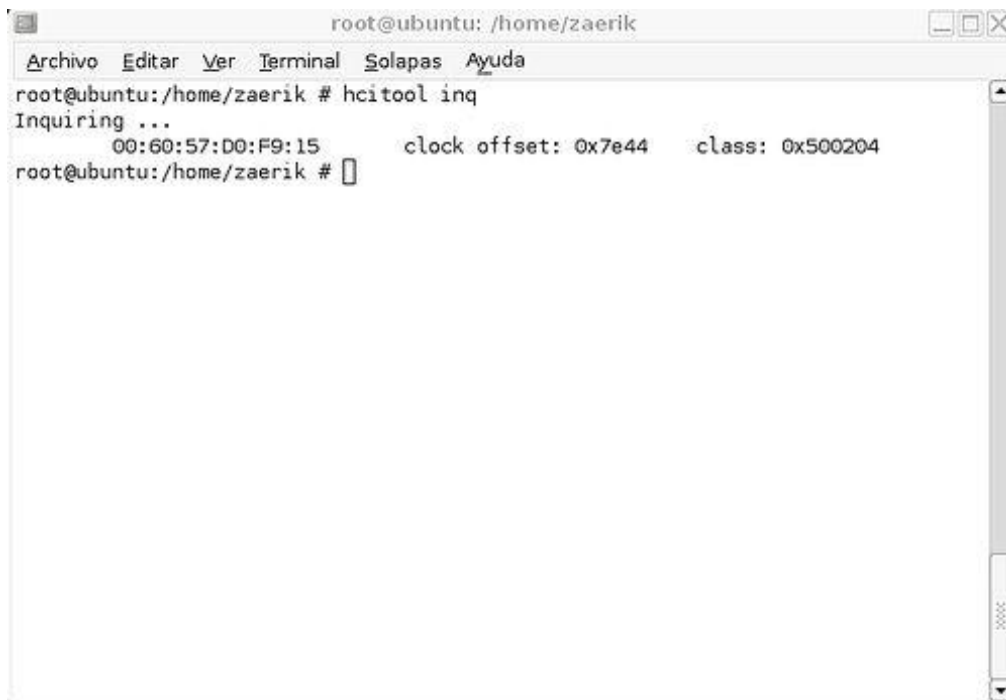
7	6	5	4	3	2	Minor Device Class	
0	0	0	0	0	0	Uncategorized, code for device not assigned	
0	0	0	0	0	1	Wrist Watch	
0	0	0	0	1	0	Pager	
0	0	0	0	1	1	Jacket	
0	0	0	1	0	0	Helmet	
0	0	0	1	0	1	Glasses	
X	X	X	X	X	X	All other values reserved	

Toy Major Class

7	6	5	4	3	2	Minor Device Class	
0	0	0	0	0	0	Uncategorized, code for device not assigned	
0	0	0	0	0	1	Robot	
0	0	0	0	1	0	Vehicle	
0	0	0	0	1	1	Doll / Action Figure	
0	0	0	1	0	0	Controller	
0	0	0	1	0	1	Game	
X	X	X	X	X	X	All other values reserved	

5. Identificando un dispositivo a partir de su campo Class of Device/Service, ejercicio práctico

Disponemos de la siguiente información:



```
root@ubuntu: /home/zaerik
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
root@ubuntu:/home/zaerik # hcitool inq
Inquiring ...
00:60:57:D0:F9:15      clock offset: 0x7e44   class: 0x500204
root@ubuntu:/home/zaerik #
```

Hemos detectado un dispositivo con la dirección MAC 00:60:57:D0:F9:15 y el campo class 0x500204.

Traducimos el campo class a formato binario

0x500204 es 01010000000001000000100 en binario.

Descomponemos el string binario en los 3 subcampos en los que se organiza el campo Class of Device/Service. La descomposición la hacemos en formato *little endian*, con el bit más significativo a la izquierda.

Recordamos la organización de los subcampos:

- 11 últimos bits reservados para las Service Classes.
- 11 siguientes bits reservados para las Device Classes.
 - 6 últimos bits reservados para las Major Device Classes.
 - 5 siguientes bits reservados para las Minor Device Classes.
- 2 primeros bits para el campo Format Type, por defecto a 0.

El resultado obtenido por la descomposición es el siguiente:

```
23 22 21 20 19 18 17 16 15 14 13 | 12 11 10 09 08 07 | 06 05 04 03 02 | 01 00
0  1  0  1  0  0  0  0  0  0  0 | 0  0  0  1  0  0 | 0  0  0  0  1  | 0  0
```

Analizamos la representación de los bits marcados en el string binario para extraer la información sobre servicios y naturaleza del dispositivo

Nos apoyamos en las tablas relacionales.

- Major Service classes

```
23 22 21 20 19 18 17 16 15 14 13
0  1  0  1  0  0  0  0  0  0  0
```

El campo tiene marcado los siguientes bits:

- 22, correspondiente a **Telephony** (Cordless telephony, Modem, Headset service, ...)
- 20, correspondiente a **Object Transfer** (v-Inbox, v-Folder, ...)

- Major Device classes

```
12 11 10 09 08
0  0  0  1  0
```

La representación de los bits marcados en este campo indica que el dispositivo se trata del siguiente tipo genérico:

```
0 0 0 1 0 | Phone (cellular, cordless, payphone, modem, ...)
```

- Minor Device classes

```
07 06 05 04 03
0  0  0  0  1
```

La representación de los bits marcados indica que el dispositivo se trata del siguiente tipo específico (dentro del tipo genérico 'Phone'):

```
0 0 0 0 0 1 | Cellular
```

La conclusión es que parece obvio que el dispositivo analizado se trata de un **Teléfono móvil**. En este caso, se trataba de un modelo Nokia NGage.

5.1. Ejercicios adicionales para coger práctica

1. Dada la class 0x140680, demostrar que el dispositivo analizado se trata de una **impresora** (grupo Imaging) con los siguientes servicios soportados: Rendering y Object Transfer

2. Dada la class 0x320114, demostrar que el dispositivo analizado se trata de una **PDA** (grupo Computer) con los siguientes servicios soportados: Networking, Object Transfer y Audio.

6. Aplicaciones prácticas de este estudio

Es posible llevar a la práctica el concepto de *las Bluetooth device classes* en los siguientes escenarios:

6.1. Obtener información más detallada sobre el dispositivo detectado.

Ya sabemos que pocas veces el nombre del dispositivo Bluetooth permite identificarlo, ya que este puede ser personalizado por el usuario. Asimismo, la dirección MAC nos permite conocer el fabricante del chipset, pero eso no acota las posibilidades; por ejemplo: Dell fabrica PCs de sobremesa, laptops, PDAs, etc.

Gracias al campo Device Class (suponiendo que este no haya sido falseado), podemos conocer de primera mano el dispositivo remoto con el que nos enfrentamos.

6.2. Realizar escaneos de víctimas filtrando los dispositivos que no nos interesan.

Por ejemplo, si estamos interesados en llevar a cabo un ataque Bluebug, sólo nos sirven teléfonos móviles y el resto de dispositivos son descartables. En base al campo Device Class podemos filtrar los contenidos de hci_inquiry obteniendo únicamente los dispositivos que posean un dev_class correspondiente a un dispositivo 'Cellular'.

Puede que a priori no importe contar con dispositivos no vulnerables a Bluebug, pero si estamos realizando un ataque masivo en un ambiente con muchos dispositivos Bluetooth a nuestro alrededor se agradece disponer de la información lo más clara posible.

6.3. Engañar a aquellos dispositivos que sólo permiten el emparejamiento con aquellos que cumplen un determinado tipo específico (o genérico) de Device Class.

Por ejemplo, algunos Manos libres están diseñados de forma que sólo es posible emparejarse desde un teléfono móvil y rechazan paquetes con origen otros dispositivos con el campo Device Class no admitido por defecto (por ejemplo, un PC).

Sabiendo como funcionan los DIACs (The General- and Device-Specific Inquiry Access Codes), podemos configurar nuestro equipo atacante falseando el campo Device Class y suplantando la identidad de un teléfono móvil. De esta forma, podemos ser capaces de conectarnos a ese dispositivo Manos libres y explotar vulnerabilidades como Car Whisperer.

7. Referencias

<https://www.bluetooth.org/foundry/assignnumb/document/baseband>
http://trifinite.org/trifinite_stuff_btclass.html

Alberto Moreno Tablado

Madrid, 12 de Diciembre de 2005