EBYTE

ZigBee 3.0 serial port commands

(ZigBee 3.0 series module in HEX mode)

成都亿佰特电子科技有限公司
Chengdu Ebyte Electronic Technology Co.,Ltd.

Contents

Disclaimer

EBYTE reserves all rights to this document and the information contained herein. Products, names, logos and designs described herein may in whole or in part be subject to intellectual property rights. Reproduction, use, modification or disclosure to third parties of this document or any part thereof without the express permission of EBYTE is strictly prohibited.

The information contained herein is provided “as is” and EBYTE assumes no liability for the use of the information. No warranty, either express or implied, is given, including but not limited, with respect to the accuracy, correctness, reliability and fitness for a particular purpose of the information. This document may be revised by EBYTE at any time. For most recent documents, visit www.ebyte.com.

1. Serial port format and mode configuration

1.1. Serial port setting mode and baud rate

- Baud rate: network manager 230400, data transmission module 115200
- Data bits: 8-bit mode
- Stop bit: 1-bit mode
- Check Digit: None
- flow control: none

1.2. Serial command format

The serial port of the ZigBee module is a full-duplex serial port. Because there is a large amount of data interaction in actual use, the serial port commands are in the format of command frames regardless of input or output, and have a mechanism to ensure the integrity of the command frame. The command sent by the host computer to the module Must have complete frame structure. At the same time, in the actual ZigBee networking environment, the messages received by the ZigBee module are random and unpredictable, so the serial port of the ZigBee module will have a high probability of random output (TX) messages.

1.2.1. Command frame structure

name	frame header	frame length	Payload
	SFD	LEN	payload
number of bytes	1	1	Variable length

Frame header: starts with 0x55 as the command

Frame length: The frame length is the frame payload length, and the maximum value is 255.

Payload: Payload is the valid data of the serial port frame (including validation). When the module receives the Payload bytes equal to the length of the frame, it receives a complete command frame

1.2.2. Frame timeout and frame interval:

When the module receives the command frame, it will start to receive the timing when any byte is received. The host computer needs to send a serial data stream with a complete frame structure starting with 0x55 to the module. The data flow cannot be interrupted, otherwise the module will receive a packet break error and return an error code of [55 , 03 , FF , FF , 00] . In addition, when the module returns command frames to the upper computer, if there are consecutive command frames returned, the interval between each command frame is greater than 200us.

1.2.3. Composition of serial port frame payload

Frame header SFD (1 byte)	Frame length LEN (1 byte)	Payload (Variable length 3~255 bytes)			
		Command type cmd type (1 byte)	Command code cmd code (1 byte)	Command data cmd Data (variable length 0~252 bytes)	Check code: check (1 byte)

The frame payload consists of 4 parts: "command type", "command code", "command data" and "check code", and each command contains these 4 units.

Command type:

According to the mode and working mechanism of the command, it is classified. The command type of input command and feedback command is from 0x00~0x7F, and the range of asynchronous command is 0x80~0xFF.

Command code:

The code corresponding to the command, the length is 1 byte, and each command has a unique command code.

Command data:

The additional parameters of the command execution, the minimum is 0 bytes, the maximum is 252 bytes

Check code:

The command payload includes the command type, command code, and all XOR8 checksums of the command data, with a length of 1 byte.

Frame payload size range:

Since each command includes the command type, command code and check code, the minimum frame payload is 4 bytes and the maximum is 255 bytes.

1.2.4. Three command modes

The ZigBee module has 3 command modes, namely input command, feedback command and asynchronous command.

Input the command:

The command frame input by the host computer to the module is a complete command frame when input.

Feedback command:

After the module receives the input command, the command is fed back to the upper computer, and each input command has a feedback command. In principle, it is necessary to continuously input a command to the module and then wait for the feedback command, but the module itself is fault-tolerant for two consecutive frames of commands that are glued together, so it may occur that multiple commands are input continuously and then multiple commands are continuously fed back. The waiting time of the feedback command is the execution time of the internal CPU of the module, which can be up to 10 seconds.

Asynchronous command:

The command sent by the module to the host computer at random. The command may have a certain causal relationship with the input command, or it may not be related. It is more of an uncertain factor, so the asynchronous command can be treated as a random event.

Feedback for invalid input command:

If an unsupported command is input to the module, an invalid command will be returned in the following format:

[0x55, 0x03, ' command type ' , 'command code' , 'checksum']

That is, the command type and command code are the same as the input command, but it does not contain any feedback of command data.

If the input command verification is not correct, the asynchronous command will be returned: 0x55 , 0x03 , 0xFF, 0xFE, 0x01

If the input command is broken or times out, the asynchronous command will be returned : 0x55, 0x03, 0xFF, 0xFF, 0x00

1.3. Command type and command code list

1.3.1. Command type list

command mode	Command type	Descriptor	command type name
input the command/ feedback command	0x00	TYPE_CFG	local configuration commands
	0x01	TYPE_ZDO_REQ	network management commands
	0x02	TYPE_ZCL_SEND	ZCL sends commands
asynchronous command	0x80 _	TYPE_NOTIFY	system notification command
	0x81	TYPE_ZDO_RSP	network management back
	0x8 2	TYPE_ZCL_IND	ZCL receives commands
	0x8F	TYPE_SEND_CNF	send confirmation

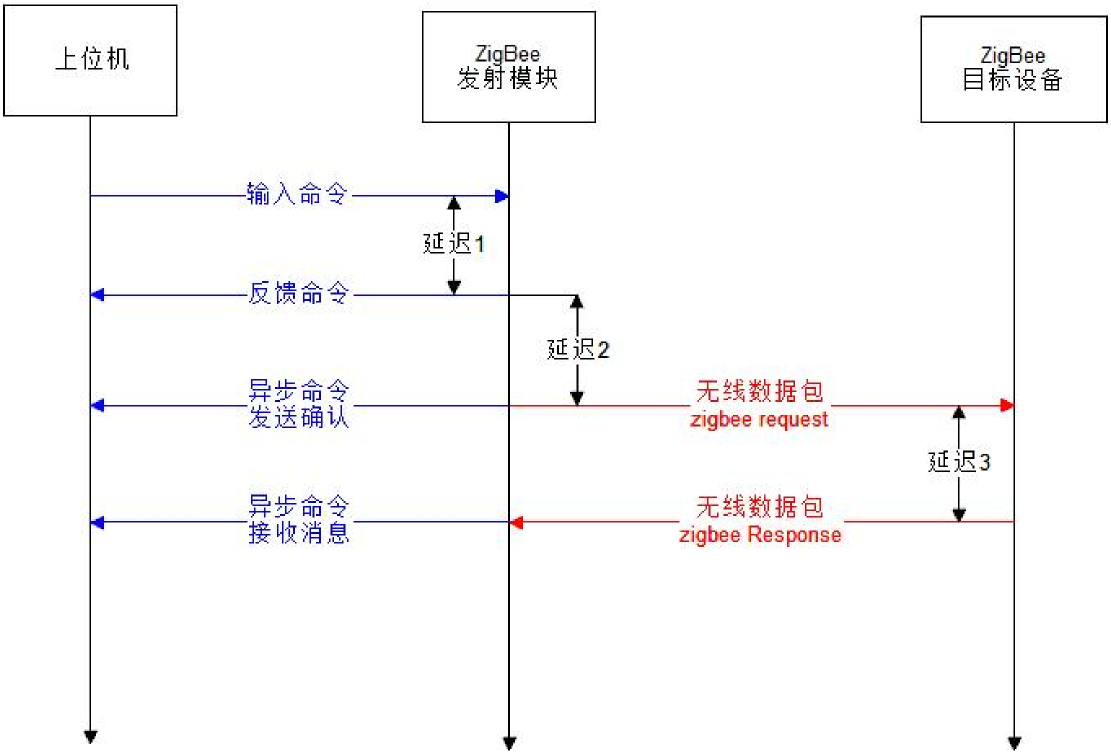
The causal relationship between input commands and asynchronous commands:

- asynchronous command TYPE_NOTIFY may have a causal relationship with the input command TYPE_CFG
- The asynchronous command TYPE_ZDO_RSP must be caused by the input command TYPE_ZDO_REQ, but the TYPE_ZDO_REQ command does not necessarily generate TYPE_ZDO_RSP
- asynchronous command TYPE_ZCL_IND is the message sent by the received device, which

may or may not be related to the input command TYPE_ZCL_SEND. If the parameter SeqNum in TYPE_ZCL_IND is equal to the SeqNum in TYPE_ZCL_SEND , it means that the asynchronous command is caused by the input command.

- every time a valid TYPE_ZDO_REQ command or TYPE_ZCL_SEND command is input, so TYPE_SEND_CNF can be used for task blocking or buffer release, especially useful when sending to multiple targets at the same time.
- input commands TYPE_ZDO_REQ and TYPE_ZCL_SEND are both wireless transmission commands. The wireless transmission itself has the possibility of delay and disorder, and the result is reflected in the corresponding asynchronous command.

Serial command flow of wireless communication



Delay 1: In this stage, the input command of the host computer needs to be preprocessed in the MCU of the module (encryption and cache query), and the average time is 2~5 milliseconds. Among them, E72-2G4M20S1E has the fastest response, and the measured average is about 1.5ms.

Delay 2: The delay is determined by the degree of channel congestion and network scale. In the on-demand mode, when the target is a non-sleeping device, it can be 1ms~50ms, and when the target is a dormant device, it can be as long as more than 7 seconds. In broadcast or multicast mode, it is about 5~10ms for E72-2G4M20S1E and E18 series, and 1 second for E180ZG120.

Delay 3: The delay is determined by the target device at the receiving end, the fastest is less than 1 second, and the slowest can be more than 10 seconds. If there is a command that the other device cannot support, there may be no return, that is, the delay time will be extended to ∞ seconds.

1.3.2. Commonly used input command list

Local configuration commands

command code	Descriptor	command name
0x00	CFG_STATUS	Query the current status of the module
0x01	CFG_START	Module boot/soft start
0x 02	CFG_OPEN_NET	Open network/start networking
0x03	CFG_CLOSE_NET	Turn off network/stop networking
0x0 4	CFG_RESET	reset/factory reset
0x05	CFG_NODE_TYPE	Set the native node type
0x06	CFG_CHANNEL	Query and set channel
0x07	CFG_GET_PANID	Query PANID
0x08	CFG_SET_PANID	set PANID
0x09	CFG_VIEW_GROUP	View local add group
0x0A	CFG_ADD_GROUP	Add the machine to the group
0x0 B	CFG_REMOVE_GROUP	This machine withdraws from the group
Commands only supported by the data transmission module		
0x10	CFG_READ_ATTR	Read local property parameters
0x11	CFG_WRITE_ATTR	Set local property parameters
0x12	CFG_GET_BIND	View frequently connected destinations
0x13	CFG_SET_BIND	Set the always-connected destination
0x14	CFG_FIND_BIND	Auto always connect
~~0x15~~	~~CFG_POLL~~	~~End node wakes up to receive once~~
0x16	CFG_AT_MODE	enter AT mode
Commands only supported by Network Manager		
0x20	CFG_GET_UTC	Get current UTC time
0x21	CFG_SET_UTC	set UTC time
0x2 2	CFG_GET_ADDRTAB	Read node address table
0x23	CFG _GET_KEYTAB	Read node keytab
0x28	CFG_EZ_MODE	Retransmit device information

Network management commands

command code	Descriptor	command name
0x 00	ZDO_ NWK_ADDR_REQ	Query node short address

0x01	ZDO_IEEE_ADDR_REQ	Query node IEEE address
0x02	ZDO_NODE_DESC_REQ	Query node network configuration information
0x04	ZDO_SIMPLE_DESC_REQ _ _	Query node port information
0x05	ZDO_ACTIVE_EP_REQ	Query the number of node ports
0x21	ZDO_BIND_REQ	Set node constant connection binding
0x22	ZDO_UN BIND_REQ	Cancel node constant connection binding
0x33	ZDO_MGMT_BIND_REQ	View Node Always Connect Bindings
0x34	ZDO_MGMT_LEAVE_REQ	delete node

Send ZCL commands

command code	Descriptor	command name
0x 00	ZCL_READ_ATTR_REQ	Read device property parameters
0x01	ZCL_WRTIE_ATTR_REQ	Modify device property parameters
0x02	ZCL_READ_REPORT_REQ _	Query device attribute reporting rules
0x03	ZCL_WRITE_REPORT_REQ _	Modifying device attribute reporting rules
0x04	ZCL_DISC_ATTR_REQ	View all properties of the device
0x05	ZCL_DISC_ATTR_EX _REQ	View all properties (with extensions)
0x06	ZCL_DISC_CMD_REC_REQ	View device receiving control commands
0x07	ZCL_DISC_CMD_GEN_REQ	View the control commands sent by the device
0x0F	ZCL_CMD	send control commands

System notification commands

command code	Descriptor	command name
0x00	NOTIFY_BOOT	device startup
0x01	NOTIFY_NET_STATUS _ _	network status change
0x02	NOTIFY_NET_OPEN	Turn on and off network

		notifications
0x03 _	NOTIFY_NODE_JOIN	Detected that the module is connected to the network
0x04	NOTIFY_NODE_ADDR	Module short address update
0x05	NOTIFY _DEVICE_JOIN	Device access information
0x06	NOTIFY _LEAVE	Module off-grid notification
0x10	NOTIFY_FIND_BIND	Always Connect Notification
0x11	NOTI FY_IDENTIFY	mark mode

Network management back

command code	Descriptor	command name
0x 00	ZDO_ NWK_ADDR_RSP	Query node short address
0x01	ZDO_IEEE_ADDR_RSP	Query node IEEE address
0x02	ZDO_NODE_DESC_RSP	Query node network configuration information
0x04	ZDO_SIMPLE_DESC_RSP	Query node endpoint information
0x05	ZDO_ACTIVE_EP_RSP _	Query the number of node endpoints
0x21	ZDO_BIND_RSP	Set the node to always connect
0x22	ZDO_UN BIND_RSP	Cancel a node's constant connection
0x33	ZDO_MGMT_BIND_RSP	View Node Frequently Connected
0x36	ZDO_MGMT_LEAVE_RSP	delete node return

Receive ZCL commands

command code	Descriptor	command name
0x 00	ZCL_READ_ATTR_RSP _	read device properties return
0x01	ZCL_WRTIE_ATTR_RSP _	Modify device properties to return
0x02	ZCL_READ_REPORT_RSP _	Query device attribute reporting rules and return
0x03	ZCL_WRITE_REPORT_RSP _	Modify the reporting rule of device properties and return
0x04	ZCL_DISC_ATTR_RSP	View all properties of the device Return
0x05	ZCL_DISC_ATTR_EX_RSP _	View all properties of the device returned (with extensions)
0x06	ZCL_DISC_CMD_REC_RSP _	View the return of the control command received by the device
0x07	ZCL_DISC_CMD_GEN_RSP	View the return of the control command sent by the device

0x0A	ZCL_REPORT_IND	Receive active report of device attributes
0x0B	ZCL_DEFAULT_RSP	The system returns the frame by default
0x0F	ZCL_CMD_IND	received control command

Send confirmation command list and send status table

command code	Descriptor	command name
0x 0 1	ZDO_SEND_CNF	Network management command sending confirmation
0x02	ZCL_SEND_CNF	ZCL sends confirmation

Wireless sending status table	
status value	status description
0x00	Successful operation
0x01	operation failed
0x02	Parameter error
The following are the error codes for TI platforms (E72 and E18 series)	
0x10	memory error
0x11	memory full
0x12	mode not supported
0xc2	the command is invalid
0xcd	target device does not exist
0xb7	The target device did not receive the message (only when APS ACK is turned on)
0xe1	channel interference
0xe9	No MAC ACK received
0xf0	Send timeout due to device sleeping
0xf1	The send queue is full
The following is the error code of Sila bs (E180-ZG120 series)	
0x03	lookup table not found
0x18	Not enough cache
0x66	Failed to send data

1.4. Common addressing format and big endian format in ZigBee protocol

In ZigBee applications, it is usually necessary to specify to send a control or message to a specific peripheral or sensor on a node, or to receive a message from a peripheral or sensor on a node, so the ZigBee protocol specification needs to use the following The addressing mode facilitates precise management and control of devices in the network.

In the serial port command in HEX format, all input and output addressing format data are in little endian mode .

1.4.1. IEEE address (8 bytes):

The IEEE address is the MAC address. The IEEE address of the ZigBee node is present when it leaves the factory. It is an 8-byte address and is globally unique.

1.4.2. PANID (2 bytes):

ZigBee coordinator creates a network, it will generate a 2-byte PANID. After the node joins the network generated by the coordinator, it obtains the same PANID as the coordinator and works on the same channel as the coordinator.

1.4.3. Short address (2 bytes)

After the ZigBee device joins the network, it will obtain a 2-byte short address. Since ZigBee is a Mesh network, data transmission in the ZigBee network needs to communicate according to the short address to obtain the correct routing and forwarding path. In the same network, an IEEE address corresponds to a short address.

1.4.4. Port:

Multiple ports can exist on a ZigBee device, which is equivalent to a virtual device. For example, a common multi-hole socket, multiple switches, only one ZigBee chip is used on a device, but multiple virtual devices are implemented by supporting multiple endpoints. Among them, the port numbers for device control are valid from 1 to 240. The three special port packetization is port 0 (ZDO port) for network management, port 242 (GP port) for Green Power protocol conversion, and 255. Ports (broadcast ports) are used to control all ports at the same time, such as turning on all switches on a multiplexer at the same time.

1.4.5. Virtual device SN number:

The virtual device SN number is a device management mechanism proposed by Ebyte based on the ZigBee protocol specification for the convenience of device management.

Each ZigBee device has an 8-byte IEEE address, and the port number of each virtual device is fixed on the device firmware, so the IEEE address + port number can be used as the SN number of the virtual device. In little endian mode, the virtual SN number format is "port number" + "IEEE address (little endian mode)")

The SN number can be used in the device's "Bind" setting to specify the source virtual device and the target virtual device. The target of the constant connection binding can also be a group, so when the target of the constant connection is a group, the port is 0xFF, the 0th and 1st of the IEEE address is the group ID, and the rest are 0xFFFF

Device virtual SN number									
	The port number	IEEE[0]	IEEE[1]	IEEE[2]	IEEE[3]	IEEE[4]	IEEE[5]	IEEE[6]	IEEE[7]
equipment	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX
grouping	0xFF	0xXX	0xXX	0xFF	0xFF	0xFF	0xFF	0xFF	0xFF

- The port number of the virtual SN is 0x01~0xF0, indicating that the target is a real virtual device
- The virtual SN port is 0xFF, indicating that the target is a packet
- When the target is a group, IEEE [0] and IEEE[1] represent the group ID

2. Local command parsing

2.1. local configuration commands

Uniform format for local configuration commands:

field	frame header	frame size	Payload			check code
			Command types	command code	Command data	
content	55		00	Please see below	Please see below	
number of bytes	1	1	1	1	variable-length	1

2.1.1. Query the current status of the module (command code 0x00)

Command code: 0x00

Function:

This command is used to query the status and parameters of the module, including the MAC address of the module, whether it is networked; what is the channel, PANID, and short address; what is the key;

input the command:

Field	command code	command data
content	0x00	NULL
number of bytes	1	0

Parameters: none

Feedback command:

Field	command code	cmd data							
content	0x00	network status	Equipment type	MAC address	channel	PANID	short address	Extended PANID	network key
number of bytes	1	1	1	8	1	2	2	8	16

Network status: 0 – networked, 0xFF – not networked

Device Type: 0 - Coordinator, 1 - Router, 2 - End Node

MAC address: The module's MAC address, fixed at the factory, unique in the world

Channel: The current channel of the module, not available when not networked
PANID: The current PANID of the module, not available when not networked
Short address: the current short address of the module, which is not available when the network is not connected
Extended PANID: None when not networked
Network key: no 0 when not networked

2.1.2. Module boot/soft start (command code 0x01)

Command code: 0x01
Note: **Only E72-2G4M20S1E supports**
Function:

After the module is powered on, it is in a standby state, and no asynchronous commands will be issued in the standby state to prevent the host computer from receiving a large amount of data during the power-on and startup process.

input the command:

Field	command code	command data
content	0x01	AutoStart
number of bytes	1	1

Auto start: set to 1 to start automatically after the next power-on, set to 0 to disable automatic start.

Feedback command:

Field	command code	command data
content	0x01	state
number of bytes	1	1

Status: 0 – Boot successful 0xFF – Boot invalid

2.1.3. Start network configuration (command code 0x02)

Command code: 0x02
Function:

When the coordinator executes this command, the permission to access the network will be enabled, and within 180 seconds, routers and terminal nodes that are also in the configuration network state will be allowed to access the network. If the coordinator is in the factory without network state, executing this command will create a new network at the same time, and generate a new PANID, channel, network key, and extended PANID.

Routes and endpoints will try to join a network created by a coordinator when this command is executed. The coordinator must also be in the network configuration mode to successfully join the network.

There will be delays when the coordinator creates a network, and routes and terminal nodes join the network. The final result is obtained in " Network Status Change " of "System

Notification Command". Execute this command after the route is connected to the network, which can prolong the time allowed by the coordinator to connect to the network.

E72-2G4M20S1E(Link72) module V1.4 added the whitelist network distribution mode. In this mode, the coordinator blocks the devices whose MAC addresses are not in the whitelist and allows the devices in the whitelist to access the network.

input the command:

Field	command code	command data
content	0x02	Distribution network mode (optional)
number of bytes	1	1

Distribution network mode:

0 Default mode, direct distribution network (default mode when the command does not include distribution network mode).

1 Coordinator enables whitelist provisioning.

Feedback command:

Field	command code	command data
content	0x02	state
number of bytes	1	1

Status: 0 – operation is valid, 0xFF – operation is invalid. This command is valid only after soft start

2.1.4. Stop network configuration (command code 0x03)

Command code: 0x03

Function:

The coordinator in the network configuration mode executes this command to prevent new devices from joining the coordinator.

Executing this command on routes and terminal nodes that have not yet joined the network has no effect. Executing this command on routes and terminal nodes that have just joined the network can also make the coordinator prevent new devices from joining.

input the command:

Field	command code	command data
content	0x03	NULL
number of bytes	1	0

Feedback command:

Field	command code	command data
content	0x03	state
number of bytes	1	0

Status: 0 – operation is valid, 0xFF – operation is invalid.

2.1.5. Reset/factory reset (0x04)

Command code: 0x04

Function:

Module reset, exit the network or restore factory settings. When restoring the factory, the parameters set by the module are all restored to their default values.

input the command:

Field	command code	command data		
content	0x04	Reset mode	PAN ID	channel
number of bytes	1	1	2	1

Reset mode: 0 - Module reset; 1-module denetwork; 2 -- The module is factory restored

PANID: The current PANID of the module. When reset, it is sufficient to fill in 0xFFFF. If you need to exit the network or restore the factory when the network has been established, fill in the current PANID of the module.

Channel: THE current channel of the module, fill in 0 when reset, need to withdraw from the network or need to restore the factory when the network has been established, fill in the current channel of the module.

Feedback command:

Field	command code	command data
content	0x04	state
number of bytes	1	0

Status: 0 – operation is valid, 0xFF – operation is invalid.

2.1.6. Set node type (command code 0x05)

Command code: 0x05

Note: Only E180ZG120 and E18 series support

Function:

Set the module as coordinator, route or endpoint (sleeping or non-sleeping). This setting needs to be set before the device is networked, and can be set in standby mode.

input the command:

Field	command code	command data
content	0x05	Device Type
number of bytes	1	1

Device Type: 0 - Coordinator, 1 - Route, 2 - End Node, 3 - Sleeping End Node

Feedback command:

Field	command code	command data
content	0x05	state
number of bytes	1	1

Status: 0 – operation is valid, 0xFF – operation is invalid.

2.1.7. Query and set channel (command code 0x06)

Command code: 0x06

Note: Only E72-2G4M20S1E and E 18 series support

Function:

The channel to enable or disable the module needs to be set before creating a network or networking, and can be set in standby mode. The module supports 7 preferred channels by default (11, 14, 15, 19, 20, 24, 25). This command can enable or disable multiple preferred channels, and the feedback command carries the enabled channels.

input the command:

Field	command code	command data	
content	0x06	Settings	Channel list
number of bytes	1	1	variable-length N

Settings: 0 – disable channel, 1 – enable channel, 2 – override channel (list cannot be 0)

Channel: Set the list of disabled or enabled channels, valid from 11 to 26.

Feedback command:

Field	command code	command data	
content	0x06	Status	Channel list
number of bytes	1	1	variable-length N

Status: 0 - setting valid, 0xFF - setting invalid

Channel list: the current module enabled channel list, maximum 16 bytes

2.1.8. Query PANID (command code 0x07)

Command code: 0x07

Note: Only E72-2G4M20S1E and E 18 series support

Function:

Set the PANID used for the module networking, the default is 0xFFFF for random mode. Setting the PANID needs to be done before the coordinator establishes the network or the node joins the network. Can be set in standby mode.

input the command:

Field	command code	command data
content	0x07	null
number of	1	0

bytes		

Parameters: none

Feedback command:

Field	command code	command data	
content	0x07	Status	PAN ID
number of bytes	1	1	2

Status: 0 – Query is valid, 1 – Query is invalid

PAN ID: Module PANID, the default value is 0xFFFF

2.1.9. Set PANID (command code 0x08)

Command code: 0x08

Note: Only E72-2G4M20S1E and E 18 series support

Function:

The module establishes a network in coordinator mode, or joins a network in routing and terminal node mode, and sets a specified PANID. This operation needs to be performed before establishing a network or joining a network, and can be performed in standby mode.

input the command:

Field	command code	command data
content	0x08	PAN ID
number of bytes	1	2

PANID : Default PANID value

Feedback command:

Field	command code	command data
content	0x08	Status
number of bytes	1	1

Status: 0 – setting valid, 1 – setting invalid

2.1.10. View module add group (command code 0x09)

Command code: 0x09

Function:

View the group that the module has joined. The operation of adding a group can be performed locally or remotely.

input the command:

Field	command code	command data
content	0x09	Port index
number of bytes	1	1

Port index: the serial number (not port number) of the endpoint of the corresponding module, the default transparent port is 0, 1 is reserved for the second serial port, and 2 and 3 are reserved for PWM, GPIO and ADC.

Feedback command:

Field	command code	command data		
content	0x09	Status	Number of added groups	Add group list
number of bytes	1	1	1	2*N

Status: 0 – Query is valid with follow-up data, 0xFF - Query is invalid

Number of added groups: the total number of groups added to this port on the module

Add group list: add group list of this port on the module

2.1.11. Module group adding(command code 0x0A)

Command code: 0x0A

Function:

Add a port on a specified module to a group

input the command:

Field	command code	command data	
content	0x0A	Port index	Group ID
number of bytes	1	1	2

Port index: the serial number of the endpoint of the corresponding module (not the port number)

Group ID: The group the mod will join

Feedback command:

Field	command code	command data
content	0x0A	Status
number of bytes	1	1

Status: 0 – operation is valid, 0xFF – operation is invalid.

2.1.12. Module ungroup (command code 0x0B)

Command code: 0x0B

Function:

A port on the specified module exits the specified group

input the command:

Field	command code	command data	
content	0x0B	Port index	Group ID

number of bytes	1	1	2

Port index: the serial number of the endpoint of the corresponding module (not the port number)
Group ID: The group the mod will exit from

Feedback command:

Field	command code	command data
content	0x0B	Status
number of bytes	1	1

Status: 0 - the operation is valid, 1 - the module port is no longer in the group, 0xFF - the operation is invalid.

2.1.13. Channel scan test (command code 0x0C)

Command code: 0x0C

Note: Only E72-2G4M20S1E supports

Function: Scan the ZigBee channel beacon to determine whether other ZigBee networks exist, and can assist the coordinator to set the channel before the coordinator starts the network. Scan results are viewed in the Beacon Scan Notification .

input the command:

Field	command code	command data		
content	0x0C	Channel list	Listening time	scan mode
number of bytes	1	4	1	1

Channel list: 32-bit channel enable bitmap list, 11-channel corresponding value is 0x00000800, and so on.
Listening time: The listening time of each channel, the time is calculated as (2^Duration)*15.36 milliseconds.
scan mode: 0 - beacon scan mode, 1- Reserve other 2.4G signal detection modes.

Feedback command:

Field	command code	command data
content	0x0C	Status
number of bytes	1	0

Status: 0 – operation is valid, 0xFF – operation is invalid.

2.1.14. Set and query the current transmit power (command code 0x0D)

Command code: 0x0D
Function: Query or set the transmit power of the module
input the command:

Field	command code	command data

content	0x0D	Mode	power
number of bytes	1	1	1

Mode: 0 - query current power, 1 - set power

power: set

Setting range:

E72-2G4M20S1E setting range (0x0E~0x14)

E18 series low power version setting range (0x00~0x05)

E18 series high power version setting range (0x00~0x14)

Feedback command:

Field	command code	command data	
content	0x0D	Status	power
number of bytes	1	1	1

Status: 0 – operation is valid, 0xFF – operation is invalid.

Power: The current power read.

2.1.15. Read local properties (command code 0x10)

Command code: 0x10

Note: E180ZG120 and E18 series support

Function:

Read the ZCL status parameters on the module

input the command:

Field	command code	command data	
content	0x10	Port index	Parameter ID
number of bytes	1	1	2

Port index: the port index number of the module, the default is 0

Parameter ID: data transmission related attribute ID, see " Ebyte Custom Attributes "

Feedback command:

Field	command code	command data	
content	0x10	Execution status	Data
number of bytes	1	1	N

Execution status: 0 – execution is valid, other – execution is invalid

Data: parameter value

2.1.16. set local attribute (command code 0x11)

Command code: 0x11

Note: E180ZG120 and E18 series support

Function:

Set the ZCL state parameters of the module

input the command:

Field	Command code	Command data		
Content	0x11	Port index	Parameter ID	Parameter data
Number of bytes	1	1	2	N

Port index: the port index number of the module, the default is 0

Parameter ID: data transmission related attribute ID, see " Ebyte Custom Attributes "

Parameter data: data of the modified parameter

Feedback command:

Field	command code	command data	
content	0x11	Execution status	Port Index
number of bytes	1	1	1

Execution status: 0 – execution is valid, other – execution is invalid

Port Index: The port index number of the module

2.1.17. Auto bind target (command code 0x14)

Command code: 0x14

Note: E180ZG120 and E18 series support

Function:

The local data transmission module and other data transmission modules automatically establish a data transparent transmission relationship. The E180ZG120 module can be bound to other data transmission modules (including E180ZG120 and E18 series) and can also be automatically bound to ZigBee lighting equipment.

input the command:

Field	command code	command data
content	0x14	null
number of bytes	1	0

Feedback command:

Field	command code	command data
content	0x14	Execution Status
number of bytes	1	1

Execution Status: 0 – Execution is valid, 0xFF – Execution is invalid

2.1.18. Enter AT command mode (command code 0x16)

Command code: 0x16

Note: Only E 180ZG120B supports

Function:

Enter AT command control mode. This command will cause the transmission mode in " Ebyte Custom Properties " to become "true".

input the command:

Field	command code	command data
content	0x16	null
number of bytes	1	0

Feedback command:

Field	command code	command data
content	0x16	Execution Status
number of bytes	1	1

Execution Status: 0 – Execution valid, 0xFF – Execution invalid

2.1.19. Get the current UTC time (command code 0x20)

Command code: 0x20

Note: Only E72-2G4M20S1E supports

Function:

Query the current UTC time of the coordinator

input the command:

Field	command code	command data
content	0x20	null
number of bytes	1	0

Parameters: none

Feedback command:

Field	command code	command data	
content	0x20	Execution status	UTC time
number of bytes	1	1	4

Execution Status: 0 – Execution is valid, 0xFF – Execution is invalid

UTC time : Coordinator's UTC32 time

2.1.20. Set UTC time (command code 0x21)

Command code: 0x21

Note: Only E72-2G4M20S1E supports

Function:

Set the UTC time of the coordinator to enable the coordinator to provide UTC services to

ZigBee devices

input the command:

Field	command code	command data
content	0x21	UTC time
number of bytes	1	4

UTC time: the UTC time that needs to be set

Feedback command:

Field	command code	command data
content	0x21	Execution Status
number of bytes	1	1

Execution Status: 0 – Execution is valid, 0xFF – Execution is invalid

2.1.21. Read the network access node address table (command code 0x22)

Command code: 0x22

Remarks: E72-2G4M20S1E and E 180ZG120B support

Function:

Query the MAC addresses and short addresses of the connected nodes, one by one, there are 255 entries for E72-2G4M20S1E and 80 entries for E180-ZG120B. It should be noted that on the E180-ZG120B, the table does not support power-down storage. It is recommended that the host computer read this table and save it in the host computer.

input the command:

Field	command code	command data	
content	0x22	Address number	Query mode
number of bytes	1	2	1

Address number: query the address number saved by the coordinator, 0x0000~0x00FE are valid

Query mode: 0 - normal query, 1 - query with flag bit (only supported by E72 manager)

Feedback command:

Field	command code	command data				
content	0x22	Status	Address number	Node short address	Node MAC address	Flag bit
number of bytes	1	1	2	2	8	1

Status: 0 – with access node, 2 – no access node, 0xFF - out of storage range

Address number: Stored address number

Node short address: the short address of the incoming node

Node MAC address: the MAC address of the network access node

Flag bit: greater than or equal to 8 is a legal device that has undergone the first network access authentication, less than 8 suspicious devices (only supported by the E72 manager)

2.1.22. Read access node key (0x23)

Command code: 0x23

Remarks: E72-2G4M20S1E and E 180ZG120B support

Function:

There is a problem with this function, and it will be improved in the next upgrade.

2.1.23. Retransmit device information notification (command code 0x28)

Command code: 0x28

Note: E72-2G4M20S1E (LINK72) supports this instruction, and the firmware of E180-ZG120 series modules upgraded to V1.2 can also support this instruction.

Function:

The " Device Information Notification " (see " Device Information Notification ") will only be available when the node accesses the network for the first time. If you miss this message, you can re-apply for the device to report it again, and it is valid only when the node is in normal operation.

input the command:

Field	command code	command data
content	0x28	Node MAC address
number of bytes	1	8

Node MAC address: The MAC address of the node that needs to be retransmitted

Feedback command:

Field	command code	command data
content	0x28	Execution status
number of bytes	1	1

Execution status: 0 - The operation is valid. Wait until the device uploads. 0xFF - The query fails and the device may not exist. (If E180-ZG120 is used as the coordinator, try one or two times (try again at an interval of 3 to 6 seconds). It may be successful.)

2.1.24. Set module PWM output duty cycle (command code 0x18)

Command code: 0x18

Note: only supported by E180ZG120B module, do not use this function in sleep terminal mode

Function:

Set the duty cycle of the 3-way PWM output of the E180ZG120 module, ranging from 0 to 255.

input the command:

Field	command code	command data	
content	0x18	PWM number	Value
number of bytes	1	1	1

PWM number: 0 - PWM on port 2, 1 - PWM on port 3, 2 - PWM on port 4.

Value: 0~255 is valid, each gear corresponds to 1/255.

Feedback command:

Field	command code	command data
content	0x18	Execution status
number of bytes	1	1

Execution status: 0 – operation is valid, 0xFF – operation is invalid

2.1.25. Module PWM marking mode (command code 0x19)

Command code: 0x19

Note: only supported by E180ZG120B module, do not use this function in sleep terminal mode

Function:

E180ZG120 module enters the Identify mode, which can only last for a maximum of 255 seconds. After entering the Identify mode, this PWM flashes with a cycle of 1 second, and can be found and bound by the automatically bound device.

input the command:

Field	command code	command data	
content	0x19	PWM number	Duration
number of bytes	1	1	1

PWM number: 0 - PWM on port 2, 1 - PWM on port 3, 2 - PWM on port 4.

Duration: The duration for which the port enters Identify mode

Feedback command:

Field	command code	command data
content	0x19	Execution status
number of bytes	1	1

Execution status: 0 – operation is valid, 0xFF – operation is invalid

2.1.26. Adding a whitelist record (0x29)

Command code: 0x29

Remarks:

Only E72-2G4M20S1E(Link72) module V1.4 firmware is supported. Older firmware can be upgraded to this version free of charge

Function:

In network configuration mode, the coordinator filters the MAC addresses of networked nodes. Only those that match the whitelist can be added. You can add a whitelist only when the whitelist distribution network is enabled. After the network distribution mode ends, all the added whitelists are cleared. You need to add them again when the whitelist distribution network is enabled next time.

Enter the command:

Field	command code	command data
content	0x29	Whitelist record
number of bytes	1	8

Whitelist record: indicates the MAC address of the node that needs to be added

Feedback command:

Field	command code	command data
content	0x29	Execution status
number of bytes	1	1

Execution status: 0 - Add succeeded, 0xFF - Add failed

2.1.27. Lock Extended PANID Networking (0x1A)

Command code: 0x1A

Remarks:

Only the V1.2 E180-ZG120 supports this function. The E180ZG120 joins the specified network in route node or terminal node mode by locking the coordinator's extended PANID in 64bit. The E180ZG120 module with the extended PANID locked will automatically continue to connect to the network until it is successfully added to the network.

Function:

This command allows you to view and set the locked extended PANID. If the command is set to the extended PANID of a coordinator in routing and terminal node mode, a module can only be added to this coordinator. If this value is set to all 0, the extended PANID lock is cancelled.

Enter the command:

Field	command code	command data	
content	0x1A	Mode	Extended PANID
number of bytes	1	1	8

Mode: 0 - Queries the locked extension PANID. 1- Sets the extension PANID

Extended PANID: 8 Byte Extended PANID. This parameter is valid in set mode

Feedback command:

Field	command code	command data	
content	0x1A	Execution status	Extended PANID

number of bytes	1	1	8

Execution status: 0 - Valid, 0xFF - invalid

Current Extended PANID: indicates the current lock PANID. If all zeros are used, the panid is not locked. This field is displayed only in query mode.

2.2. system notification command

The uniform format of system notification commands is shown in this table:

field	frame header	frame size	Payload			
			Command types	command code	Command data	check code
content	55		0x80	Please see below	Please see below	
number of bytes	1	1	1	1	variable-length	1

2.2.1. Device startup (command code 0x00)

Command code: 0x00

Function:

The notification message when the module is powered on, including the MAC address of the module

Asynchronous command:

Field	Command code	Command data		
Content	0x00	Reset mode	Version	MAC Address
Number of bytes	1	1	1	8

Reset mode: It is determined by the chip type, and the reset mode of different chips is different .

Version: The software version of the mod

MAC Address: The MAC address of the module

2.2.2. Network status change (command code 0x01)

Command: 0x01

Function:

This asynchronous command will be generated when the module networking is successful, but the module networking fails.

Asynchronous command:

Field	command code	cmd data						
content	0x01	Network	MAC	Channel	PANID	Short	Extended	Network

		Status	address			address	PANID	key
number of bytes	1	1	8	1	2	2	2	8

Network Status: 0 – not networked, 1 – networked, 2 – network configuration mode

MAC address: The module's MAC address, fixed at the factory, unique in the world

Channel: the current channel of the module, 0 when the networking fails

PANID: The current PANID of the module, 0xFFFF when the networking fails

Short address: the current short address of the module, 0xFFFE when the networking fails

Extended PANID: All 0s when networking fails

Network key: all 0s when networking fails

2.2.3. Allow network access time window notification (command code 0x02)

Command code: 0x02

Function:

After the coordinator starts to configure the network, the asynchronous command notifies the window time for allowing network access. If a new device joins the network, the new device may increase the coordinator's window time. In addition, the routers and terminals that have already entered the network can also use the coordinator's network configuration command to increase the window time for the coordinator to open the network, but if the coordinator's network is closed, the routes and terminals cannot be opened. This command is also issued when the coordinator shuts down the network and the window time becomes 0.

Asynchronous command:

Field	command code	command data
content	0x02	Window time
number of bytes	1	1

Window time: the window time for the coordinator network to open, when it is 0, it means to close the network.

2.2.4. Detect node access to the network (command code 0x03)

Command code: 0x03

Remarks: E72-2G4M20S1E and E 180ZG120 support

Function:

When a module or node is detected to be connected or re-connected to the network, the End Device switches to the parent node, and the router re-synchronizes, all of which will lead to re-connection to the network.

Asynchronous command:

Field	command code	cmd data			
content	0x03	MAC address	Short address	Parent node address	Network access mode
number of bytes	1	8	2	2	1

MAC address: The MAC address of the network access device
Short address: the short address of the network access device
Parent node address: the parent node address of the network access device, the parent node address is required to kick off the End Device
Network access mode: 0 – first access to the network, 1 – re-entry, 2 – re-entry and re-synchronize the key (the manager reserves the key replacement function)

2.2.5. Node short address notification (command code 0x04)

Command code: 0x04
Function:

When a module or node is connected to the network, it reports the MAC address or short address to the coordinator, and when the short address changes during operation, this command will be used as a notification. After receiving the command, the host computer should update the mapping relationship between the MAC address and the short address in time.

Asynchronous command:

Field	Command code	Command data		
Content	0x04	MAC address	short address	Node Type
Number of bytes	1	8	2	1

MAC address: The MAC address of the target node
short address: the short address of the target node
Node Type: 1 - Route, 2 - Do Not Sleep End Node, 3 - Sleep End Node

2.2.6. Device information notification (command code 0x05)

Command code: 0x05

Note: E72-2G4M20S1E all support, E180-ZG120 series upgrade V1.2 firmware support and E18 series upgrade V1.4 firmware support this command (E18 series V1.4 firmware must use the "Retransmit device information notification" to get this message, the other two modules can automatically get this message when the node is connected to the network, You can also use "Retransmit Device Information Notification" to obtain this message. E180-ZG120 series modules may lose this message if there are more than 12 nodes in the distribution network within 5 seconds.)

Function:

When the node accesses the network for the first time, it automatically obtains the peripheral information on the node, including the device ID information and the cluster information supported by each port.

Asynchronous command:

Field	command code	cmd data							
content	0x05	Termination flag	DevSN	Short address	Port number	Port profile	Device ID	Input cluster table	Output cluster table

number of bytes	1	1	9	2	1	2	1	variable-length	variable-length

The format of the cluster list is as follows:

Field	command code		command data	
content	Input cluster table		Output cluster table	
	quantity	list	quantity	list
number of bytes	1	2*N	1	2*N

Termination flag: A single node will carry multiple ports when it enters the network. The flag is 1 to indicate that the port reporting of the node ends.

DevSN: device virtual SN number, see " Virtual SN "

Short address: device short address

Port number: the port number of the device, see " Port "

Port profile: profile ID, the application layer only needs to pay attention to 0x0104, see " Port Profile "

Device ID: Indicates the function of the device, which is determined by the ZCL protocol specification, see the table " Device ID Table ".

Input cluster table: The input clusters supported by the device, including the number of clusters and the cluster list, see " Cluster " and " Server and Client ".

Output cluster table: The output clusters supported by the device, including the number of clusters and the list of clusters, see " Clusters " and " Server and Client ".

2.2.7. Module off-grid notification (command code 0x06)

Command code: 0x06

Note: E72-2G4M20S1E and E180ZG120 support

Function:

When the device is actively disconnected from the network, the coordinator will receive this message, and the device may send multiple packets of this message each time it is disconnected from the network. If the device is not in the coverage of the coordinator when it is actively disconnected from the network, the coordinator cannot receive the message, but the data transmission module can be disconnected from the network normally.

Asynchronous command:

Field	command code	command data
content	0x06	MAC Address
number of bytes	1	8

MAC Address: The MAC address of the off-grid device

2.2.8. Automatic binding target result notification (command code 0x10)

Command code: 0x10

Remarks: E18 and E180ZG120 support

Function:

The target result found when the target is automatically bound, the target is the target of data transparent transmission and AT command control (E180ZG120).

Asynchronous command:

Field	Command code	Command data		
Content	0x10	target short address	target port	Cluster ID
Number of bytes	1	2	1	2

target short address: the target short address found

target port: find the target port

Cluster ID: The cluster ID for establishing the connection. This field is only supported by E180ZG120. The value is 0xFC08 to establish transparent transmission. 0x0006 and 0x0008 establish AT command control of lighting equipment.

2.2.9. Beacon scan notification (command code 0x0C)

Command code: 0x0C

Note: Only E72-2G4M20S1E supports

Function:

" Channel Scanning Test ", multiple beacons will be returned in beacon scan mode. Both the coordinator and the router will generate beacons. According to the number of beacons, you can roughly know how many coordinator routers are in the space, which channels are distributed, what are their PANIDs and short addresses, and how strong the signal strength is. A termination signal command will be generated after the scan is over.

Asynchronous command:

Field	command code	cmd data					
content	0x0C	Scan status	Channel	PANID	Short address	Extended PANID	Signal strength
number of bytes	1	1	2	2	2	8	1

Scan status: 0-scan to valid beacon, 0xFF-scan end

Channel: Scan to the channel to which the beacon belongs, 0xFF indicates the end of the scan

PANID: Scan to the PANID to which the beacon belongs, 0xFFFF indicates the end of the scan

Short address: scan to the short address of the beacon, 0xFFFE means the end of the scan

Extended PANID: The extended PANID of the scanned beacon, there is no such information at the end of the scan

Signal strength: The LQI signal strength of the scanned beacon, 255 is the strongest, 0 is the weakest, and the closer the distance, the stronger.

2.2.10. System background debugging messages (command code 0x0F)

Command code: 0x0F

Note: Only E72-2G4M20S1E supports

Function:

Background debug messages output when the coordinator is running

Asynchronous command:

Field	Command code	Command data	
Content	0x0F	Debug code	debug data
Number of bytes	1	2	variable-length

Debug code: There are only three kinds of debug codes output in the background.

debug data: debug data output in the background

Three debug messages:

① **failed to get the total number of ports automatically:**

Debug code: 0x0001

Debug data format and content:

Field	Command code	Command data	
		Debug code	debug data
Content	0x0F	0x01,0x00	MAC addres
Number of bytes	1	2	8

describe:

When a new node is connected to the network, the coordinator will automatically obtain the number of ports of the connected node. When the number of ports fails to be obtained, it will output the MAC address of the node. However, the coordinator has a retransmission mechanism to obtain the port number of the access node. It does not matter even if there is one failure. Only if there are three consecutive access failures, it is possible that the node access to the network is invalid (it may be immediately exit the network after access).

② the **automatic acquisition of port information fails:**

Debug code: 0x0002

Debug data format and content:

Field	Command code	Command data		
		Debug code	debug data	
Content	0x0F	0x02,0x00	MAC addres	port number
Number of bytes	1	2	8	1

describe:

When a new node is connected to the network, the coordinator will automatically obtain the information of each port of the connected node (port profile , device ID , cluster table), and when it fails to obtain the port information, it will output the MAC address and port number of the port. However, the coordinator has a retransmission mechanism to obtain the port information of the access node. It does not matter if there is a failure. Only if there are three consecutive access failures, the node may fail (may be immediately exit the network after accessing the network).

③ **automatically bind notifications**

Debug code: 0x0003

Debug data format and content:

Field	Command code	Command data			
		Debug code	debug data		
Content	0x0F	0x03,0x00	MAC addres	The port number	binding cluster
Number of bytes	1	2	8	1	

describe:

When a new node joins the network, the coordinator will automatically instruct the port of the joining node to bind the coordinator. Then the key attributes under the bound cluster on the port of the network access node can be automatically reported to the coordinator for use as device state change notification and heartbeat packets. Ports that are automatically bound must support the following input clusters :

Cluster ID	cluster name
0x0006	switch on-off cluster
0x0008	Level Control Cluster
0x0101	lock control cluster
0x0102	Shade Control Cluster
0x0300	RGB Control Cluster
0x0400	Light Sensing Cluster
0x0402	temperature sensor cluster
0x0500	Security Alarm Cluster

2.2.11. Whitelist interception Notification (Command code 0x07)

Command code: 0x07

Note: Only the E72-2G4M20S1E(Link72) V1.4 firmware is supported

Function:

E72-2G4M20S1E(Link72) (V1.4 firmware) When the whitelist network distribution mode is enabled, the whitelist is not detected. Procedure This parameter can be used together with Adding a Whitelist Record (2.1.26) to add a whitelist after an intercept is detected. However, network configuration fails for the access node. If the access node fails to configure the network, it needs to try again immediately.

Asynchronous command:

Field	Command code	Command data
Content	0x07	MAC address
Number of bytes	1	8

MAC address: indicates the MAC address that is intercepted

3. Network management commands (ZDO commands)

3.1. Introduction to ZDO Commands

ZDO is the abbreviation of ZigBee Device Object, which is used for networking management of ZigBee devices. Has the following characteristics

- ZDO uses port 0 and the port profile of 0x0000 , as a special port, each ZigBee device must have a ZDO port to complete the interaction of ZDO commands.
- ZDO commands all use short addresses for communication. Most ZDO commands have two forms of Request and Response, that is, a "one question and one answer" method is used for communication and interaction.
- The ZDO command can be used to query the MAC address and short address of the network access device, especially some ZigBee devices will have short address change errors in complex network environments, which can be remedied by the ZDO command.
- Through the ZDO command, the coordinator can query all ports of the networked device and the port profile , device ID , and supported clusters of the port , so as to determine what functions the networked device has.
- The coordinator can set the constant connection binding of the network access node through the ZDO command, and can perform three basic operations of setting, canceling and viewing the binding relationship of each port on each node.

3.2. Unified header format for ZDO commands

The network management command sends the input command, the first time the feedback command is received, the second time the asynchronous command "send confirmation" is received, and the third time the asynchronous command "network management return" is received. Each time a command is received, it determines whether the next command will be received.

3.2.1. input command format

Input command format of network management commands

Field	Frame header	Frame size	Payload				
			Command type	command code	Command data		check code
Content	0x55	Need to calculate	0x01	See Table 3.1	Short address	Command parameters	Need to calculate
Number of bytes	1	1	1	1	2	variable-length	1

Short address: The short address of the control target, little endian mode

Command parameters: Different command parameters are different, and the parameters of different commands are analyzed later

Table 3.1 ZDO command Table	
command code	Command function
0x00	Query the node short address
0x01	Query the node MAC address

0x02	Query node network configuration information
0x04	Query node port information
0x05	Query the number of node ports
0x21	Set the node frequent connection binding
0x22	Remove node frequent connection bindings
0x33	View node frequent connection bindings
0x34	Removing nodes
0x31	Look at the network links

3.2.2. Feedback command format

Feedback command format for network management commands

Field	Frame header	Frame size	Payload				
			Command type	command code	Command data		check code
Content	0x55	0x05	0x01	See Table 3.1	executing state	Command number	Need to calculate
Number of bytes	1	1	1	1	1	1	1

Execution status: 0 – the execution is valid, and a confirmation of transmission will be generated, other values – see " Wireless Transmission Status Table "

Command number: the number assigned by the system to the command, which can be traced back to the corresponding input command in the sending confirmation and the network management command return.

3.2.3. Send confirmation format

Asynchronous Command "Send Confirmation" Format for Network Management Commands

Field	Frame header	Frame size	Payload					
			Command type	command code	Command data			check code
Content	0x55	0x07	0x8F	0x01	Short address	Command number	Sending result	Need to calculate
Number of bytes	1	1	1	1	2	1	1	1

Short address : The short address of the sending target

Command number: the number assigned by the system to the command

Sending result: wireless sending result, see " Wireless Sending Status Table "

3.2.4. Receive network management response commands

Asynchronous Response Command Format for Network Management Commands

Field	Frame header	Frame size	Payload						
			Command type	command code	Command data				check code
Content	0x55	Need to calculate	0x81	See Table 3.1	Short address	Command number	Sending result	Command parameter	Need to calculate
Number of bytes	1	1	1	1	2	1	1	variable-length	1

Short address: The short address of the device that responds to the command

Command number: consistent with the system allocation when sending, the sender will return what the receiver generates

Execution result: For the execution result of the command at the receiving end , please refer to the "Execution Result Status Table" below.

Command parameter: This parameter is valid only when the execution result is 0.

Execution result status table

Numerical value	significance
0x00	The operation is successful and effective
0x80	Invalid request operation
0x81	device not found
0x82	Invalid port number (query node port information)
0x83	The port cannot be queried (query node port information)
0x84	This command does not support
0x85	Operation timed out
0x86	Binding matching failed (set constant connection)
0x88	The binding relationship does not exist (cancel the constant connection)
0x8C	Insufficient space (set constant connection)

3.2.5. Instructions for sending and receiving commands

The network management command is sent by the host computer to the data transmission module or networking manager. The function of the feedback command only indicates whether the command is entered correctly and whether the module is in a state that can send messages. Send acknowledgment indicates whether the message was sent, or even to the target (not lost halfway). The received response command is the result of the counterpart device executing the command.

3.3. Network management command parsing

Network management command parsing only parses the command parameter part of the input command and network management command response

3.3.1. Query node short address (command code 0x00)

Command code: 0x00

Function:

Query the short address of the target node according to the IEEE address. The short address input in this command needs to use the 0xFFFD broadcast address.

Enter the command:

Field	Command code	Command data	
		Short address	Command parameter
Content	0x00	0xFD,0xFF	MAC addres
Number of bytes	1	2	8

MAC address: the MAC address of the queried node

Response command:

Field	Command code	Command data			
Content	0x00	Short address	Command number	result of enforcement	Command parameter
					MAC addres
Number of bytes	1	2	1	1	8

MAC address: the MAC address of the queried node, the short address of the queried node is in the command header

3.3.2. Query node MAC address (command code 0x01)

Command code: 0x01

Function:

Query the MAC address of the target node based on the short address

input the command:

Field	Command code	Command data	
Content	0x01	Short address	Command parameter
			NULL
Number of bytes	1	2	0

Command parameters: none

Response command:

Field	Command code	Command data			
Content	0x01	Short address	Command number	result of enforcement	Command parameter
					MAC addres
Number of bytes	1	2	1	1	8

MAC address: the MAC address of the queried node

3.3.3. Query node network configuration information (command code 0x02)

Command code: 0x02

Note: Only E72-2G4M20S1E supports

Function:

Query the network configuration information of a node

input the command:

Field	Command code	Command data	
Content	0x02	Short address	Command parameter
			NULL
Number of bytes	1	2	0

Command parameters: none

Response command:

Field	Command code	Frame size	Command data								
Content	0x02	Short address	Command number	result of enforcement	Command parameter						
					Logical type	band limits	ZigBee version	Manufacturer code	Maximum command length	Maximum reception	Maximum send
Number of bytes	1	2	1	1	1	1	1	2	1	2	2

Logic Type: 0 - Coordinator, 1 - Route, 2 - End Node, 3 - Low Power Node

Frequency Band: Bitmap of the working frequency band of the node, bit 1 - 800MHz, bit4 - 900MHz, bit8 - 2.4GHz

ZigBee version: Convert to decimal, if greater than or equal to 21, it conforms to ZigBee 3.0

Vendor code: node vendor code, which can be used for clusters of private protocols

Maximum command length: the maximum length of network management commands supported by the peer device network

Maximum reception: The counterpart device supports the maximum data reception length

Maximum sending: The counterpart device supports the maximum sending data length

3.3.4. Query node port information (command code 0x04)

Command code: 0x04

Function:

Query the details of the specified port on the node.

input the command:

Field	Command code	Command data	
Content	0x04	Short address	Command parameter
			port number
Number of bytes	1	2	1

port number: the port number of the target device

Field	Command code	Command data										
Content	0x04	Short address	Command number	result of enforcement	Command parameter							
					The port number	Port profile	Device ID	Device version	input cluster table		output cluster table	
									Quantity N1	list	Quantity N2	list
Number of bytes	1	2	1	1	1	2	2	1	1	2*N1	1	2*N2

Response command:

Port number: the port number of the device, see " Port "

Port profile: profile ID, the application layer only needs to pay attention to 0x0104, see " Port Profile "

Device ID: Indicates the function of the device, which is determined by the ZCL protocol specification, see the table " Device ID Table ".

Device Version: The version of the device

Input cluster table: The input clusters supported by the device, including the number of clusters and the cluster list, see " Cluster " and " Server and Client ".

Output cluster table: The output clusters supported by the device, including the number of clusters and the list of clusters, see " Clusters " and " Server and Client ".

3.3.5. Query the number of node ports (command code 0x05)

Command code: 0x05

Function:

To query all ports supported by the node, see the description of " Ports ".

input the command:

Field	Command code	Command data	
Content	0x05	Short address	Command parameter
			Null
Number of bytes	1	2	0

Command parameters: none

Response command:

Field	Command code	Command data				
Content	0x05	Short address	Command number	result of enforcement	Command parameter	
					Number of ports N	Port list
Number of bytes	1	2	1	1	1	N

Number of ports : the number of ports of the queried node

Port list: the port list of the queried node

3.3.6. Set node constant connection binding (command code 0x21)

Command code: 0x21

Remarks: E72-2G4M20S1E and E 180ZG120B support

Function:

Using the ZigBee Bind method, the ports on the two nodes are set to be always connected and bound. The nodes remember each other through the MAC address plus the port number, and connect one of their own ports to the other port's port for a permanent connection. The two ports that establish the binding relationship can be on the same node, but the two ports must form the relationship between the controller and the executor, see " Server and Client ". Since the constant connection binding needs to remember the MAC address and port number of the other party and use its own port to bind the other party, the concept of virtual SN is added when managing the binding, see " Virtual SN ".

input the command:

Field	Command code	Command data			
Content	0x21	Short address	Command parameter		
			Source virtual SN	Cluster ID	target virtual SN
Number of bytes	1	2	9	2	9

Source virtual SN: The SN number of the source virtual device that is often connected, see " Virtual SN ". The source virtual SN cannot be a packet and must correspond to an actual device.
Cluster ID: The cluster ID used for frequent connection communication, see " Cluster (cluster) "
Target virtual SN: The virtual SN number of the target device, see " Virtual SN ". The target can be a group. If the target SN is filled with 0x00, it is the coordinator itself. This setting will cause the set object to transmit the data to the coordinator.

Response command:

Field	Command code	Command data			
Content	0x21	Short address	Command number	result of enforcement	Command parameter
					Null
Number of bytes	1	2	1	1	0

Parameters: None, directly judge the result from the "execution result" in the unified header

3.3.7. Unbind the node's constant connection (command code 0x22)

Command code: 0x22

Remarks: E72-2G4M20S1E and E 180ZG120B support

Function:

To release the existing constant connection binding, the target node must save the binding record to have the meaning of unbinding

input the command:

Field	Command code	Command data			
Content	0x22	Short address	Command parameter		
			Source virtual SN	Cluster ID	target virtual SN
Number of bytes	1	2	9	2	9

Source virtual SN: Because of the constant connection binding, it is necessary to remember the MAC address and sum of the counterparty, see " Virtual SN ".
Cluster ID: Cluster ID for constant connection communication
Target virtual SN: The virtual SN number of the target device, see " Virtual SN ". The target can be a group. If the target SN is filled with 0x00, it is the coordinator itself. This setting will cause the set object to transmit the data to the coordinator.

Response command:

Field	Command code	Command data			
Content	0x22	Short address	Command number	result of enforcement	Command parameter
					Null
Number of bytes	1	2	1	1	0

Parameters: None, directly judge the result from the "execution result" in the unified header

3.3.8. View node constant connection binding (command code 0x33)

Command code: 0x33

Remarks: E72-2G4M20S1E and E 180ZG120B support

Function:

View existing FC bindings, and output all FC bindings in a one-by-one list.

input the command:

Field	Command code	Command data	
Content	0x33	Short address	Command parameter
			start index
Number of bytes	1	2	1

Start index: query the starting number of the frequently connected record, and can return multiple records in response. Multiple queries can check all the frequently connected relationships on a node.

Response command:

Field	Command code	Command data			
Content	0x33	Short	Command	result of	Command parameter

		address	number	enforcement	Total number of records	Start Index	Number of records returned	Frequent connection record(struct)
Number of bytes	1	2	1	1	1	1	1	20*N

Frequently connected record (struct) parsing： Frequently connected record ={Source virtual SN[9 bytes],Cluster ID[2 bytes],target SN[9 bytes]}*N

Content	Frequent connection record(struct)		
	Source virtual SN	Cluster ID	target SN
Number of bytes	9	2	9

Total number of records: The total number of constant connections established on the node
Start Index: The start number of the current returned record
Number of records returned: the number of records currently returned
Source virtual SN: the virtual SN number that initiates binding to the source port on the node
Cluster ID: The cluster ID for which the binding is established
Target SN: The virtual SN number of the binding target, which can be a single device port or a group

3.3.9. delete node (command code 0x34)

Command code: 0x34

Function:

Delete specified node based on MAC address

Precautions:

If the deleted node is a terminal node or a dormant terminal node (the " Node Type " item in "Module Short Address Notification (Command Code 0x04)" is 2 or 3), the terminal node needs to be entered in the "Short Address" field of the command header address of the parent node. The parent node can be obtained after receiving the "detection node access network (command code 0x03)", including the parent node switching during the operation of the terminal node. Because the parent node of the terminal node has a large variable during the operation, the ZigBee module (including the coordinator mode module) is not responsible for recording the parent node of each node. To ensure the correct deletion of the node, the host computer must make a record.

For the terminal node of the newer version of ZigBee 3.0 R22, you can also directly fill in its own short address in the "short address" field.

input the command:

Field	Command code	Command data			
Content	0x34	Short address	Command parameter		
			MAC	Re-entry	delete child

			address	network	node
Number of bytes	1	2	8	1	1

MAC address: The MAC address of the node to be deleted
Re-entry network: fill in 0 by default
Delete child node: fill in 0 by default

Response command:

Field	Command code	Command data			
Content	0x34	Short address	Command number	result of enforcement	Command parameter
					Null
Number of bytes	1	2	1	1	0

Parameters: None, directly judge the result from the "execution result" in the unified header

3.3.10. View network link (0x31)

Command code: 0x31

Note: E72-2G4M20S1E only supports

Function:

View the link relationship table of a node, and use this function to obtain the entire network topology.

input the command:

Field	Command code	Command data	
Content	0x31	Short address	Command parameter
			start index
Number of bytes	1	2	1

Start index: Query the start number of the frequently connected record. When returning, multiple records can be returned. Multiple queries can complete all link relationships on a node.

Response command:

Field	Command code	Command data			
Content	0x31	Short	Command	result of	Command parameter

		address	number	enforcement	Total number of records	Start Index	Number of records returned	Link record (struct)
Number of bytes	1	2	1	1	1	1	1	14*N

Link record (struct)： Link record ={Short address[2byte], MAC address[8byte],Node type[1byte]，Node relationship[1byte]， Network Depth[1byte]， Signal strength[1byte]} * N

Content	*Link record (struct)					
	Short address	MAC address	Node type	Node relationship	Network Depth	Signal strength
Number of bytes	2	8	1	1	1	1

Total number of records: The total number of constant connections established on the node

Start Index: The start number of the current returned record

Number of records returned: the number of records currently returned

Short address: The short address of the link node

MAC address: The MAC address of the link node

Node type: the node type of the link node, 0-coordinator, 1-router, 2-terminal node (including dormant terminal)

Node relationship: the relationship of link nodes, 0-parent node, 1-child node, 2-neighbor node, 3-irrelevant node

Network Depth: The network depth of the node

Signal strength: The average signal strength of the link node, the maximum 255 is equivalent to 100%, which means the best quality.

4. ZigBee Control and Management (ZCL Protocol)

4.1. ZCL specification introduction and table

The ZCL (ZigBee Cluster Library) specification is an application layer specification in the ZigBee protocol. This specification defines how various ZigBee devices are distinguished, how to control, and how to represent their current control state or physical state, such as sensor readings, lighting equipment light and dark, etc. Through the arbitrary arrangement and combination of ZCL command contents, all ZigBee modules of Ebyte can support up to 60,000+ ZigBee device types and 16,000,000+ device control commands, including various ZigBee devices on the market and those that will appear in the future. ZigBee devices.

4.1.1. Introduction to ZCL Architecture

Port Profile : (Profile)

Each port on a ZigBee node has its own port outline to describe the purpose of the port.

Except Profile=0xC05E is used for Touch Link network access, Profile=0xA1E0 is used for GP port, other profiles can be used for application layer control. The two Endpoints must have the same Profile in order to interact with application layer data. Among them, the ZigBee smart home application (Home Automatic) has Profile=0x0104, and the Ebyte data transmission module also uses this Profile as data transmission to meet the requirements of interoperability with other manufacturers’ devices. .

Device ID :

The device ID exists on each port of the ZigBee device, and a port has one and only one device ID, which is used to define the specific device type corresponding to this port. See " Device ID Table " for details

Cluster:

It is used to define the function of ZigBee device. Any port (port number from 1 to 240) on a ZigBee device supports one or more clusters, indicating that the device supports a certain function. A cluster usually contains several physical states and control instructions, and different clusters represent different functions (for example, the CPU temperature of the ZigBee device and the ambient temperature detected by the sensor are two different clusters). There are two cluster tables on each port, namely the input cluster table (in cluster) and the output cluster table (out cluster). The input cluster indicates that the device has the ability to control and execute a function, and is the executor of the function; the output cluster is the ability to initiate a function and the controller of the function.

Server side (execution side or provider) and client side (control side or user):

When a cluster appears in the input cluster table of the port, it means that the port is the server side on the cluster, that is, the provider of the function service corresponding to the cluster, that is, the execution side. On the contrary, if a certain cluster appears in the output cluster table of the port, it means that the port is the client end on the cluster, that is, the user of the function service corresponding to the cluster, that is, the control end. The ZCL command needs to mark the command direction, namely Server-to-Client (S2C) and Client-to-Server (C2S), to indicate whether the command is initiated by the provider or the user.

Manufacturer code:

The manufacturer code is used when the device manufacturer adds a custom cluster. When the ZigBee standard cluster cannot meet the application, the manufacturer can customize the cluster (starting from cluster ID=0xFC00). In order to prevent "cluster collision" by different manufacturers using the same custom cluster, manufacturers can add a manufacturer code field to the custom cluster to prevent collisions.

Attribute :

Attribute is used to represent an actual state under a cluster, so the size of the attribute is fixed, and it usually exists in the form of a global variable in the device. Properties can be used to represent the current state of the device, such as temperature, level, on/off, etc. Attributes can be defined as variable types that conform to the C language specification, such as char type, bool type, int type, floating point type, string type..., each attribute has a fixed data type (Data Type), see "Data Type " Type Table ".

Each attribute has a 16-bit attribute ID. The execution and control terminals of each cluster can define their own attributes, and the attribute IDs can be reused and different data types can be used.

General Command (Global Command) :

Common commands are used to access and control device-side attributes, including reading attributes, writing attributes, actively reporting attributes to fixed targets, setting attribute reporting rules, querying attribute reporting rules, and statistics on all attributes. General commands directly control attributes, and can only operate fixed-size attribute values. At the same time, attributes on devices usually correspond to global variables. In order to prevent dangerous operations on the device side, it is rare to control the device or change the physical state of the device by writing properties. In addition, a general command can carry multiple attributes under the same cluster, that is, SIMD (Single Instruction Multiple Data) operation.

Control command (Special Command) :

The control command does not directly operate on the attribute, but controls the target device through the command ID plus the attached command parameters, so it is more practical than the general command. 256 control commands can be defined under each cluster, plus the different command directions, a total of 512 different control commands can be defined by the control end device and the executive end device. And each command can be accompanied by command parameters of different lengths.

Using control commands to control the target device can directly act on the physical state of the target device. For example, using a control command to change the PWM pulse width of the target device, or adding an unlock password to the control command, the change of the PWM pulse width of the execution device or the change of the lock state transmission will be synchronized to the corresponding attribute, and then the corresponding attribute can be accessed through the general command. , the control result can be obtained.

Control commands can only be sent from the control end to the executive end, but general commands can be sent to the control end and the executive end by a third device.

Often connected binding (Bind):

port on a node to bind another port with a fixed cluster ID . Source ports remember each other by MAC address and port number. Since the finished ZigBee device MAC address and port will not change, it will take effect even if the target device is not currently in the network, but the target device must join the same network as the source device to communicate normally. Always connect binding must have the following characteristics.

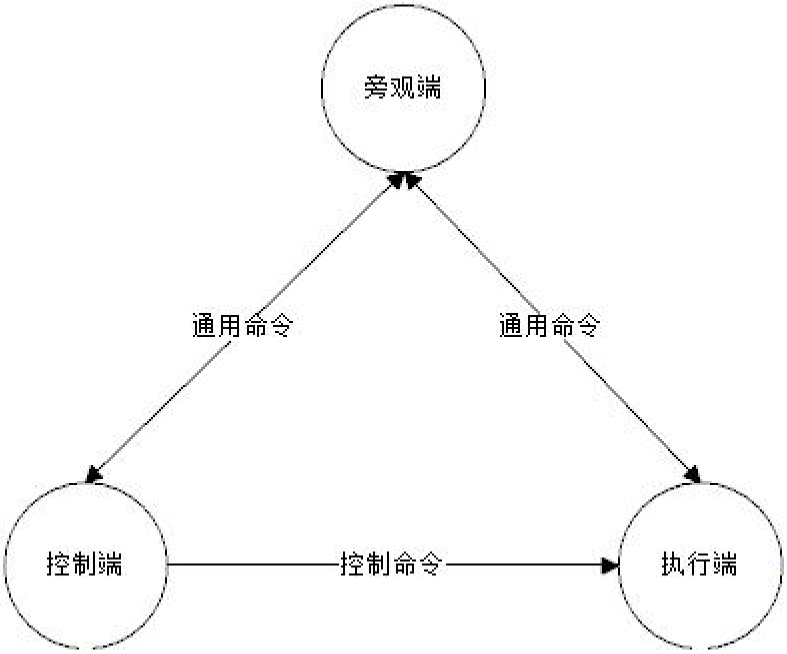
- The source port and destination port can be on the same node, i.e. their MAC addresses are the same.
- source port and destination port must be in the relationship between Server and Client , and the cluster used for binding must exist in the input cluster table or output cluster table of the source port.

There are two ways to set bindings:

- The coordinator sends instructions: the coordinator sets and manages the binding settings and management of the node ports including itself through the three ZDO commands of " set binding ", " unbinding " and " view binding ", and the receiving object of the ZDO command To bind the source port, if you need to set up two-way interaction (such as data transparent transmission), you need to set both ports to bind each other.
- Node-initiated binding: The data transmission module can automatically search for the opposite port through the "one-key binding" function. The source port is the own port 1 of the data transmission module (supports Ebyte custom clusters), and the destination port can be the port 1 of other data transmission modules, or it can be ZigBee lighting equipment (including the PWM control port of E180ZG120).

Endian mode:

In the ZCL command, in addition to the target short address, the parameters that need to be input and output include cluster ID, manufacturer code, attribute ID, and the input and output formats are all in little endian mode.



4.1.2. ZCL related entries

Device ID table			
Classification	Device	Equipment name	Device ID
Generic	On/Off Switch	On-off switch	0x0000
	Level Control Switch	Stage controller (knob)	0x0001
	On/Off Output	switch output	0x0002
	Level Controllable Output	Knob output	0x0003

	Scene Selector	scene controller	0x0004
	Configuration Tool	Configuration Tool	0x0005
	Remote Control	remote control	0x0006
	Combined Interface		0x0007
	Range Extender	repeater	0x0008
	Mains Power Outlet	power output device	0x0009
	Door Lock	door lock	0x000A
	Door Lock Control	door lock controller	0x000B
	Simple Sensor	Ordinary sensor	0x000C
	Consumption Awareness Device	Consumer-aware devices	0x000D
	Home Gateway	home gateway	0x0050
	Smart Plug	smart socket	0x0051
	White Goods	white goods	0x0052
Light Lighting	On/Off Light	switch lights	0x0100
	Dimmable Light	Dimming lights	0x0101
	Color Dimmable Light	colored lights	0x0102
	On/Off Light Switch	switch light controller	0x0103
	Dimmer Switch	Dimmer light controller	0x0104
	Color Dimmer	color controller	0x0105
	Light Sensor	light sensor	0x0106
	Occupancy Sensor		0x0107
Closures Doors and windows	Shade	shading equipment	0x0200
	Shade Controller	sunshade controller	0x0201
	Window Cover	curtain	0x0202
	Window Cover control	Curtain Controller	0x0203
HVAC HVAC	Heating/Cooling Unit	Heating and cooling controller	0x0300
	Thermostat	thermostat	0x0301
	Temperature Sensor	temperature sensor	0x0302
	Pump	Pump	0x0303
	Pump Controller	pump controller	0x0304
	Pressure Sensor	Pressure Sensor	0x0305
	Flow Sensor	Flow Sensors	0x0306
IAS Security class	IAS Control and Indicating Equipment	Security controller	0x0400
	IAS Ancillary Control Equipment	Security Gateway	0x0401

	IAS Zone	security sensor	0x0402
	IAS Warning Device	security siren	0x0403

ZCL attribute data type table					
category	type of data	ID	number of bytes	invalid value	Report alignment
NULL	nodata	0x00	0		0
Ordinary data	data8	0x08	1		0
	data16	0x09	2		0
	data24	0x0a	3		0
	data32	0x0b	4		0
	data40	0x0c	5		0
	data48	0x0d	6		0
	data56	0x0e	7		0
	data64	0x0f	8		0
logical data	bool	0x10	1	0xff	0
binary data	bit8	0x18	1		0
	bit16	0x19	2		0
	bit24	0x1a	3		0
	bit32	0x1b	4		0
	bit40	0x1c	5		0
	bit48	0x1d	6		0
	bit56	0x1e	7		0
	bit64	0x1f	8		0
unsigned integer	uint8	0x20	1		4
	uint16	0x21	2		4
	uint24	0x22	3		4
	uint32	0x23	4		4
	uint40	0x24	5		8
	uint48	0x25	6		8
	uint56	0x26	7		8
	uint64	0x27	8		8
signed integer	int8	0x28	1		4
	int16	0x29	2		4
	int24	0x2a	3		4
	int32	0x2b	4		4
	int40	0x2c	5		8
	int48	0x2d	6		8

	int56	0x2e	7		8
	int64	0x2f	8		8
enumerate	enum8	0x30	1	0xff	0
	enum16	0x31	2	0xffff	0
floating point	semi	0x38	2		4
	single	0x39	4		4
	double	0x3a	8		8
string	octstr	0x41	first byte	header is 0xff	0
	string	0x42	first byte	header is 0xff	0
	octstr16	0x43	first double byte	header is 0xffff	0
	string16	0x44	first double byte	header is 0xffff	0
serial type	uint8_array _	0x48	2 + sum of content length	header is 0xffff	0
	struct	0x4C	2 + sum of content length	header is 0xffff	0
time	ToD	0xe0	4	0xffffffff	4
	date	0xe1	4	0xffffffff	4
	UTC	0xe2	4	0xffffffff	4
identifier	clusterID	0xe8	2	0xffff	0
	attriID	0xe9	2	0xffff	0
	bacOID	0xea	4	0xffffffff	0
other data	EUI64	0xf0	8	0xffffffff	0
	key128	0xf1	16		0

ZCL state table		
Value	describe	what happens
0x00	Successful operation	all commands
0x01	operation failed	all commands
0x7E	The operation is not authorized	When reading and writing Attribute

0x80	Incorrect command format	Send proprietary commands
0x81	ZCL proprietary command is not supported	Send proprietary commands
0x82	ZCL generic command is not supported	Send general command
0x83	Vendor-defined ZCL proprietary commands are not supported	specific commands with vendor ID
0x84	Vendor-defined ZCL common commands are not supported	general command with manufacturer ID
0x85	invalid field	Parameter error for proprietary command
0x86	Unsupported Attribute	General command
0x87	wrong input value	all commands
0x88	Attribute read only	When writing Attribute
0x89	not enough space	Proprietary command (with memory function)
0x8A	there are duplicates	Proprietary command (with memory function)
0x8B	did not find	Proprietary command (with memory function)
0x8C	Attribute does not support active reporting	Configure active reporting or read configuration
0x8D	Invalid data type	Generic commands with data types
0x8E	Invalid option	Proprietary command
0x8F	Attribute write only	When reading Attitude
0x90	Inconsistent startup status	
0x91	Out Of Band	
0x92	inconsistency error	
0x93	deny this action	
0x94	time out	
0x95	Abort	OTA _
0x96	invalid image data	OTA _
0x97	waiting for data	OTA or other big data transfer
0x98	no image file	OTA _
0x99	need more image data	OTA _

0xc0	hardware error	
0xc1	software bug	
0xc2	Calibration error	

Common cluster ID table			
cluster ID	describe	Function	manufacture code
0x0000	ZCL_CLUSTER_ID_GEN_BASIC	Equipment basic information	none
0x0003	ZCL_CLUSTER_ID_GEN_IDENTIFY	Device identification (ident)	none
0x0004	ZCL_CLUSTER_ID_GEN_GROUPS	Group Function Protocol	none
0x0005	ZCL_CLUSTER_ID_GEN_SCENES	scene function protocol	none
0x0006	ZCL_CLUSTER_ID_GEN_ON_OFF	light switch agreement	none
0x0008	ZCL_CLUSTER_ID_GEN_LEVEL_CONTROL	Dimming Protocol	none
0x0019	ZCL_CLUSTER_ID_OTA	OTA upgrade	none
0x0400	ZCL_CLUSTER_ID_MS_ILLUMINANCE_MEASUREMENT	Light Sensing Protocol	none
0x0500	ZCL_CLUSTER_ID_SS_IAS_ZONE	security protocol	none
0x1000	ZCL_CLUSTER_ID_TOUCHLINK	Touch Link function	none
0xFC08	ZCL_CLUSTER_ID_EBYTE	Ebyte transparent transmission	0x2000

4.1.3. Ebyte serial port data transmission ZCL cluster specification

Ebyte serial data transmission equipment complies with the ZigBee standard specification, strictly abides by the ZCL protocol rules, and customizes the serial data transmission cluster, which is defined as follows

Manufacturer code: 0x2000

Serial port data transmission cluster ID: 0xFC08

Serial port data transmission related properties:

Ebyte custom attributes (execution side)					
AttrID	Descriptor	name	type of data	operate	initial value
0x0000	Baud	baud rate	uint32	R	115200
0x0001	targetAddr	target short address	u i nt16	RW	0xFFFF
0x0002	targetEP	destination port	uint8	RW	0xFF
0x0003	sendMode	Transparent mode	bool	RW	FALSE
0x0004	LP Level	low power mode	E num8	RP	0
0x0005	target IEEE	destination MAC address	EUI64	R	0x0000000000000000

- In order to prevent setting the wrong value, the baud rate can only be modified by the control command. The control command has the function of error correction. Once the wrong baud rate is set, it can be corrected to the closest correct baud rate.
- The target short address defaults to the broadcast address, and when it is set to 0xFFFE, it is transparently transmitted to the binding target.
- When the target port is 1~240, the on-demand mode goes to the corresponding target port, usually set to 1. If set to 0, it is multicast mode, and the target short address is the group address.
- If the transparent transmission mode is set to TRUE, it is the transparent transmission mode or AT command mode.
- There are 4 grades of low power mode, namely 0, 1, 2, 3. 0 is 1 second to wake up for 2 minutes of heartbeat, 1 is 3 seconds to wake up for 4 minutes of heartbeat, 2 is 5 seconds to wake up for 6 minutes of heartbeat, and 3 is not to wake up 8 minutes heartbeat.
- The destination MAC address is only supported by the E180ZG120, and only the destination MAC address of the current communication is displayed.

Serial port data transmission related control commands			
cmdID	Dir	Descriptor	Function
0x00	C2S	Send Data	data sending
0x00	S2C	Data Notify	Default transparent transmission
0x01	C2S	Set Baud req	set baud rate
0x01	S2C	Set baud rsp	Response baud rate setting result
0x02	C2S	Set Target req	Set the destination short address and port
0x02	S2C	Set Target rsp	Response to target short address and port setting result
0x03	C2S	Set LP req	Set low power mode
0x03	S2C	Set LP rsp	Responding to low power mode setting results

4.2. Unified Frame Header Format for ZCL Commands

ZCL commands are designed to use a limited number of command formats to combine ever-changing control commands of different devices, including accessing Attributes in devices and initiating control of these devices.

ZCL commands include input commands, feedback commands, and two asynchronous commands of "send confirmation" and "receive command". The access to the device adopts the sending method of short address + port number.

ZCL commands support unicast, multicast, and broadcast three transmission modes. The ports for multicast and broadcast are 0xFF.

4.2.1. input command format

Entering a command results in a ZCL wireless command from the coordinator to the device, whose unified header format is as follows

Field	Frame header	Frame size	Payload（unfinished）	
			Command type	command code（unfinished）
Content	0x55	Need to calculate	0x02	See Table 4.1
Number of bytes	1	1	1	1

Field	Payload									
	Command data（continued table）									check code
Content	Transmit mode	Target short address	Target port	Frame serial number	Command direction	Cluster ID	Manufacturer Code	Response Mode	Extended data	Need to calculate
Number of bytes	1	2	1	1	1	2	2	1	variable-length	1

Native port: native port index, the lower 4 bits are valid, the default is 0
Transmit mode: bit 6 – APS encryption, bit 7 - forcibly sent (no routing, no forwarding)
Target short address: send target short address, 0xFFFC~0xFFFF is broadcast (0xFFFE is invalid address)
Target port: the port of the sending target, fill in 0xFF and the short address is not broadcast, then use multicast sending
Frame serial number: The host computer generates the frame serial number. If the frame serial number and short address of the ZCL frame are received, and the port is equal to the sending, the message is the reply message of the target device.
Command direction: refer to ZCL framework, 0 - C2S, 1 - S2C
Cluster ID: The cluster ID of the sending message, in little endian mode.

Manufacturer Code: The manufacturer code for sending the message. The target device needs to support the manufacturer code to be valid. The default value is 0x0000.

Response Mode:

0 - Answer with Default Response,

1 - Answer with APS Ack.

2 - Turn off Default Response and APS Ack at the same time without any reply, suitable for high-speed transmission and no requirement for data transmission stability application scenarios, this mode only E180-ZG120A/E180-ZG120B module V1.2 firmware, E18 full series V1.4 firmware, E72-2G4M20S1E(LINK72)V1.4 firmware support.

Extended data: The extended data of different commands is different, and the subsequent command parsing will only analyze the extended data part

Feedback command:

Field	Frame header	Frame size	Payload				
			Command type	command code	Command data		check code
Content	0x55	0x05	0x02	Corresponding send	Execution status	Frame sequence number	Need to calculate
Number of bytes	1	1	1	1	1	1	1

Execution status: 0 -- Valid execution will result in sending confirmation, other values -- invalid execution see "Wireless Sending Status Table"

Frame sequence number: The frame sequence number when the command is sent.

4.2.2. Feedback command format

Field	Frame header	Frame size	Payload			
			Command type	command code	Command data（unfinished）	
Content	0x55	0x0A	0x8F	0x02	Sending mode	Target short address
Number of bytes	1	1	1	1	1	2

Field	Payload	
	Command data（continued table）	check code

Content	Target port	Frame serial number	Command direction	Send results	Need to calculate
Number of bytes	1	1	1	1	1

Send mode: Same as when sending

Target short address: The target short address is sent as when it is sent

Destination port: The port on which the destination is sent, as when it was sent

Frame sequence number: The frame sequence number when the command is sent

Command direction: The direction to send the command, 0-C2S, 1-S2C

Send results: Wireless send results, see" Wireless Transmission Status Table "

4.2.3. Asynchronous Command "Send Confirmation" Format

Sending acknowledgment can be blocked as a busy state sent to a certain target. If the reply mode is enabled when sending, you can obtain whether the sent frame has reached the target from the sending result, but it will consume more wireless resources and increase the delay.

Field	Frame header	Frame size	Payload（unfinished）	
			Command type	command code（unfinished）
Content	0x55	Need to calculate	0x82	See Table 4.1
Number of bytes	1	1	1	1

Field	Payload									
	Command data（continued table）									check code
Content	Transmit mode	Source short address	Target port	Frame serial number	Command direction	Cluster ID	Manufacturer Code	Signal strength	Extended data	Need to calculate
Number of bytes	1	2	1	1	1	2	2	1	variable-length	1

Receiver port: The index of the native receiver port, the lower 4 bits valid

Opponent mode: Bit-4, received broadcast or multicast, bit-5 signal strength valid

Source short address: The short address of the other device

Source port: The port of the other device

Frame sequence number: The frame sequence number of the received message, if the received frame sequence number is the same as the sent message, and the source address and source port are the same as the sender

Command direction: Refer to ZCL architecture, 0-C2S, 1-S2C

Cluster ID: The cluster ID from which the message is received, in little endian mode.

Vendor code: The vendor code to receive the message, which needs to be supported by the source device

Send the same target, the opposite direction of the command, the received message is a return frame.

Signal strength: The signal strength of the received message

Extended data: The extended data of different commands are different, and the subsequent command parses only the extended data part

4.3. ZCL command function introduction and analysis

ZCL command parsing, parsing only the "extended data" part of the input command and received message. There is a causal relationship between certain commands, so commands with a causal relationship between sending and receiving are parsed uniformly.

ZCL commands can be divided into two categories: " general commands " and " control commands ". The command codes from 0x00 to 0x0B are general commands and can directly access attributes; 0x0F is a control command, which is two-way peer-to-peer for sending and receiving, and the control commands under different clusters carry The parameters are different.

Table 4.1 ZCL command code table

Function	command code	send	take over	type
read device status	0x 00	ZCL_READ_ATTR_REQ _	ZCL_READ_ATTR_RSP _	General command
Modify device status	0x01	ZCL_WRTIE_ATTR_REQ _	ZCL_WRTIE_ATTR_RSP _	General command
Query status reporting rules	0x02	ZCL_READ_REPORT_REQ _	ZCL_READ_REPORT_RSP _	General command
Modify status reporting rules	0x03	ZCL_WRITE_REPORT_REQ _	ZCL_WRITE_REPORT_RSP _	General command
View all status	0x04	ZCL_DISC_ATTR_REQ _	ZCL_DISC_ATTR_RSP _	General command
View All Status Band Extensions	0x05	ZCL_DISC_ATTR_EX _REQ	ZCL_DISC_ATTR_EX_RSP _	General command
Active status report	0x0A	none	ZCL_REPORT_IND	General command
The system returns by default	0x0B	none	ZCL_DEFAULT_RSP	General command
send control commands	0x0F	ZCL_CMD_SEND _	none	control commands
receive control commands	0x0F	none	ZCL_CMD_IND _	control commands

Enter the ZCL request:

Field	Command code	Command data	
Content		From [Send mode] To [reply mode]	extended data
Number of bytes	1	11	

Return the ZCL message asynchronously:

Field	Command code	Command data	
Content		From [Send mode] To [signal strength]	extended data
Number of bytes	1	11	

4.3.1. Read device properties (command code 0x00)

Command code: 0x00

Function:

Read ZCL attributes, that is, state parameters, can read multiple state parameters in a specified cluster on a port

Enter the ZCL request:

Field	Command code	Command data		
Content	0x00	From [Send mode] To [reply mode]	extended data	
			Number of attributes N	Attribute list
Number of bytes	1	11	1	2*N

Number of attributes: The number of attributes read at a time, the actual read attributes can only be less than or equal to this value.

Attribute list: A uint16 array list of attribute ids, which are little endian mode inputs.

Return the ZCL message asynchronously:

Field	Command code	Command data

Content	0x00	From [Send mode] To [signal strength]	extended data				
			Number of attributes N	Read property returns struct array [N]			
				Attribute ID	ZCL status	Data type	Data value
Number of bytes	1	11	1	2	1	1	variable-length

Number of attributes: The number of attributes read. If the device supports some attribute IDs contained in the read command, the returned command does not contain these attributes.
Attribute ID: The read 16-bit attribute ID, in little endian mode.
ZCL status: see " ZCL Status Table ", only " operation successful " has the following data
Data type: data type, see " ZCL Data Type Table "
Data value: The state value corresponding to this attribute, the size is determined by the "bytes" item in the data type

4.3.2. Modify device properties (command code 0x01)

Command code: 0x01
Function:

To modify the specified attribute, multiple attributes can be modified at one time, but the attribute must exist and be writable in the target device, and the data type must be the same as that in the target device. If the modification is invalid, which attributes will be invalidated in the returned command.

Enter the ZCL request:

Field	Command code	Command data				
Content	0x01	From [Send mode] To [reply mode]	extended data			
			Number of attributes N	Write property struct array [N]		
				Attribute ID	Data type	Data value
Number of bytes	1	11	1	2	1	variable-length

Number of attributes: The number of attributes that need to be modified
Attribute ID: The attribute ID to be modified, input in little endian mode.
Data type: data type, see " ZCL Data Type Table "
Data value: The state value corresponding to this attribute, the size is determined by the "bytes" item in the data type

Return the ZCL message asynchronously:

Field	Command code	Command data		
Content	0x01	From [Send mode]	extended data	
			Number of	Write property struct array [N]

		To [signal strength]	errors	Attribute ID	ZCL Status
Number of bytes	1	11	1	2	1

Number of errors: The number of attributes that are invalid to be modified, and only the attributes that are invalid to be modified are returned. If the value is 0, it is all OK.
Attribute ID: Modify invalid attribute ID, little endian mode.
ZCL Status: Error cause, see " ZCL Status Table "

4.3.3. Query attribute reporting rules (command code 0x02)

Command code: 0x02

Note: Only E72-2G4M20S1E and E 180ZG120 support

Function:

Query the rules of automatic reporting of attributes, provided that the queried attributes support automatic reporting, and the attributes that support automatic reporting will return the ZCL status success and include valid reporting rule parameters when queried. For attributes that support automatic reporting, you need to bind the port where the attribute is located and the cluster of the attribute (see Setting Binding) to the receiving target to start automatic reporting (E72-2G4M20S1E will automatically set the peer port binding attribute to upload when it acts as a coordinator. cluster to the coordinator's receive port).

Enter the ZCL request:

Field	Command code	Command data		
Content	0x02	From [Send mode] To [reply mode]	extended data	
			Number of attributes N	Property list
Number of bytes	1	11	1	2*N

Number of properties: The number of properties queried.
Property list: The ID of the property being queried, input in little-endian mode.

Return the ZCL message asynchronously:

Field	Command code	Command data							
Content	0x02	From [Send mode] To [signal strength]	extended data						
			Number of attributes N	Read property returns struct array [N]					
				Attribute ID	ZCL status	Minimum time	Maximum time	Data type	Variable value
Number of bytes	1	11	1	2	1	2	2	1	Aligned variable-length

Number of properties: Returns the number of properties for the query
Attribute ID: The returned attribute ID, in little endian mode.
ZCL status: see " ZCL Status Table ", only " operation successful " has the following data
Minimum time: The minimum interval for continuous reporting of this attribute, which can filter data reporting due to continuous jitter of the status value.
Maximum time: the maximum interval time reported by this attribute, which can be used as the heartbeat cycle
Data type: The data type of the variable value, see " ZCL Data Type Table "
Variable value: The change of the attribute value exceeds the variable value to trigger the report, and the value needs to be aligned by 4 bytes according to the size in "Report Alignment" in the " ZCL Data Type Table ".

4.3.4. Set attribute reporting rule (command code 0x03)

Command code: 0x03

Note: Only E72-2G4M20S1E and E 180ZG120 support

Function:

By modifying the automatic reporting rule of attributes, you can modify the period of automatic reporting of attributes and the amount of changes in attribute values that trigger the reporting. In the "Report Alignment" item in the " ZCL Data Type Table ", if the "Report Alignment" corresponding to the attribute type is 0, only the modification of the reporting period is supported, and the modification of the attribute value change is not supported.

Enter the ZCL request:

Field	Command code	Command data						
Content	0x03	From [Send mode] To [reply mode]	extended data					
			Number of attributes N	Set property report struct array [N]				
				Attribute ID	Minimum time	Maximum time	Data type	Variable value
Number of bytes	1	11	1	2	2	2	1	Aligned variable-length

Number of properties: the number of properties to set
Attribute ID: The set attribute ID, input in little endian mode.
Minimum time: The minimum interval for continuous reporting of this attribute, which can filter data reporting due to continuous jitter of the status value.
Maximum time: the maximum interval time reported by this attribute, which can be used as the heartbeat cycle
Data type: The data type of the variable value, see " ZCL Data Type Table "
Variable value: The change of the attribute value exceeds the variable value to trigger the report, and the value needs to be aligned by 4 bytes according to the size in "Report Alignment" in the "

ZCL Data Type Table ". If the alignment length is 0, this property does not need to set the variable value.

Return the ZCL message asynchronously:

Field	Command code	Command data			
Content	0x03	From [Send mode] To [signal strength]	extended data		
			Number of errors	Set property report struct array [N]	
				Attribute ID	ZCL Status
Number of bytes	1	11	1	2	1

errors: Number of properties with invalid settings , return only properties with invalid settings

Attribute ID: Set invalid attribute ID, little endian mode.

ZCL Status: Error cause, see " ZCL Status Table "

4.3.5. View all properties (command code 0x04)

Command code: 0x04

Note: Only E72-2G4M20S1E supports

Function:

View all attributes supported by the target device, which can be viewed in multiple packages.

Enter the ZCL request:

Field	Command code	Command data		
Content	0x04	From [Send mode] To [reply mode]	extended data	
			Number of properties	Starting attribute ID
Number of bytes	1	11	1	2

Number of properties: the number of properties expected to be queried

Starting attribute ID: start from the starting attribute ID, input in little endian mode.

Return the ZCL message asynchronously:

Field	Command code	Command data				
Content	0x04	From [Send mode] To [signal strength]	extended data			
			End flag	Number of attributes	Read property struct array [N]	
					Attribute ID	Data type
Number of bytes	1	11	1	1	2	1

End flag: if the flag is 1, it means that the returned attribute ID contains the last attribute ID of the cluster

Number of attributes: The number of attributes returned by this query

Attribute ID: The returned attribute ID, in little endian mode.

Data type: The data type corresponding to the attribute ID

4.3.6. View all status with extended fields (command code 0x05)

Command code: 0x05

Note: Only E72-2G4M20S1E supports

Function:

Check all the attributes supported by the target device, and return the query result including whether each attribute supports writability and active reporting.

Enter the ZCL request:

Field	Command code	Command data		
Content	0x05	From [Send mode] To [reply mode]	extended data	
			Number of properties	Starting attribute ID
Number of bytes	1	11	1	2

Number of properties: the number of properties expected to be queried

Starting attribute ID: start from the starting attribute ID, input in little endian mode.

Return the ZCL message asynchronously:

Field	Command code	Command data					
Content	0x05	From [Send mode] To [signal strength]	extended data				
			End flag	Number of attributes	Read property struct array [N]		
					Attribute ID	Data type	Supported operations
Number of bytes	1	11	1	1	2	1	1

End flag: if the flag is 1, it means that the returned attribute ID contains the last attribute ID of the cluster

Number of attributes: The number of attributes returned by this query

Attribute ID: The returned attribute ID, in little endian mode.

Data type: The data type corresponding to the attribute ID

Supported operations: bit0 enable = readable, bit1 enable = writable, bit2 enable = support active reporting

4.3.7. Receive attribute active report (command code 0x0A)

Command code: 0x0A

Function:

The device automatically reports the attribute, and the attribute state value changes beyond the variable value, or reaches the maximum time, and reports the state value. Since only the E72-2G4M20S1E as the coordinator will automatically set the peer port binding attribute to upload the cluster to the coordinator's receiving port, when the E180ZG120 and E18 modules are used as the coordinator, "setting binding" is required to receive

Receive ZCL messages asynchronously:

Field	Command code	Command data				
Content	0x0A	From [Send mode] To [signal strength]	extended data			
			Number of attributes	Attribute report struct array [N]		
				Attribute ID	Data type	Data value
Number of bytes	1	11	1	2	1	variable-length

Number of attributes: The number of attributes received and reported. If the equipment department supports some attribute IDs contained in the read command, the returned command does not contain these attributes.

Attribute ID: The 16-bit attribute ID reported, in little endian mode.

Data type: data type, see " ZCL Data Type Table "

Data value: The state value corresponding to this attribute, the size is determined by the "bytes" item in the data type

4.3.8. Default return frame (command code 0x0B)

Command code: 0x0B

Function:

The default return frame returned by the target device, the target device does not support this command, or sends a short response with Default Request enabled, this return frame will be triggered. The frame number of this command is used to trace the corresponding send command

Receive ZCL messages asynchronously:

Field	Command code	Command data		
Content	0x0B	From [Send mode] To [signal strength]	extended data	
			Command ID	ZCL Status
Number of bytes	1	11	1	1

Command ID: Returns the corresponding command ID. This value is only meaningful for "control commands", and has no meaning for other commands involving attribute status. The attribute status command is traced back through the frame number.

ZCL Status: See " ZCL Status Table "

4.3.9. Send control command (command code 0x0F)

Command code: 0x0F

Function:

When sending device control commands, each command can carry variable-length command parameters. Command parameters are relatively complex relative attribute states, which can be multiple variables, arrays, or data streams. Send the wrong control command to the wrong device, or set the "response mode" in the input command to 0, and receive the default return frame. You can use the cmd ID and frame number in the default return frame to detect whether it matches the sent control command. correspond.

Enter the ZCL request:

Field	Command code	Command data		
Content	0x0F	From [Send mode] To [reply mode]	extended data	
			Command ID	Command parameters
Number of bytes	1	11	1	variable-length

Command ID: Command ID of the control command

Command parameters: The parameters carried by the control command and the content of the command parameters are determined according to the different clusters, manufacturer codes, and command IDs.

4.3.10. Control command received (command code 0x0F)

Command code: 0x0F

Function:

Receive a control command. The received control command may be a return message of the sent command, or it may be an active notification by a remote device. The frame sequence number can be used to judge whether the received control command sends a return message of the command. Usually, after receiving the control command, the controlled device returns the default return frame without returning the control command.

Receive ZCL messages asynchronously:

Field	Command code	Command data		
Content	0x0F	From [Send mode] To [signal strength]	extended data	
			Command ID	Command parameters
Number of bytes	1	11	1	variable-length

Command ID: Command ID of the received control command

Command parameters: The parameters carried by the received control command and the content of the command parameters are determined according to the different clusters, manufacturer codes, and command IDs.

4.4. Attributes and control commands under each cluster

According to the cluster classification, the attributes and control commands under each cluster are listed

4.4.1. (BASIC Cluster = 0x0000)

Function:

This cluster defines the factory information of the device, and almost all devices must support this cluster

Property sheet:

Cluster = 0000, Server				
AttrID	Descriptor	name	type of data	operate
0x0000	ZCL Version	ZigBee version	uint8	read only
0x0001	Application Version	Software version	uint8	read only
0x0002	Stack Version	Protocol version	uint8	read only
0x0003	Hardware Version	hardware version	uint8	read only
0x0004	Manufacturer Name	Trade Names	string	read only
0x0005	Model Identifier	Product number	string	read only
0x0006	Date Code	compile date	string	read only
0x0007	Power Source	Power mode	enum8	read only

Send control command: none

Receive control commands: none

4.4.2. Device Tag Cluster (IDENTIFY Cluster = 0x0003)

Function:

It is used to mark the device. In the marked state, the device can be discovered by human flesh, and can also be discovered by other ZigBee devices and establish a constant connection with it.

Property sheet:

Cluster = 000 3 , Server				
AttrID	Descriptor	name	type of data	operate
0x0000	Identify Time	mark time	Uint16	read and write

Send control commands:

Cluster = 000 3 , Client->Server			
cmdID	Descriptor	name	parameter
0x00	Identify	marking equipment	uint16 IdentifyTime: Mark Mode Duration
0x01	IdentifyQuery	Query marking equipment	none

Receive control commands:

Cluster = 000 3 , Sever -> Client			
cmdID	Descriptor	name	parameter
0x00	IdentifyQueryresponse	Back to Query Marking Devices	uint16 timeout : remaining mark time

Special Note:

- When "querying marked devices", the query can be broadcast or multicast
- Only devices in tagging mode will return the "Return to query tagging devices" message

4.4.3. Group Management Cluster (GROUP Cluster = 0x0004)

Function:

Group management for devices

Property sheet:

Cluster = 0004, Server				
AttrID	Descriptor	name	type of data	operate
0x0000	NameSupport	Support group naming	bit8	read only

- "Support group naming" can save a string of group names in the device when the device is added to a group, which has little actual value

Send control commands:

Cluster = 0004, Client->Server			
cmdID	Descriptor	name	parameter
0x00	AddGroup	device grouping	uint 16 groupID: The group ID of the device added to the group string name: group name
0x01	ViewGroup	Query group information	uint16 groupID: the queried group ID (for checking the group name)
0x02	GetMembership	View (all) groups	uint 8 count: Query the number of groups, fill in 0 when checking all uint16 groupList[ ]: The grouping array to be queried
0x03	RemoveGroup	remove a group	uint 16 groupID: group ID of the removed group
0x04	RemoveAll	delete all groups	none
0x05	AddGroupIdentify	mark state device add group	uint 16 groupID: The group ID of the device added to the group string name: group name

- When adding a device to a group, the group name can be omitted, only the group ID is needed. If you really want to add it, the header should not exceed 16 characters.
- When viewing groups, fill in count with 0 to query all groups, and if it is not 0, query whether the groups in the groupList exist in the device.
- The query group information command is used to query the group name and has little effect.
- It is recommended to use broadcast to send the marked state device to the group. There is no corresponding return for this command, and only "default return" can be received during unicast.

Receive control commands:

Cluster = 0004, Sever -> Client			
cmdID	Descriptor	name	parameter
0x00	AddGroupRsp	return equipment group	uint8 status: ZCL status uint 16 groupID: The group ID of the device added to the group
0x01	ViewGroupRsp	Query group information return	uint8 status: ZCL status uint16 groupID: the queried group ID string name: query group name
0x02	GetMembershipRsp	View (all) group return	uint8 capacity: how many more groups can be added uint 8 count: the number of devices added to the group uint16 groupList[ ]: the group the device joins
0x03	RemoveGroupRsp	remove a group return	uint8 status: ZCL status uint 16 groupID: group ID of the removed group

4.4.4. Scene Management Cluster (SCENES Cluster = 0x0005)

Function:

The scene management function of the device. In the scene mode, the device outputs a preset physical state, and multiple devices can input a preset physical state through multicast or broadcast to achieve the effect of controlling different outputs at the same time.

Property sheet:

Cluster = 0005, Server				
AttrID	Descriptor	name	type of data	operate
0x0000	SceneCount	number of scenes	uint8	read only
0x0001	CurrentScene	current scene	uint8	read only
0x0002	CurrentGroup	current scene grouping	uint16	read only
0x0003	SceneValid	in scene mode	bool	read only
0x0004	NameSupport	Support scene name	bit8	read only

- A scene consists of 8bit scene ID + 16bit group ID, that is, a scene needs to be valid under a specific group. At the same time, it is equivalent to extending the scene to 24bit.

Send control commands:

Cluster = 0005, Client->Server			
cmdID	Descriptor	name	parameter
0x00	AddScene	Add a scene	uint16 groupID : The group where the scene is located, the device must be added to the group first uint8 sceneID: scene ID uint16 transTime: scene transition time string sceneName: string scene name uint8 sceneData[]: scene data, placed at the end of the command frame
0x01	ViewScene	read scene	uint16 groupID : The group where the scene is located uint8 sceneID: read scene ID
0x02	RemoveScene	remove scene	uint16 groupID : remove the group where the scene is located uint8 sceneID: removed scene ID
0x03	RemoveAllScene	remove all scenes	uint16 groupID : remove the group where the scene is located
0x04	StoreScene	save current scene	uint16 groupID : The group where the scene is located, the device must be added to the group first uint8 sceneID: scene ID
0x05	RecallScene	execution scenario	uint16 groupID : The group where the scene is located uint8 sceneID: scene ID
0x06	GetSceneMembership	Query all scenes	uint16 groupID : The group where the scene is located

- The format of scene data is determined by the device itself, and the device saves attributes under certain clusters as scene data. When executing, it is equivalent to restoring the attribute to the state when it was saved.

Receive control commands:

Cluster = 0005, Server -> Client			
cmdID	Descriptor	name	parameter
0x00	AddSceneRsp	Add scene back	uint8 status: ZCL status uint16 groupID : The group where the scene is located uint8 sceneID: scene ID
0x01	ViewScene Rsp	read scene return	uint8 status: ZCL status uint16 groupID : The group where the scene is located uint8 sceneID: read scene ID uint16 transTime: scene transition time string sceneName: string scene name uint8 sceneData[]: scene data
0x02	RemoveScene Rsp	remove scene return	uint8 status: ZCL status uint16 groupID : remove the group where the scene is

			located uint8 sceneID: removed scene ID
0x03	RemoveAllScene Rsp	Remove all scenes and return	uint8 status: ZCL status uint16 groupID : remove the group where the scene is located
0x04	StoreScene Rsp	Save the current scene and return	uint8 status: ZCL status uint16 groupID : The group where the scene is located uint8 sceneID: scene ID
0x06	GetSceneMembership Rsp	Query all scenes return	uint8 status: ZCL status uint8 capacity: how many scenes can be added uint16 groupID : The group where the scene is located uint8 sceneCount: the number of existing scenes uint8 sceneList[]: List of existing scenes

scene data structure

The scene data is an array that satisfies the following structure

```
{
    uint 16 clusterID,
    uint8 size,
    uint8 data[]
}
```

The size determines the size of the data. The scene data is composed of multiple such structures, with a maximum of 32 bytes in total, which can save multiple attributes under multiple clusters at the same time.

4.4.5. Switch on-off control cluster (ON_OFF cluster = 0x0006)

Function:

Device switch status control

Property sheet:

Cluster = 0x0006 , Server				
AttrID	Descriptor	name	type of data	operate
0x0000	OnOff	switch status	bool	reading + newspaper + scene

Send control commands:

Cluster = 0006, Client->Server			
cmdID	Descriptor	name	parameter
0x00	Off	closure	none
0x01	On	Open	none
0x02	Toggle	reverse	none

Receive control commands: (none)

4.4.6. Level control cluster (LEVEL cluster = 0x0008)

Function:

Device Level Control

Property sheet:

Cluster = 0x000 8, Server				
AttrID	Descriptor	name	type of data	operate
0x0000	current Level	current level	uint8	reading + newspaper + scene

Send control commands:

Cluster = 0008, Client->Server			
cmdID	Descriptor	name	parameter
0x00	MoveToLevel	adjust to level	uint8 level: target level uint16 transTime: gradient time
0x01	Move	Adjust relative level	enum8 mode: mode, 0-rising, 1-falling uint8 rate: adjustment rate
0x02	Step	single step level	enum8 mode: mode, 0-rising, 1-falling uint8 step: step ratio uint16 transTime: gradient time
0x03	Stop	stop gradient	none
0x04	MoveToLevelOnOff	Adjust to level with switch	uint8 level: target level uint16 transTime: gradient time
0x05	MoveOnOff	Adjust relative level with switch	enum8 mode: mode, 0-rising, 1-falling uint8 rate: adjustment rate
0x06	StepOnOff	One-step level with switch	enum8 mode: mode, 0-rising, 1-falling uint8 step: step ratio uint16 transTime: gradient time
0x07	Stop	stop gradient	none

Receive control commands: (none)

4.4.7. Ebyte data transmission control cluster (EBYTE cluster = 0xFC08 / manuCode=0x2000)

Function:

Ebyte data transparent transmission custom cluster

Property sheet:

Cluster = 0xFC08, manuCode=0x2000, Server

AttrID	Descriptor	name	type of data	operate
0x0000	Baud	baud rate	uint32	read only
0x0001	targetAddr	Default destination short address	u i nt16	read and write
0x0002	targetEP	Default destination port	uint8	read and write
0x0003	sendMode	Transparent mode	bool	read and write
0x0004	LP Level	low power mode	enum8	read only + report
0x0005	target IEEE	Destination MAC address display	EUI64	read only
0x0006	modbus ID	Modbus address	uint8	read and write+reported
0x0010	customer uint32	Custom 32-bit state	uint32	read and write
0x0011	customer uint16	Custom 16-bit state	uint16	read and write
0x0012	customer uint8 A	Custom 8-bit state A	uint8	read and write
0x0013	customer uint8 B	Custom 8-bit state B	uint8	read and write

Baud rate support 9600, 19200, 38400, 57600, 115200

Transparent transmission mode: 0-command mode, 1-transparent transmission mode

Low power mode: 0-1 second wake up, 1-3.33 second wake up, 2-second wake up, 3- always sleep

The target MAC display is only supported by the E180ZG120 module. The E180ZG120 can be bound to multiple targets. The target MAC address only displays the recently communicated targets.

Send control commands:

Cluster = 0xFC08, manuCode=0x2000, Client- >Server			
cmdID	Descriptor	name	parameter
0x00	UartSend	Transparent transmission	uint8 data[]: transparent data
0x01	SetDstAddr	Set default target	uint16 dstAddr: target short address uint8 endpoint: destination port
0x02	SetBaud	set baud rate	uint32 baud: the new baud rate set, restart to take effect
0x03	SetLP_Level	Set low power mode	uint8 LP_level: low power level

- The baud rate needs to be set to the correct value, so the properties cannot be modified directly
- The low power mode needs to set the correct value, so the properties cannot be modified directly

Receive command:

Cluster = 0xFC08, manuCode=0x2000, Sever - > Client

cmdID	Descriptor	name	parameter
0x00	Data Notify	Transparent transmission	uint8 data[]: transparent data
0x01	SetDstAddrRsp	set default target return	uint8 status: ZCL status
0x02	SetBaudRsp	set baud rate return	uint8 status: ZCL status
0x03	SetLP_LevelRsp	Set low power return	uint8 status: ZCL status

4.5. Revision history

version	Date of revision	Amendment note	maintainer
1.0	2022-11-02	First edition	Bin
1.1	2022-12-28	Error correction	Bin
1.2	2023-2-15	Error correction	Bin
1.3	2023-3-06	Add New Attribute	Bin
1.4	2023-4-07	Format modification	Bin
1.5	2023-7-06	Modify the format and correct errors	Bin

4.6. About us

Technical support: support@cdebyte.com

Documents and RF Setting download link:：https://www.cdebyte.com

Thank you for using Ebyte products! Please contact us with any questions or suggestions: info@cdebyte.com

Official hotline:028-61543675

Web: https://www.cdebyte.com

Address: B5 Mould Park, 199# Xiqu Ave, High-tech District, Sichuan, China

EBYTE Chengdu Ebyte Electronic Technology Co.,Ltd.