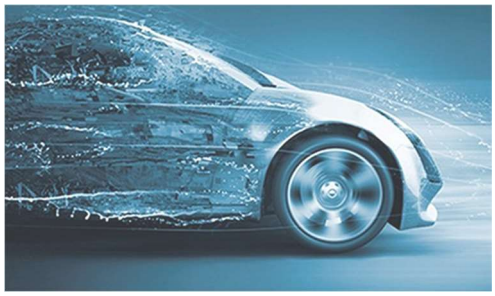
BLUETOOTH RADIO TEST CASES AND PROVISIONING HCI COMMANDS

for HCI-base Controllers

Abstract

List HCI Commands commonly used at testing Bluetooth radio,
Illustrate frequently used test cases.



Infineon Technologies AG

Contents

1 Introduction

The purpose of this document is to list the HCI commands required to be sent to the Bluetooth Controller by a Bluetooth Host stack so that the Bluetooth Controller may enter proper test mode to conduct Bluetooth radio tests. Complete details of these commands can be found in the BLUETOOTH CORE SPECIFICATIONS, https://www.bluetooth.com/specifications/.

This documented set of commands are intended for use with a Cypress Bluetooth BR/EDR and BLE Controllers.

2 HCI Commands

This section lists most common HCI standard and vendor specific commands which will be used when configuring Bluetooth Controller to conduct Bluetooth radio tests.

2.1 SIG Standard HCI Commands

2.1.1 HCI_Inquiry

Command (Core Spec. v. 4.2 and above)	
HCI_Inquiry	OGF:0x01, OCF:0x0001
Parameters	
LAP	Size: 3 octets (little endian format) 0x9E8B33 – General/Unlimited inquiry access code (GIAC) 0x9E8B00 – Limited dedicated inquiry access code (LIAC)
Inquiry_Length	Size: 1 octet N = 0x01 to 0x30 Specified time period = N * 1.28 seconds
Num_Responses	Size: 1 octet 0x00 – Unlimited number of responses 0xXX – Maximum number of responses before the Inquiry stops
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Example:

```
11:32.140  com13  c>  Inquiry                                   LAP: 0x9E8B33
            HCI Command
         com13@115200
   [01 04 05]: 33 8B 9E 08 00
   opcode = 0x401 (1025, "Inquiry")
   LAP = 0x9E8B33 (10390323)
   Inquiry_Length = 0x8 (8, N * 1.28 sec, 0=infinite)
   Num_Responses = 0x0 (0, 0=unlimited)

11:32.145  com13  <e  Command Status
            HCI Event
         com13@115200
   [0F 04]: 00 01 01 04
   event = 0xF (15, "Command Status")
   Status = 0x0 (0, "Success")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0x401 (1025, "Inquiry")

11:32.459  com13  <e  Inquiry Result                        Num_Responses: 0x1
            HCI Event
         com13@115200
   [02 0F]: 01 66 55 44 33 22 11 01 00 00 00 00 00 C5 06
   event = 0x2 (2, "Inquiry Result")
   Num_Responses = 0x1 (1)
   BD_ADDR[0] = "112233445566"
   Page_Scan_Repetition_Mode[0] = 0x1 (1, "R1")
   Page_Scan_Period_Mode[0] = 0x0 (0, "P0")
   Page_Scan_Mode[0] = 0x0 (0, "Mandatory Page Scan Mode")
   Class_of_Device[0] = 0x0 (0)
   Clock_Offset[0] = 0x6C5 (1733)

…
…

11:42.387  com13  <e  Inquiry Complete
            HCI Event
         com13@115200
   [01 01]: 00
   event = 0x1 (1, "Inquiry Complete")
   Status = 0x0 (0, "Success")
```

2.1.2 HCI_Create_Connection

Command (Core Spec. v. 4.2 and above)	
HCI_Create_Connection	OGF:0x01, OCF:0x0005
Parameters	
BD_ADDR	Size: 6 octets (little endian format) 0xXXXXXXXXXXXX – BD_ADDR of the device to be connected
Packet_Type	Size: 2 octets Bit_1 = 2-DH1 shall **not** be used Bit_2 = 3-DH1 shall **not** be used Bit_3 = ignored Bit_4 = DH1 may be used Bit_8 = 2-DH3 shall **not** be used Bit_9 = 3-DH3 shall **not** be used Bit_10 = DM3 may be used Bit_11 = DH3 may be used Bit_12 = 2-DH5 shall **not** be used Bit_13 = 3-DH5 shall **not** be used Bit_14 = DM5 may be used Bit_15 = DH5 may be used
Page_Scan_Repetition_Mode	Size: 1 octet 0x00 – R0 0x01 – R1 0x02 – R2
Reserved	Size: 1 octet 0x00
Clock_Offset	Size: 2 octets Bits 14~0 – Bits 16~2 of CLKNslave-CLK Bit_15 – Clock_Offset_Valid_Flag (0:invalid, 1:valid)
Allow_Role_Switch	Size: 1 octet 0x00 – Link Master and will not accept role switch during connection setup 0x01 – Will accept role switch during connection setup
Return	
None	

Example:

```
49:32.371  usb0  c>  Create_Connection                    BD_ADDR: 112233445566
            HCI Command
   [05 04 0D]: 66 55 44 33 22 11 18 CC 01 00 00 00 00
   opcode = 0x405 (1029, "Create_Connection")
   BD_ADDR = "112233445566"
   Packet_Type = 0xCC18 (52248, "DM1 | DH1 | DM3 | DH3 | DM5 | DH5")
   Page_Scan_Repetition_Mode = 0x1 (1, "R1")
   Reserved = 0x0
   Clock_Offset_Valid = 0x0 (0)
   Allow_Role_Switch = 0x0 (0)

49:32.375  usb0  <e  Command Status
            HCI Event
   [0F 04]: 00 01 05 04
   event = 0xF (15, "Command Status")
   Status = 0x0 (0, "Success")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0x405 (1029, "Create_Connection")

49:33.834  usb0  <e  Connection Complete                  Connection_Handle: 0xB
            HCI Event
   [03 0B]: 00 0B 00 66 55 44 33 22 11 01 00
   event = 0x3 (3, "Connection Complete")
   Status = 0x0 (0, "Success")
   Connection_Handle = 0xB (11)
   BD_ADDR = "112233445566"
   Link_Type = 0x1 (1, "ACL connection")
   Encryption_Status = 0x0 (0, "Link level encryption disabled")
```


2.1.3 HCI_Reset

Command (Core Spec. v. 4.2 and above)	
HCI_Reset	OGF:0x03, OCF:0x0003
Parameters	
None	
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Example:

```
59:04.975  com13  c>  Reset
            HCI Command
        com13@115200
   [03 0C 00]
   opcode = 0xC03 (3075, "Reset")

59:04.980  com13  <c  Reset
            HCI Command Complete Event
        com13@115200
   [0E 04]: 01 03 0C 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0xC03 (3075, "Reset")
   Status = 0x0 (0, "Success")
```

2.1.4 HCI_Set_Event_Filter

Command (Core Spec. v. 4.2 and above)		
HCI_Set_Event_Filter		OGF:0x03, OCF:0x0005
Parameters		
Filter_Type		Size: 1 octet
		0x00 – Clear All Filters (check SIG Core spec. for details) 0x01 – Inquiry Result 0x02 – Connection Setup
Filter_Condition_Type		Size: 1 octet
		Type = Inquiry Result
		0x00 – Report Responses from All Devices 0x01 – Specific Class of Device 0x02 – Specific BD_ADDR
		Type = Connection Setup
		0x00 – Allow Connections from All Devices 0x01 – Specific Class of Device 0x02 – Specific BD_ADDR
Condition		Size: 1, 6 or 7 octets
		Type = Inquiry Result, Condition = Class of Device
	Class_Of_Device	Size: 3 octets 0x000000 – All Devices 0xXXXXXX – Specific Interest
	Class_Of_Device_Mask	Size: 3 octets 0xXXXXXX – Bit Mask
		Type = Inquiry Result, Condition = BD_ADDR
	BD_ADDR	Size: 6 octets
		Type = Connection Setup, Condition = All Devices
	Auto_Accept_Flag	Size: 1 octet 0x01 – Do NOT auto accept 0x02 – Do auto accept w/o role switch 0x03 – Do auto accept with role switch
		Type = Connection Setup, Condition = Class of Device
	Class_Of_Device	Size: 3 octets 0x000000 – All Devices 0xXXXXXX – Specific Interest
	Class_Of_Device_Mask	Size: 3 octets 0xXXXXXX – Bit Mask
	Auto_Accept_Flag	Size: 1 octet 0x01 – Do NOT auto accept 0x02 – Do auto accept w/o role switch 0x03 – Do auto accept with role switch
		Type = Connection Setup, Condition = BD_ADDR
	BD_ADDR	Size: 6 octets
	Auto_Accept_Flag	Size: 1 octet 0x01 – Do NOT auto accept

		0x02 – Do auto accept w/o role switch 0x03 – Do auto accept with role switch
Return		
Status		Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Example:

```
07:19.547  com13  c>  Set_Event_Filter                    Filter_Type: Connection Setup
            HCI Command
          com13@115200
   [05 0C 03]: 02 00 02
   opcode = 0xC05 (3077, "Set_Event_Filter")
   Filter_Type = 0x2 (2, "Connection Setup")
   Connection_Setup_Filter_Condition_Type = 0x0 (0, "Allow Connections from all devices")
   Auto_Accept_Flag = 0x2 (2, "Do Auto accept the connection with role switch disabled")

07:19.551  com13  <c  Set_Event_Filter
            HCI Command Complete Event
          com13@115200
   [0E 04]: 01 05 0C 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0xC05 (3077, "Set_Event_Filter")
   Status = 0x0 (0, "Success")
```

2.1.5 HCI_Write_Scan_Enable

Command (Core Spec. v. 4.2 and above)	
HCI_Write_Scan_Enable	OGF:0x03, OCF:0x001A
Parameters	
Scan_Enable	Size: 1 octet 0x00 – No Scans enabled 0x01 – Inquiry Scan enabled, Page Scan disabled 0x02 – Inquiry Scan disabled, Page Scan enabled 0x03 – Inquiry Scan enabled, Page Scan enabled
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Example:

```
12:17.557  com13  c>  Write_Scan_Enable                Scan_Enable: Inquiry and Page Scan enabled
            HCI Command
         com13@115200
   [1A 0C 01]: 03
   opcode = 0xC1A (3098, "Write_Scan_Enable")
   Scan_Enable = 0x3 (3, "Inquiry and Page Scan enabled")

12:17.560  com13  <c  Write_Scan_Enable
            HCI Command Complete Event
         com13@115200
   [0E 04]: 01 1A 0C 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0xC1A (3098, "Write_Scan_Enable")
   Status = 0x0 (0, "Success")
```

2.1.6 HCI_Read_BD_ADDR

Command (Core Spec. v. 4.2 and above)	
HCI_Read_BD_ADDR	OGF:0x04, OCF:0x0009
Parameters	
None	
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail
BD_ADDR	Size: 6 octets 0xXXXXXXXXXXXX – BD_ADDR of the local device

Example:

```
03:19.907  com6   c>  Read_BD_ADDR
            HCI Command
        com6@115200
   [09 10 00]
   opcode = 0x1009 (4105, "Read_BD_ADDR")

03:19.920  com6   <c  Read_BD_ADDR                          BD_ADDR: 112233445566
            HCI Command Complete Event
        com6@115200
   [0E 0A]: 01 09 10 00 66 55 44 33 22 11
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0x1009 (4105, "Read_BD_ADDR")
   Status = 0x0 (0, "Success")
   BD_ADDR = "112233445566"
```

2.1.7 HCI_Read_RSSI

Command (Core Spec. v. 4.2 and above)	
HCI_Read_RSSI	OGF:0x05, OCF:0x0005
Parameters	
Handle	Size: 2 octets 0xXXXX = the Connection_Handle for which RSSI is to be read (little endian format) Range – 0x0000 to 0x0EFF
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail
Handle	Size: 2 octets 0xXXXX – the Connection_Handle for which RSSI has been read
RSSI	Size: 1 octet **BR/EDR** – returns the difference between the measured RSSI and the limits of the Golden Receive Power Range. Any positive value indicates how many dB the RSSI is above the upper limit. Any negative value indicates how many dB the RSSI is below the lower limit. The value 0 indicates that the RSSI is inside the Golden Receive Power Range. (Refer to SIG Core spec. for details of Golden Receive Power Range definition) Range: -128 to 127 Units: dB **LE** – returns an absolute receiver signal strength value in dBm to +/- 6dB accuracy Range: -127 to 20, or 127 if the RSSI cannot be read Units: dBm

Example: Made the DUT (BDADDR=112233445566) connectable @**com6**; Had another device (BDADDR=E31AEA57DD1B) @**usb0** created a connection to the DUT; then issued HCI_Read_RSSI command on DUT @**com6** to retrieve RSSI value

```
48:56.331 com6  c> Set_Event_Filter                    Filter_Type: Connection Setup
          HCI Command
      com6@115200
  [05 0C 03]: 02 00 02
  opcode = 0xC05 (3077, "Set_Event_Filter")
  Filter_Type = 0x2 (2, "Connection Setup")
  Connection_Setup_Filter_Condition_Type = 0x0 (0, "Allow Connections from all devices")
  Auto_Accept_Flag = 0x2 (2, "Do Auto accept the connection with role switch disabled")
```

```
48:56.354  com6   <c  Set_Event_Filter
            HCI Command Complete Event
         com6@115200
   [0E 04]: 01 05 0C 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0xC05 (3077, "Set_Event_Filter")
   Status = 0x0 (0, "Success")

49:07.107  com6   c>  Write_Scan_Enable                    Scan_Enable: Inquiry and Page Scan
enabled
            HCI Command
         com6@115200
   [1A 0C 01]: 03
   opcode = 0xC1A (3098, "Write_Scan_Enable")
   Scan_Enable = 0x3 (3, "Inquiry and Page Scan enabled")

49:07.120  com6   <c  Write_Scan_Enable
            HCI Command Complete Event
         com6@115200
   [0E 04]: 01 1A 0C 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0xC1A (3098, "Write_Scan_Enable")
   Status = 0x0 (0, "Success")

49:32.371  usb0   c>  Create_Connection                    BD_ADDR: 112233445566
            HCI Command
   [05 04 0D]: 66 55 44 33 22 11 18 CC 01 00 00 00 00
   opcode = 0x405 (1029, "Create_Connection")
   BD_ADDR = "112233445566"
   Packet_Type = 0xCC18 (52248, "DM1 | DH1 | DM3 | DH3 | DM5 | DH5")
   Page_Scan_Repetition_Mode = 0x1 (1, "R1")
   Page_Scan_Mode = 0x0 (0, "Mandatory")
   Clock_Offset_Valid = 0x0 (0)
   Allow_Role_Switch = 0x0 (0)

49:32.375  usb0   <e  Command Status
            HCI Event
   [0F 04]: 00 01 05 04
   event = 0xF (15, "Command Status")
   Status = 0x0 (0, "Success")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0x405 (1029, "Create_Connection")
```

```
49:33.834  usb0  <e  Connection Complete                    Connection_Handle: 0xB
           HCI Event
   [03 0B]: 00 0B 00 66 55 44 33 22 11 01 00
   event = 0x3 (3, "Connection Complete")
   Status = 0x0 (0, "Success")
   Connection_Handle = 0xB (11)
   BD_ADDR = "112233445566"
   Link_Type = 0x1 (1, "ACL connection")
   Encryption_Status = 0x0 (0, "Link level encryption disabled")

49:33.840  com6  <e  Connection Complete                    Connection_Handle: 0xB
           HCI Event
       com6@115200
   [03 0B]: 00 0B 00 1B DD 57 EA 1A E3 01 00
   event = 0x3 (3, "Connection Complete")
   Status = 0x0 (0, "Success")
   Connection_Handle = 0xB (11)
   BD_ADDR = "E31AEA57DD1B"
   Link_Type = 0x1 (1, "ACL connection")
   Encryption_Status = 0x0 (0, "Link level encryption disabled")

51:47.828  com6  c>  Read_RSSI                              Connection_Handle: 0xB
           HCI Command
       com6@115200
   [05 14 02]: 0B 00
   opcode = 0x1405 (5125, "Read_RSSI")
   Connection_Handle = 0xB (11)

51:47.832  com6  <c  Read_RSSI                              Connection_Handle: 0xB
           HCI Command Complete Event
       com6@115200
   [0E 07]: 01 05 14 00 0B 00 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0x1405 (5125, "Read_RSSI")
   Status = 0x0 (0, "Success")
   Connection_Handle = 0xB (11)
   RSSI = 0 (dB)
```

2.1.8 HCI_Enable_Device_Under_Test_Mode

Command (Core Spec. v. 4.2 and above)	
HCI_Enable_Device_Under_Test_Mode	OGF:0x06, OCF:0x0003
Parameters	
None	
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Example:

```
03:47.425  com13  c>  Enable_Device_Under_Test_Mode
            HCI Command
        com13@115200
   [03 18 00]
   opcode = 0x1803 (6147, "Enable_Device_Under_Test_Mode")

03:47.430  com13  <c  Enable_Device_Under_Test_Mode
            HCI Command Complete Event
        com13@115200
   [0E 04]: 01 03 18 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0x1803 (6147, "Enable_Device_Under_Test_Mode")
   Status = 0x0 (0, "Success")
```

2.1.9 HCI_LE_Receiver_Test

Command (Core Spec. v. 4.2 and above)	
HCI_LE_Receiver_Test [v1]	OGF:0x08, OCF:0x001D
Parameters	
RX_Channel	Size: 1 octet N = (Frequency - 2402) / 2 Range – 0x00 (i.e. 2402 MHz) to 0x27 (i.e. 2480 MHz)
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Command (Core Spec. v. 5.0 and above)	
HCI_LE_Receiver_Test [v2]	OGF:0x08, OCF:0x0033
Parameters	
RX_Channel	Size: 1 octet N = (Frequency - 2402) / 2 Range – 0x00 (i.e. 2402 MHz) to 0x27 (i.e. 2480 MHz)
PHY	Size: 1 octet 0x01 – LE 1M PHY 0x02 – LE 2M PHY 0x03 – LE Coded PHY
Modulation_Index	Size: 1 octet 0x01 – Transmitter will have a standard modulation index 0x02 – Transmitter will have a stable modulation index
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Command (Core Spec. v. 5.1 and above)	
HCI_LE_Receiver_Test [v3]	OGF:0x08, OCF:0x004F
Parameters	
RX_Channel	Size: 1 octet N = (Frequency - 2402) / 2 Range – 0x00 (i.e. 2402 MHz) to 0x27 (i.e. 2480 MHz)
PHY	Size: 1 octet 0x01 – LE 1M PHY 0x02 – LE 2M PHY 0x03 – LE Coded PHY
Modulation_Index	Size: 1 octet 0x01 – Transmitter will have a standard modulation index 0x02 – Transmitter will have a stable modulation index
Expected_CTE_Length	Size: 1 octet

	0x00 – No Constant Tone Extension expected 0x02 to 0x14 – Expected length in 8us units
Expected_CTE_Type	Size: 1 octet 0x00 – AoA Constant Tone Extension 0x01 – AoD Constant Tone Extension with 1us slot 0x02 – AoD Constant Tone Extension with 2us slot
Slot_Durations	Size: 1 octet 0x01 – Switching and sampling slots are 1us each 0x02 – Switching and sampling slots are 2us each
Switching_Pattern_Length	Size: 1 octet 0x02 to 0x4B – the number of Antenna IDs in the pattern
Antenna_IDs[i]	Size: Length_of_Switching_Pattern * 1 octet 0xXX … 0xXX – List of Antenna IDs in the pattern
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Example: Core Spec. v. 5.0 and above

```
15:30.159  com13  c>  LE_Enhanced_Receiver_Test                    RX_Channel: 0x0
          HCI Command
       com13@115200
   [33 20 03]: 00 01 00
   opcode = 0x2033 (8243, "LE_Enhanced_Receiver_Test")
   RX_Channel = 0x0 (0,  (F = 2402 + [k * 2 MHz]))
   PHY = 0x1 (1, "Receiver set to receive data at 1Ms/s")
   Modulation_Index = 0x0 (0, "Assume Transmitter will have a standard modulation index")

15:30.163  com13  <c  LE_Enhanced_Receiver_Test
          HCI Command Complete Event
       com13@115200
   [0E 04]: 01 33 20 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0x2033 (8243, "LE_Enhanced_Receiver_Test")
   Status = 0x0 (0, "Success")
```

2.1.10 HCI_LE_Transmitter_Test

Command (Core Spec. v. 4.2 and above)	
HCI_LE_Transmitter_Test [v1]	OGF:0x08, OCF:0x001E
Parameters	
TX_Channel	Size: 1 octet N = (Frequency - 2402) / 2 Range – 0x00 (i.e. 2402 MHz) to 0x27 (i.e. 2480 MHz)
Test_Data_Length	Size: 1 octet 0x00 to 0xFF – length in bytes of payload in each packet
Packet_Payload_Pattern	Size: 1 octet 0x00 – PRBS9 sequence 0x01 – repeated `11110000` 0x02 – repeated `10101010` 0x03 – PRBS15 sequence 0x04 – repeated `11111111` 0x05 – repeated `00000000` 0x06 – repeated `00001111` 0x07 – repeated `01010101`
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Command (Core Spec. v. 5.0 and above)	
HCI_LE_Transmitter_Test [v2]	OGF:0x08, OCF:0x0034
Parameters	
TX_Channel	Size: 1 octet N = (Frequency - 2402) / 2 Range – 0x00 (i.e. 2402 MHz) to 0x27 (i.e. 2480 MHz)
Test_Data_Length	Size: 1 octet 0x00 to 0xFF – length in bytes of payload in each packet
Packet_Payload_Pattern	Size: 1 octet 0x00 – PRBS9 sequence 0x01 – repeated `11110000` 0x02 – repeated `10101010` 0x03 – PRBS15 sequence 0x04 – repeated `11111111` 0x05 – repeated `00000000` 0x06 – repeated `00001111` 0x07 – repeated `01010101`
PHY	Size: 1 octet 0x01 – LE 1M PHY 0x02 – LE 2M PHY 0x03 – LE Coded PHY with S=8 data coding 0x04 – LE Coded PHY with S=2 data coding

Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Command (Core Spec. v. 5.1 and above)	
HCI_LE_Transmitter_Test [v3]	OGF:0x08, OCF:0x0050
Parameters	
TX_Channel	Size: 1 octet N = (Frequency - 2402) / 2 Range – 0x00 (i.e. 2402 MHz) to 0x27 (i.e. 2480 MHz)
Test_Data_Length	Size: 1 octet 0x00 to 0xFF – length in bytes of payload in each packet
Packet_Payload_Pattern	Size: 1 octet 0x00 – PRBS9 sequence 0x01 – repeated `11110000` 0x02 – repeated `10101010` 0x03 – PRBS15 sequence 0x04 – repeated `11111111` 0x05 – repeated `00000000` 0x06 – repeated `00001111` 0x07 – repeated `01010101`
PHY	Size: 1 octet 0x01 – LE 1M PHY 0x02 – LE 2M PHY 0x03 – LE Coded PHY with S=8 data coding 0x04 – LE Coded PHY with S=2 data coding
CTE_Length	Size: 1 octet 0x00 – Do NOT transmit a Constant Tone Extension 0x02 to 0x14 – Length of the CTE in 8us units
CTE_Type	Size: 1 octet 0x00 – AoA Constant Tone Extension 0x01 – AoD Constant Tone Extension with 1us slot 0x02 – AoD Constant Tone Extension with 2us slot
Switching_Pattern_Length	Size: 1 octet 0x02 to 0x4B – the number of Antenna IDs in the pattern
Antenna_IDs[i]	Size: Length_of_Switching_Pattern * 1 octet 0xXX … 0xXX – List of Antenna IDs in the pattern
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Command (Core Spec. v. 5.2 and above)	
HCI_LE_Transmitter_Test [v4]	OGF:0x08, OCF:0x007B
Parameters	

TX_Channel	Size: 1 octet N = (Frequency - 2402) / 2 Range – 0x00 (i.e. 2402 MHz) to 0x27 (i.e. 2480 MHz)
Test_Data_Length	Size: 1 octet 0x00 to 0xFF – length in bytes of payload in each packet
Packet_Payload_Pattern	Size: 1 octet 0x00 – PRBS9 sequence 0x01 – repeated `11110000` 0x02 – repeated `10101010` 0x03 – PRBS15 sequence 0x04 – repeated `11111111` 0x05 – repeated `00000000` 0x06 – repeated `00001111` 0x07 – repeated `01010101`
PHY	Size: 1 octet 0x01 – LE 1M PHY 0x02 – LE 2M PHY 0x03 – LE Coded PHY with S=8 data coding 0x04 – LE Coded PHY with S=2 data coding
CTE_Length	Size: 1 octet 0x00 – Do NOT transmit a Constant Tone Extension 0x02 to 0x14 – Length of the CTE in 8us units
CTE_Type	Size: 1 octet 0x00 – AoA Constant Tone Extension 0x01 – AoD Constant Tone Extension with 1us slot 0x02 – AoD Constant Tone Extension with 2us slot
Switching_Pattern_Length	Size: 1 octet 0x02 to 0x4B – the number of Antenna IDs in the pattern
Antenna_IDs[i]	Size: Length_of_Switching_Pattern * 1 octet 0xXX … 0xXX – List of Antenna IDs in the pattern
Transmit_Power_Level	Size: 1 octet 0xXX – Approximate transmit power, -127 to +20 dBm 0x7E – Minimum transmit power 0x7F – Maximum transmit power
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Example: Core Spec. v. 5.0 and above

```
10:32.062  com13  c>  LE_Enhanced_Transmitter_Test                    TX_Channel: 0x0
            HCI Command
        com13@115200
   [34 20 04]: 00 25 00 01
   opcode = 0x2034 (8244, "LE_Enhanced_Transmitter_Test")
   TX_Channel = 0x0 (0,  (F = 2402 + [k * 2 MHz]))
   Length_of_Test_Data = 0x25 (37)
   Packet_Payload = 0x0 (0, "Pseudo-Random bit sequence 9")
   PHY = 0x1 (1, "Transmitter set to transmit data at 1Ms/s")

10:32.081  com13  <c  LE_Enhanced_Transmitter_Test
            HCI Command Complete Event
        com13@115200
   [0E 04]: 01 34 20 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0x2034 (8244, "LE_Enhanced_Transmitter_Test")
   Status = 0x0 (0, "Success")
```

2.1.11 HCI_LE_Test_End

Command (Core Spec. v. 4.2 and above)	
HCI_LE_Test_End	OGF:0x08, OCF:0x001F
Parameters	
None	
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail
Num_Packets	Size: 2 octets 0xXXXX – Numbers of packets received

Example:

```
13:00.679  com13  c>  LE_Test_End
          HCI Command
       com13@115200
  [1F 20 00]
  opcode = 0x201F (8223, "LE_Test_End")

13:00.683  com13  <c  LE_Test_End                    Num_Of_Packets_Received: 0xA0D7
          HCI Command Complete Event
       com13@115200
  [0E 06]: 01 1F 20 00 D7 A0
  event = 0xE (14, "Command Complete")
  Num_HCI_Command_Packets = 0x1 (1)
  Command_Opcode = 0x201F (8223, "LE_Test_End")
  Status = 0x0 (0, "Success")
  Num_Of_Packets_Received = 0xA0D7 (41175)
```

2.2 Cypress Vendor Specific HCI Commands

2.2.1 Set_Tx_Carrier_Frequency_ARM

Vendor Specific Command	
Set_Tx_Carrier_Frequency_ARM	OGF:0x3F, OCF:0x0014
Parameters	
Carrier_Enable	Size: 1 octet 0x00 – Carrier On 0x01 – Carrier Off
Carrier_Frequency (encoded)	Size: 1 octet N = (Frequency - 2400) Range – 0x02 (i.e. 2402 MHz) to 0x50 (i.e. 2480 MHz)
Modulation_Mode	Size: 1 octet 0x00 – Un-modulated 0x01 – PRBS9 sequence 0x02 – PRBS15 sequence 0x03 – repeated `00000000` 0x04 – repeated `11111111` 0x05 – incrementing symbols
Modulation_Type	Size: 1 octet 0x00 – GFSK (1Mb/s) 0x01 – QPSK (2Mb/s) 0x02 – 8DPSK (3Mb/s)
Transmit_Power	Size: 1 octet 0x00 – 0 dBm 0x01 – -4 dBm 0x02 – -8 dBm 0x03 – -12 dBm 0x04 – -16 dBm 0x05 – -20 dBm 0x06 – -24 dBm 0x07 – -28 dBm 0x08 – Specify power in dBm 0x09 – Specify power table index Note: To enable maximum output power, set the last 3 parameters as below *Transmit_Power* = 0x09 *Transmit_Power_dBm* = 0x00 *Transmit_Power_Table_Index* = 0x00
Transmit_Power_dBm	Size: 1 octet When *Transmit_Power* = 0x08, specify output power in dBm.
Transmit_Power_Table_Index	Size: 1 octet When *Transmit_Power* = 0x09, specify output power table index.

Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Example:

```
23:10.488  com13  c>  Set_Tx_Carrier_Frequency_ARM                Carrier_Enable: Carrier on
            HCI Command
        com13@115200
   [14 FC 07]: 00 02 01 00 09 00 00
   opcode = 0xFC14 (64532, "Set_Tx_Carrier_Frequency_ARM")
   Carrier_Enable = 0x0 (0, "Carrier on")
   Carrier_Frequency_Encoded = 0x2 (2)
   Carrier_Frequency = 0x962 (2402, MHz)
   Mode = 0x1 (1, "PRBS9")
   Modulation Type = 0x0 (0, "GFSK")
   Transmit_Power = 0x9 (9, "Specify Power Table index")
   Transmit_Power_Table_Index = 0x0 (0)

23:10.494  com13  <c  Set_Tx_Carrier_Frequency_ARM
            HCI Command Complete Event
        com13@115200
   [0E 04]: 01 14 FC 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0xFC14 (64532, "Set_Tx_Carrier_Frequency_ARM")
   Status = 0x0 (0, "Success")
```

2.2.2 Read_Raw_RSSI

Vendor Specific Command	
Read_Raw_RSSI	OGF:0x3F, OCF:0x0048
Parameters	
Handle	Size: 2 octets 0xXXXX = the Connection_Handle for which RSSI is to be read (little endian format) Range – 0x0000 to 0x0EFF
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail
Handle	Size: 2 octets 0xXXXX – the Connection_Handle for which RSSI has been read
RSSI	Size: 1 octet BR/EDR – returns receiver signal strength indicator Range: -110 to 0 Units: dB

Example: Made the DUT (BDADDR=112233445566) connectable @**com6**; Had another device (BDADDR=E31AEA57DD1B) @**usb0** created a connection to the DUT; then issued Read_Raw_RSSI command on DUT @**com6** to retrieve raw RSSI value

```
48:56.331  com6   c>  Set_Event_Filter                    Filter_Type: Connection Setup
          HCI Command
       com6@115200
   [05 0C 03]: 02 00 02
   opcode = 0xC05 (3077, "Set_Event_Filter")
   Filter_Type = 0x2 (2, "Connection Setup")
   Connection_Setup_Filter_Condition_Type = 0x0 (0, "Allow Connections from all devices")
   Auto_Accept_Flag = 0x2 (2, "Do Auto accept the connection with role switch disabled")

48:56.354  com6   <c  Set_Event_Filter
          HCI Command Complete Event
       com6@115200
   [0E 04]: 01 05 0C 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0xC05 (3077, "Set_Event_Filter")
   Status = 0x0 (0, "Success")
```

```
49:07.107  com6   c>  Write_Scan_Enable                    Scan_Enable: Inquiry and Page Scan
enabled
            HCI Command
         com6@115200
   [1A 0C 01]: 03
   opcode = 0xC1A (3098, "Write_Scan_Enable")
   Scan_Enable = 0x3 (3, "Inquiry and Page Scan enabled")

49:07.120  com6   <c  Write_Scan_Enable
            HCI Command Complete Event
         com6@115200
   [0E 04]: 01 1A 0C 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0xC1A (3098, "Write_Scan_Enable")
   Status = 0x0 (0, "Success")

49:32.371  usb0   c>  Create_Connection                    BD_ADDR: 112233445566
            HCI Command
   [05 04 0D]: 66 55 44 33 22 11 18 CC 01 00 00 00 00
   opcode = 0x405 (1029, "Create_Connection")
   BD_ADDR = "112233445566"
   Packet_Type = 0xCC18 (52248, "DM1 | DH1 | DM3 | DH3 | DM5 | DH5")
   Page_Scan_Repetition_Mode = 0x1 (1, "R1")
   Page_Scan_Mode = 0x0 (0, "Mandatory")
   Clock_Offset_Valid = 0x0 (0)
   Allow_Role_Switch = 0x0 (0)

49:32.375  usb0   <e  Command Status
            HCI Event
   [0F 04]: 00 01 05 04
   event = 0xF (15, "Command Status")
   Status = 0x0 (0, "Success")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0x405 (1029, "Create_Connection")

49:33.834  usb0   <e  Connection Complete                  Connection_Handle: 0xB
            HCI Event
   [03 0B]: 00 0B 00 66 55 44 33 22 11 01 00
   event = 0x3 (3, "Connection Complete")
   Status = 0x0 (0, "Success")
   Connection_Handle = 0xB (11)
   BD_ADDR = "112233445566"
   Link_Type = 0x1 (1, "ACL connection")
   Encryption_Status = 0x0 (0, "Link level encryption disabled")
```

```
49:33.840  com6   <e  Connection Complete                    Connection_Handle: 0xB
          HCI Event
       com6@115200
   [03 0B]: 00 0B 00 1B DD 57 EA 1A E3 01 00
   event = 0x3 (3, "Connection Complete")
   Status = 0x0 (0, "Success")
   Connection_Handle = 0xB (11)
   BD_ADDR = "E31AEA57DD1B"
   Link_Type = 0x1 (1, "ACL connection")
   Encryption_Status = 0x0 (0, "Link level encryption disabled")

52:28.765  com6   c>  Read_Raw_RSSI                        Connection_Handle: 0xB
          HCI Command
       com6@115200
   [48 FC 02]: 0B 00
   opcode = 0xFC48 (64584, "Read_Raw_RSSI")
   Connection_Handle = 0xB (11)

52:28.782  com6   <c  Read_Raw_RSSI                        Connection_Handle: 0xB
          HCI Command Complete Event
       com6@115200
   [0E 07]: 01 48 FC 00 0B 00 D7
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0xFC48 (64584, "Read_Raw_RSSI")
   Status = 0x0 (0, "Success")
   Connection_Handle = 0xB (11)
   RSSI = -41 (dB)
```

2.2.3 Tx_Test

Vendor Specific Command	
Tx_Test	OGF:0x3F, OCF:0x0051
Parameters	
BD_ADDR	Size: 6 octets Local Bluetooth Device Address (little endian format)
Hopping_Mode	Size: 1 octet 0x00 – All Channels 0x01 – Single Channel 0x02 – Fixed Pattern
TX_Channel	Size: 1 octet When *Hopping_Mode* = `Single Channel`, N = (Frequency - 2402) Range – 0x00 (i.e. 2402 MHz) to 0x4E (i.e. 2480 MHz)
Modulation_Mode	Size: 1 octet 0x01 – repeated `00000000` 0x02 – repeated `11111111` 0x03 – repeated `10101010` 0x04 – PRBS9 sequence 0x09 – repeated `11110000`
Logical_Channel	Size: 1 octet 0x00 – ACL Enhanced Data Rate 0x01 – ACL Basic Data Rate 0x02 – eSCO Enhanced Data Rate 0x03 – eSCO Basic Data Rate 0x04 – SCO Basic Data Rate Note: When *Hopping_Mode* = `Fixed Pattern`, the only valid *Logical_Channel* is ACL Basic Data Rate.
Baseband_Packet_Type	Size: 1 octet 0x00 – NULL 0x01 – POLL 0x02 – FHS 0x03 – DM1 0x04 – DH1 / 2-DH1 0x05 – HV1 0x06 – HV2 / 2-EV3 0x07 – HV3 / EV3 / 3-EV3 0x08 – DV / 3-DH1 0x09 – AUX1 / PS 0x0A – DM3 / 2-DH3 0x0B – DH3 / 3-DH3 0x0C – EV4 / 2-EV5 0x0D – EV5 / 3-EV5 0x0E – DM5 / 2-DH5 0x0F – DH5 / 3-DH5

	Note: When *Hopping_Mode* = `Fixed Pattern`, the only valid *Baseband_Packet_Type* is DH1 / 2-DH1.
Baseband_Packet_Length	Size: 2 octets 0xXXXX – Length in bytes (little endian format). 0xFFFF – Firmware will use its maximum length of each selected *Baseband_Packet_Type*. Note: To get highest duty cycle, use below setting in each packet type – DH1 – 27 DH3 – 183 DH5 – 339 2-DH1 – 54 2-DH3 – 367 2-DH5 – 679 3-DH1 – 83 3-DH3 – 552 3-DH5 – 1021
Transmit_Power	Size: 1 octet 0x00 – 0 dBm 0x01 – -4 dBm 0x02 – -8 dBm 0x03 – -12 dBm 0x04 – -16 dBm 0x05 – -20 dBm 0x06 – -24 dBm 0x07 – -28 dBm 0x08 – Specify power in dBm 0x09 – Specify power table index Note: To enable maximum output power, set the last 3 parameters as below *Transmit_Power* = 0x09 *Transmit_Power_dBm* = 0x00 *Transmit_Power_Table_Index* = 0x00
Transmit_Power_dBm	Size: 1 octet When *Transmit_Power* = 0x08, specify output power in range of -127 to +128. Example – 0xFC (-4dBm), 0xFB (-5dBm), 0xFA (-6dBm), …
Transmit_Power_Table_Index	Size: 1 octet When *Transmit_Power* = 0x09, specify output power table index.
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Example:

```
38:00.000  com13  c>  Tx_Test                                  Local_Device_BD_ADDR: 112233445566
            HCI Command
        com13@115200
   [51 FC 10]: 66 55 44 33 22 11 01 00 04 01 0F FF FF 09 00 00
   opcode = 0xFC51 (64593, "Tx_Test")
   Local_Device_BD_ADDR = "112233445566"
   Hopping_Mode = 0x1 (1, "Single frequency")
   Frequency = 0x0 (0, "2402 MHz")
   Modulation_Type = 0x4 (4, "PRBS9 Pattern")
   Logical_Channel = 0x1 (1, "ACL Basic")
   BB_Packet_Type = 0xF (15, "DH5 / 3-DH5")
   BB_Packet_Length = 0xFFFF (65535, Firmware will limit len to max for BB_Packet_Type)
   Tx_Power_Level = 0x9 (9, "Specify Power Table index")
   Transmit_Power_Table_Index = 0x0 (0)

38:00.005  com13  <c  Tx_Test
            HCI Command Complete Event
        com13@115200
   [0E 04]: 01 51 FC 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0xFC51 (64593, "Tx_Test")
   Status = 0x0 (0, "Success")
```

2.2.4 Rx_Test

Vendor Specific Command	
Rx_Test	OGF:0x3F, OCF:0x0052
Parameters	
BD_ADDR	Size: 6 octets Remote "the side runs Tx_Test" Bluetooth Device Address (little endian format)
Report_Period	Size: 2 octets Time duration in milliseconds (little endian format). Example – `0xE8 0x03` means 1000 milliseconds (1000=0x03e8).
RX_Channel	Size: 1 octet When *Hopping_Mode*=`Single Channel` on peer Tx_Test, N = (Frequency - 2402) Range – 0x00 (i.e. 2402 MHz) to 0x4E (i.e. 2480 MHz) When *Hopping_Mode*=`Fixed Pattern` on peer Tx_Test, N = 0xF0 The Fixed Pattern hopping mode will cause the Rx_Test to attempt synchronization with a transmitter which is transmitting the fixed pattern.
Modulation_Mode	Size: 1 octet 0x01 – repeated `00000000` 0x02 – repeated `11111111` 0x03 – repeated `10101010` 0x04 – PRBS9 sequence 0x09 – repeated `11110000`
Logical_Channel	Size: 1 octet 0x00 – ACL Enhanced Data Rate 0x01 – ACL Basic Data Rate 0x02 – eSCO Enhanced Data Rate 0x03 – eSCO Basic Data Rate 0x04 – SCO Basic Data Rate Note: When *RX_Channel* = 0xF0 (`Fixed Pattern`), the only valid *Logical_Channel* is ACL Basic Data Rate.
Baseband_Packet_Type	Size: 1 octet 0x03 – DM1 0x04 – DH1 / 2-DH1 0x05 – HV1 0x06 – HV2 / 2-EV3 0x07 – HV3 / EV3 / 3-EV3 0x08 – DV / 3-DH1 0x09 – AUX1 0x0A – DM3 / 2-DH3 0x0B – DH3 / 3-DH3

	0x0C – EV4 / 2-EV5 0x0D – EV5 / 3-EV5 0x0E – DM5 / 2-DH5 0x0F – DH5 / 3-DH5 Note: When *RX_Channel* = 0xF0 (`Fixed Pattern`), the only valid *Baseband_Packet_Type* is DH1 / 2-DH1.
Baseband_Packet_Length	Size: 2 octets 0xXXXX – Length in bytes (little endian format). 0xFFFF – Firmware will assume its maximum length of each selected *Baseband_Packet_Type*.
Return	
Status	Size: 1 octet 0x00 – Success 0x01 to 0xFF – Fail

Example: Ran Rx_Test on com13; Started Tx_Test on com5; then Received Rx_Test statistics update on com13

```
48:57.890  com13  c>  Rx_Test                          Remote_Device_BD_ADDR: 112233445566
          HCI Command
       com13@115200
  [52 FC 0E]: 66 55 44 33 22 11 E8 03 00 04 01 0F FF FF
  opcode = 0xFC52 (64594, "Rx_Test")
  Remote_Device_BD_ADDR = "112233445566"
  Report_Period = 0x3E8 (1000, milliseconds)
  Frequency = 0x0 (0, "2402 MHz")
  Modulation_Type = 0x4 (4, "PRBS9 pattern")
  Logical_Channel = 0x1 (1, "ACL Basic")
  BB_Packet_Type = 0xF (15, "DH5 / 3-DH5")
  BB_Packet_Length = 0xFFFF (65535, Firmware will limit len to max for BB_Packet_Type)

48:57.902  com13  <c  Rx_Test
          HCI Command Complete Event
       com13@115200
  [0E 04]: 01 52 FC 00
  event = 0xE (14, "Command Complete")
  Num_HCI_Command_Packets = 0x1 (1)
  Command_Opcode = 0xFC52 (64594, "Rx_Test")
  Status = 0x0 (0, "Success")

49:17.419  com5   c>  Tx_Test                          Local_Device_BD_ADDR: 112233445566
          HCI Command
       com5@115200nfc
  [51 FC 10]: 66 55 44 33 22 11 01 00 04 01 0F FF FF 09 00 00
  opcode = 0xFC51 (64593, "Tx_Test")
```

```
   Local_Device_BD_ADDR = "112233445566"
   Hopping_Mode = 0x1 (1, "Single frequency")
   Frequency = 0x0 (0, "2402 MHz")
   Modulation_Type = 0x4 (4, "PRBS9 Pattern")
   Logical_Channel = 0x1 (1, "ACL Basic")
   BB_Packet_Type = 0xF (15, "DH5 / 3-DH5")
   BB_Packet_Length = 0xFFFF (65535, Firmware will limit len to max for BB_Packet_Type)
   Tx_Power_Level = 0x9 (9, "Specify Power Table index")
   Transmit_Power_Table_Index = 0x0 (0)

49:17.437  com5   <c  Tx_Test
          HCI Command Complete Event
       com5@115200nfc
   [0E 04]: 01 51 FC 00
   event = 0xE (14, "Command Complete")
   Num_HCI_Command_Packets = 0x1 (1)
   Command_Opcode = 0xFC51 (64593, "Tx_Test")
   Status = 0x0 (0, "Success")

49:18.429  com13  <e  Vendor Specific              Event_Sub_Code: Connectionless Rx Test Statistics
          HCI Event
       com13@115200
   [FF 21]:
   07 00 00 00 00 00 00 00 00 0B 01 00 00 0B 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00
   event = 0xFF (255, "Vendor Specific")
   Event_Sub_Code = 0x7 (7, "Connectionless Rx Test Statistics")
   Sync_Timeout_Count = 0x0 (0)
   HEC_Error_Count = 0x0 (0)
   Total_Received_Packets = 0x10B (267)
   Good_Packets = 0x10B (267)
   CRC_Error_Packets = 0x0 (0)
   Total_Received_Bits = 0x0 (0)
   Good_Bits = 0x0 (0)
   Error_Bits = 0x0 (0)

49:19.430  com13  <e  Vendor Specific              Event_Sub_Code: Connectionless Rx Test Statistics
          HCI Event
       com13@115200
   [FF 21]:
   07 00 00 00 00 00 00 00 00 16 02 00 00 16 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00
   event = 0xFF (255, "Vendor Specific")
   Event_Sub_Code = 0x7 (7, "Connectionless Rx Test Statistics")
```

```
   Sync_Timeout_Count = 0x0 (0)
   HEC_Error_Count = 0x0 (0)
   Total_Received_Packets = 0x216 (534)
   Good_Packets = 0x216 (534)
   CRC_Error_Packets = 0x0 (0)
   Total_Received_Bits = 0x0 (0)
   Good_Bits = 0x0 (0)
   Error_Bits = 0x0 (0)

49:20.432  com13  <e  Vendor Specific                Event_Sub_Code: Connectionless Rx Test Statistics
            HCI Event
        com13@115200
   [FF 21]:
   07 00 00 00 00 00 00 00 00 21 03 00 00 21 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   00
   event = 0xFF (255, "Vendor Specific")
   Event_Sub_Code = 0x7 (7, "Connectionless Rx Test Statistics")
   Sync_Timeout_Count = 0x0 (0)
   HEC_Error_Count = 0x0 (0)
   Total_Received_Packets = 0x321 (801)
   Good_Packets = 0x321 (801)
   CRC_Error_Packets = 0x0 (0)
   Total_Received_Bits = 0x0 (0)
   Good_Bits = 0x0 (0)
   Error_Bits = 0x0 (0)

… etc
```

3 Frequently Used Test Cases

When starting a new test case, the HCI_Reset shall always be the first HCI command sent to the Bluetooth Controller.

3.1 DUT Test Mode

The sequence of HCI commands to enable Bluetooth DUT mode on the Bluetooth Controller:

1. HCI_Reset
2. HCI_Set_Event_Filter

   Filter_Type = 0x02[1], "Connection Setup"
   Filter_Condition_Type = 0x00[2], "Allow connections from all devices"
   Condition = 0x02[3], "Auto accept the connection w/o role switch"
3. HCI_Write_Scan_Enable

   Scan_Enable = 0x03[4], "Inquiry Scan enabled, Page Scan enabled"
4. HCI_Enable_Device_Under_Test_Mode

Command Samples:

NOTICE – *In our command sample table, each command parameter byte has been labelled with a superscript number as a reference index to the corresponding annotation described in the command sequence paragraph.*

Command	Raw Bytes: *OpCode1 OpCode2 Length Parameter(s)*
HCI_Reset	0x03 0x0C 0x00
HCI_Set_Event_Filter	0x05 0x0C 0x03 0x02[1] 0x00[2] 0x02[3]
HCI_Write_Scan_Enable	0x1A 0x0C 0x01 0x03[4]
HCI_Enable_Device_Under_Test_Mode	0x03 0x18 0x00

Command	BlueZ Format: hcitool cmd *OGF OCF Parameter(s)*
HCI_Reset	hcitool -i hci0 cmd 0x03 0x003
HCI_Set_Event_Filter	hcitool -i hci0 cmd 0x03 0x005 0x02[1] 0x00[2] 0x02[3]
HCI_Write_Scan_Enable	hcitool -i hci0 cmd 0x03 0x01A 0x03[4]
HCI_Enable_Device_Under_Test_Mode	hcitool -i hci0 cmd 0x06 0x003

3.2 Inquiry Test

The sequence of HCI commands to start inquiry transmission on the Bluetooth Controller:

1. HCI_Reset
2. HCI_Inquiry

LAP = 0x9E8B33[3,2,1], "GIAC"
Inquiry_Length = 0x08[4], "8 x 1.28 = 10.24 seconds"
Num_Responses = 0x00[5], "Unlimited"

Command Samples:

Command	Raw Bytes: *OpCode1 OpCode2 Length Parameter(s)*
HCI_Reset	0x03 0x0C 0x00
HCI_Inquiry	0x01 0x04 0x05 0x33[1] 0x8B[2] 0x9E[3] 0x08[4] 0x00[5]

Command	BlueZ Format: hcitool cmd *OGF OCF Parameter(s)*
HCI_Reset	hcitool -i hci0 cmd 0x03 0x003
HCI_Inquiry	hcitool -i hci0 cmd 0x01 0x001 0x33[1] 0x8B[2] 0x9E[3] 0x08[4] 0x00[5]

3.3 Fixed Frequency Continuous Waveform (CW) Transmission Test

The sequence of HCI commands to enable un-modulated CW transmission on the Bluetooth Controller:

1. HCI_Reset
2. Set_Tx_Carrier_Frequency_ARM

Carrier_Enable = 0x00[1], "Carrier On"
Carrier_Frequency =

Value	Frequency
0x02[2]	2402MHz
0x2A	2442MHz
0x50	2480MHz

Module_Mode = 0x00[3], "Un-modulated"
Module_Type = 0x00[4], N/A when un-modulated
Transmit_Power† = 0x09[5]
Transmit_Power_dBm† = 0x00[6]
Transmit_Power_Table_Index† = 0x00[7]
†Note: (0x09,0x00,0x00) combination sets maximum TX output

Command Samples:

Command	Raw Bytes: *OpCode1 OpCode2 Length Parameter(s)*
HCI_Reset	0x03 0x0C 0x00
Set_Tx_Carrier_Frequency_ARM	0x14 0xFC 0x07 0x00[1] 0x02[2] 0x00[3] 0x00[4] 0x09[5] 0x00[6] 0x00[7]

Command	BlueZ Format: hcitool cmd *OGF OCF Parameter(s)*
HCI_Reset	hcitool -i hci0 cmd 0x03 0x003
Set_Tx_Carrier_Frequency_ARM	hcitool -i hci0 cmd 0x3F 0x014 0x00[1] 0x02[2] 0x00[3] 0x00[4] 0x09[5] 0x00[6] 0x00[7]

3.4 Connectionless Transmitter Test

The sequence of HCI commands to enable modulated transmission with specific packet type and frequency on the Bluetooth Controller:

1. HCI_Reset
2. Tx_Test

BD_ADDR = 0x010203040506[6,5,4,3,2,1] can be any value for connectionless TX only test
Hopping_Mode =

Value	Hopping
0x00	All Channels
0x01[7]	Fixed Single Channel

TX_Channel =

Value	Frequency
0x00[8]	2402MHz
0x28	2442MHz
0x4E	2480MHz

Module_Mode = 0x04[9], "PBRS9"
Logical_Channel and Baseband_Packet_Type =

Logical_Channel	*Baseband_Packet_Type*	"TX Packet"
0x01[10]	0x04[11]	DH1
0x01	0x0B	DH3
0x01	0x0F	DH5
0x00	0x04	2-DH1
0x00	0x0A	2-DH3
0x00	0x0E	2-DH5
0x00	0x08	3-DH1
0x00	0x0B	3-DH3
0x00	0x0F	3-DH5

Baseband_Packet_Length = 0xFFFF[13,12], "Maximum length in each packet type"
Transmit_Power† = 0x09[14]
Transmit_Power_dBm† = 0x00[15]
Transmit_Power_Table_Index† = 0x00[16]
†Note: (0x09,0x00,0x00) combination sets maximum TX output

Command Samples:

Command	Raw Bytes: *OpCode1 OpCode2 Length Parameter(s)*
HCI_Reset	0x03 0x0C 0x00
Tx_Test (DH1@2402MHz)	0x51 0xFC 0x10 0x06[1] 0x05[2] 0x04[3] 0x03[4] 0x02[5] 0x01[6] 0x01[7] 0x00[8] 0x04[9] 0x01[10] 0x04[11] 0xFF[12] 0xFF[13] 0x09[14] 0x00[15] 0x00[16]

Command	BlueZ Format: hcitool cmd *OGF OCF Parameter(s)*
HCI_Reset	hcitool -i hci0 cmd 0x03 0x003
Tx_Test (DH1@2402MHz)	hcitool -i hci0 cmd 0x3F 0x051 0x06[1] 0x05[2] 0x04[3] 0x03[4] 0x02[5] 0x01[6] 0x01[7] 0x00[8] 0x04[9] 0x01[10] 0x04[11] 0xFF[12] 0xFF[13] 0x09[14] 0x00[15] 0x00[16]

3.5 Fixed Frequency Receiver Test

The Receiver Test requires two Cypress Bluetooth devices, one runs Tx_Test as a test transmitting source and the other runs Rx_Test as the test sink which composes reception statistics result. The sequence of HCI commands:

1. HCI_Reset @ both Test Source and Sink devices
2. Rx_Test @ Test Sink device

   BD_ADDR = 0x112233445566[6,5,4,3,2,1], the device address of the TX device
   Report_Period = 0x03E8[8,7] (1000 ms)
   RX_Channel =

Value	Frequency
0x00	2402MHz
0x28[9]	2442MHz
0x4E	2480MHz

   Module_Mode = 0x04[10], "PBRS9"
   Logical_Channel and Baseband_Packet_Type =

Logical_Channel	*Baseband_Packet_Type*	"TX Packet"
0x01	0x04	DH1
0x01	0x0B	DH3
0x01	0x0F	DH5
0x00	0x04	2-DH1
0x00	0x0A	2-DH3
0x00[11]	0x0E[12]	2-DH5
0x00	0x08	3-DH1
0x00	0x0B	3-DH3
0x00	0x0F	3-DH5

   Baseband_Packet_Length = 0xFFFF[14,13], "Maximum length in each packet type"

3. Tx_Test @ Test Source device. Note: Tx_Test command parameters should exactly match to the corresponding settings given in the Rx_Test command.

   BD_ADDR = 0x112233445566[20,19,18,17,16,15], the TX local device address
   Hopping_Mode = 0x01[21], must be "Fixed Single Channel"
   TX_Channel = 0x28[22], "2442MHz"
   Module_Mode = 0x04[23], "PBRS9"
   Logical_Channel = 0x00[24], "ACL EDR"
   Baseband_Packet_Type = 0x0E[25], "2-DH5"
   Baseband_Packet_Length = 0xFFFF[27,26], "Maximum length in each packet type"
   Transmit_Power† = 0x09[28]
   Transmit_Power_dBm† = 0x00[29]
   Transmit_Power_Table_Index† = 0x00[30]
   †Note: (0x09,0x00,0x00) combination sets maximum TX output

Command Samples:

Command (RX side)	Raw Bytes: *OpCode1 OpCode2 Length Parameter(s)*

HCI_Reset	0x03 0x0C 0x00
Rx_Test (2-DH5@2442MHz)	0x52 0xFC 0x0E 0x66[1] 0x55[2] 0x44[3] 0x33[4] 0x22[5] 0x11[6] 0xE8[7] 0x03[8] 0x28[9] 0x04[10] 0x00[11] 0x0E[12] 0xFF[13] 0xFF[14]
(TX side)	
HCI_Reset	0x03 0x0C 0x00
Tx_Test (2-DH5@2442MHz)	0x51 0xFC 0x10 0x66[15] 0x55[16] 0x44[17] 0x33[18] 0x22[19] 0x11[20] 0x01[21] 0x28[22] 0x04[23] 0x00[24] 0x0E[25] 0xFF[26] 0xFF[27] 0x09[28] 0x00[29] 0x00[30]

Command (RX side)	BlueZ Format: hcitool cmd *OGF OCF Parameter(s)*
HCI_Reset	hcitool -i hci0 cmd 0x03 0x003
Rx_Test (2-DH5@2442MHz)	hcitool -i hci0 cmd 0x3F 0x52 0x66[1] 0x55[2] 0x44[3] 0x33[4] 0x22[5] 0x11[6] 0xE8[7] 0x03[8] 0x28[9] 0x04[10] 0x00[11] 0x0E[12] 0xFF[13] 0xFF[14]
(TX side)	
HCI_Reset	hcitool -i hci0 cmd 0x03 0x003
Tx_Test (2-DH5@2442MHz)	hcitool -i hci0 cmd 0x3F 0x051 0x66[15] 0x55[16] 0x44[17] 0x33[18] 0x22[19] 0x11[20] 0x01[21] 0x28[22] 0x04[23] 0x00[24] 0x0E[25] 0xFF[26] 0xFF[27] 0x09[28] 0x00[29] 0x00[30]

3.6 BLE Transmitter Test

The sequence of HCI commands to enable BLE transmission on the Bluetooth Controller:

1. HCI_Reset
2. HCI_LE_Transmitter_Test

   [v1]
   TX_Channel =

Value	Frequency
0x00	2402MHz
0x14	2442MHz
0x27[1]	2480MHz

   Test_Data_Length = 0x25[2], "37 bytes"
   Packet_Payload_Pattern = 0x00[3], "PRBS9"
3. To end the test, send HCI_Reset again.

Command Samples:

Command	Raw Bytes: *OpCode1 OpCode2 Length Parameter(s)*
HCI_Reset	0x03 0x0C 0x00
HCI_LE_Transmitter_Test [v1‡] (@2480MHz)	0x1E‡ 0x20 0x03 0x27[1] 0x25[2] 0x00[3]

Command	BlueZ Format: hcitool cmd *OGF OCF Parameter(s)*
HCI_Reset	hcitool -i hci0 cmd 0x03 0x003
HCI_LE_Transmitter_Test [v1‡] (@2480MHz)	hcitool -i hci0 cmd 0x08 0x01E‡ 0x27[1] 0x25[2] 0x00[3]

3.7 BLE Receiver Test

The sequence of HCI commands to enable BLE receiver on the Bluetooth Controller:

1. HCI_Reset
2. HCI_LE_Receiver_Test

   [v1]
   TX_Channel =

Value	Frequency
0x00	2402MHz
0x14	2442MHz
0x27[1]	2480MHz

3. To end the test, send HCI_LE_Test_End

Command Samples:

Command	Raw Bytes: *OpCode1 OpCode2 Length Parameter(s)*
HCI_Reset	0x03 0x0C 0x00
HCI_LE_Receiver_Test [v1‡] (@2480MHz)	0x1D‡ 0x20 0x01 0x27[1]
HCI_LE_Test_End	0x1F 0x20 0x00

Command	BlueZ Format: hcitool cmd *OGF OCF Parameter(s)*
HCI_Reset	hcitool -i hci0 cmd 0x03 0x003
HCI_LE_Receiver_Test [v1‡] (@2480MHz)	hcitool -i hci0 cmd 0x08 0x01D‡ 0x27[1]
HCI_LE_Test_End	hcitool -i hci0 cmd 0x08 0x01F

3.8 RSSI Test

The RSSI Test requires two Cypress Bluetooth devices (@DUT and @Peer) with a pre-established ACL connection. The sequence of HCI commands:

1. HCI_Reset @ both devices
2. HCI_Set_Event_Filter @ DUT device

   Filter_Type = 0x02[1], "Connection Setup"
   Filter_Condition_Type = 0x00[2], "Allow connections from all devices"
   Condition = 0x02[3], "Auto accept the connection w/o role switch"
3. HCI_Write_Scan_Enable @ DUT device

   Scan_Enable = 0x03[4], "Inquiry Scan enabled, Page Scan enabled"
4. HCI_Read_BD_ADDR @ DUT device

   Take a note of what *BD_ADDR* information returned by the Controller; for example, assume that we received 0x112233445566[10,9,8,7,6,5]
5. HCI_Create_Connection @ Peer device to establish a connection with DUT. Note: the BD_ADDR parameter should exactly match to DUT's device address which was retrieved at Step4.

   BD_ADDR = 0x112233445566[10,9,8,7,6,5], the remote (DUT) device address
   Packet_Type = 0xCC18[12,11], "DM1 | DH1 | DM3 | DH3 | DM5 | DH5"
   Page_Scan_Repetition_Mode = 0x01[13], "R1"
   Reserved = 0x00[14]
   Clock_Offset = 0x0000[16,15]
   Allow_Role_Switch = 0x00[17], "Master, no role switch during connection setup"
6. @ DUT device, note the Connection_Handle of new established link (reported from Controller); for example, assume that we got 0x000B[19,18]
7. HCI_Read_RSSI @ DUT device

   Connection_Handle = 0x000B[19,18], must use the Connection_Handle retrieved at Step6
8. (**Optional**) Instead, if desired, may issue Read_Raw_RSSI @ DUT device

   Connection_Handle = 0x000B[19,18], must use the Connection_Handle retrieved at Step6

Command Samples:

Command (DUT side)	Raw Bytes: *OpCode1 OpCode2 Length Parameter(s)*
HCI_Reset	0x03 0x0C 0x00
HCI_Set_Event_Filter	0x05 0x0C 0x03 0x02[1] 0x00[2] 0x02[3]
HCI_Write_Scan_Enable	0x1A 0x0C 0x01 0x03[4]
HCI_Read_BD_ADDR	0x09 0x10 0x00
… wait for connection establishment …	
HCI_Read_RSSI	0x05 0x14 0x02 0x0B[18] 0x00[19]
Read_Raw_RSSI	0x48 0xFC 0x02 0x0B[18] 0x00[19]
(Peer side)	

HCI_Reset	0x03 0x0C 0x00
HCI_Create_Connection	0x05 0x04 0x0D 0x66[10] 0x55[9] 0x44[8] 0x33[7] 0x22[6] 0x11[5] 0x18[11] 0xCC[12] 0x01[13] 0x00[14] 0x00[15] 0x00[16] 0x00[17]

Command (RX side)	BlueZ Format: hcitool cmd *OGF OCF Parameter(s)*
HCI_Reset	hcitool -i hci0 cmd 0x03 0x003
HCI_Set_Event_Filter	hcitool -i hci0 cmd 0x03 0x005 0x02[1] 0x00[2] 0x02[3]
HCI_Write_Scan_Enable	hcitool -i hci0 cmd 0x03 0x01A 0x03[4]
HCI_Read_BD_ADDR	hcitool -i hci0 cmd 0x04 0x009
… wait for connection establishment …	
HCI_Read_RSSI	hcitool -i hci0 cmd 0x05 0x005 0x0B[18] 0x00[19]
Read_Raw_RSSI	hcitool -i hci0 cmd 0x3F 0x048 0x0B[18] 0x00[19]
(TX side)	
HCI_Reset	hcitool -i hci0 cmd 0x03 0x003
HCI_Create_Connection	hcitool -i hci0 cmd 0x01 0x005 0x66[10] 0x55[9] 0x44[8] 0x33[7] 0x22[6] 0x11[5] 0x18[11] 0xCC[12] 0x01[13] 0x00[14] 0x00[15] 0x00[16] 0x00[17]