Communication Protocol Specification for Zigbee Ad Hoc Module

Chengdu Ebyte Electronic Technology Co., Ltd.

1. HEX transmitting Command format (AT HEX controlled via switch P1.6)

(AT HEX controlled via switch P1.6, when P1.6=0, it is HEX mode)

Command（COM）1Byte	length（LEN）1Byte	content（DATA）	End bit（END）1Byte
FE/FD	LEN	DATA	FF

Description COM：

Command	Description
FE	read
FD	configure

LEN：valid length of content(DATA)

END：FF is valid

Notes：

When UART access, return: F7 FF is wrong format

Coordinator starts network, notify: FF FF

When coordinator devices build a network, notify: FF FF

When devices access the network, notify: FF AA

When module devices offline or fail to access network, notify: FF 00

2. HEX read command description (see more in parameter description)

Command description	Command format	Command example
Read device type	Send：FE 01 01 FF Return：FB dev_type	Send：FE 01 01 FF Return：FB 02
Read network state	Send：FE 01 02 FF Return：FB nwk_state	Send：FE 01 02 FF Return：FB 01
Read network PAN_ID	Send：FE 01 03 FF Return：FB pan_id	Send：FE 01 03 FF Return：FB 02 F4
Read network key	Send：FE 01 04 FF Return：FB key	Send：FE 01 04 FF Return :FB 11 13 15 17 19 1B 1D 1F 10 12 14 16 18 1A 1C 1D
Read local short address	Send：FE 01 05 FF Return：FB ShortAddr	Send：FE 01 05 FF Return：FB F2 EF
Read local MAC address	Send：FE 01 06 FF Return：FB Mac_Addr	Send：FE 01 06 FF Return :FB 89 6C 50 09 00 4B 12 00
Read short address of father nodes	Send：FE 01 07 FF Return：FB Coor_shortAddr	Send：FE 01 07 FF Return：FB 00 00
Read short MAC address of father nodes	FE 01 08 FF Return：FB Coor _Mac_Addr	Send：FE 01 08 FF Return：FB 20 39 EA 0A 00 4B 12 00
Read network group number	Send：FE 01 09 FF Return：FB group	Send：FE 01 09 FF Return：FB 01

Command description	Command format	Command example
Read communication channel	Send：FE 01 0A FF Return：FB channel	Send：FE 01 0A FF Return：FB 0B
Read Send power	Send：FE 01 0B FF Return：FB txpower	Send：FE 01 0B FF Return：FB 04
Read UART baud rate	Send：FE 01 0C FF Return：FB baud	Send：FE 01 0C FF Return：FB 09
Read sleep state (valid for terminal nodes)	Send：FE 01 0D FF Return：FB sleep_time	Send：FE 01 0D FF Return：FB 05
Read data storage time of the node(valid for router and coordinator)	Send：FE 01 0E FF Return：FB 1E	Send：FE 01 0E FF Return：FB 1E
Read all device data	Send：FE 01 FE FF Return：FB all_info	Send：FE 01 FE FF Return：FB 02 01 02 F4 11 13 15 17 19 1B 1D 1F 10 12 14 16 18 1A 1C 1D F2 EF 89 6C 50 09 00 4B 12 00 00 00 20 39 EA 0A 00 4B 12 00 01 0B 04 09 05
Acquire short address of random MAC address in network	Send：FE 09 10 Mac_Addr FF Return：FB shortAddr	Send：FE 09 10 AF 99 E9 0A 00 4B 12 00 FF Return：FB 08 35
Read remote/local GPIO input and output state	Command：FE 04 20 addr gpiox FF Return：FB 20 addr In/Out	FE 04 20 F9 DE 04 FF
Read remote/local GPIO level	Command：FE 04 21 addr gpiox FF Return：FB 21 addr In/Out level	FE 04 21 FF FF 04 FF
Read remote/local PWM state	Command：FE 04 22 addr 22 FF Return：FB 22 addr period duty1 duty2 duty3 duty4 duty5	FE 04 22 FFFF 22 FF
Read remote/local ADC state	Command：FE 04 23 addr pin FF Return：FB 23 addr adc_value	FE 04 23 FF FF 01 FF

3. HEX configuration command description (see more in parameter description)

Command description	Command format	Command example
Configure device type	Send：FD 02 01 dev_type FF Return：FA 01	Send：FD 02 01 02 FF Return：FA 01
Configure PAN_ID	Send：FD 03 03 pan_id FF Return：FA 03	Send：FD 03 03 12 34 FF Return：FA 03
Configure network key	Send：FD 11 04 key FF Return：FA 04	Send：FD 11 04 11 13 15 17 19 1B 1D 1F 10 12 14 16 18 1A 1C 1D FF Return：FA 04
Configure network group number	Send：FD 02 09 group FF Return：FA 09	Send：FD 02 09 01 FF Return：FA 09
Configure communication channel	Send：FD 02 0A channel FF Return：FA 0A	Send：FD 02 0A 0B FF Return：FA 0A
Configure Send power	Send：FD 02 0B txpower FF Return：FA 0B	Send：FD 02 0B 04 FF Return：FA 0B
Configure UART baud rate	Send：FD 02 0C baud FF Return：FA 0C	Send：FD 02 0C 09 FF Return：FA 0C
Configure sleep mode (valid for terminal)	Send：FD 02 0D sleep_time FF Return：FA 0D	Send：FD 02 0D 05 FF Return：FA 0D
Configure data storage time of the node（valid for router and coordinator）	Send：FD 02 0E time FF Return：FA 0E	Send：FD 02 0E 07 FF Return：FA 0E
Configure remote/local GPIO input and output state	Command：FD 05 20 addr gpiox In/Out FF Return：FA 20 addr	Send：FD 05 20 FF FF 04 01 FF Return：FA 20 FFFF
Configure remote/local GPIO output level (valid for output mode)	Command：FD 05 21 addr gpiox level FF Return：FA 21 addr	Send：FD 05 21 FF FF 04 02 FF Return：FA 21 FFFF
Configure remote/local PWM state	Command：FD 0F 22 addr period duty1 duty2 duty3 duty4 duty5 FF Return：FA 22 addr	Send：FD 0F 22 FFFF FFFF 1FFF 3FFF 5FFF 7FFF 9FFF FF Return：FA 22 FFFF
Device restart	Send：FD 01 12 FF Return：FA 12	Send：FD 01 12 FF Return：FA 12
Recover factory configuration	Send：FD 01 13 FF Return：FA 13	Send：FD 01 13 FF Return：FA 13
Configure all information	Send：FD 2E FE all_info FF Return：FA FE	Send：FD 2E FE 02 01 02 F4 11 13 15 17 19 1B 1D 1F 10 12 14 16 18 1A 1C 1D F2 EF 89 6C 50 09 00 4B 12 00 00 00 20 39 EA 0A 00 4B 12 00 01 0B 04 09 05 FF Return：FA FE

4. HEX command parameter description

1. Device type dev_type : 00 coordinator
01 router
02 terminal (default)
2. Network state nwk_state : 00 no network
01 network exists
3. Network PAN_ID pan_id : 0000~FFFE fixed network PAN_ID
FFFF stochastic network PAN_ID
4. Network key key : 16 bits network key
5. Network short address shortAddr : 2 Byte address
6. MAC address Mac_Addr : 8 Byte address
7Short address of father nodes Coor_shortAddr : 2 Byte address
8. MAC address of father nodes Coor_Mac_Addr : : 8 Byte address
9. Network group number group : range from 1~99 (default 1)
10. Channel channel : range from 11~26 (default 11)
11. Power txpower table (default 0dBm) :

txpower	power (dBm)
00	-3
01	-1.5
02	0

txpower	power (dBm)
03	2.5
04	4.5
05	

12. Buad rate baud table (default 115200) :

baud	Baud rate
00	2400
01	4800
02	9600
03	14400
04	19200
05	38400
06	43000
07	57600

baud	Baud rate
08	76800
09	115200
0A	128000
0B	230400
0C	256000
0D	460800
0E	921600
0F	1000000

13. Sleep time sleep_time : 0 sleep mode closed (default)
Otherwise sleep mode open , sleep time is sleep_time, unit S

14. Storage time of father nodes time : range from 0~120 (default 30) , unit S

15. Gpio parameter

（1）gpio portal table

GPIO	P0_0	P0_1	P0_2	P0_3	P0_4	P0_5	P0_6	P2_0	P2_1	P2_2
HEX	00	01	02	03	04	05	06	07	08	09

（2）gpio input/output state

In/Out： 1 input state

0 output state

（3）gpio state value（ invalid for input state configuration）

level 0 low level

1 high level

2 switch

16. pwm parameter

（1）pwm portal table

pwmx	duty1	duty2	duty3	duty4	duty5
GPIO	P0_2	P0_3	P0_4	P0_5	P0_6

（2）period： period unit 62.5ns 0~0xffff

（3）dutyx： duty cycle unit 62.5ns 0~0xffff

17. adc parameter：

（1）adc state value

adc_state 0 ADC enabled

1 ADC closed

（2）adc sample value

adc_value 0~0XFFFF

18. Peripheral addr parameter description

Addr value

FFFF check/configure local information

0~FFF8 check/configure information with network address addr

FFFE FFFD FFFC check/configure information for all devices receiving broadcast

（FFFE：broadcast to all devices in network

FFFD：broadcast to devices receiving when free (except devices in sleep）

FFFC：broadcast to coordinator and router）

19. All information all_info

dev_type	(1 Byte (0))	device type
nwk_state	(1 Byte (1))	network state
pan_id	(2 Byte (2~3))	PAN_ID
key	(16 Byte (4~20))	network key
shortAddr	(2 Byte (21~22))	network short address
Mac_Addr	(8 Byte (23~30))	MAC address
Coor_shortAddr	(2 Byte (31~32))	Short address of father nodes
Coor_Mac_Addr	(8 Byte (33~40))	MAC address of father nodes
group	(1 Byte (41))	network group number
channel	(1 Byte (42))	communication channel
txpower	(1 Byte (43))	transmit power
baud	(1 Byte (44))	UART baud rate
sleep_time	(1 Byte (45))	sleep state

Detailed parameter for example :

all_info : 02 01 02 F4 11 13 15 17 19 1B 1D 1F 10 12 14 16 18 1A 1C 1D F2 EF 89 6C 50 09 00 4B 12 00 00 00 20 39 EA 0A 00 4B 12 00 01 0B 04 09 05

Device type :	02 (Terminal)
Network state :	01 (Network exists)
Network PANID :	02 F4 (PAN_ID=0X02F4)
Network key :	11 13 15 17 19 1B 1D 1F 10 12 14 16 18 1A 1C 1D
Short address of local network :	F2 EF (Short Address=0XF2EF)
Local MAC address :	89 6C 50 09 00 4B 12 00
Short address of father nodes :	00 00 (Short Address=0X0000)
MAC address of father nodes :	20 39 EA 0A 00 4B 12 00
Network group number :	01
Network channel :	0B (channel 11)
Transmit power :	04 (transmit power 4.5dBm)
Baud rate :	09 (baud rate 115200)
Sleep time :	05 (sleep mode starts , sleep time is 5s)

(Notes : Father node reserve time is not listed here, please use corresponding command for configuration and examination.)

5. HEX command data communication format

1. Command format description

Command（COM）1Byte	Data length（LEN）1Byte	Data content（DATA）
FC	LEN	DATA

2. DATA parameter description（data is content awaiting to send）

1）Broadcast data

Command：01+type+data

Parameter description：type

01：broadcast mode1 —broadcast the message to all devices in network

02：broadcast mode2 —broadcast the message to receiving devices(except ones in sleep mode)

03 : broadcast mode3 —broadcast the message to all functional devices （router and coordinator）

2）Multicast data

Command：02+ group+data

Parameter description：group

0~99：number for the multicasted message

3） Unicast data

Command：03+ type +addr+data

Parameter description： type

01：transparent transmission mode（no carry message）

02：short address mode（carry message is short address）

03：MAC address mode（carry message is MAC address）

Parameter description：addr: network short address valid unicast address 0x0000—0xFFF8）

6. AT command function table

（AT HEX controlled via switch P1.6，when P1.6=1, it is AT mode）

Command description	Command format	Return	Parameter description
read/configure device type(configure reset takes effect ）	AT+DEV=type	Configure:+OK Read:DEV=type	type: C coordinator R router E end device ? read
Read network state	AT+NWK=?	NWK=nwk_state	nwk_state: 0 no network 1 network already exists
Read /configure network PAN_ID（configure reset takes effect）	AT+PANID=panid	Configure:+OK Read:PANID=panid	panid: 0000-FFFF fixed PANID FFFF random PANID
Read /configure network key（configure reset takes effect）	AT+KEY=key	Configure:+OK Read:KEY=key	key: 16*1 Byte network key ? Read

Command description	Command format	Return	Parameter description
Read local network short address	AT+SHORT_ADDR=?	SHORT_ADDR=ShortAddr	ShortAddr: 0000-FFFF network short address
Read local MAC address	AT+MAC_ADDR=?	MAC_ADDR=MacAddr	MacAddr: 8*1Byte MAC length address
Read short address of father node	AT+COOR_ SHORT_ADDR=?	COOR_ SHORT_ADDR= ShortAddr	ShortAddr: 0000-FFFF network short address
Read MAC address of father node	AT+COOR_MAC_ADDR=?	COOR_MAC_ADDR=MacAddr	MacAddr: 8*1Byte MAC length address
Get random short address of MAC address	AT+GET_SHORT_ADDR= MacAddr	GET_SHORT_ADDR=ShortAddr	ShortAddr: 0000-FFFF network short address
Read/configure network group number	AT+GROUP=group	Configure +OK Read GROUP=group	group: 0-99 network group number ?Read
Read/Configure communication channel（configure reset takes effect）	AT+CH=ch	Configure +OK Read CH=ch	ch: 11-26 communication channel ? Read
Read/Configure transmitting power	AT+TXPOWER=txpower	Configure +OK Read TXPOWER=txpower	tpower: （see more in parameter power table） 0-4 transmitting power ? Read
Read/Configure UART baud rate	AT+UART=baud	Configure +OK Read UART=baud	baud: (see more in baud rate table) 0-15 baud rate ? Read
Read/Configure sleep mode	AT+SLEEP=sleep_time	Configure +OK Read SLEEP=sleep_time	sleep_time: （valid for end node） 0 close sleep mode 1-120 sleep time，unit:S ? Read
Read/Configure data storage time for the node （configure reset takes effect）	AT+DATA_TIME=data_time	Configure +OK Read DATA_TIME=data_time	sleep_time: （valid for router and coordinator） 0-120 data storage time，unit:S ? Read
Read software version	AT+SOFT_ID=?	SOFT_ID=soft_id	soft_id:Return current version
Device reset	AT+RESET	+OK	N/A
Restore factory setting	AT+RESTORE	+OK	
Configure GPIO input and output	AT+GPIO_PUT=addr,gpiox,inout	+OK	addr: 0000-FFF8 network short address

Command description	Command format	Return	Parameter description
Read GPIO input and output	AT+RGPIO_PUT=addr, gpiox	RGPIO=addr ,inout	FFFF local read gpiox: 0-9 GPIO portal number inout: 0 output state 1 input state level: 0 low level 1 high level 2 switch period: (period *62.5ns) 0~65535 PWM period， when it is 0, close all PWM channel，otherwise, all channels share one period dutyx(x=1~5): (dutyx *62.5ns) 0~65535 (x=2~5)when duty cycle for corresponding channel is 0 or below period，pwm close for current channel Notes: duty1(x=1) is regularly 50% duty cycle. When it is 0, close，not 0, enabled. adcx: 0~6 read ADC corresponding channel val: 0~3300 voltage unit mV
Configure GPIO level	AT+GPIO_LEVEL=addr, gpiox,level	+OK	
Read GPIO level	AT+RGPIO_LEVEL=addr,gpiox	GPIO_LEVEL=addr, inout,level	
Configure PWM state	AT+PWM=addr,period ,duty1, duty2,duty3,duty4,duty5	+OK	
Read PWM state	AT+RPWM= addr	RPWM=addr,period,duty1, duty2,duty3,duty4,duty5	
Read ADC state	AT+ADC=addr,adcx	ADC=addr,val	

Notes： When remotely control modules, controlled end will print the controlled message and master address from UART(serial port)

When UART accessing return: + ERROR is wrong format

Coordinator starts network, notify: start network success

Devices join network, notify: join network

Module devices offline or lose network, notify: no network