BT RF Test Commands for Linux

Revision History

Date	Version	Description	Author
2013/01/22	0.1	Initial revision	Terence Hsieh
2013/01/22	0.2	Fix BT Test Mode command	Terence Hsieh
2013/04/02	0.3	Update driver to fix bcm20710a1 initial issue	Terence Hsieh
2013/05/31	0.4	Add BLE command	Jay Wu
2013/06/14	0.5	Add BT Rx_Test command	Terence Hsieh
2017/7/18	0.6	Fix error in 2.2 and provide more explanation on bring up hci interface	Luke Chen
2018/8/15	0.7	Add LE enhanced TX/RX test command and remove unused 2045-tx command.	Luke Chen

1. Prerequisites:

Assume that you have bluetooth function enabled in normal mode here. If you are using bluez(hci interface is up), please skip this step1 and step2.

1) hciconfig, hcitool (Compiled out from BlueZ)
2) brcm_patchram_plus (Download from https://android.googlesource.com/platform/system/bluetooth/+/master/brcm_patchram_plus/brcm_patchram_plus.c)
3) bcmdhd.hcd (Provided by Ampak)

2. Enable BT function

1) echo 0 > /sys/class/rfkill/rfkill0/state // Bluetooth power OFF (depend on platform)
2) echo 1 > /sys/class/rfkill/rfkill0/state // Bluetooth power ON (depend on platform)
3) brcm_patchram_plus--enable_hci --no2bytes --tosleep 200000 --baudrate 115200 --patchram /system/etc/firmware/bcmdhd.hcd /dev/ttyS0 // please change patchram patch and uart port accordingly.
4) hciconfig hci0 up

2-1. BT Test Mode Command (Enable_Device_Under_Test_Mode):

1) hcitool cmd 0x03 0x0003
2) hcitool cmd 0x03 0x1a 0x03
3) hcitool cmd 0x03 0x05 0x02 0x00 0x02
4) hcitool cmd 0x06 0x03

2-2. BT Continuous Tx command (Tx_Test)

1) hcitool cmd 0x03 0x0003
2) hcitool cmd 0x3f 0x0051 55 44 33 22 11 00 00 00 04 01 04 10 27 09 00 00
   (A B C D E F G H I J)

C: Local_Device_BD_ADDR	Hex value
00:11:22:33:44:55	55 44 33 22 11 00

D: Hopping_Mode	Hex value
79 Channel	00
Single Frequency	01
Fixed pattern	02

E: Frequency	Hex value
0 - **78** (2402 - 2480)	**00** - **4E**

F: Modulation_Type	Hex value
00000000 bit pattern	01
11111111 bit pattern	02
01010101 bit pattern	03
11110000 bit pattern	09
PRBS9 pattern	04

G: Logical_Channel	Hex value
ACL EDR	00
ACL Basic	01
eSCO EDR	02
eSCO Basic	03
SCO Basic	04

H: BB_Packet_Type	Hex value
NULL	00
POLL	01
FHS	02
DM1	03
DH1/2-DH1	04
HV1	05
HV2/2-EV2	06
HV3/EV3/3-EV3	07
DV/3-DH1	08
AUX1/PS	09
DM3/2-DH3	0A
DH3/3-DH3	0B
EV4/2-EV5	0C
EV5/3-EV5	0D
DM5/2-DH5	0E
DH5/3-DH5	0F

I: BB_Packet_Length (The length of the payload in the Tx packets)	Hex value
10000	10 27 (0x2710)
20000	20 4E (0x4E20)
65535	FF FF (0xFFFF)

Example:

1) Packet Type :DH1, MAC:112233445566, Hopping ON,PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 00 00 04 01 04 10 27 09 00 00

2) Packet Type :2-DH1, MAC:112233445566, Hopping ON,PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 00 00 04 00 04 10 27 09 00 00

3) Packet Type :3-DH1, MAC:112233445566, Hopping ON,PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 00 00 04 00 08 10 27 09 00 00

4) Packet Type :DH3, MAC:112233445566, Hopping ON, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 00 00 04 01 0B 10 27 09 00 00

5) Packet Type :2-DH3, MAC:112233445566, Hopping ON, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 00 00 04 00 0A 10 27 09 00 00

6) Packet Type :3-DH3, MAC:112233445566, Hopping ON, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 00 00 04 00 0B 10 27 09 00 00

7) Packet Type :DH5, MAC:112233445566, Hopping ON, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 00 00 04 01 0F 10 27 09 00 00

8) Packet Type :2-DH5, MAC:112233445566, Hopping ON, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 00 00 04 00 0E 10 27 09 00 00

9) Packet Type :3-DH5, MAC:112233445566, Hopping ON, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 00 00 04 00 0F 10 27 09 00 00

10) Packet Type :DH1, MAC:112233445566,CH0,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 00 04 01 04 10 27 09 00 00

11) Packet Type :2-DH1, MAC:112233445566,CH0,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 00 04 00 04 10 27 09 00 00

12) Packet Type :3-DH1, MAC:112233445566,CH0,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 00 04 00 08 10 27 09 00 00

13) Packet Type :DH3, MAC:112233445566,CH0,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 00 04 01 0B 10 27 09 00 00

14) Packet Type :2-DH3, MAC:112233445566,CH0,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 00 04 00 0A 10 27 09 00 00

15) Packet Type :3-DH3, MAC:112233445566,CH0,Hopping OFF , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 00 04 00 0B 10 27 09 00 00

16) Packet Type :DH5, MAC:112233445566,CH0,Hopping OFF , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 00 04 01 0F 10 27 09 00 00

17) Packet Type :2-DH5, MAC:112233445566,CH0,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 00 04 00 0E 10 27 09 00 00

18) Packet Type :3-DH5, MAC:112233445566,CH0,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 00 04 00 0F 10 27 09 00 00

19) Packet Type :DH1, MAC:112233445566,CH39,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 27 04 01 04 10 27 09 00 00

20) Packet Type :2-DH1, MAC:112233445566,CH39,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 27 04 00 04 10 27 09 00 00

21) Packet Type :3-DH1, MAC:112233445566,CH39,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 27 04 00 08 10 27 09 00 00

22) Packet Type :DH3, MAC:112233445566,CH39,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 27 04 01 0B 10 27 09 00 00

23) Packet Type :2-DH3, MAC:112233445566,CH39,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 27 04 00 0A 10 27 09 00 00

24) Packet Type :3-DH3, MAC:112233445566,CH39,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 27 04 00 0B 10 27 09 00 00

25) Packet Type :DH5, MAC:112233445566,CH39,Hopping OFF, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 27 04 01 0F 10 27 09 00 00

26) Packet Type :2-DH5, MAC:112233445566,CH39, PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 27 04 00 0E 10 27 09 00 00

27) Packet Type :3-DH5, MAC:112233445566,CH39,Hopping OFF , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 27 04 00 0F 10 27 09 00 00

28) Packet Type :DH1, MAC:112233445566,CH78,Hopping OFF , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 4E 04 01 04 10 27 09 00 00

29) Packet Type :2-DH1, MAC:112233445566,CH78,Hopping OFF , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 4E 04 00 04 10 27 09 00 00

30) Packet Type :3-DH1, MAC:112233445566,CH78 , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 4E 04 00 08 10 27 09 00 00

31) Packet Type :DH3, MAC:112233445566,CH78,Hopping OFF , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 4E 04 01 0B 10 27 09 00 00

32) Packet Type :2-DH3, MAC:112233445566,CH78,Hopping OFF , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 4E 04 00 0A 10 27 09 00 00

33) Packet Type :3-DH3, MAC:112233445566,CH78,Hopping OFF , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 4E 04 00 0B 10 27 09 00 00

34) Packet Type :DH5, MAC:112233445566,CH78,Hopping OFF , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 4E 04 01 0F 10 27 09 00 00

35) Packet Type :2-DH5, MAC:112233445566,CH78,Hopping OFF , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 4E 04 00 0E 10 27 09 00 00

36) Packet Type :3-DH5, MAC:112233445566,CH78,Hopping OFF , PRBS9 mode, Packet length: 10000 = 0x2710,Power : Max

hcitool cmd 0x3f 0x0051 66 55 44 33 22 11 01 4E 04 00 0F 10 27 09 00 00

2-3. BT Rx Command (Rx_Test):

1) Select “Continuous Tx” from your equipment and start to transmit
2) hcitool cmd 0x03 0x0003
3) hcitool cmd 0x3f 0x0052 EE FF C0 88 00 00 E8 03 26 04 00 04 FF FF
   (A B C D E F G H I)
4) hcidump -x
5) You can find the HCI event from hcidump every “Report_Period” millisecond and the event format as below:
   1’st event:
   > HCI Event: Vendor (0xff) plen 33
   07 96 00 00 00 46 00 00 00 55 B6 00 00 F8 B5 00 00 00 00 00
   00 30 C6 38 01 D7 BF 38 01 59 06 00 00
   X1 Y1
   2’nd event:
   > HCI Event: Vendor (0xff) plen 33
   07 98 00 00 00 46 00 00 00 64 BC 00 00 07 BC 00 00 00 00 00
   00 C0 E8 3D 01 67 E2 3D 01 59 06 00 00
   X2 Y2
6) Calculate the BER
   BER = ((X2-X1) - (Y2-Y1)) / (X2 - X1)
   = (20834496-20497968)–(20832871-20496343)/(20834496-20497968)
   = (336528-336528)/336528
   = 0
7) The BER of BDR(1M) should be less than 0.001 and 0.0001 for EDR
8) If you want to stop testing, you should have to stop “Continuous Tx” from your equipment at first, or Rx_Test will be in wrong state at next time.

C: Local_Device_BD_ADDR	Hex value
00:00:88:C0:FF:EE	EE FF C0 88 00 00

D: Report_Period	Hex value
250	FA 00 (0x00FA)
1000	E8 03 (0x03E8)
2000	D0 07 (0x07D0)

E: Frequency	Hex value
0 - **78** (2402 - 2480)	**00** - **4E**

F: Modulation_Type	Hex value
00000000 bit pattern	01
11111111 bit pattern	02
01010101 bit pattern	03
11110000 bit pattern	09
PRBS9 pattern	04

G: Logical_Channel	Hex value
ACL EDR	00
ACL Basic	01
eSCO EDR	02
eSCO Basic	03
SCO Basic	04

H: BB_Packet_Type	Hex value
NULL	00
POLL	01
FHS	02
DM1	03
DH1/2-DH1	04
HV1	05
HV2/2-EV2	06
HV3/EV3/3-EV3	07
DV/3-DH1	08
AUX1/PS	09
DM3/2-DH3	0A
DH3/3-DH3	0B
EV4/2-EV5	0C
EV5/3-EV5	0D
DM5/2-DH5	0E
DH5/3-DH5	0F

I: BB_Packet_Length (The length of the payload in the Tx packets)	Hex value
10000	10 27 (0x2710)
20000	20 4E (0x4E20)
65535	FF FF (0xFFFF)

2-4. BT Rx Command (Write_Receive_Only):

1) hcitool cmd 0x03 0x0003
2) hcitool cmd 0x3f 0x002b 00
   (A B C)

C: Receive_Frequency_Encoded (Frequency)	Hex value
0 - 78 (24**02** - 24**80**)	**02** - **50**

Example:

1) Channel 0
   hcitool cmd 0x3f 0x002b 02
2) Channel 39
   hcitool cmd 0x3f 0x002b 29
3) Channel 78
   hcitool cmd 0x3f 0x002b 50

2-5. BLE Tx Command (LE_Transmitter_Test):

1) hcitool cmd 0x03 0x0003
2) hcitool cmd 0x08 0x001e **00 25 00**
(A B **C D E**)

C: Tx_channel	Hex value
0 - 39 (24**02** - 24**80**)	**00** - **27**

D: Length_of_Test_Data	Hex value
0 - 255	**00** - **FF**

E: Packet_payload	Hex value
Pseudo-Random bit sequence 9	00
Pattern of alternating bit '11110000'	01
Pattern of alternating bit '10101010'	02
Pseudo-Random bit sequence 15 – Optional	03
Pattern of All '1' bits – Optional	04
Pattern of All '0' bits – Optional	05
Pattern of alternating bits '00001111'	06
Pattern of alternating bits '01010101'	07

Example:

1) channel **10**, data length **37**, payload type **Pseudo-Random bit sequence 9**
hcitool cmd 0x08 0x001e **0A 25 00**
2) channel **25**, data length **37**, packet payload type **Pattern of All '1' bits**
hcitool cmd 0x08 0x001e **19 25 04**

2-6. BLE Rx Command (LE_ Receiver _Test):

1) hcitool cmd 0x03 0x0003
2) hcitool cmd 0x08 0x001d 01
(A B C)
3) Transmit 1000 packets from equipment
4) hcitool cmd 0x08 0x001f
> HCI Event 0x0e plen 6
01 1F 20 00 C0 03
5) Calculate PER
(1000 - 960) / 1000 = 40/1000 = 4%
where 0x03C0 is 960 in decimal.

C: Tx_channel	Hex value
0 - 39 (24**02** - 24**80**)	**00** - **27**

Example:

1) Channel **1**
hcitool cmd 0x08 0x001d **01**
2) Channel **39**
hcitool cmd 0x08 0x001d **27**

2-7. BLE Enhanced Tx Command (LE_Enhanced_Transmitter_Test_Command):

1) hcitool cmd 0x03 0x0003
2) hcitool cmd 0x08 0x0034 **00** **25** **00** **02**
(A B **C** **D** **E** F)

C: Tx_channel	Hex value
0 - 39 (24**02** - 24**80**)	**00** - **27**

D: Length_of_Test_Data	Hex value
0 - 255	**00** - **FF**

E: Packet_payload	Hex value
Pseudo-Random bit sequence 9	00
Pattern of alternating bit '11110000'	01
Pattern of alternating bit '10101010'	02
Pseudo-Random bit sequence 15 – Optional	03
Pattern of All '1' bits – Optional	04
Pattern of All '0' bits – Optional	05
Pattern of alternating bits '00001111'	06
Pattern of alternating bits '01010101'	07

F: PHY	Hex value
Reserved for future used	00
Transmitter set to use the LE 1M PHY	01
Transmitter set to use the LE 2M PHY	02
Transmitter set to use the LE Coded PHY with S=8 data coding	03
Transmitter set to use the LE Coded PHY with S=2 data coding	04

Example:

1) channel **10**, data length **37**, payload type **Pseudo-Random bit sequence 9**, Phy rate 1Mbps
hcitool cmd 0x08 0x0034 **0A** **25** **00** **01**
2) channel **10**, data length **37**, payload type **Pseudo-Random bit sequence 9**, Phy rate 2Mbps
hcitool cmd 0x08 0x0034 **0A** **25** **00** **02**

2-8. BLE Enhanced Rx Command (LE_Enhanced_Receiver _Test):

1) hcitool cmd 0x03 0x0003
2) hcitool cmd 0x08 0x0033 01 02 00
(A B C D E)
3) Transmit 1000 packets from equipment

4) hcitool cmd 0x08 0x001f
   > HCI Event 0x0e plen 6
   01 1F 20 00 C0 03
5) Calculate PER
   (1000 - 960) / 1000 = 40/1000 = 4%
   where 0x03C0 is 960 in decimal.

C: Tx_channel	Hex value
0 - 39 (24**02** - 24**80**)	**00** - **27**

D: PHY	Hex value
Reserved for future used	00
Transmitter set to use the LE 1M PHY	01
Transmitter set to use the LE 2M PHY	02
Transmitter set to use the LE Coded PHY	03

E: Modulation	Hex value
Assume transmitter will have a standard modulation index	00
Assume transmitter will have a standard mo dulation index	01

Example:

1) Channel **1,** 2M PHY, standard modulation.
   hcitool cmd 0x08 0x001d **01 02 00**