Chapter 6B: More Classic Bluetooth

Time: 3 Hours

At the end of this chapter you will know about additional Classic Bluetooth Profiles such as A2DP, AVRCP, HSP, HFP, and HID as well as other more advanced topics.

6B.1 Profiles 1

6B.1.1 Advanced Audio Distribution Profile (A2DP) 1

6B.1.2 Audio/Video Remote Control Profile (AVRCP) 1

6B.1.3 Headset Profile (HSP) 2

6B.1.4 Hands-Free Profile (HFP) 2

6B.1.5 Human Interface Device Profile (HID) 2

6B.1.6 Object Exchange (OBEX) 2

6B.1.7 PAN, FTP, Image Exchange 2

6B.1.8 Intercom Profile (ICP) 3

6B.1.9 Device ID Profile (DIP) 3

6B.1.10 Health Device Profile (HDP) 3

6B.2 Master 3

6B.3 OTA 3

6B.4 Exercises 4

# Profiles

Classic Bluetooth devices communicate with one another by using one or more of a standard set of profiles (often called services) which is maintained by the Bluetooth Special Interest Group (SIG). By using standard profiles, devices only need to determine the profile to use to start communicating rather than having to transmit the communication parameters themselves. A list of Bluetooth Profiles can be found at:

<https://en.wikipedia.org/wiki/List_of_Bluetooth_profiles>

Some of the more commonly used profiles are:

## Advanced Audio Distribution Profile (A2DP)

The A2DP profile is used for streaming multi-media audio. It is used, for example, when streaming audio from a mobile phone to a wireless headset or a car sound system. This profile is often used in conjunction with AVRCP, HSP, or HFP as described below.

The A2DP profile is designed for a unidirectional audio stream of up to 2-channel stereo. There may be more than one A2DP profile on a single device.

## Audio/Video Remote Control Profile (AVRCP)

The AVRCP profile is designed to provide a standard remote-control interface for devices such as televisions, stereo equipment, in-car navigation systems, etc.

There are several versions available depending on the functionality required, each of which is a superset of the previous version.

|  |  |
| --- | --- |
| Version | Functionality |
| 1.0 | Basic remote (play, pause, stop, etc.). |
| 1.3 | 1.0 plus metadata (such as artist, track name, etc.) and player state (such as playing, stopped, etc.) |
| 1.4 | 1.3 plus multiple media player browsing including a "Now Playing" list and search capabilities. Also has support for absolute volume. |
| 1.5 | 1.4 plus corrections/clarifications to absolute volume control |
| 1.6 | 1.5 plus browsing and track information. Support for sending cover art through BIP/OBEX (Basic Imaging Profile and Object Exchange Profile) |

## Headset Profile (HSP)

The HSP provides support for headsets including two-way 64 kbit/sec audio and minimal controls for ringing, answer a call, hang up and adjust the volume.

In a typical headset, A2DP will be used when listening to music since it provides the best quality stereo connection, but HSP will be used when making a phone call since it allows two-way communication.

## Hands-Free Profile (HFP)

The HFP is commonly used to allow car hands-free kits to communicate with mobile phones. It provides relatively low-quality monaural audio to allow the user to control some features of their phone such as making calls, playing music, etc. It is often used with other profiles such as A2DP to provide high quality audio streaming.

## Human Interface Device Profile (HID)

The HID is used for devices such as mice, keyboards, and joysticks. It provides a low-latency link with minimal power requirements.

Keyboards and keypads must be secure, but for other devices using the HID profile security is optional.

## Object Exchange (OBEX)

The OBEX (short for OBject EXchange, also called IrOBEX) is used to transmit binary objects between devices (such as business cards, data, or even applications). The transfer is similar to HTTP, as it provides a way to connect to a server (another Bluetooth device) and request or provide objects.

## PAN, FTP, Image Exchange

This profile is intended to allow the use of Bluetooth Network Encapsulation Protocol on Layer 3 protocols for transport over a Bluetooth link

Provides the capability to browse, manipulate and transfer objects (files and folders) in an object store (file system) of another system. Uses GOEP as a basis.

## Intercom Profile (ICP)

Commonly referred to as “walkie-talkie profile”, this profile is used to allow voice calls between two Bluetooth-capable handsets over Bluetooth, but the standard was withdrawn in 2010.

## Device ID Profile (DIP)

This profile is used to enable identification of the manufacturer, project ID, product version, and the version of the Device ID specification being met. This assists in identifying the correct drivers when a Bluetooth device attempts to connect to a PC.

## Health Device Profile (HDP)

This profile is used for the transmission and reception of Medical Device data.

The Health Thermometer Profile (HTP) and Heart Rate Profile (HRP) fall under this category as well.

# Master

**TODO: Write this**

# OTA

The firmware upgrade feature provided in WICED Studio allows an external device to install a newer firmware version on devices equipped with CYW20719 (as well as CYW20706 and CYW20735) chips. This section describes the functionality of the WICED Firmware Upgrade library used in various WICED Studio sample applications.

The library is split into two parts. The over the air (OTA) firmware upgrade module of the library provides a simple implementation of the GATT procedures to interact with the device performing the upgrade. The firmware upgrade HAL module of the library provides support for storing data in the non-volatile memory and switching the device to use the new firmware when the upgrade is completed. The embedded application may use the OTA module functions (which in turn use the HAL module functions), or the application may choose to use the HAL module functions directly. It is assumed that the reader is familiar with the Bluetooth Core Specification.

The library contains functionality to support secure and non-secure versions of the upgrade. In the non-secure version, a simple CRC32 verification is performed to validate that all bytes that have been sent from the device performing the upgrade are correctly saved in the serial flash of the device. The secure version of the upgrade validates that the image is correctly signed and has correct production information in the header.

## Design and Architecture

External or on-chip flash memory of the Cypress WICED chips is organized into two partitions for the failsafe upgrade capability. During the startup operation the boot code of the chip checks the first partition and if a valid image is found, assumes that the first partition is active and then starts executing the code in the first partition. If the first partition does not contain a valid image, the boot code checks the second partition and then starts execution of the code in the second partition if a valid image is found there. If neither partition is valid, the boot code enters download mode and waits for the code to be downloaded over HCI UART. The addresses of the partitions are programmed in a file with extension “btp” located in the platform directory of the SDK.

The firmware upgrade process stores received data in the inactive partition. When the download procedure is completed and the received image is verified and activated, the currently active partition is invalidated, and then the chip is restarted. After the chip reboots, the previously inactive partition becomes active. If for some reason the download or the verification step is interrupted, the valid partition remains valid and chip is not restarted. This guarantees the failsafe procedure.

The following table shows the recommended memory configuration for an application upgrading the firmware on a device with external 4Mbit serial flash:

|  |  |  |  |
| --- | --- | --- | --- |
| **Section Name** | **Offset** | **Length** | **Description** |
| Static Section (SS) | 0x0000 | 0x2000 | Static section used internally by the chip firmware |
| Volatile Section (VS1) | 0x2000 | 0x1000 | First volatile section used for the application and the stack to store data in the external or on-chip flash memory. One serial flash sector. |
| Volatile Section (VS2) | 0x3000 | 0x1000 | Used internally by the firmware when VS1 needs to be defragmented. |
| Data Section (DS1) | 0x4000 | 0x3E000 | First partition. |
| Data Section (DS2) | 0x42000 | 0x3E000 | Second partition. |

During an OTA upgrade the device performing the procedure (Downloader) pushes chunks of the new image to the device being upgraded. The embedded application receives the image and stores it in the external or on-chip flash. When all the data has been transferred, the Downloader sends a command to verify the image passing a 32-bit CRC checksum. The embedded app reads the image from the flash and verifies the image. For the non-secure download, the library calculates the checksum and verifies that it matches received CRC. For the secure download case, the library performs ECDSA verification and verifies that the Product Information stored in the new image is consistent with the Product Information of the firmware currently being executed on the device. If verification succeeds, the embedded application invalidates the active partition and restarts the chip. The simple CRC check can be easily replaced with crypto signature verification if desired, without changing the download algorithm described in this document.

# Exercises

* 1. WICED OTA Bootloader

**TODO: Write this**