

Chapter 4C: Even More Advanced BLE

Time 2 Hours

This chapter covers more advanced topics such as low power, OTA firmware upgrade, and mesh networks.

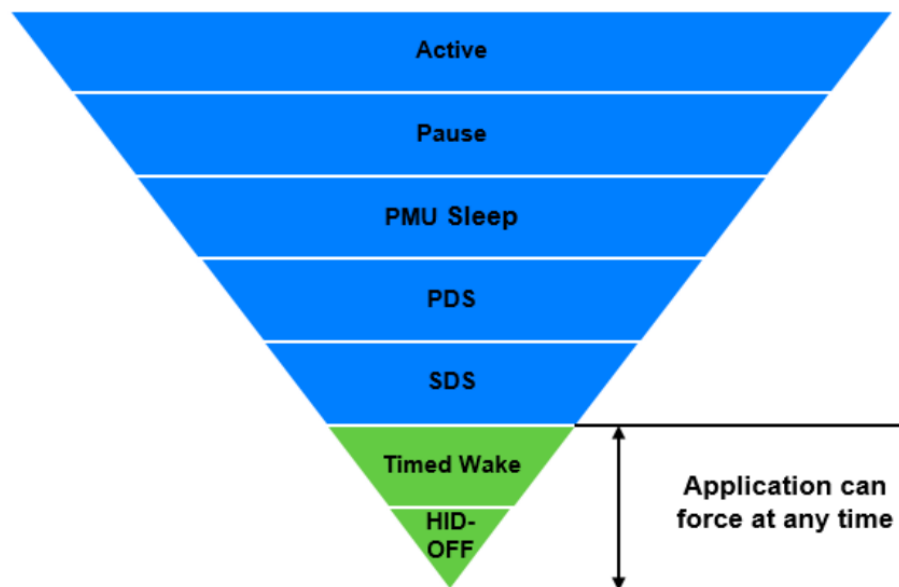
4C.1	LOW POWER	2
4C.1.1	POWER MODE OVERVIEW	2
4C.1.2	WICED LOW-POWER CODE	6
4C.2	OTA (OVER THE AIR) UPGRADE	11
4C.2.1	DESIGN AND ARCHITECTURE	11
4C.3	MESH NETWORKS	21
4C.4	CLIENTS	22
4C.5	EXERCISES	22
EXERCISE 4C.1	BLE LOW POWER (PDS)	22
EXERCISE 4C.2	OTA FIRMWARE UPGRADE (NON-SECURE)	24
EXERCISE 4C.3	(ADVANCED) OTA FIRMWARE UPGRADE (SECURE)	26
EXERCISE 4C.4	(ADVANCED) MESH NETWORKS	27
EXERCISE 4C.5	(ADVANCED) BLE LOW POWER (SDS)	28

4C.1 Low Power

4C.1.1 Power Mode Overview

WICED Bluetooth devices support different power modes. However, it is important to note that not all the devices support every mode. The following figure shows the modes from highest to lowest power. The 20719 does not support Timed-Wake or HID-OFF modes.

The Power Management Unit (PMU) is responsible for managing sleep transitions as described below.



The following table provides additional details of each of the WICED Power Modes:

Mode	Description
Active	Active mode is the normal operating mode in which all peripherals are available, and the CPU is active.
Pause	In this mode, the CPU is in Wait for Interrupt (WFI) and the HCLK, which is the high frequency clock derived from the main crystal oscillator, is running at a lower clock speed. Other clocks are active, and the state of the entire chip is retained. Pause mode is chosen when the other lower power modes are not possible.
PMU Sleep	In this mode, the CPU is in WFI and the HCLK is not running. The PMU determines if other clocks can be turned off and does so accordingly. The state of the entire chip is retained, the internal LDOs run at a lower voltage (voltage is managed by the PMU), and SRAM is retained.
Power Down Sleep (PDS)	This mode is an extension of the PMU Sleep wherein most of the peripherals such as UART and SPI are turned OFF. The entire memory is retained, and on wakeup the execution resumes from where it was paused.
Shut Down Sleep (SDS)	Everything is turned OFF except LHL GPIOs, RTC, and LPO. The device can come out of this mode either due to Bluetooth activity, an LHL interrupt, or a timer. This mode makes use of micro-Bluetooth Core Scheduler (μBCS), which is a compressed scheduler different from the regular BCS. Before going into this mode, the application can store some bytes of data into the Always-On RAM (AON). When the device comes out of this mode, the data from AON is restored. After

	waking from SDS, the application will start from the beginning (fastboot) and must restore its state based on information stored in AON. In the SDS mode, a single Bluetooth task with no data activity, such as an ACL connection, BLE connection, or BLE advertisement can be performed. If there is data activity during these tasks, the system will undergo full boot and normal BCS will be called.
Timed-Wake	The device can enter this mode asynchronously, that is, the application can force the device into this mode at any time without asking the permission from other blocks. LHL, RTC, and LPO are the only active blocks. A timer that runs off the LPO is used to wake the device after a pre-determined fixed time. The LPO source can either be an external 32 kHz crystal, internal 32 kHz crystal, or external 24 MHz crystal. The recommended option is an external 32 kHz crystal which is the default.
HID-OFF	This mode is similar to Timed-Wake, but in HID-OFF mode even the LPO and RTC are turned OFF. So, the only wakeup source is a LHL interrupt.

The power domains on the chip (and the peripherals they supply) are managed by the PMU as described in the following table:

S. No	Power Domain	Peripherals	Operational Power Modes
1	VDDC	PWM	If ACLK is used, then the hardware block can operate until the PMU enters Sleep. If LHL clock is used, then the hardware block can operate until the PMU enters SDS.
2	VDDCG	I2C, SPI, PUART, WDT, ARM GPIO, Dual Input 32-bit Timer	The hardware blocks can operate until the PMU enters Sleep.
3	VBAT/LHL	LHL GPIO, Analog PMU, RTC	The hardware blocks can operate until the PMU enters SDS.
4	VBAT/LHL	Aux ADC	The Aux ADC can operate until the PMU enters Sleep.

PMU Mode Transitions

The Power Management Unit (PMU) determines all power mode transitions except Timed-Wake and HID-OFF. The firmware can control whether PDS or SDS are allowed but it cannot not prevent Pause or PMU Sleep. It is up to the PMU to determine which sleep mode to enter depending on scheduled events. For example, if the firmware allows SDS, the PMU may decide to go into PDS instead of SDS because of an event scheduled for a short time in the future. In that case, going to SDS would not be beneficial because there is time (and power) required to shut down and re-initialize the system. The PMU can transition to Pause or PMU sleep any time.

In the firmware, you configure sleep by providing wake sources and by providing a callback function that the PMU will call whenever it wants to go to PDS or SDS. In the callback function, you can: (1) disallow sleep completely; (2) allow PDS; or (3) allow SDS depending on your firmware's requirements.

Additional SDS Mode Details

A global variable can be set in different sections of the firmware so that whenever the callback is called the appropriate sleep state will be allowed. In general, for a GAP Peripheral:

1. SDS can be used while advertising or with one connection with no pending activities.
 - a. SDS will be entered while advertising only if the timeout for that advertising type is set to 0. If not, the system will only enter PDS. For example, if the high duty cycle timeout is 30 seconds and the low duty cycle timeout is 0 then the device will use PDS during high duty cycle advertising (for 30 seconds) and will use SDS during low duty cycle advertising.
 - b. If SDS is entered while advertising, a connection request will have to be sent twice to initiate a connection. However, this may be worthwhile in applications where advertising continues for a long time.
2. SDS should not be used while pairing (i.e. encryption) is being negotiated.
3. PDS is allowed at any time unless you are interacting with peripherals that require no sleep.

For a GAP Central, SDS should not be used.

Upon wake from SDS, the device re-initializes from application_start. The boot type can be determined as initial power up or reset (cold boot) or wake from SDS (fast boot). Differences required between cold and fast boot are handled by using the boot type.

SDS mode cannot be entered if you have any active application threads. Therefore, if you have threads they must include an RTOS delay with ALLOW_THREAD_TO_SLEEP as the second parameter so that the thread will sleep.

Variables are not retained in SDS unless they are stored in Always On (AON) RAM. There are 256 bytes of AON RAM available to the application. This will be discussed in more detail in a minute.

For SDS, the connection interval should be set to 100ms or longer. Otherwise, SDS will not save significant power because the system will wake frequently.

Using RPA (i.e. the RPA refresh timeout is set to something other than WICED_BT_CFG_DEFAULT_RANDOM_ADDRESS_NEVER_CHANGE) causes two issues in SDS:

1. During a connection, the timer for RPA will cause the firmware to wake frequently (about twice per second). This will cause increased power consumption.
2. During advertising, the address will change every time a fast boot occurs. Since this happens about twice per second if RPA is enabled, it is very difficult to connect because the address will change before you can connect to the device.

HCI UART and other BT pins such as host and dev wake are powered down in SDS.

In newer devices (e.g. 20819) SDS is replaced by ePDS. In ePDS, RAM is retained (including CPU registers). There are 2 main advantages to ePDS:

1. Upon wake from ePDS, the application resumes execution from where it left off after the system boots.
2. Resuming execution from ePDS can be done in as little as 3ms (currently it is ~7ms) as compared to the 10ms it takes to resume operation from SDS.

It can be difficult to achieve lower power using SDS than with PDS – much depends on how frequent the system must wakeup due to the overhead in re-initializing everything on every wakeup.

Current Consumption

The exact current consumption depends on the firmware, but the approximate values to be expected are as follows:

Mode	Typical Current (μA)
Active	>50
PDS	10 – 50
SDS	<10

4C.1.2 WICED Low-Power Code

To use low power modes in the firmware, there are 5 (or 6) things required if you are using PDS and 8 if you are using SDS:

1. Add sleep header files
2. Setup sleep configuration
3. Create a sleep callback function
4. Update connection parameters on a GATT connection
5. Create wakeup events (timers, threads, etc.)
6. Update sleep permission variables at appropriate locations (usually SDS only)
7. Configure AON variables (SDS only)
8. Determine boot type and perform system initialization based on the value (SDS only)

Sleep Header Files

The header file *wiced_sleep.h* contains the API related to low power operation of CYW20719. That header file must be included in the source code to call the sleep API functions. You should also include *wiced_bt_l2c.h* so that we will be able to update the connection parameters in the firmware.

Sleep Configuration

The function *wiced_sleep_configure* is used to enable low power operation of the device. The parameter passed to this function is a pointer to a structure of type *wiced_sleep_config_t* that contains the sleep configuration information. The structure is defined like this:

```
/** Sleep configuration parameters */
typedef struct
{
    wiced_sleep_mode_type_t      sleep_mode;           /**< Requested sleep mode */
    wiced_sleep_wake_type_t      host_wake_mode;       /**< Active level for host wake */
    wiced_sleep_wake_type_t      device_wake_mode;     /**< Active level for device wake */
    uint8_t                     device_wake_source;    /**< Device wake source(s). GPIO mandatory for
                                                         WICED_SLEEP_MODE_TRANSPORT */
    uint32_t                     device_wake_gpio_num; /**< GPIO# to wake the device, mandatory for
                                                         WICED_SLEEP_MODE_TRANSPORT */
    wiced_sleep_allow_check_callback sleep_permit_handler; /**< Call back to be called by sleep framework
                                                         to poll for sleep permission */
}wiced_sleep_config_t;
```

In the firmware, you need to: (1) declare a global variable of type *wiced_sleep_config_t*; (2) initialize all the elements of the structure just after stack initialization; and (3) call *wiced_sleep_configure*.

The elements in the structure are:

sleep_mode: This can be either *WICED_SLEEP_MODE_NO_TRANSPORT* or *WICED_SLEEP_MODE_TRANSPORT*. If you select the former, the device will enter sleep only if no host is connected (i.e. HCI UART CTS line not asserted). If you select the latter, the device will enter sleep only when an external HCI host is connected (i.e. HCI UART CTS line is asserted). If the device is being used stand-alone without an external HCI host, you should choose *WICED_SLEEP_NO_TRANSPORT*.

host_wake_mode: This can be either *WICED_SLEEP_WAKE_ACTIVE_LOW* or *WICED_SLEEP_WAKE_ACTIVE_HIGH* depending on the polarity of the interrupt to wake the host (if a host is connected). This only applies if *sleep_mode* is *WICED_SLEEP_MODE_TRANSPORT*. The Host Wake function is on a dedicated device pin, but it can be multiplexed into other IOs (this multiplexing feature is not currently supported in the API).

device_wake_mode: This can be either *WICED_SLEEP_WAKE_ACTIVE_LOW* or *WICED_SLEEP_WAKE_ACTIVE_HIGH* depending on the polarity of the interrupt for the host to wake the device (if a host is connected). This only applies if *sleep_mode* is *WICED_SLEEP_MODE_TRANSPORT*. The Device Wake function is on a dedicated device pin, but it can be multiplexed into other IOs (this multiplexing feature is not currently supported in the API). This pin is not available on the 20719 40-pin package but the *device_wake_source* pin can be used for this purpose.

device_wake_source: The wake source can be keyscan, quadrature sensor, GPIO, or a combination of those. For example, you may want to use an interrupt from a sensor as a GPIO wake source so that the device wakes whenever new sensor data is available.

```
/** Wake sources.*/
#define WICED_SLEEP_WAKE_SOURCE_KEYSCAN (1<<0) /**< Enable wake from keyscan */
#define WICED_SLEEP_WAKE_SOURCE_QUAD (1<<1) /**< Enable wake from quadrature sensor */
#define WICED_SLEEP_WAKE_SOURCE_GPIO (1<<2) /**< Enable wake from GPIO */
```

device_wake_gpio_num: This entry specifies which GPIO is used to wake the device from sleep. This only applies if *device_wake_source* includes GPIO.

sleep_permit_handler: This element requires you to provide a function pointer for callback function that will be called by the PMU to request sleep permission and when sleep is entered. This function will be described next.

Sleep Callback Function

The sleep permission callback function takes one argument of type *wiced_sleep_poll_type_t* which specifies the reason for the callback (*WICED_SLEEP_POLL_SLEEP_PERMISSION* or *WICED_SLEEP_POLL_TIME_TO_SLEEP*) and it returns a *uint32_t*.

For a *WICED_SLEEP_POLL_SLEEP_PERMISSION* callback, the return value must be one of the following based on the requirements of the firmware:

- *WICED_SLEEP_NOT_ALLOWED* – The application can return this value if it does not want the device to enter Sleep mode.
- *WICED_SLEEP_ALLOWED_WITHOUT_SHUTDOWN* -The application can return this value if low power is allowed, but the device should not enter SDS. This means that the lowest power mode that the device can enter is PDS. If an application will have activity within a short (e.g. 10ms) period of time, this mode is preferable since SDS requires time to shut down and re-start which may result in increased power.
- *WICED_SLEEP_ALLOWED_WITH_SHUTDOWN* – When this value is returned, the device can enter any of the low power modes including SDS.

If you are using PDS, you can always return that value (unless the firmware requires that the system stay awake sometimes). If you are using SDS, the value you return will depend on the current state of the system. You will typically set Global variables in various BLE stack callback events so that sleep permit handler can determine what type of sleep (if any) should be allowed at any given time.

For a *WICED_SLEEP_POLL_TIME_TO_SLEEP* callback, you must return the maximum time that the system should be allowed to sleep. This is typically set to *WICED_SLEEP_MAX_TIME_TO_SLEEP* but may also be returned as 0 if you don't want the system to go to sleep at that time. If you want to wake at a specific time, it is better to use a timer. You should not depend on this parameter as a wake source.

Remember that the PMU makes the final decision – it polls the firmware and each peripheral to see which type of sleep is allowed and how long sleep will be possible, and then decides which mode makes sense.

Connection Parameter Update

The connection interval, latency and timeout are typically chosen by the Central. However, upon a connection, the Peripheral may request to update those values. The Central may or may not agree to the request. To reduce power consumption, it is recommended that the connection interval be set to 100ms or more once a GATT connection is established. In addition, the timeout should be set appropriately based on the connection interval, latency, and other application requirements.

An L2CAP function is used to request new values for the connection interval and timeout. This is done in the GATT connection callback when the connection state is "connected" (i.e. when the connection comes up). The function takes the *BD_ADDR*, the min and max intervals in units of 1.25ms, latency in number of connection intervals that can be missed, and the timeout in units of 10ms.

To request new connection parameters, use the following function:

```
wiced_bt_l2cap_update_ble_conn_params (  
    wiced_bt_device_address_t rem_bdRa, // BD_ADDR of remote device  
    uint16_t min_int, // Min connection interval in units of 1.25ms  
    uint16_t max_int, // Max connection interval in units of 1.25ms  
    uint16_t latency, // Latency - number of connection intervals  
    uint16_t timeout); // Timeout in units of 10ms
```

Wakeup Events

The firmware may need events that cause it to wake periodically or on specific events. For example, you may need to read a sensor value every few seconds or respond to user input such as a button press.

For periodic wakeup, you can either use a timer or you can use threads with delays that allow the thread to sleep (i.e. *ALLOW_THREAD_TO_SLEEP*). The device will not enter sleep unless all threads and timers are in a sleep state.

As previously discussed, during sleep configuration the device wake source may be configured. If that source is set to GPIO then the specified GPIO will wakeup the system. However, you will not get a GPIO interrupt handler callback unless you register the callback function using

wiced_hal_gpio_register_pin_for_interrupt. Note that while the GPIO configuration (set using wiced_hal_gpio_configure_pin) is retained during SDS, the callback registration is NOT retained so you need to register the callback during both cold and fast boot.

If you do not have any periodic wakeup sources at all, or if your wakeup source delays are longer than (or close to) the supervision timeout then the connection may be dropped when you are in SDS mode.

Sleep Permission Variable Update

One or more global variables may be used to keep track of the sleep type allowed. These variables are used in the sleep callback function to determine what value to return. For example, one possibility would be to:

1. Start out with sleep disabled
2. Allow either PDS or SDS during advertisement
 - a. This depends on how long advertising is expected to last and if it is acceptable to have to send 2 connection requests.
3. Allow only PDS once a GATT connect happens (to allow pairing/encryption)
 - a. Another option is to initiate the pairing request from the device immediately after connection so that the device can go to SDS sooner.
4. Switch between SDS and PDS once encryption of the link has completed (BTM_ENCRYPTION_STATUS_EVT with WICED_SUCCESS) depending on firmware requirements for activity.

There are other possible flows depending on the firmware's requirements.

If you are not using SDS, then you can always return *WICED_SLEEP_ALLOWED_WITHOUT_SHUTDOWN* from the sleep callback function for the poll sleep permission case unless your firmware needs to stay awake at certain times for other reasons. In that case, you won't need any sleep permission variables.

AON Variable Configuration

During SDS, variables are not retained unless they are stored in Always On (AON) RAM or NVRAM. The AON RAM space is limited to 256 bytes for the user application.

For example, you should store whether the device is connected or not so that when fast boot occurs you will be able to determine if the device was connected when it went to sleep. You may also need to store the advertising type or sensor values so that you can determine if they have changed from when the device went to sleep (e.g. to determine if a notification should be sent). To store values in AON RAM, use *PLACE_IN_ALWAYS_ON_RAM* when declaring the variable. For example:

```
PLACE_IN_ALWAYS_ON_RAM uint16_t connection_id;
```

Determine Boot Type and Perform System Initialization

The function `wiced_sleep_get_boot_mode` is called in the `application_start` function to determine whether the chip is starting up for the first time (cold boot) or coming out of SDS (fast boot). It returns a variable of type `wiced_sleep_boot_type_t` which can be `WICED_SLEEP_COLD_BOOT` or `WICED_SLEEP_FAST_BOOT`. Settings such as GPIO configuration are retained during SDS so they only need to be configured for a cold boot.

For a fast boot, it is important to check to see if the device was already connected when it went into SDS. If it is already connected, then advertisements should not be started, and you may need to read values from NVRAM or restore GATT array values. Typically, NVRAM is only used if bonding information is being saved. If not, you can store GATT array values that need to be saved during SDS in AON RAM.

4C.2 OTA (Over the Air) Upgrade

The firmware upgrade feature provided in WICED Studio allows an external device to use the Bluetooth link to transfer and 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.

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. This ensures that unknown firmware is not uploaded to your device.

4C.2.1 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 the 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 and passes a 32-bit CRC checksum. The embedded app reads the image from the flash and verifies the image as follows. For the non-secure download, the library calculates the CRC 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.

Applications for Loading New Firmware

WICED Studio contains two peer applications that can be used to transmit new firmware – one for Android and one for Windows over BLE. Both applications contain the source file as well as pre-compiled executables (.apk for Android and .exe for Windows). The Windows executable is provided for 32-bit (x86) and 64-bit (x64) architectures.

These peer applications can be found in the peer_apps folder inside the ota_firmware_upgrade application folder, or in the file system at:

```
<SDK Install Dir>\WICED-Studio-n.n\common\peer_apps\ota_firmware_upgrade\Windows\WsOtaUpgrade\Release
```

```
<SDK Install Dir>\WICED-Studio-n.n\common\peer_apps\ota_firmware_upgrade\Android\LeOTAAApp\app\build\outputs\apk
```

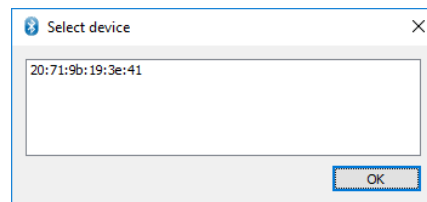
The default <SDK Install Dir> is in your Documents folder.

Windows

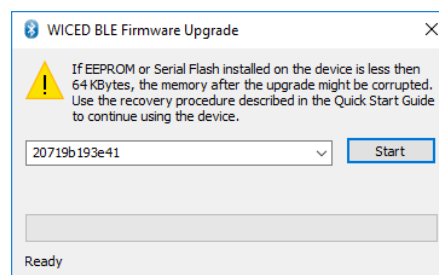
To use the Windows peer application, you must first copy the *.bin file from the build directory of the WICED application into the same folder as the Windows peer application. Then run the application with the *.bin file provided as an argument. For example, from a command or PowerShell window:

```
.\WsOtaUpgrade.exe ex02_ota-WW101_2_CYW900719Q40EVB_01-rom-ram-Wiced-release.ota.bin
```

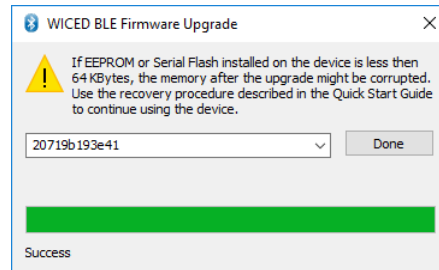
You will get a window that looks like the following. Select the device you want to update and click "OK".



On the next window, verify that the device type is correct and click "Start".



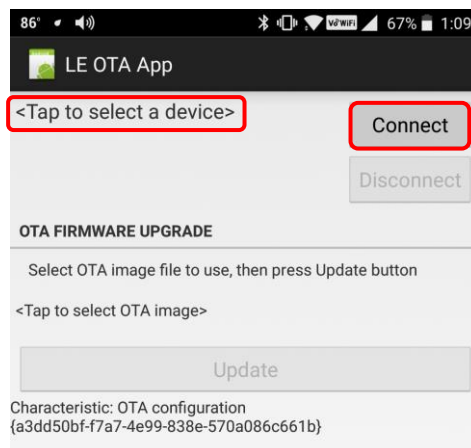
If the update worked, the window will show "Success" at the bottom. Click "Done" to close the window.



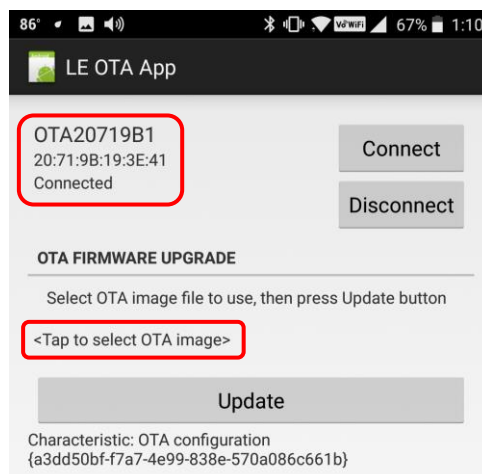
Android

To use the Android app:

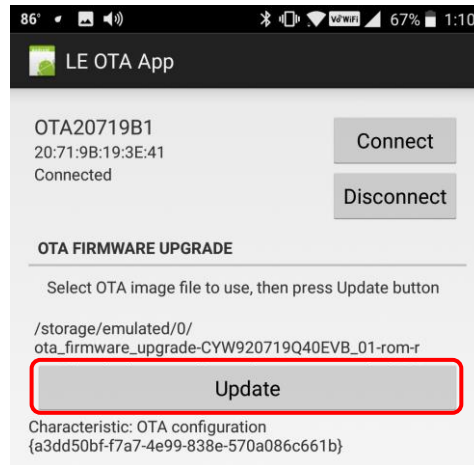
1. Install the app-debug.apk file on your Android device if you have not already done so.
2. Copy the *.bin file from the build directory onto the device in a location where you can find it.
3. Run the app called *LE OTA App*. The startup screen will look like this:



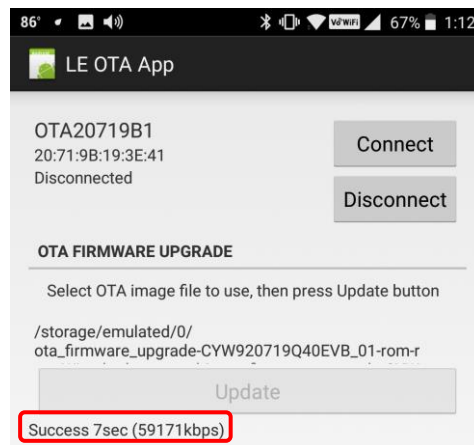
4. Tap where it says <Tap to select a device> and choose your device from the list.
5. Tap on the "Connect" button. Once connected, the screen will look like this:



6. Tap where it says <Tap to select OTA Image>, navigate to where you saved the *.bin file on your device and select it. Once the file is selected, the screen will look like this:



7. Tap the Update button. Once the update is done, you should see "Success" at the bottom of the screen. Disconnect from the device and close the app.



OTA Firmware

In the firmware, OTA requires the following:

Header Files

Include the following header files at the top of your main C file:

```
#include "wiced_bt_firmware_upgrade.h"
#include "wiced_bt_fw_upgrade.h"
```

Library

Include the OTA library in the makefile.mk:

```
$(NAME)_COMPONENTS := fw_upgrade_lib.a
```

BLE OTA Service (Non-Secure)

The GATT database must have a Primary Service defined for the OTA service. The Service and its two Characteristics are defined as follows:

```
// OTA Firmware Upgrade Service
PRIMARY_SERVICE_UUID128(HANDLE_OTA_FW_UPGRADE_SERVICE, UUID_OTA_FW_UPGRADE_SERVICE),

    CHARACTERISTIC_UUID128_WRITABLE(HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_CONTROL_POINT,
    HANDLE_OTA_FW_UPGRADE_CONTROL_POINT, UUID_OTA_FW_UPGRADE_CHARACTERISTIC_CONTROL_POINT,
    LEGATTDDB_CHAR_PROP_WRITE | LEGATTDDB_CHAR_PROP_NOTIFY | LEGATTDDB_CHAR_PROP_INDICATE,
    LEGATTDDB_PERM_VARIABLE_LENGTH | LEGATTDDB_PERM_WRITE_REQ /*| LEGATTDDB_PERM_AUTH_WRITABLE*/
    ),

    CHAR_DESCRIPTOR_UUID16_WRITABLE(HANDLE_OTA_FW_UPGRADE_CLIENT_CONFIGURATION_DESCRIPTOR,
    UUID_DESCRIPTOR_CLIENT_CHARACTERISTIC_CONFIGURATION, LEGATTDDB_PERM_READABLE |
    LEGATTDDB_PERM_WRITE_REQ /*| LEGATTDDB_PERM_AUTH_WRITABLE */),

    CHARACTERISTIC_UUID128_WRITABLE(HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_DATA,
    HANDLE_OTA_FW_UPGRADE_DATA, UUID_OTA_FW_UPGRADE_CHARACTERISTIC_DATA,
    LEGATTDDB_CHAR_PROP_WRITE, LEGATTDDB_PERM_VARIABLE_LENGTH | LEGATTDDB_PERM_WRITE_REQ /*|
    LEGATTDDB_PERM_AUTH_WRITABLE */),
```

Note that the LEGATTDDB_PERM_AUTH_WRITABLE are commented out in all three of the above so writes can be done without an authenticated link. Uncomment them if you want an authenticated link before allowing OTA updates.

Initialization

During the application initialization (typically just after initializing the GATT database with wiced_bt_gatt_db_init), the following function call must be made:

```
/* Initialize OTA (non-secure) */
wiced_ota_fw_upgrade_init(NULL, NULL);
```


GATT Connect Callback

In the GATT connection status callback function, it is necessary to pass the connection status information to the OTA library by calling the following:

```
wiced_ota_fw_upgrade_connection_status_event(p_conn_status);
```

This should be called on both a connection and dis-connection.

GATT Event Handler Functions

The handler functions for the GATT events *GATTS_REQ_TYPE_READ*, *GATTS_REQ_TYPE_WRITE*, and *GATTS_REQ_TYPE_CONF* must call the appropriate OTA functions. Note that these are in addition to any other functionality required for the normal application functionality.

If your starting project does not have an indication confirmation handler function, it must be created, and that case must be added to the GATT event callback function:

```
case GATTS_REQ_TYPE_CONF:
    status = ex02_ota_indication_cfm_handler(p_data->conn_id, p_data->data.handle);
    break;
```

Handler for *GATTS_REQ_TYPE_READ*:

```
wiced_bt_gatt_status_t ex02_ota_read_handler( wiced_bt_gatt_read_t *p_read_req, uint16_t
conn_id )
{
    wiced_bt_gatt_status_t status = WICED_BT_GATT_INVALID_HANDLE;

    switch(p_read_req->handle)
    {
        // If the indication is for an OTA service handle, pass it to the library to process
        case HANDLE_OTA_FW_UPGRADE_SERVICE:
        case HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_CONTROL_POINT:
        case HANDLE_OTA_FW_UPGRADE_CONTROL_POINT:
        case HANDLE_OTA_FW_UPGRADE_CLIENT_CONFIGURATION_DESCRIPTOR:
        case HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_DATA:
        case HANDLE_OTA_FW_UPGRADE_DATA:
        case HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_APP_INFO:
        case HANDLE_OTA_FW_UPGRADE_APP_INFO:
            status = wiced_ota_fw_upgrade_read_handler(conn_id, p_read_req);
            break;
        default:
            // Handle normal (non-OTA) read requests here
    }

    return status;
}
```

Handler for `GATTS_REQ_TYPE_WRITE`:

```
wiced_bt_gatt_status_t ex02_ota_write_handler( wiced_bt_gatt_write_t *p_write_req,
uint16_t conn_id )
{
    wiced_bt_gatt_status_t status = WICED_BT_GATT_INVALID_HANDLE;

    switch(p_write_req->handle)
    {
        // If the indication is for an OTA service handle, pass it to the library to process
        case HANDLE_OTA_FW_UPGRADE_SERVICE:
        case HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_CONTROL_POINT:
        case HANDLE_OTA_FW_UPGRADE_CONTROL_POINT:
        case HANDLE_OTA_FW_UPGRADE_CLIENT_CONFIGURATION_DESCRIPTOR:
        case HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_DATA:
        case HANDLE_OTA_FW_UPGRADE_DATA:
        case HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_APP_INFO:
        case HANDLE_OTA_FW_UPGRADE_APP_INFO:
            wiced_set_debug_uart( WICED_ROUTE_DEBUG_NONE); // This is needed due to a timing
            // issue with the Windows peer client
            status = wiced_ota_fw_upgrade_write_handler(conn_id, p_write_req);
            break;
        default:
            // Handle normal (non-OTA) read requests here
    }

    return status;
}
```

Handler for `GATTS_REQ_TYPE_CONF`:

```
wiced_bt_gatt_status_t ex02_ota_indication_cfm_handler(uint16_t handle, uint16_t conn_id)
{
    wiced_bt_gatt_status_t status = WICED_BT_GATT_INVALID_HANDLE;

    switch(handle)
    {
        // If the indication is for an OTA service handle, pass it to the library to process
        case HANDLE_OTA_FW_UPGRADE_SERVICE:
        case HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_CONTROL_POINT:
        case HANDLE_OTA_FW_UPGRADE_CONTROL_POINT:
        case HANDLE_OTA_FW_UPGRADE_CLIENT_CONFIGURATION_DESCRIPTOR:
        case HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_DATA:
        case HANDLE_OTA_FW_UPGRADE_DATA:
        case HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_APP_INFO:
        case HANDLE_OTA_FW_UPGRADE_APP_INFO:
            status = wiced_ota_fw_upgrade_indication_cfm_handler(conn_id, handle);
            break;
        default:
            // Handle normal (non-OTA) indication confirmation requests here
    }

    return status;
}
```

Buffer Pool Sizes

The large buffer pool (defined at the bottom of `wiced_bt_cfg.c`) should be increased from the default size of 512 to a size of 1024 for OTA. (Note: it must be at least the MTU size plus 12).

Disabling of UART

Note in the WRITE handler above, the debug UART is disabled before calling the OTA library write handler function. This is only required if the UART is being used. For some reason, the UART interferes with the OTA process when using the Windows peer app and causes the update to fail frequently.

Secure OTA

To use secure OTA firmware upgrade, we must create a key pair (public/private) and make a few changes in the firmware. The changes are shown in detail below.

Key Generation

Tools are provided in the WICED SDK to create, sign, and verify random keys. Executables for Windows can be found in:

```
<WICED_SDK_INSTALL_DIR>/wiced_tools/ecdsa256/Win32
```

The steps are:

1. Double-click on ecdsa_genkey.exe from Windows explorer to run the program. This will generate random keys. Note that if you re-run the program, it will overwrite any existing key files. The files created are:
 - a. ecdsa256_key.pri.bin
 - b. ecdsa256_key.pub.bin
 - c. ecdsa256_key_plus.pub.bin
 - d. ecdsa256_pub.c
2. Copy the file ecdsa256_pub.c to the application folder.
3. The OTA file will be signed once it is generated below.

Include Keys in Firmware

Add a line to the project's makefile.mk to include the ecdsa256_pub.c file. For example:

```
APP_SRC += ecdsa256_pub.c
```

Header files and Global Variables

Add the following header files to the main application C file:

```
#include "bt_types.h"  
#include "p_256_multprecision.h"  
#include "p_256_ecc_pp.h"
```

Add an external global variable declaration of type "Point" for the public key that is defined in ecdsa256_pub.c. For example:

```
extern Point    ecdsa256_public_key;
```

BLE OTA Service (Secure)

In the OTA BLE Service description in the GATT database, change the UUID for the service to the UUID for secure OTA. The change is shown here in bold:

```
// OTA Firmware Upgrade Service
PRIMARY_SERVICE_UUID128(HANDLE_OTA_FW_UPGRADE_SERVICE, UUID_OTA_SEC_FW_UPGRADE_SERVICE)
```

Initialization

In the firmware initialization section, change the first argument to the OTA init function from NULL to a pointer to a public key that was generated earlier. For example:

```
/* Initialize OTA (secure) */
wiced_ota_fw_upgrade_init(&ecdsa256_public_key, NULL);
```

Build Firmware and Sign OTA Image

To build the firmware and generate then convert the output file to a signed output file follow these steps:

1. Build the firmware as usual.
2. Once the firmware is built, copy the bin file from the build folder for the application to the <WICED_SDK_INSTALL_DIR>/wiced_tools/ecdsa256/Win32 folder.
3. Open a command terminal or power shell window (shift-right-click in the folder from Windows explorer) and enter the command:

```
.\ecdsa_sign.exe .\<fileName>.bin
```

This will produce a file called <fileName>.bin.signed.

4. Load the signed file into the device using the preferred OTA tool (i.e. Windows or Android).

4C.3 Mesh Networks

Mesh networks in BLE are accomplished using Advertising packets. The Advertising packet is 31 bytes, 12 of which are available for the Mesh packet's data. This is further divided up as:

1. Opcode: 1, 2, or 3 bytes
2. Company ID
3. Vendor Info
4. Payload

Each Mesh network has an address space. Each node has one or more addresses associated with it. The address space is 2-bytes divided up as:

1. 32K unicast addresses – these map 1 address to 1 node
2. 16K group addresses – these map 1 address to multiple nodes

The types of nodes that exist are:

1. Standard Node
2. Relay Node
3. Friend Node (a Friend Node supports 1 or more Low Power Nodes)
4. Low Power Node (a Low Power Node must be associated with exactly 1 Friend Node)
5. GATT Proxy
6. Provisioner

Devices have 2 or more Models associated with them. These are analogous to Services in regular BLE devices. There are two required models for every Bluetooth Mesh node:

1. Mesh Model to allow Provisioning
2. Node Health Model to allow the network to check on the health of a node

Other models are used to control what the node can do. Models may be hierarchical.

Models Bind to Encryption Keys

Models Subscribe to Group Addresses

Encryption:

1. Network Key – needs to be known by the relays – distributed by provisioner
2. Application Key – only known by endpoints of a message – distributed by provisioner
3. Device Key – unique per device

The Mesh Packet Header and Address are encrypted with the network key

The Mesh Packet Payload is encrypted with the application key

Provisioning can be done over GATT, Advertising channel, or Mesh network

TBD

4C.4 BLE Clients

TBD

4C.5 Exercises

Exercise 4C.1 BLE Low Power (PDS)

Introduction

In this exercise, you will create a project that implements low power using PDS. You will measure the power consumption in different power modes. The project will be based on the exercise that stores BLE bonding information in NVRAM (ch04b/ex04_ble_bond).

Project Creation

1. Copy the project from ch04b/ex04_ble_bond to ch04c/ex01_low_power. If you did not complete that exercise, copy it from the solution projects.
 - a. Hint: Don't forget to update header file names in the two C files and don't forget to update the source file names in the makefile.
 - b. Hint: Change the device name from `<init>_bond` to `<init>_lp` in the `wiced_bt_cfg.c` file and the `ex01_low_power.c` file.
 - c. Hint: Update the `maxlen` and `curlen` values in the `gatt_db_lookup_table` entry for the device name to match the new length.
2. Hint: Many function names and variable names start with `ex04_ble_bond`. You can do a global search/replace to change these to `ex01_low_power` if you want them to be consistent with the project name. Make sure you do this in the `ex01_low_power_db.h` file too.
3. Create a Make Target and verify that it still builds before proceeding.
4. Enable Low Power Operation with PDS sleep. You can enable PDS all the time in this project.
 - a. Hint: You will need to: add the sleep API header file; setup sleep configuration; create a sleep callback function; and update the connection parameters.
 - b. Hint: Refer to the WICED Low-Power code section of this chapter.
 - c. Hint: Use `WICED_GPIO_PIN_BUTTON_1` as the `device_wake_gpio_num` so that the button will wake the device when we want remove bonding information.
 - d. Hint: In the low power callback, print a single character whenever sleep permission is requested and when sleep is entered so that you can tell when the mode changes.
 - e. Hint: Use 80, 80, 0, 512 for the connection interval min, max, latency, and timeout. This results in 100ms, 100ms, 0, 5120ms.

Testing

Use the steps listed below to fill in the table with measured current consumption values:

Condition	Current (μ A)	
	Enabled	Disabled
Paired		
Notifications Enabled – Notification Not Being Sent		
Notifications Enabled – Notification Being Sent		
Advertising – Fast		
Advertising – Slow		
Paired		

Note: PUART debug printing will increase power from the device. If you want to see power numbers without debug printing change `wiced_set_debug_uart(WICED_ROUTE_DEBUG_TO_PUART)` to `wiced_set_debug_uart(WICED_ROUTE_DEBUG_NONE)` in the firmware before building/programming the kit.

Note: Before pairing, LED1 will be blinking on the shield. You should pair first then disconnect and re-connect to measure the Advertising and Connected current with the LED off.

1. Connect an ammeter across jumper J15 to allow current measurement.
2. Turn off the DIP switched on the baseboard to disable LED1 and LED2 on the baseboard. Otherwise, these will be continuously ON since they are opposite polarity to the LEDs on the shield.
3. Download the project onto the kit.
4. Open a UART terminal window (note: this won't display anything if you disabled the PUART in the firmware).
5. Open the PC CySmart app. Start scanning and then stop once your device appears.
6. Connect to the device. You will see a notification asking to confirm the connection parameters. Select 'Yes'.
7. Discover all attributes in the GATT database, and Pair with the device. Record the current (Paired).
8. Enable all notifications and record the current (Notifications Enabled – Notification Not Being Sent).
9. Tap one of the CapSense buttons repeatedly so that notifications are sent and record the current (Notifications Enabled – Notification Being Sent).
10. Disconnect from the device and record the current (Advertising – Fast).
11. Wait until advertising switches to slow mode and record the current (Advertising – Slow).
12. Pair with the device and record the current (Paired).
13. Disconnect again and clear the Device Information from the Device List in CySmart.
14. Comment out the line containing the call to `wiced_sleep_configre` to disable low power and repeat steps 2 -11 to record the current measurements.

Exercise 4C.2 OTA Firmware Upgrade (Non-Secure)

Introduction

In this exercise, you will modify chapter 4A exercise 1 to add OTA firmware upgrade capability. Once OTA support is added, you will modify the project to control 2 LEDs instead of just one and you will upload the new firmware using OTA.

Project Creation

1. Copy Chapter 4A, Exercise 1 to a new folder (i.e. ch04c). Rename the project folder and project files to `ex02_ota`.
 - a. Hint: Don't forget to update header file names in the two C files and don't forget to update the source file names in the makefile.
 - b. Hint: Change the device name from `<init>_LED` to `<init>_ota` in the `wiced_bt_cfg.c` file and the `<init>_ota.c` file.
 - c. Hint: Many function names and variable names start with `<init>_led`. You can do a global search/replace to change these to `ex02_ota` if you want them to be consistent with the project name. Make sure you do this in the `ex02_ota_db.h` file too.
 - d. Hint: Delete the `.wic` file since it is no longer a valid starting point for this project.
2. Create a Make Target for the project and verify that it still builds before proceeding.
3. Review the OTA Firmware section in this chapter and update the files as necessary:
 - a. Add additional header files to the C files
 - b. Add the OTA library to `makefile.mk`
 - c. Add the OTA service to `ex02_ota_db.c`
 - d. Update the GATT event handler functions
 - e. Increase the large buffer pool size to 1024
 - f. Disable the PUART before OTA write

Testing

1. Build the project and program it to your kit.
2. Use CySmart to make sure the project functions as expected. Write values of 00, 01, 02, and 03 to the LED characteristic. The LED should only turn on for a value of 01.
 - a. Hint: The Service with a single Characteristic is the LED Service and the Service with two Characteristics is the OTA Service.
3. Disconnect from the kit in CySmart.
4. Unplug the kit from your computer. This will ensure that OTA is used instead of regular programming to update the firmware.

5. Update the project so that the values written control the LEDs like this:

Characteristic Value	LED2	LED1
00	OFF	OFF
01	OFF	ON
02	ON	OFF
03	ON	ON

6. Copy the Make Target for the project and change "download" to "build". This will allow you to build the project without it trying to download to the kit.
7. Build the project.
8. Connect your kit directly to a power outlet using a USB charger.
9. Use OTA to update your kit. You can use either the Windows or the Android app.
 - a. Hint: Don't forget to copy over the *.bin file from the build folder every time you re-build the project so that you are updating the latest firmware.
 - b. Hint: If you need to find the Bluetooth Address of your device, use CySmart (either PC or Phone) to scan for it.
 - c. Hint: If the OTA process fails on Windows, try resetting the kit and trying again. If that still fails, try using the Android version since it is more robust.
10. Once OTA upgrade is done, connect to the kit using CySmart and verify that the new firmware functionality is working.

Exercise 4C.3 (Advanced) OTA Firmware Upgrade (Secure)

Introduction

In this exercise, you will update the previous OTA exercise to use Secure OTA firmware upgrade.

Project Creation

1. Copy and rename the previous OTA exercise to *ex05_ota_secure*.
 - a. Hint: Don't forget to update header file names in the two C files and don't forget to update the source file names in the makefile.
 - b. Hint: Change the device name from *<init>_ota* to *<init>_otas* in the *wiced_bt_cfg.c* file and the *<init>_ota_secure.c* file.
 - c. Hint: Many function names and variable names start with *ex02_ota*. You can do a global search/replace to change these to *ex05_ota_secure* if you want them to be consistent with the project name. Make sure you do this in the *ex03_ota_secure_db.h* file too.
2. Create a Make Target for the project and verify that it still builds before proceeding.
3. Review the Secure OTA Firmware section in this chapter to generate the keys and update the files as necessary.

Testing

1. Build the project and program it to your kit.
2. Use CySmart to make sure the project functions as expected.
3. Disconnect from the kit in CySmart.
4. Unplug the kit from your computer. This will ensure that OTA is used instead of regular programming to update the firmware.
5. Update the project to change the LED behavior in some way.
6. Copy the Make Target for the project and change "download" to "build". This will allow you to build the project without it trying to download to the kit.
7. Build the project.
8. Connect your kit directly to a power outlet using a USB charger.
9. Use OTA to update your kit. You can use either the Windows or the Android app.
 - a. Hint: Don't forget that every time you re-build the project you must re-sign the bin file and copy the resulting *.bin.signed to the Windows OTA folder or Android device.
 - b. Hint: If you need to find the Bluetooth Address of your device, use CySmart (either PC or Phone) to scan for it.
 - c. Hint: If the OTA process fails on Windows, try resetting the kit and trying again. If that still fails, try using the Android version since it is more robust.
10. Once OTA upgrade is done, connect to the kit using CySmart and verify that the new firmware functionality is working.



Exercise 4C.4 (Advanced) Mesh Networks

Introduction

Project Creation

Testing

Exercise 4C.5 (Advanced) BLE Low Power (SDS)

Introduction

In this exercise, you will copy a template project that implements low power using SDS.

Project Creation

1. Copy the project from the class files at WBT101_Files/Templates/ch04c/ex05_low_power_sds.
2. Create a Make Target.
3. Change "key" to your initials in ex05_low_power_sds.c and wiced_app_cfg.c so that you will be able to find your device.

Firmware Changes

To enable SDS, the following changes were made:

1. A global variable was added and used to set desired sleep mode in different phases of the application.
2. The sleep callback function was updated to return different values depending on the desired sleep mode.
3. Variables needed during a fast boot were stored in AON RAM.
4. Cold Boot vs. Fast Boot changes were made.
5. Low Duty Cycle Advertising timeout was set to 0 (never timeout).
6. RPA was disabled.

Testing

1. Open a UART terminal window.
2. Download the project onto the kit.
3. Observe the UART while the device is in high duty cycle advertising and when it is in low duty cycle advertising.
4. Open the PC CySmart app. Start scanning and then stop once your device appears.
5. Connect to the device. You will see a notification asking to confirm the connection parameters. Select 'Yes'.
6. Observe the UART when the connection happens.
7. Discover all attributes in the GATT database, and Pair with the device.
8. Observe the UART when pairing completes.
9. Enable all notifications and touch the CapSense buttons.
10. Observe the UART while notifications are being sent.
11. Disconnect and clear the Device Information from the Device List in CySmart.

Questions

1. What variable is used to control sleep permissions? What are its states?
2. What is printed to the UART when:
 - a. A sleep request is denied: _____
 - b. A sleep request is allowed without shutdown: _____
 - c. A sleep request is allowed with shutdown: _____
 - d. A fast boot occurs: _____
3. When is sleep not allowed? When is sleep allowed but without shutdown (PDS)? When is sleep allowed with shutdown (SDS)?
4. When does SDS happen (Hint: you can determine that SDS occurred when you see a fast boot)?
5. What is done differently for a cold boot vs. a fast boot? Why?
6. What is AON RAM? What values is it used for and why?
7. Where are the connection parameters (interval and timeout) updated? Why?