

ⒼⒷ Operating Instructions

RS485 - Zigbee® 3.0 Transceiver, 20 dB

Item No. 3345310



1 Table of contents



2	Introduction	8
3	Operating Instructions for download	8
4	Intended use	8
5	Features and functions	8
6	Delivery content	9
7	Description of symbols	10
8	Safety instructions	10
	8.1 General information	10
	8.2 Handling	10
	8.3 Operating environment	10
	8.4 Operation	10
	8.5 Connected devices	10
9	Product overview	11
	9.1 Interface Description	11
	9.2 Indicator light description	11
	9.3 Product size	13
10	Interface Definition	14
11	Working Mode	14
	11.1 Transmission mode	14
	11.2 HEX command mode (configuration mode)	14
	11.3 Mode switching	14
	11.4 Related parameters in transmission mode	15
12	Quick Start	16
	12.1 Quickly build a ZigBee® network	16
	12.2 Quickly join a ZigBee® network	19
	12.3 Data transmission	21
	12.4 Data transmission between network nodes	23
13	Sending and receiving methods	28
	13.1 The way of sending data in transparent transmission mode	28
	13.1.1 Broadcast mode	28
	13.1.2 Unicast mode	28
	13.1.3 Multicast mode	28
	13.2 The way of sending data in HEX command mode	28
14	Application Function	28

14.1 Function.....	28
14.1.1 Detailed explanation of LINK light.....	28
14.1.2 Detailed Explanation of RUN Light.....	28
14.1.3 Detailed explanation of SMART button.....	29
14.1.4 Automatic Pairing and Mark Adaptation (Identify) Mode.....	29
14.1.4.1 Mark Adaptation (Identify) mode.....	29
14.1.4.2 Automatic pairing.....	29
14.2 Wireless remote configuration function.....	30
15 Network structure.....	30
15.1 Practical Application Fields.....	31
16 ZigBee® 3.0 serial port commands.....	31
16.1 Serial port format and mode configuration.....	31
16.1.1 Serial port setting mode and baud rate.....	31
16.1.2 Serial command format.....	31
16.1.3 Command frame structure.....	32
16.1.4 Frame timeout and frame interval.....	32
16.1.5 Three command modes.....	33
16.1.6 Command type and command code list.....	33
16.1.7 Commonly used input command list.....	35
16.1.8 Common addressing format and big endian format in ZigBee® protocol.....	38
16.2 Local command parsing.....	39
16.2.1 Local configuration commands.....	39
16.2.1.1 Query the current status of the module (command code 0x00).....	40
16.2.1.2 Module boot/soft start (command code 0x01).....	40
16.2.1.3 Start network configuration (command code 0x02).....	41
16.2.1.4 Stop network configuration (command code 0x03).....	41
16.2.1.5 Reset/factory reset (0x04).....	42
16.2.1.6 Set node type (command code 0x05).....	43
16.2.1.7 Query and set channel (command code 0x06).....	43
16.2.1.8 Query PAN-ID (command code 0x07).....	44
16.2.1.9 Set PAN-ID (command code 0x08).....	44
16.2.1.10 View module add group (command code 0x09).....	45
16.2.1.11 Module group adding(command code 0x0A).....	45
16.2.1.12 Module ungroup (command code 0x0B).....	46
16.2.1.13 Channel scan test (command code 0x0C).....	46

16.2.1.14 Set and query the current transmit power (command code 0x0D)	47
16.2.1.15 Read local properties (command code 0x10):	48
16.2.1.16 Set local attribute (command code 0x11)	48
16.2.1.17 Auto bind target (command code 0x14)	49
16.2.1.18 Get the current UTC time (command code 0x20)	50
16.2.1.19 Set UTC time (command code 0x21)	50
16.2.1.20 Read the network access node address table (command code 0x22)	51
16.2.1.21 Read access node key (0x23)	52
16.2.1.22 Retransmit device information notification (command code 0x28)	52
16.2.1.23 Set module PWM output duty cycle (command code 0x18)	53
16.2.1.24 Module PWM marking mode (command code 0x19)	54
16.2.1.25 Adding a whitelist record (0x29)	54
16.2.1.26 Lock Extended PAN-ID Networking (0x1A)	55
16.2.2 System notification command	56
16.2.2.1 Device startup (command code 0x00)	56
16.2.2.2 Network status change (command code 0x01)	56
16.2.2.3 Allow network access time window notification (command code 0x02)	57
16.2.2.4 Detect node access to the network (command code 0x03)	57
16.2.2.5 Node short address notification (command code 0x04)	58
16.2.2.6 Device information notification (command code 0x05)	58
16.2.2.7 Module off-grid notification (command code 0x06)	59
16.2.2.8 Automatic binding target result notification (command code 0x10)	60
16.2.2.9 Beacon scan notification (command code 0x0C)	60
16.2.2.10 System background debugging messages (command code 0x0F)	61
16.2.2.11 Three debug messages:	61
16.2.2.12 The automatic acquisition of port information fails	61
16.2.2.13 Automatically bind notifications	62
16.2.2.14 Whitelist interception Notification (Command code 0x07)	63
16.3 Network management commands (ZDO commands)	63
16.3.1 Introduction to ZDO Commands	63
16.3.2 Unified header format for ZDO commands	63
16.3.2.1 Input command format	64
16.3.2.2 Feedback command format	64
16.3.2.3 Send confirmation format	65
16.3.2.4 Receive network management response commands	65

16.3.2.5 Instructions for sending and receiving commands.....	66
16.4 Network management command parsing.....	66
16.4.1 Query node short address (command code 0x00)	66
16.4.2 Query node MAC address (command code 0x01)	67
16.4.3 Query node network configuration information (command code 0x02)	68
16.4.4 Query node port information (command code 0x04)	68
16.4.5 Query the number of node ports (command code 0x05)	69
16.4.6 Set node constant connection binding (command code 0x21)	70
16.4.7 Unbind the node's constant connection (command code 0x22)	71
16.4.8 View node constant connection binding (command code 0x33).....	72
16.4.9 Delete node (command code 0x34).....	73
16.4.10 View network link (0x31).....	74
16.5 ZigBee® Control and Management (ZCL Protocol).....	75
16.5.1 ZCL specification introduction and table.....	75
16.5.2 Introduction to ZCL Architecture	75
16.5.2.1 Device ID	75
16.5.2.2 Cluster	75
16.5.2.3 Client and server.....	75
16.5.2.4 Manufacturer code.....	75
16.5.2.5 Attribute.....	75
16.5.2.6 General Command (Global Command)	76
16.5.2.7 Control command (Special Command).....	76
16.5.2.8 Often connected binding (Bind)	76
16.5.2.9 Endian mode.....	77
16.5.2.10 Serial port data transmission ZCL cluster specification	82
16.6 Unified Frame Header Format for ZCL Commands.....	83
16.6.1 Input command format.....	83
16.6.2 Asynchronous Command "Send Confirmation" Format.....	85
16.7 ZCL command function introduction and analysis	85
16.7.1 Read device properties (command code 0x00)	87
16.7.2 Modify device properties (command code 0x01)	88
16.7.3 Query attribute reporting rules (command code 0x02)	88
16.7.4 Set attribute reporting rule (command code 0x03)	89
16.7.5 View all properties (command code 0x04).....	91
16.7.6 View all status with extended fields (command code 0x05)	92

16.7.7	Receive attribute active report (command code 0x0A).....	93
16.7.8	Default return frame (command code 0x0B).....	93
16.7.9	Send control command (command code 0x0F).....	94
16.7.10	Control command received (command code 0x0F).....	94
16.8	Attributes and control commands under each cluster.....	95
16.8.1	(BASIC Cluster = 0x0000).....	95
16.8.2	Device Tag Cluster (IDENTIFY Cluster = 0x0003).....	96
16.8.3	Group Management Cluster (GROUP Cluster = 0x0004).....	97
16.8.4	Scene Management Cluster (SCENES Cluster = 0x0005).....	98
16.8.5	Switch on-off control cluster (ON_OFF cluster = 0x0006).....	101
16.8.6	Level control cluster (LEVEL cluster = 0x0008).....	101
16.8.7	Data transmission control cluster (Cluster = 0xFC08 / manuCode=0x2000).....	102
17	Module Network Distribution & Identification in HEX Command Mode	103
	17.1 The first step is to set the device type of the module:.....	103
17.1.1	Modul reset.....	104
17.1.2	Configure module A as the coordinator.....	104
17.1.3	Configure module B as a non-sleeping endpoint.....	104
17.1.4	Configure module B as a router.....	104
17.2	Second step: Module connected to network.....	105
17.2.1	Module A starts to configure the network and module A successfully establishes the network	105
17.2.2	Module B starts to configure the network, and module B joins the network.	106
17.2.3	Module A detects that module B is connected to the network.	106
17.3	The third step is to identify the network access node:.....	108
18	Zigbee 3.0 Module Three Types of Serial Mode Switch	113
18.1	Query Current Mode and distribution network status	114
18.2	Mutual Switch between three modes.....	115
18.2.1	HEX Command Mode to Transparent Transmission Mode	115
18.2.2	HEX Command Mode to AT Command Mode (for E180ZG120 only).....	115
18.2.3	AT Command Mode to Transparent Transmission Mode (for E180ZG120A/B only)	115
18.2.4	AT Command Mode to HEX Command Mode (for E180ZG120A/B only).....	115
18.2.5	Transparent Transmission Mode to HEX Command Mode	115
18.2.6	Transparent Transmission Mode to AT Command Mode (for E180ZG120A/B only)	116
19	Range considerations	116
20	Cleaning and care.....	116
21	Disposal.....	117

22 Declaration of Conformity (DOC)..... 117

23 Technical data..... 118

23.1 Power supply 118

23.2 RTU W/ 2 DI, 2 DO 118

23.3 Configuration software..... 118

23.4 Other 118

23.5 Ambient conditions..... 118

2 Introduction

Thank you for purchasing this product.

If there are any technical questions, please contact: www.conrad.com/contact

3 Operating Instructions for download



Use the link www.conrad.com/downloads (alternatively scan the QR code) to download the complete operating instructions (or new/current versions if available) and other supporting documents.

4 Intended use

The “RS485 - Zigbee® 3.0 Transceiver” is designed for wireless transmission of RS485 signals based on the Zigbee® 3.0 protocol. It enables the creation of wireless networks for transmitting control and measurement data with a range of up to 1.2 kilometres.

The product supports various network topologies, offering high flexibility for system integration. It ensures compatibility with ZHA (Zigbee® Home Automation) and ZLL (Zigbee® Light Link) network protocols as well as other compliant Zigbee® protocols.

The product is intended for indoor use only. Do not use it outdoors. Contact with moisture must be avoided under all circumstances.

Using the product for purposes other than those described above may damage the product. Improper use can result in short circuits, fires, or other hazards.

This product complies with statutory national and European regulations. For safety and approval purposes, you must not rebuild and/or modify the product.

Read the operating instructions carefully and store them in a safe place. Always provide these operating instructions when giving the product to a third party.

All company and product names contained herein are trademarks of their respective owners. All rights reserved.

Zigbee® is a registered trademark of the Connectivity Standards Alliance.

5 Features and functions

- **Centralised network management:** Zigbee® 3.0 security standard with a centralised network access mechanism for high data security and reliability.
- **Interoperability:** Compatible with the Zigbee® 3.0 standard network mechanism and ZCL network protocol.
- **Role switching:** Users can flexibly switch the device between coordinator, router, and end-device roles via serial port commands.
- **Support for multiple network topologies:** Point-to-point, star and mesh networks.
- **Network self-healing:** In case of a failure of an intermediate node, a new mesh topology is automatically formed. The failed node is automatically reintegrated into the network upon restart.
- **Automatic retransmission:** In on-demand mode (unicast), failed transmissions to the next node are automatically retried (up to 2 retries per message).

- **Automatic routing:** The module supports network routing, where routers and coordinators manage data forwarding to enable multi-hop connectivity.
- **Network open/close control:** The coordinator manages the opening and closing of the network. Devices compliant with Zigbee® 3.0 can join while the network is open. After closing, no further devices can join. If not explicitly closed, the network automatically closes after 180 seconds.
- **One-click network joining:** Nodes require no PAN-ID or channel configuration and only need to trigger network joining within the coordinator's open window.
- **Automatic channel and PAN-ID:** The coordinator automatically creates a network on the optimal channel and assigns a PAN-ID to avoid conflicts with other coordinators.
- **Automatic MAC address detection:** The coordinator captures the MAC address and short address of a node upon joining, without additional processing on the device side.
- **Diverse data communication:** Supports network-wide broadcast, multicast and on demand (unicast) functions, with various transmission modes in broadcast and on-demand settings.
- **Address lookup:** Users can retrieve the corresponding short address of a joined node using its unique, fixed MAC address or determine the corresponding long address of any node in the network based on its short address.
- **Data security:** Incorporates Zigbee® 3.0 secure communication standards with multi-level security keys in the network.
- **Channel switching:** Supports 16 channels (11 to 26, 2405 – 2480 MHz), each corresponding to a specific frequency band.
- **Network PAN-ID modification:** Flexible PAN-ID changes are possible, allowing users to specify a PAN-ID for joining a specific network or use automatic PAN-ID selection for network joining.
- **Serial interface configuration:** The module features built-in serial port commands that enable users to configure and view its parameters and functions.
- **One-key baud rate recovery:** If the current baud rate of the wireless module is lost, it can be reset to 115200 baud using the SMART button.
- **Baud rate adjustment:** Users can set the serial interface baud rate (up to 115200 baud).
- **Default settings:** 8 data bits, 1 stop bit, no parity.
- **Module reset:** The module can be reset via the serial interface.
- **Factory reset:** Possible via the serial interface or the SMART button.
- **Over-the-air configuration:** Users can remotely configure other devices on the network.
- **Multiple command formats:** Supports hexadecimal and AT commands for module configuration and control, network setup, transparent transmission, lighting control and other operations.
- **Holder of a national invention patent certificate:** Invention title: A Zigbee® 3.0-based method for connecting wireless transparent transmission modules. Patent number: ZL 2019 1 1122430.X.

6 Delivery content

- RS485 - Zigbee® 3.0 Transceiver, 27 dB
- Antenna
- Operating instructions

7 Description of symbols

The following symbols are on the product/appliance or are used in the text:



The symbol warns of hazards that can lead to personal injury.

8 Safety instructions



Read the operating instructions carefully and especially observe the safety information. If you do not follow the safety instructions and information on proper handling in this manual, we assume no liability for any resulting personal injury or damage to property. Such cases will invalidate the warranty/guarantee.

8.1 General information

- The device is not a toy. Keep it out of the reach of children and pets.
- Do not leave packaging material lying around carelessly. This may become dangerous playing material for children.
- If you have questions which remain unanswered by these operating instructions, contact our technical support service or other technical personnel.
- Maintenance, modifications and repairs must only be completed by a technician or an authorised repair centre.

8.2 Handling

- Please handle the product carefully. Jolts, impacts or a fall even from a low height can damage the product.

8.3 Operating environment

- Do not place the product under any mechanical stress.
- Protect the appliance from extreme temperatures, strong jolts, flammable gases, steam and solvents.
- Protect the product from high humidity and moisture.
- Protect the product from direct sunlight.
- Never operate the product in direct proximity of strong magnetic or electromagnetic fields or transmitter aerials or HF generators. Doing so can prevent the product from functioning properly.

8.4 Operation

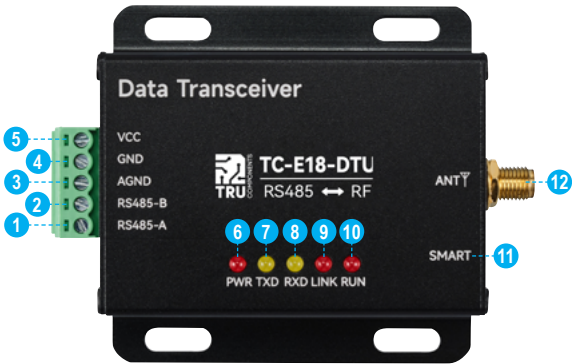
- Consult an expert when in doubt about the operation, safety or connection of the appliance.
- If it is no longer possible to operate the product safely, take it out of operation and protect it from any accidental use. DO NOT attempt to repair the product yourself. Safe operation can no longer be guaranteed if the product:
 - is visibly damaged,
 - is no longer working properly,
 - has been stored for extended periods in poor ambient conditions or
 - has been subjected to any serious transport-related stresses.

8.5 Connected devices

Always observe the safety information and operating instructions of other devices connected to the product.

9 Product overview

9.1 Interface Description



Number	Name	Function	Illustrate
5	VCC	Crimp type power interface, positive pole	DC 8 - 28 V/DC, 12 V/DC or 24 V/DC is recommended
4	GND	Crimp type power interface, negative pole	The negative pole of the power supply is connected to the system ground and the shell
3	AGND	Common ground interface	It can be connected to the ground terminal of external equipment, or it can not be processed
2	RS485-B	Serial terminal	Connect to the B terminal of other RS485 devices
1	RS485-A	Serial terminal	Connect to the A terminal of other RS485 devices
12	Antenna connector	SMA-K interface	External thread and inner hole, length 8 mm, characteristic impedance 50 Ω

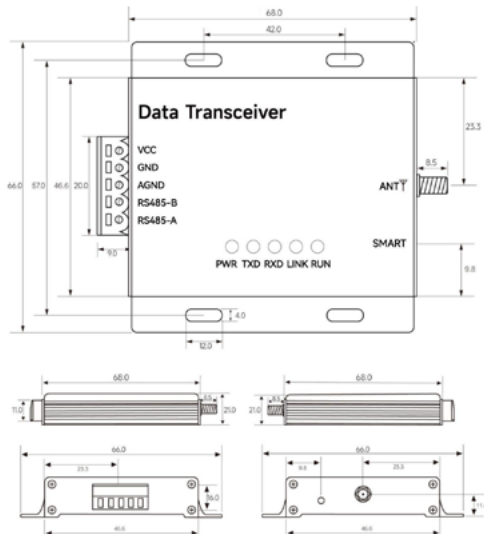
9.2 Indicator light description

Number	Name	Function	Instructions
6	PWR-LED	Power Indicator	Red, always on when the power is on
7	TXD-LED	Send Light	Yellow, blinking when sending data
8	RXD-LED	Receive indicator	Yellow, blinking when receiving data

Number	Name	Radio status	LED status	Remark
9	LINK-LED	Not networked	turn off	
		Network provisioning - the coordinator or router opens the network	1 Hz flickering	
		Network provisioning - a router or terminal that is not connected to the network joins the network	10 Hz flashing	
		The router or terminal network joins successfully	2 Hz flashes for 3 seconds and then stays on	
		The network connection is normal	always on	
		Network establishment/join failure	Turn off	
			5 Hz flashing, 3 times per second	
Number	Name	Function	LED status	Remark
10	RUN-LED	Automatic pairing mode	1 Hz flickering	
		Reset	Always on	"SMART" button long press 5 sec.
		Serial port baud rate recovery	Off → On → Off	For details, see the description of SMART button functions.
			Turn off	

Number	Name	Station status	Function	Button action	LED status
11	SMART (Button)	The coordinator did not create the network	The coordinator creates the network	Short press	LINK light flashes at 10 Hz
		The coordinator has created the network	Coordinator Open Network	Short press	LINK light flashes at 1 Hz
		The router/terminal is not configured with a network	Start to configure the network	Short press	LINK light flashes at 10 Hz
		The router/terminal has been configured with a network	The router/terminal has been configured with a network	Long press for 5 seconds	The RUN light is always on
			Clear the network (exit the current network)	Long press for 5 seconds	The RUN light is always on
		The router/terminal is not configured with a network	Restore Factory	Long press for 5 seconds	The RUN light is always on
		Any state	Serial port baud rate recovery 115200 baud	Press button "SMART" while the radio is powered on, wait for 5 seconds, and release the SMART button after the RUN light is on.	RUN light: off→on→off

9.3 Product size



Unit : mm
Tolerance value: X.X±0.2mm

10 Interface Definition

Users need to use the VCC terminal (1) and GND terminal in (2) to supply power. RS485 - Zigbee® 3.0 Transceiver can use 8 - 28 V/DC power supply, and 12 V or 24 V/DC power supply is recommended.



When the radio is connected to multiple devices, the communication is not smooth, but there is no such phenomenon with a single device, please try to connect a 120 Ω resistor in parallel between the 485_A terminal and the 485_B terminal.

11 Working Mode

11.1 Transmission mode

When the module enters the transmission mode, any data received by the serial port will be sent out wirelessly. The transmission mode is wireless communication between network nodes. The communication methods include unicast, broadcast, multicast, etc..

There are 4 transmission modes:

1. The first is normal transmission. In this mode, "OK" will be returned if the transmission is successful, and errors such as "ERROR" or "FAIL" or "BUSY" will be returned if the transmission is lost or data error occurs. There is a system logo output when the module is disconnected or abnormal.
2. The second is no response transmission, in which there is no message returned when the transmission is successful, but when there is failure or error in the transmission, or the module is offline, an error reminder will be printed.
3. The third is no Printing mode, the module will send any data received by the serial port to the designated target when the connection is normal, and the module will not return any message when the transmission fails or the module is abnormal.
4. The fourth is the Modbus host mode, in which the first byte of the data frame received by the module serial port is ModbusID, and there will be no normal or abnormal print messages during transmission. In this mode, the ModbusID of the slave needs to be set, and the slave needs to be bound to the master. This mode is recommended used on coordinator or router only.

11.2 HEX command mode (configuration mode)

When the module enters the HEX command mode, the data received by the serial port defaults to the HEX command. If the serial port data sent does not conform to the HEX command format, it will be automatically filtered out by the device as a HEX command in the wrong format. In the HEX command mode, the data received by the module serial port is considered as HEX command.

11.3 Mode switching

The power-on initialization of the module defaults to the HEX command mode.

Switch from HEX command mode (configuration mode) to transmission mode:

When the module serial port receives the HEX format command "55 07 00 11 00 03 00 01 13", the module enters the normal transmission mode, and returns the

HEX format command "55 04 00 11 00 11" after entering the transmission mode successfully.

If you need to enter the no-response transmission mode, enter the HEX format command

"55 07 00 11 00 03 00 02 10". For no printing mode, enter the HEX format command

"55 07 00 11 00 03 00 03 11".

For the Modbus host mode, enter the HEX format command "55 07 00 11 00 03 00 04 16".

Switch the transmission mode to HEX command mode (configuration mode):

In the transmission mode, when the serial port of the module receives the "+++" character, it enters the configuration mode, and returns the system notification command "device start" after successfully entering the configuration mode.

11.4 Related parameters in transmission mode

The below parameters can be read and set through the HEX commands "read local attribute" and "set local attribute". The below parameters of the module can be read and modified remotely through the HEX command "ZCL command - read device attribute" and "ZCL command - modify device attribute". Note that remote modification is limited to items with "W" in "Operation".

AttrID	Descriptor	Name	Type of data	Operation	Initial value
0x0000	Baud	baud rate	uint32	R	115200 (decimal)
0x0001	Target Addr	Transparent transmission target short address	uint16	RW	0xFFFF
0x0002	Target EP	Transparent transmission target port	uint8	RW	0xFF or 255
0x0003	Send Mode	Transparent mode	bool	RWP	0
0x0004	LP Level	Low power mode	enum8	RP	0
0x0006	Modbus ID	Modbus number	uint8	RWP	0xFF
0x0010	User Attr 0	User-defined variable 0	uint32	RW	0x00000000
0x0011	User Attr 1	User-defined variable 1	uint16	RW	0x0000
0x0012	User Attr 2	User-defined variable 2	uint8	RW	0x00
0x0013	User Attr 3	User-defined variable 3	uint8	RW	0x00

This parameter to set or query the current baud rate of the module.

targetAddr: The target address in the transmission mode, 0xFFFF is broadcast transmission, and 0xFFFE is sent to the binding target MAC.

targetEP: The target port in the transmission mode, set the value to 0xFF for broadcast sending or binding sending, set it to 0x01 for sending to the specified target short address, and set it to 0x00 for multicast sending.

send Mode: Transmission mode setting, 0 - HEX command mode, 1 - normal transmission mode, 2 - no response mode, 3 - no printing mode, 4 - Modbus host mode.

target IEEE: Bind the target MAC, this item is only for viewing. The module can bind multiple target MACs, and the heartbeat packet will be sent to all bound MACs in turn, but in the transmission mode, only the data is sent to the last binding target in the binding table.

Modbus ID: The module will send this parameter to the coordinator and the bound target MAC in the form of a heartbeat packet (once every 300 seconds). If the target device is a Modbus master, the Modbus master can find the Zigbee® network address of the slave according to the Modbus ID of the slave.

User-defined variables: There are one 32bit, one 16bit, and two 8bit, total 4 user-defined variables. These values can be set and queried through "Read Local Attributes" and "Set Local Attributes", remote setting and query are also supported to facilitate the status management of the module.

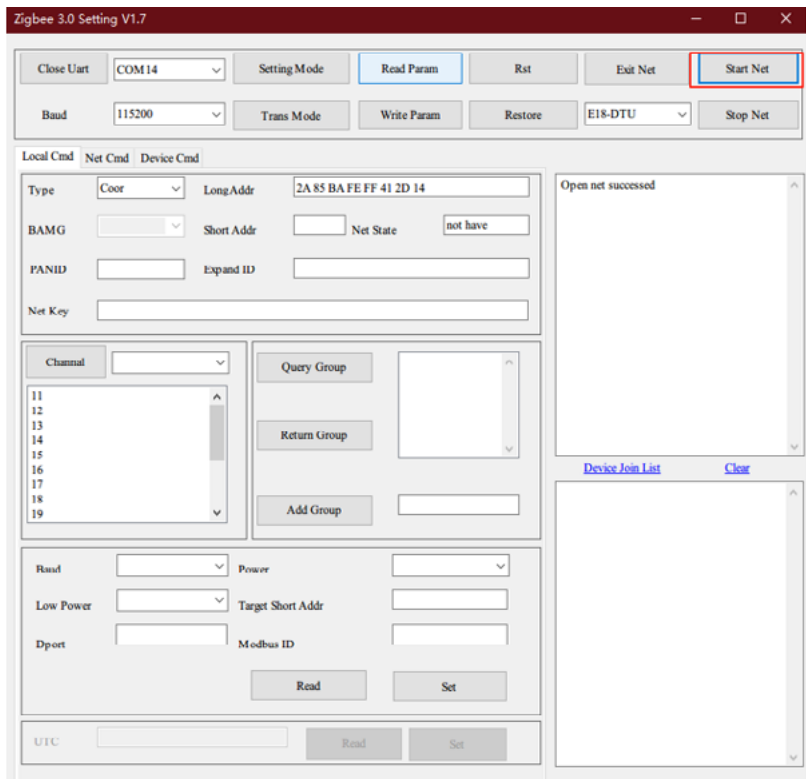
12 Quick Start

In order to allow users to quickly familiarize themselves with the radio, this section will guide users to build a ZigBee® network through simple configuration with the host computer, including node type configuration, PAN-ID setting, channel setting, and transmit power setting.

12.1 Quickly build a ZigBee® network

Combined with the host computer software to quickly and easily establish a ZigBee® network, the specific steps are as follows:

1. Connect the radio to the computer, open the host computer software “ZigBee® 3.0 Setting”, select the device type (1), select the serial port number (2), select the serial port baud rate (3) (default 115200), and click to “Open Uart” (4).



2. The module leaves the factory in HEX command configuration mode, click “Read Param”, the message box prompts “Read succeed”, the main network parameters include: long address, the default radio type is coordinator (if not, please set it to Coordinator), the network status is “not have” (if it is not, pls exit the network or restore the factory). If failing to read parameters, it is possible that the module is currently in transmission mode, and you need to click “Setting mode”, and a message box will prompt “Enter Configuration Status Successfully”.

The screenshot shows the 'Zigbee 3.0 Setting V1.7' application window. At the top, there are buttons for 'Close Uart', 'Setting Mode', 'Read Param' (highlighted with a red box), 'Rst', 'Exit Net', and 'Start Net'. Below these are 'Baud' (set to 115200), 'Trans Mode', 'Write Param', 'Restore', 'E18-DTU', and 'Stop Net'. The main area has tabs for 'Local Cmd', 'Net Cmd', and 'Device Cmd'. Under 'Local Cmd', there are fields for 'Type' (set to 'Coor'), 'Long Addr' (2A 85 BA FE FF 41 2D 14), 'BAMG', 'Short Addr' (00 00), 'Net State' (connect), 'PANID' (13 D4), 'Expand ID' (44 E1 A0 40 80 69 BB 1F), and 'Net Key' (0C CF B7 46 CF 9A CC 1B AD 3E F4 BC 9F 7E 58 D7). Below this is a 'Channel' dropdown (set to 0B) and a list of channels from 11 to 19. To the right of the channel list are buttons for 'Query Group', 'Return Group', and 'Add Group'. At the bottom of the main area are fields for 'Baud', 'Power', 'Low Power', 'Target Short Addr', 'Dport', and 'Modbus ID', with 'Read' and 'Set' buttons. At the very bottom is a 'UTC' field with 'Read' and 'Set' buttons. On the right side of the window, there are two large empty text areas, one with a 'Device Join List' link and a 'Clear' button.

3. Click "Start Net" to coordinate and establish an open network. After the coordinator creates a new network, it will continue to open the network for 180 seconds. The LINK light flashes at 1Hz. Routers and terminals can join the network within this time.

Zigbee 3.0 Setting V1.7

Close Uart: COM14 Setting Mode: Read Param Rst Exit Net **Start Net**

Baud: 115200 Trans Mode: Write Param Restore E18-DTU Stop Net

Local Cmd Net Cmd Device Cmd

Type: Coor LongAddr: 2A85BAFEFF412D14

BAMG: Short Addr: Net State: not have

PANID: Expand ID: Net Key:

Channel: Query Group: Return Group: Add Group:

Baud: Power: Low Power: Target Short Addr: Dport: Modbus ID: Read Set

UTC: Read Set

Open net succeeded

[Device Join List](#) [Clear](#)

12.2 Quickly join a ZigBee® network

1. Open the host computer software "ZigBee® 3.0 Setting", select the device type (1), select the serial port number (2), select the serial port baud rate (3) (default 115200), click to "Open Uart" (4). Then set the module type to "Router" or "Node" (5), then click "Write Param" (6), and then click "RST" (7), at this time the role of the device is switched successfully.

The screenshot shows the 'Zigbee 3.0 Setting V1.7' window. The interface includes several sections with numbered annotations:

- Top Bar:** Contains buttons for 'Close Uart' (4), 'COM14' (2), 'Setting Mode', 'Read Param', 'Rst' (7), 'Exit Net', 'Start Net', 'Baud' (3), '115200', 'Trans Mode', 'Write Param' (6), 'Restore', 'E18-DTU' (1), and 'Stop Net'.
- Local Cmd Section:** Includes tabs for 'Local Cmd', 'Net Cmd', and 'Device Cmd'. The 'Device Cmd' tab is active, showing fields for 'Type' (5) set to 'node', 'Long Addr' (2A 85 BA FE FF 41 2D 14), 'BAMG', 'Short Addr', 'Net State' (not have), 'PANID', 'Expand ID', and 'Net Key'.
- Channel Section:** A list of channels from 11 to 19.
- Query Group Section:** Includes 'Query Group', 'Return Group', and 'Add Group' buttons.
- Bottom Section:** Includes fields for 'Baud', 'Power', 'Low Power', 'Target Short Addr', 'Dport', 'Modbus ID', and buttons for 'Read' and 'Set'.
- UTC Section:** Includes a 'UTC' field and 'Read' and 'Set' buttons.

On the right side, there are two large text areas. The top one is labeled 'Device Join List' and the bottom one is labeled 'Clear'.

- Click "Start Net", and the LINK light of the DTU device flashes rapidly at 10Hz. At this time, it is necessary to ensure that the coordinator device is also in the "Start Net" state (see section 12.1). Wait for a while, the LINK light of the DTU becomes solid or flashes at 1Hz (router mode), click "Read Param", you can view the network access information of the device, and the "Net state" is "connect". If the LINK light turns off and the network status is "not have", the module fails to add the network, please check whether the coordinator device is in the "Start Net" state, and whether the distance between the coordinator device and the router/node is within a reasonable range.

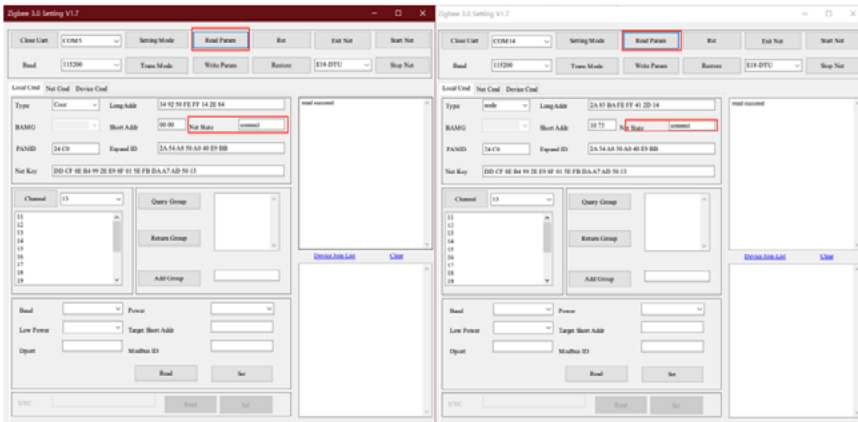
The screenshot shows the 'Zigbee 3.0 Setting V1.7' window. At the top, there are buttons for 'Close Uart', 'Setting Mode', 'Read Param', 'Rst', 'Exit Net', and 'Start Net' (highlighted with a red box). Below these are 'Baud' (115200), 'Trans Mode', 'Write Param', 'Restore', 'E18-DTU', and 'Stop Net'. The main area has tabs for 'Local Cmd', 'Net Cmd', and 'Device Cmd'. Under 'Net Cmd', there are fields for 'Type' (node), 'Long Addr' (2A 85 BA FE FF 41 2D 14), 'BAMG', 'Short Addr' (10 75), 'PANID' (24 C0), 'Expand ID' (2A 54 A8 50 A0 40 E9 BB), and 'Net Key' (DD CF 8E B4 99 2E E9 8F 01 5E FB DAA7AD 50 13). The 'Net State' is set to 'connect' (highlighted with a red box). Below this are 'Channel' (13), 'Query Group', 'Return Group', and 'Add Group' buttons. At the bottom, there are fields for 'Baud', 'Power', 'Low Power', 'Target Short Addr', 'Dport', and 'Modbus ID', along with 'Read' and 'Set' buttons. A 'UTC' field is also present at the very bottom.

Precautions:

For routers or terminal nodes that have joined the network, if they need to switch to the network established by other coordinators, they need to operate "Exit Net" or "Restore", and then follow the process of 12.2 to set up again. Similarly, if a router that has joined the network needs to be changed to an end node, or an end node that has joined the network needs to be changed to a router, the operation of "Exit Net" or "Restore" is also required.

12.3 Data transmission

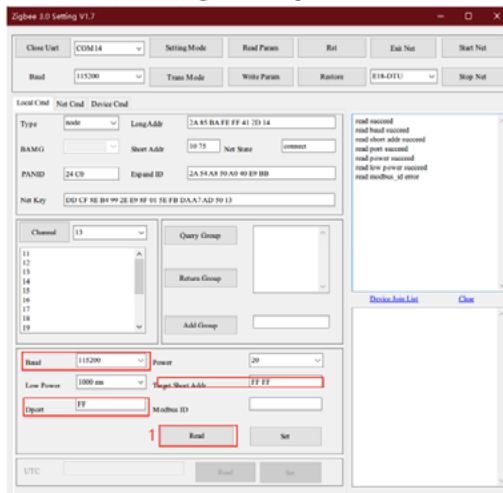
- Open the host computer software of the coordinator device and the network-connected device, click "Read Param", and confirm that the current "Net State" of the device is "connect", indicating that the device has been networked.



Coordinator device

Router device

- Click "read" to query the serial port configuration parameters of the device. The default serial port baud rate of the device is 115200, the short address of the transparent transmission target is 0xFFFF, and the target port is 0xFF (ie. 255), that is, the device defaults to broadcasting in the transparent transmission mode.



- Then set the router device to transparently transmit data to the coordinator device in the form of on-demand, and the coordinator device uses broadcast mode to transparently transmit data. In the host computer interface of the router device, set the target short address to 00 00 (that is, 0x0000), set the target port to 01 (that is, 0x01 or 1), and then click "set". After setting, you can click "read" again to confirm whether the setting is successful.

Zigbee 3.0 Setting V1.7

Close Uart: COM14 Setting Mode Read Param Rst Exit Net Start Net

Baud: 115200 Trans Mode Write Param Restore E18-DTU Stop Net

Local Cmd Net Cmd Device Cmd

Type: node LongAddr: 2A 85 BA FE FF 41 2D 14

BAMG: Short Addr: 10 75 Net State: connect

PANID: 24 C0 Expand ID: 2A 54 A8 50 A0 40 E9 BB

Net Key: DD CF 8E B4 99 2E E9 8F 01 5E FB DAA7 AD 50 13

Channel: 13

Query Group

Return Group

Add Group

Baud: 115200 Power: 20

Low Power: 1000 ms Target Short Addr: 00 00 **1**

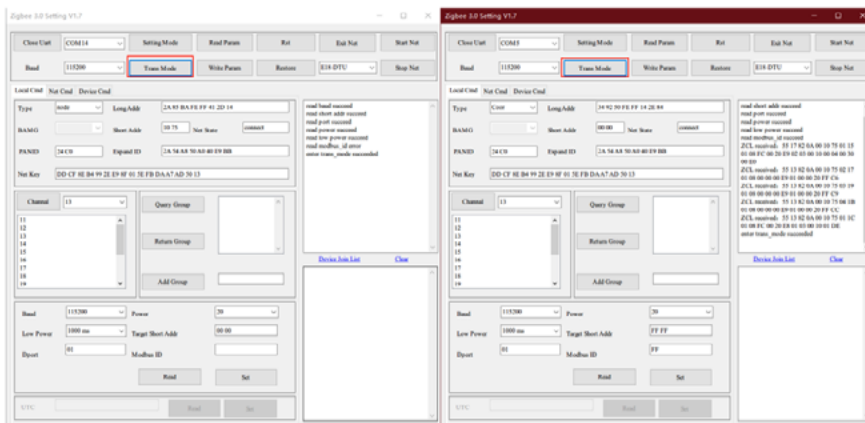
Dport: 01 **2** Modbus ID: **4** Read **3** Set

UTC: Read Set

read succeed
read baud succeed
read short addr succeed
read port succeed
read low power succeed
read modbus_id error

Device Join List Clear

- Enter the transparent transmission mode. After clicking "Trans mode" on the host computer interface of the coordinator device and the router device, both can enter the transparent transmission mode. One serial port inputs any data, and the other serial port can completely output the same data.



Router device

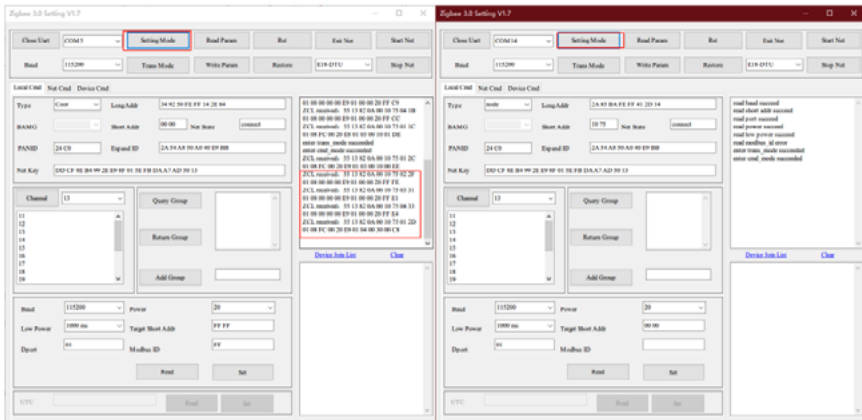
Coordinator device

After entering the transparent transmission mode, close the host computer configuration software and open the serial port assistant. Input any data on either side, the other side will output the same data. The party that sends data will return "OK" after sending data each time, indicating that the sending is successful, while return "FAIL" or "ERROR" is to indicate failing to send.

12.4 Data transmission between network nodes

The coordinator of the ZigBee® 3.0 data transmission module needs to undertake the network management function. If it works in the transparent transmission mode, it may miss important messages related to network changes. Therefore, we recommend that the coordinator work in the HEX command configuration mode when adding a large number of network nodes, and assign network nodes to transmit data between each other.

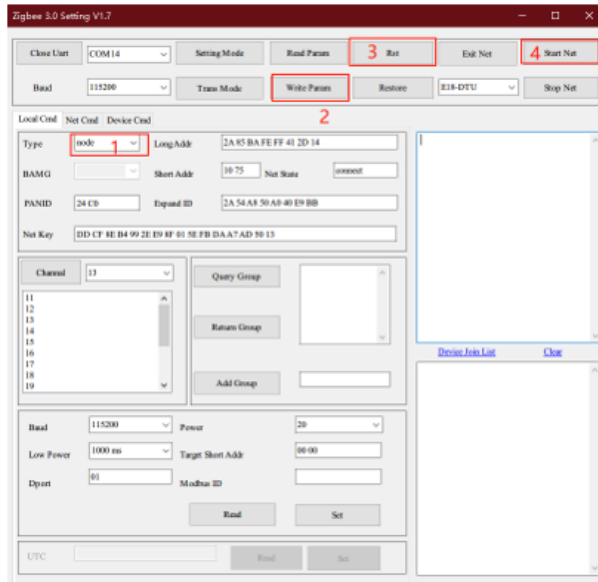
1. Click "Setting mode" in the host computer interface, and the coordinator device and router device will return to the configuration mode. After the coordinator returns to the configuration mode, it will receive the heartbeat packets periodically reported by the network-connected devices.



Coordinator device

Router device

2. The coordinator adds several network access nodes, sets a new device as a “node”, clicks “write Param” → “RST”, and adds the terminal node device to the coordinator device network (see Section 10.3).



3. The new node device is successfully configured and connected to the network. Click "read Param" and check that the "Net State" is "connect", indicating that the terminal node device has joined the coordinator device network.

Zigbee 3.0 Setting V1.7

Close Uart COM14 Setting Mode **Read Param** Rst Exit Net Start Net

Baud 115200 Trans Mode Write Param Restore E18-DTU Stop Net

Local Cmd Net Cmd Device Cmd

Type node Long Addr 2A 85 BA FE FF 41 2D 14

BAMG Short Addr 10 75 **Net State connect**

PANID 24 C0 Expand ID 2A 54 A8 50 A0 40 E9 BB

Net Key DD CF 8E B4 99 2E E9 8F 01 5E FB DA A7 AD 50 13

Channel 13

Query Group

Return Group

Add Group

Baud 115200 Power 20

Low Power 1000 ms Target Short Addr 00 00

Dport 01 Modbus ID

Read Set

UTC Read Set

read succeed

Device Join List Clear

4. On the host computer interface of the terminal device, set the "target short addr" to "4B 9C" and "DPORT" to "01" (Router's short address and end-point), click "set". Then enter "01 00" in "Add Group", click "Add Group", add the terminal device to 0x0001 group , and then click "Trans mode".

Zigbee 3.0 Setting V1.7

Close Uart COM14 Setting Mode Read Param Rst Exit Net Start Net

Baud 115200 7 Trans Mode Write Param Restore E18-DTU Stop Net

Local Cmd Net Cmd Device Cmd

Type node LongAddr 2A 85 BA FE FF 41 2D 14

BAMG Short Addr 10 75 Net State connect

PANID 24 C0 Expand ID 2A 54 A8 50 A0 40 E9 BB

Net Key DD CF 8E B4 99 2E E9 8F 01 5E FB DAA 7AD 50 13

Channel 13

Query Group 01 00

Return Group

6 Add Group 01 00 5

Baud 115200 Power 20

Low Power 1000 ms Target Short Addr 4B 9C 2

Dport 01 3 Modbus ID

Read 4 Set

UTC Read Set

enter cmd_mode succeeded
read succeed

Device Join List Clear

- On the host computer interface of the router device, set the "DPORT" to "00" (the target port is set to 0x00, which means multicast mode), and then set the target short address to "01 00" (the target short address in multicast mode is Multicast address, here multicast to group 0x0001), click "set", the router will send transparent transmission packets to group 0x0001 multicast. Then click "Trans mode".

Through the above configuration, the router device and the terminal device can transmit data to each other, and the coordinator no longer receives the data transmitted by them. The coordinator can add more devices and set them up to communicate with each other.

13 Sending and receiving methods

13.1 The way of sending data in transparent transmission mode

The data transmission mode in the transparent transmission mode includes broadcast, unicast, and multicast.

13.1.1 Broadcast mode

In broadcast mode, the sending device sends the data received by the serial port to every node in the network, and all devices in the network will receive the data.

13.1.2 Unicast mode

In unicast mode, the devices in the network communicate point-to-point through the network address, and the sending device sends the received serial port data to the target address device. In unicast mode, you can determine the transparent transmission target by setting the target short address and target port, or you can determine the transparent transmission target by setting the binding method.

13.1.3 Multicast mode

In the multicast mode, first set the group number (grouping) for the devices in the network, the sending device must specify the target group number, set the target short address and target port, and then the sending device sends the data received by the serial port to the network, devices with the same group number in the network will receive the data.

13.2 The way of sending data in HEX command mode

In the HEX command mode, any message (including transparent transmission data message, ZigBee® control command, and other manufacturer's ZigBee® device command) can be sent to the specified target device (unicast, multicast, broadcast), and the sending format can be found in ZigBee® 3.0 Module HEX Command Standard Specification".

14 Application Function

14.1 Function

14.1.1 Detailed explanation of LINK light

The LINK light is used to indicate the current network status of the module. After the device is successfully connected to the network, the LINK light is always on, and when the device has no network, the LINK light is off. In the coordinator mode, this pin indicates whether the module has established a network normally, and the LINK light of coordinator and router flashes at 1 Hz during

"OPEN net". In the router/terminal node mode, the device enters the configure network mode, and the LINK light flashes at a frequency of 10 Hz. After successfully connecting to the network, the LINK light will flash 6 times at 3 Hz. If the router is successfully connected to the network for the first time, the LINK light will continue to 1 Hz blinking, indicating that the router can complete the relay function within the coverage of the coordinator, and the terminal node is always on. After the coordinator ends the open network, the LINK light of the router also keeps on. In the terminal node mode, if node is disconnected, the LINK light flashes 3 times per second at a continuous 5 Hz.

14.1.2 Detailed Explanation of RUN Light

The RUN light indicates the current working status of the device. The RUN light flashes at 1 Hz in the marking mode of the device, press and hold SMART for a long time or press and hold SMART after power on, the RUN light is on to indicate that the button is active, and then the button can be released.

14.1.3 Detailed explanation of SMART button

Short press: Short press for unnetworked devices to configure the network, and short press for the coordinator to open the network. The networked routers or terminal nodes establish point-to-point transmission with each other after a short press.

Long press: Long press SMART on routers or terminals to exit the network, and long press SMART on unnetworked devices to restore the factory. As the coordinator does not support long press to exit the network, you need to press and hold this button for 5 seconds until the RUN light turns on and then release it.

Baud rate reset: The baud rate is restored to 115200 baud: Power on the radio while holding down the SMART button until the RUN light is on and release it.

14.1.4 Automatic Pairing and Mark Adaptation (Identify) Mode

14.1.4.1 Mark Adaptation (Identify) mode

The Identify mode of ZigBee® is a special state of ZigBee® devices, and the ZigBee® devices which support the ZCL protocol is able to use this mode. The mark adaptation mode can be entered by the device itself (such as a key trigger), or other devices send ZCL commands (belonging to the ZCL-Identify command set) to it.

ZigBee® equipment mainly fulfils the following two purposes under mark adaptation:

1. **Used to indicate its own installation position to the operator's:**

The ZigBee® device enters the mark adaptation mode after receiving the mark adaptation command (ZCL command), and can expose its installation position through LED flashing or buzzer, motor and other peripherals, so that users can find the device conveniently.

2. **For discovery or device binding between devices:**

The ZigBee® device receives the mark adaptation command (ZCL command) or actively triggers to enter the adaptation mode and other devices in the same network can broadcast and query (ZCL command) which devices are in the mark adaptation state. Then you can automatically bind the devices in the mark adaptation state, or perform a unified grouping operation on them.

Note:

There is a timeout period for the device to enter the mark adaptation state. Usually, the local trigger enters the mark adaptation mode by default 180 seconds, and the timeout period is determined by the command initiator if using the ZCL command control enters the mark adaptation mode. The mark adaptation state can be terminated prematurely in either way.

14.1.4.2 Automatic pairing

After pressing the Smart button, the DTU that has already configured the network will enter the mark adaptation mode, and at the same time it will look for other DTUs that are also in the mark adaptation mode. Then establish a point-to-point direct connection relationship with other DTUs through MAC address binding (SN number binding). This method is only applicable to routers and end nodes. The coordinator does not need to use this mode because it saves the MAC addresses of all network-connected devices. If there is a DTU and other ZigBee® devices in the mark adaptation mode at the same time in the network, the paired DTU will filter the DTU device through the cluster (cluster ID) of the device.

14.2 Wireless remote configuration function

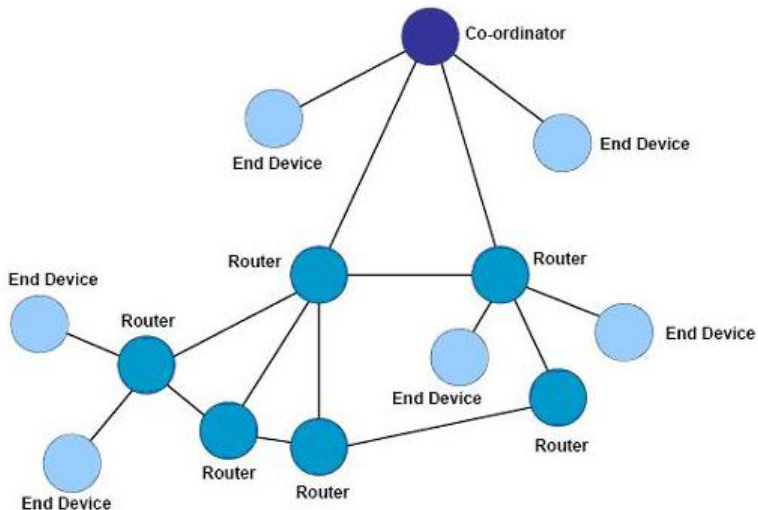
The module supports remote configuration function, use the ZCL protocol to configure the Attribute under cluster 0xFC08 (need to cooperate with Manufacture Code 0x2000), which can be modified.

AttrID	Descriptor	Name	Type of data	Operation	Initial value
0x0000	Baud	Baud rate	uint32	R	115200 (decimal)
0x0001	Target Addr	Transparent transmission target short address	uint16	RW	0xFFFF
0x0002	Target EP	Transparent transmission target port	uint8	RW	0xFF or 255
0x0003	Send Mode	Transparent mode	bool	RWP	0
0x0004	LP Level	Low power mode	enum8	RP	0
0x0006	Modbus ID	Modbus number	uint8	RWP	0xFF
0x0010	User Attr 0	User-defined variable 0	uint32	RW	0x00000000
0x0011	User Attr 1	User-defined variable 1	uint16	RW	0x0000
0x0012	User Attr 2	User-defined variable 2	uint8	RW	0x00
0x0013	User Attr 3	User-defined variable 3	uint8	RW	0x00

15 Network structure

The network structure of this module is a mesh network structure (MESH).

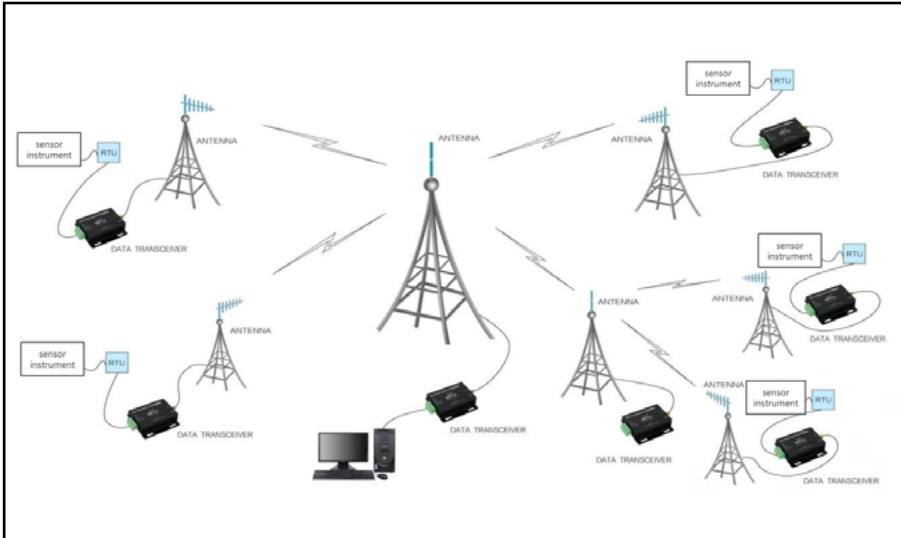
The network of MESH mesh network topology has powerful functions, and the network can communicate through "multi-level jumps". This topology can also form an extremely complex network. The network also has self-organizing and self-healing functions.



15.1 Practical Application Fields

RS485 - Zigbee® 3.0 Transceiver, 27 dB digital radio is suitable for all kinds of point-to-point and point-to-multipoint wireless data transmission systems, such as smart home, Internet of Things transformation, power load monitoring, distribution network automation, hydrology and water regime monitoring, tap water pipe network monitoring, urban street lights Monitoring, air defence alarm control, railway signal monitoring,

centralized control of railway water supply, oil and gas supply pipeline network monitoring, GPS positioning system, remote meter reading, electronic crane scale, automatic target reporting, earthquake forecasting, fire prevention and anti-theft, environmental monitoring and other industrial automation system, as shown below.



16 ZigBee® 3.0 serial port commands

16.1 Serial port format and mode configuration

16.1.1 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

16.1.2 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.

16.1.3 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.

16.1.4 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 200 us.

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 to 0x7F, and the range of asynchronous command is 0x80 to 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.

16.1.5 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

16.1.6 Command type and command code list

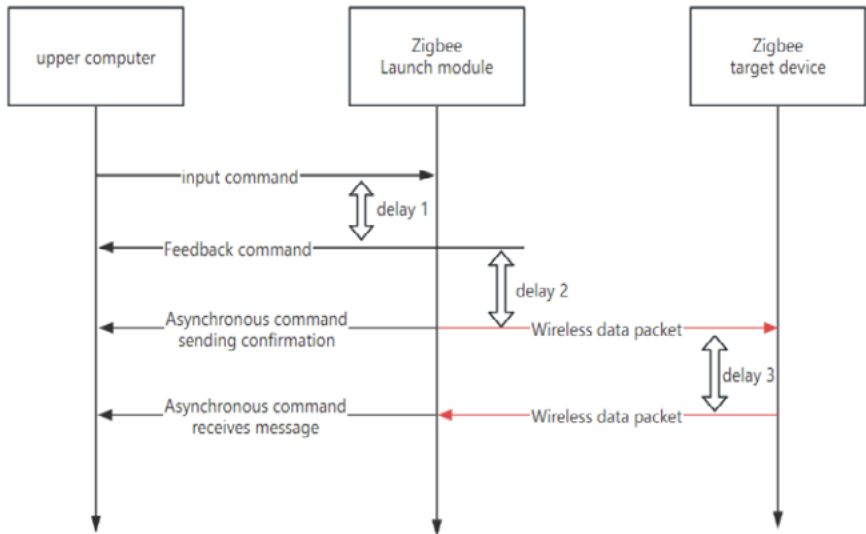
Command type list:

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
	0x82	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 pre-processed in the MCU of the module (encryption and cache query), and the average time is 2 to 5 milliseconds.

Among them, E72-2G4M20S1E has the fastest response, and the measured average is about 1.5 ms.

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 to 50 ms, 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 to 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.

16.1.7 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
0x02	CFG_OPEN_NET	Open network/start networking
0x03	CFG_CLOSE_NET	Turn off network/stop networking
0x04	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 PAN-ID
0x08	CFG_SET_PANID	Set PAN-ID
0x09	CFG_VIEW_GROUP	View local add group
0x0A	CFG_ADD_GROUP	Add the machine to the group
0x0B	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
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
0x22	CFG_GET_ADDRTAB	Read node address table
0x23	CFG_GET_KEYTAB	Read node key tab
0x28	CFG_EZ_MODE	Retransmit device information

Network management commands:

Command code	Descriptor	Command name
0x00	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_UNBIND_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
0x00	ZCL_READ_ATTR_REQ	Read device property parameters
0x01	ZCL_WRITE_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	NOTIFY_IDENTIFY	Mark mode

Network management back:

Command code	Descriptor	Command name
0x00	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_UNBIND_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
0x00	ZCL_READ_ATTR_RSP	Read device properties return
0x01	ZCL_WRITE_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
0x01	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 Silabs (E180-ZG120 series)	
0x03	Lookup table not found
0x18	Not enough cache
0x66	Failed to send data

16.1.8 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.

Note:

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

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.

PAN-ID (2 bytes):

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

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.

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.

Virtual device SN number:

The virtual device SN number is a device management mechanism 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 to 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.

16.2 Local command parsing

16.2.1 Local configuration commands

Uniform format for local configuration commands:

Field	Frame header	Frame size	Payload			
			Command types	Command code	Command data	Check code
Content	55		0	Please see below	Please see below	
Number of bytes	1	1	1	1	variable-length	1

16.2.1.1 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, PAN-ID, 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	PAN-ID	Short address	Extended PAN-ID	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.

PAN-ID: The current PAN-ID 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 PAN-ID: None when not networked

Network key: No 0 when not networked

16.2.1.2 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 start-up 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.

16.2.1.3 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 PAN-ID, channel, network key, and extended PAN-ID. 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 white list network distribution mode. In this mode, the coordinator blocks the devices whose MAC addresses are not in the white list and allows the devices in the white list 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.

16.2.1.4 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.

16.2.1.5 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.

PAN-ID: The current PAN-ID 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 PAN-ID 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.

16.2.1.6 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.

16.2.1.7 Query and set channel (command code 0x06)

Command code: 0x06

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.

16.2.1.8 Query PAN-ID (command code 0x07)

Command code: 0x07

Note:

Only E72-2G4M20S1E and E 18 series support.

Function:

Set the PAN-ID used for the module networking, the default is 0xFFFF for random mode.

Setting the PAN-ID 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 bytes	1	0

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 PAN-ID, the default value is 0xFFFF.

16.2.1.9 Set PAN-ID (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 PAN-ID. 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

PAN-ID: Default PAN-ID value.

Feedback command:

Field	Command code	Command data
Content	0x08	Status
Number of bytes	1	2

Status: 0 – setting valid, 1 – setting invalid.

16.2.1.10 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.

16.2.1.11 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.

16.2.1.12 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.

16.2.1.13 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. See [“16.2.2.9 Beacon scan notification \(command code 0x0C\)” on page 60](#).

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 $(2^{\text{Duration}}) * 15.36$ 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.

16.2.1.14 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.

16.2.1.15 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 [“ZCL attribute data type table” on page 80](#).

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.

16.2.1.16 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 [“Custom attributes \(execution side\)” on page 82](#).

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.

16.2.1.17 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.

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 custom attributes to become "true". See "[ZCL attribute data type table](#)" on page 80.

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.

16.2.1.18 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.

16.2.1.19 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.

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

Command code: 0x22

Note:

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 to 0x00FE are valid.

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

Feedback command:

Field	Command code	cmd 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).

16.2.1.21 Read access node key (0x23)

Command code: 0x23

Note:

E72-2G4M20S1E and E 180ZG120B support.

Function:

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

16.2.1.22 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" 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.

See ["16.2.2.6 Device information notification \(command code 0x05\)" on page 58](#).

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.)

16.2.1.23 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 to 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.

16.2.1.24 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.

16.2.1.25 Adding a whitelist record (0x29)

Command code: 0x29

Note:

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 white list can be added. You can add a white list only when the white list distribution network is enabled. After the network distribution mode ends, all the added white lists are cleared. You need to add them again when the white list distribution network is enabled next time.

Input the command:

Field	Command code	Command data
Content	0x29	White list record
Number of bytes	1	8

White list 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.

16.2.1.26 Lock Extended PAN-ID Networking (0x1A)

Command code: 0x1A

Note:

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 PAN-ID in 64 bit. The E180ZG120 module with the extended PAN-ID 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 PAN-ID. If the command is set to the extended PAN-ID 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 PAN-ID lock is cancelled.

Input the command:

Field	Command code	Command data	
Content	0x1A	Mode	Extended PAN-ID
Number of bytes	1	1	8

Mode: 0 - Queries the locked extension PAN-ID. 1- Sets the extension PAN-ID.

Extended PAN-ID: 8 byte Extended PAN-ID. This parameter is valid in set mode.

Feedback command:

Field	Command code	Command data	
Content	0x1A	Execution status	Extended PAN-ID
Number of bytes	1	1	8

Execution status: 0 - Valid, 0xFF – invalid.

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

16.2.2 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

16.2.2.1 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.

16.2.2.2 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 Status	MAC Address	Channel	PAN-ID	Short Address	Extended PAN-ID	Network 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.

PAN-ID: The current PAN-ID of the module, 0xFFFF when the networking fails.

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

Extended PAN-ID: All 0s when networking fails.

Network key: All 0s when networking fails.

16.2.2.3 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.

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

Command code: 0x03

Note:

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).

16.2.2.5 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.

16.2.2.6 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	Com- mand code	CMD data							
Content	0x01	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

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 [“5 Virtual device SN number:” on page 39](#).

Short address: Device short address.

Port number: The port number of the device. See [“4 Port:” on page 39](#).

Port profile: Profile ID, the application layer only needs to pay attention to 0x010. See [“Port Profile: \(Profile\)” on page 75](#)

Device ID: Indicates the function of the device, which is determined by the ZCL protocol specification. See [“Device ID table” on page 78](#)

Input cluster table: The input clusters supported by the device, including the number of clusters and the cluster list. See [“16.5.2.2 Cluster” on page 75](#) and [“16.5.2.3 Client and server” on page 75](#).

Output cluster table: The output clusters supported by the device, including the number of clusters and the list of clusters. See [“16.5.2.2 Cluster” on page 75](#) and [“16.5.2.3 Client and server” on page 75](#).

16.2.2.7 Module off-grid notification (command code 0x06)

Command code: 0x06

Note:

E72-2G4M20S1E and E 180ZG120 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.

16.2.2.8 Automatic binding target result notification (command code 0x10)

Command code: 0x10

Note:

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.

16.2.2.9 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 PAN-IDs and short addresses, and how strong the signal strength is. A termination signal command will be generated after the scan is over.

For details, see ["16.2.1.13 Channel scan test \(command code 0x0C\)" on page 46](#)

Asynchronous command:

Field	Command code	Cmd data					
Content	0x0C	Scan status	Channel	PANID	Short address	Extended PANID	Signal strength
Number of bytes	1	1	2ss	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.

PAN-ID: Scan to the PAN-ID 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 PAN-ID: The extended PAN-ID 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.

16.2.2.10 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.

16.2.2.11 Three debug messages:

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 address
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).

16.2.2.12 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 address	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).

See [“Port Profile: \(Profile\)” on page 75](#)

See [“16.5.2.1 Device ID” on page 75](#)

See [“16.5.2.2 Cluster” on page 75](#)

16.2.2.13 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 address	The port number	Binding cluster
Number of bytes	1	2	8	1	

For ports, see [“16.5.2.8 Often connected binding \(Bind\)” on page 76](#)

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

For binding, see [“16.5.2.8 Often connected binding \(Bind\)” on page 76](#)

For attributes, see [“16.5.2.5 Attribute” on page 75](#)

For input clusters, see [“16.5.2.2 Cluster” on page 75](#)

16.2.2.14 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 white list network distribution mode is enabled, the whitelist is not detected. Procedure this parameter can be used together with Adding a White list Record (2.1.26) to add a white list 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.

16.3 Network management commands (ZDO commands)

16.3.1 Introduction to ZDO Commands

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

- 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. For profiles, see [“Port Profile: \(Profile\)” on page 75](#).
- 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. For details, see [“Port Profile: \(Profile\)” on page 75](#), [“16.5.2.1 Device ID” on page 75](#), [“Port:” on page 39](#), [“16.5.2.2 Cluster” on page 75](#)
- 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, cancelling and viewing the binding relationship of each port on each node. For details, [“16.5.2.8 Often connected binding \(Bind\)” on page 76](#).

16.3.2 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.

16.3.2.1 Input command format

Input command format of network management commands.

Field	Frame header	Frame size	Payload				
			Command types	Command code	Command data		Check code
Content	0x55	Need to calculate	0x01	See Table 16.1	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 16.1 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

16.3.2.2 Feedback command format

Feedback command format for network management commands.

Field	Frame header	Frame size	Payload				
			Command types	Command code	Command data		Check code
Content	0x55	0x05	0x01	See Table 16.1	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 Sending Status Table”. See [“Wireless sending status table” on page 38](#).

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.

16.3.2.3 Send confirmation format

Asynchronous Command "Send Confirmation" Format for Network Management Commands.

Field	Frame header	Frame size	Payload					
			Command types	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". For details, see "Wireless Transmission Status Table". See ["Wireless sending status table" on page 38](#).

16.3.2.4 Receive network management response commands

Asynchronous Response Command Format for Network Management Commands.

Field	Frame header	Frame size	Payload						
			Command types	Command code	Command data				Check code
Content	0x55	Need to calculate	0x81	See Table 16.1	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:

Command code	Command function
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)

16.3.2.5 Instructions for sending and receiving commands

The network management command is sent by the host computer to the data transmission module or network-ing 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.

16.4 Network management command parsing

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

16.4.1 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 0xFFFF broadcast address.

Input the command:

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

MAC address: the MAC address of the queried node.

Feedback command:

Field	Command code	Command data			
		Short address	Command number	Result of enforcement	Command parameter
Content	0x00				MAC address
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.

16.4.2 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

Feedback command:

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

MAC address: The MAC address of the queried node.

16.4.3 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

Feedback 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.

16.4.4 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	Com- mand number	Result of enforce ment	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". See ["Port:" on page 39](#)

Port profile: Profile ID, the application layer only needs to pay attention to 0x0104, see ["Port Profile: \(Profile\)" on page 75](#).

Device ID: Indicates the function of the device, which is determined by the ZCL protocol specification, see the table "Device ID Table". See ["Device ID table" on page 78](#).

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 ["16.5.2.2 Cluster" on page 75](#) and ["16.5.2.3 Client and server" on page 75](#).

Output cluster table: The output clusters supported by the device, including the number of clusters and the list of clusters, see ["16.5.2.2 Cluster" on page 75](#) and ["16.5.2.3 Client and server" on page 75](#).

16.4.5 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". See ["Port:" on page 39](#).

Input the command:

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

Command parameters: none

Feedback 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.

16.4.6 Set node constant connection binding (command code 0x21)

Command code: 0x21

Note:

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. 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 [“16.5.2.3 Client and server” on page 75](#)

See [“5 Virtual device SN number:” on page 39](#)

Input the command:

Field	Command code	Command data			
		Short address	Command parameter		
Content	0x21		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.

See [“5 Virtual device SN number:” on page 39](#).

Cluster ID: The cluster ID used for frequent connection communication, see “Cluster (cluster)”.

See [“16.5.2.2 Cluster” on page 75](#).

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.

See [“5 Virtual device SN number:” on page 39](#).

Feedback command:

Field	Command code	Command data			
		Short address	Command parameter	Result of enforcement	Command parameter
Content	0x21				NULL
Number of bytes	1	2	1	1	0

Parameters: None, directly judge the result from the “execution result” in the unified header.

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

Command code: 0x22

Note:

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			
		Short address	Command parameter		
Content	0x22		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 [“5 Virtual device SN number:” on page 39.](#)

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. See [“5 Virtual device SN number:” on page 39.](#)

Feedback command:

Field	Command code	Command data			
		Short address	Command parameter	Result of enforcement	Command parameter
Content	0x22				NULL
Number of bytes	1	2	1	1	0

Parameters: None, directly judge the result from the “execution result” in the unified header.

16.4.8 View node constant connection binding (command code 0x33)

Command code: 0x33

Note:

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.

Feedback command:

Field	Command code	Command data						
Content	0x33	Short address	Command number	Result of enforcement	Command parameter			
					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.

16.4.9 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			
		Short address	Command parameter		
Content	0x34		MAC address	Re-entry network	delete child 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.

Feedback command:

Field	Command code	Command data			
		Short address	Command parameter	Result of enforcement	Command parameter
Content	0x34				NULL
Number of bytes	1	2	1	1	0

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

16.4.10 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.

Feedback command:

Field	Com-mand code	Command data						
Content	0x31	Short address	Command number	Result of enforcement	Command parameter			
					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.

16.5 ZigBee® Control and Management (ZCL Protocol)

16.5.1 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, the product 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.

16.5.2 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 data transmission module also uses this Profile as data transmission to meet the requirements of interoperability with other manufacturer's devices.

See ["4 Port:" on page 39](#).

16.5.2.1 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.

See ["4 Port:" on page 39](#).

See ["Device ID table" on page 78](#)

16.5.2.2 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.

See ["4 Port:" on page 39](#).

16.5.2.3 Client and server

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.

16.5.2.4 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.

16.5.2.5 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.

16.5.2.6 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.

16.5.2.7 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.

16.5.2.8 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.

See ["4 Port:" on page 39](#)

See ["ZCL attribute data type table" on page 79](#)

See ["16.5.2.2 Cluster" on page 75](#)

See ["16.5.2.3 Client and server" on page 75](#)

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 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).

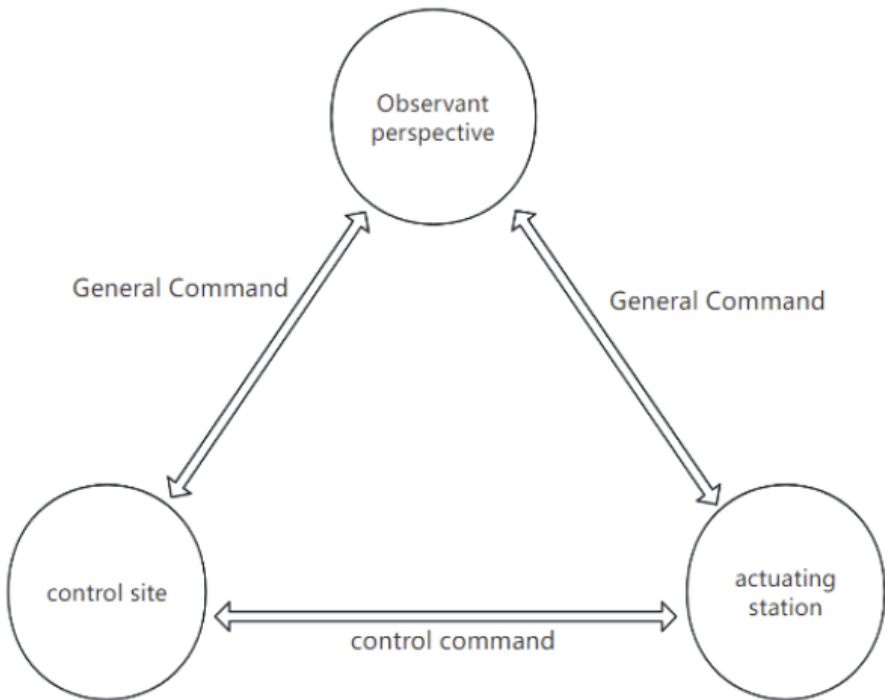
See [“16.4.6 Set node constant connection binding \(command code 0x21\)” on page 70](#)

For “view binding”, see [“16.4.8 View node constant connection binding \(command code 0x33\)” on page 72](#)

For “unbinding”, see [“16.4.7 Unbind the node’s constant connection \(command code 0x22\)” on page 71](#)

16.5.2.9 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.



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 Sensor	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	No data	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

ZCL attribute data type table (continued)					
Category	Type of data	ID	Number of bytes	Invalid value	Report alignment
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
	attrID	0xE9	2	0xFFFF	0
	bacOID	0xEA	4	0xFFFFFFFF	0
other data	EUI64	0xF0	8	0xFFFFFFFF	0
	key128	0xF1	16		0

ZCL status 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 start-up 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_SUPPLIER	Transparent transmission	0x2000

16.5.2.10 Serial port data transmission ZCL cluster specification

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:

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	uint16	RW	0xFFFF
0x0002	targetEP	Destination port	uint8	RW	0xFF
0x0003	sendMode	Transparent mode	bool	RW	FALSE
0x0004	LP Level	Low power mode	Enum8	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 0xFFFFE, it is transparently transmitted to the binding target.
- When the target port is 1 to 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

16.6 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.

16.6.1 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	
			Command types	Command code (unfinished)
Content	0x55	Need to calculate	0x02	See Table 16.2
Number of bytes	1	1	1	1

Field	Payload									Check code
	Command data (continued table)									
Content	Transmit mode	Target short address	Target port	Frame serial number	Com- mand direction	Cluster ID	Manu- facturer Code	Re- sponse Mode	Extend- ed 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 to 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 types	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.

Feedback command format:

Field	Frame header	Frame size	Payload			
			Command types	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				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 sending status table" on page 38](#).

16.6.2 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 types	Command code (unfinished)
Content	0x55	Need to calculate	0x02	See Table 16.2
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	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.

16.7 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.

See [“16.5.2.6 General Command \(Global Command\)” on page 76](#)

See [“16.5.2.7 Control command \(Special Command\)” on page 76](#)

Table 16.2 ZCL command code table				
Function	Command code	Send	Take over	Type
Read device status	0x00	ZCL_READ_ATTR_REQ	ZCL_READ_ATTR_RSP	See A
Modify device status	0x01	ZCL_WRTIE_ATTR_REQ	ZCL_WRTIE_ATTR_RSP	See A
Query status reporting rules	0x02	ZCL_READ_REPORT_REQ	ZCL_READ_REPORT_RSP	See A
Modify status reportin rules	0x03	ZCL_WRITE_REPORT_REQ	ZCL_WRITE_REPORT_RSP	See A
View all status	0x04	ZCL_DISC_ATTR_REQ	ZCL_DISC_ATTR_RSP	See A
View All Status Band Extensions	0x05	ZCL_DISC_ATTR_EX_REQ	ZCL_DISC_ATTR_EX_RSP	See A
Active status report	0x0A	none	ZCL_REPORT_IND	See A
The system returns by default	0x0B	none	ZCL_DEFAULT_RSP	See A
Send control commands	0x0F	ZCL_CMD_SEND	none	See B
Receive control commands	0x0F	none	ZCL_CMD_IND	See B

See A: [“16.5.2.6 General Command \(Global Command\)” on page 76](#)

See B: [“16.5.2.7 Control command \(Special Command\)” on page 76](#)

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	

16.7.1 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		
		From [Send mode] To [reply mode]		Extended data
Content	0x00			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]			
					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. See ["ZCL status table" on page 81](#).

Data type: See ["ZCL attribute data type table" on page 79](#)

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

16.7.2 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: See [“ZCL attribute data type table” on page 79](#).

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] To [signal strength]	Extended data		
			Number of errors	Write property struct array [N]	
				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” on page 81](#).

16.7.3 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 [“16.4.6 Set node constant connection binding \(command code 0x21\)” on page 70](#)) 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		
		From [Send mode] To [reply mode]		Extended data
Content	0x02			Number of attributes N
Number of bytes	1	11		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. See [“ZCL status table” on page 81](#)

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”. See [“ZCL attribute data type table” on page 80](#).

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 attribute data type table”. See [“ZCL attribute data type table” on page 80](#).

16.7.4 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 attribute 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. See [“ZCL attribute data type table” on page 80](#).

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 attribute data type table" on page 79](#).

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 attribute data type table". If the alignment length is 0, this property does not need to set the variable value. See ["ZCL attribute data type table" on page 79](#).

Return the ZCL message asynchronously:

Field	Command code	Command data			
Content	0x03	From [Send mode] To [signal strength]	Extended data		
			Number of errors	Write property 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" on page 81](#).

16.7.5 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		
		From [Send mode] To [reply mode]		Extended data
Content	0x04			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.

16.7.6 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 write ability 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.

16.7.7 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 attribute data type table" on page 79](#).

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

16.7.8 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 [reply mode]	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" on page 81](#).

16.7.9 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.

16.7.10 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 [reply mode]	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.

16.8 Attributes and control commands under each cluster

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

16.8.1 (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

16.8.2 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 = 0003, Server				
AttrID	Descriptor	Name	Type of data	Operate
0x0000	Identify Time	mark time	uint16	read and write

Send control commands:

Cluster = 0003 , Client -> Server			
cmdID	Descriptor	Name	Parameter
0x00	Identify	marking equipment	unit16 IdentifyTime: Mark Mode Duration
0x01	IdentifyQuery	Query marking equipment	none

Receive control commands:

Cluster = 0003 , 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.

16.8.3 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	uint16 groupID: The group ID of the device added to the group string name: group name
0x01	ViewGroup	Query group infor-mation	uint16 groupID: the queried group ID (for checking the group name)
0x02	GetMembership	View (all) groups	uint8 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	uint16 groupID: group ID of the removed group
0x04	RemoveAll	Delete all groups	none
0x05	AddGroupIdentify	Mark state device add group	uint16 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 , Server-> Client			
cmdID	Descriptor	Name	Parameter
0x00	AddGroupRsp	Return equipment group	uint8 status: ZCL status uint16 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 uint8 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 uint16 groupID: Group ID of the removed group

16.8.4 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 + 16 bit 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 24 bit.

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: re-moved 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 scene-Name: 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
0x03	RemoveAllScene Rsp	Remove all scenes and re-turn	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 capaci-ty: 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.

```
{  
    uint16 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.

16.8.5 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 + news-paper + 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

16.8.6 Level control cluster (LEVEL cluster = 0x0008)

Function:

Device Level Control.

Property sheet:

Cluster = 0x0008, Server				
AttrID	Descriptor	Name	Type of data	Operate
0x0000	current Level	Current level	uint8	reading + news-paper + scene

Send control commands:

Cluster = 0x0008, 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

16.8.7 Data transmission control cluster (Cluster = 0xFC08 / manuCode=0x2000)**Function:**

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	uint16	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

17 Module Network Distribution & Identification in HEX Command Mode

This section introduces how the Zigbee module configures the network and identifies the device. The main operations are all carried out on the coordinator, through which the coordinator controls the access of nodes to the network, and how the coordinator knows which nodes are connected to the network, and how the coordinator knows the specific device information of the nodes connected to the network.

Preparation:

One E18 series module, E180ZG120A/B module or E72-2G4M20S1E (Link72) network management module is used as a coordinator, and another E180-ZG120A/B module is used as a network access node (routing node or terminal node).

Make sure the module is in the HEX command mode, and the module defaults to the HEX command mode. Among them, E18 series modules support transparent transmission mode. If the module is in transparent transmission mode, send "+++" string (3 bytes "+" symbol) to its UART RX port to switch to HEX command mode. E180-ZG120A/B supports AT command mode and transparent transmission mode. If the module is in transparent transmission mode, it will send "+++" to its UART to switch to HEX command mode. If the module is in AT command mode, it will send "AT+EXIT" to switch to HEX command mode.

17.1 The first step is to set the device type of the module:

Prepare module A and module B, and confirm that the module is in the HEX command mode. If not, please switch it to the HEX command mode. Configure module A as a coordinator and module B as a router or end node.

17.1.1 Modul reset

Command	Response
55 07 00 04 00 FF FF 00 04	55 04 00 04 00 04
Description: After receiving the Response, the module starts to reset	

Receive asynchronous command "device startup notification" after successful reset.

Asynchronous	
De: 55 0D 80 00 01 10	F3 4C 60 FE EF 14 43 0C 14
Firmware Version	Module MAC address
Description: After receiving the Response, the module starts to reset	

17.1.2 Configure module A as the coordinator

Command	Response
55 04 00 05 00 05	55 04 00 05 00 05
Coordinator	Setting succeed

17.1.3 Configure module B as a non-sleeping endpoint

Command	Response
55 04 00 05 02 07	55 04 00 05 00 05
Terminal node	Setting succeed

17.1.4 Configure module B as a router

Command	Response
55 04 00 05 01 04	55 04 00 05 00 05
Terminal node	Setting succeed

Note:

After setting the module as a coordinator, router, terminal node, or dormant terminal, you must reset the module to take effect. Command reset, button reset, and power-on reset are all available.

17.2 Second step: Module connected to network

17.2.1 Module A starts to configure the network and module A successfully establishes the network.

Command	Response
55 03 00 02 02	55 04 00 02 00 02
Received 2 asynchronous Command	
Received <system notification-network status change>: 55 29 80 01 01 F3 4C 60 FE EF 14 43 0C 19 91 14 00 00 22 44 EAD4 CA FD 93 2D D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF FO	
01	Indicates that the network has been established
F3 4C 60 FE EF 14 43 0C	is Module A (Coordinator) MAC
19	is channel
91 14	is PANID
00 00	is short address
22 44 EAD4 CA FD 93 2D	is expand PANID
D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF	is network key
Description: The coordinator establishes a network on channel $0 \times 19 = 25$, the PANID is 0×1491 , and the short address is 0×0000	
Receive <system nification-network access time window notification>:	
55 04 80 02 B4 36	
Allow connecting network 180s	
Description: Module A has successfully established a network	

17.2.2 Module B starts to configure the network, and module B joins the network.

Command	Response
55 03 00 02 02	55 04 00 02 00 02
Received asynchronous Command	
Received <system notification-network status change>:	
55 29 80 01 02 E9 CE D6 FE EF 14 43 0C 19 91 14 2C 6A 22 44 EA D4 CA FD 93 2D D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF 9B	
02	Indicates the first access to the network
E9 CE D6 FE EF 14 43 0C	Indicates module B (terminal node) MAC
19	Is channel
91 14	Is PANID
2C 6A	Is short address
22 44 EA D4 CA FD 93 2D	Is expand PANID
D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF	Is network key
Description: Module B joined the network successfully. Module B joined coordinator A as a terminal node. The channel, PANID, extended PANID, network key are the same as those of the coordinator, and the short address is 0 x 6A2C	

17.2.3 Module A detects that module B is connected to the network.

Module	Receive data
Module A	Received <system notification-detection node network>:
	55 10 80 03 E9 CE D6 FE EF 14 43 0C 2C 6A 00 00 00 6E
	E9 CE D6 FE EF 14 43 0C
	Is module B's MAC
	2C 6A
	It is the short address of module B
	00 00
	Is short address for the parent node
	00
	Indicates the first access to the network
	Description: The terminal node module B accesses the network through the coordinator module A as the parent node, and the coordinator module A detects the terminal node module B
Module A	Receive <system notification-node short address notification>:
	55 0E 80 04 E9 CE D6 FE FF 14 43 0C 2C 6A 02 6B
	E9 CE D6 FE FF 14 43 0C
	Is Module B MAC
	2C 6A
	Is the short address of module B
	02
	Is a non-dormant endpoint
	Analysis: Module B joins the network as a non-dormant terminal node. This message is broadcast by module B to the entire network, and both the coordinator and routing nodes can receive it. If module B modifies its own short address during operation, or powers on again, it will notify the whole network of the news.

When B accesses the network through a route, A detects that B has entered the network:

Module	Receive data	
Module A	Received <system notification-detection node network>: 55 10 80 03 E9 CE D6 FE EF 14 43 0C 88 FC 52 19 00 17	
	E9 CE D6 FE EF 14 43 0C	Is module B MAC
	88 FC	Is the short address of module B
	52 19	Is short address for the parent node
	00	Indicates the first access to the network
	Explanation: B accesses the network through routing, and the coordinator can detect which parent node B accesses the network through.	
	The second time to receive <system notification-detection node network>: 55 10 80 03 E9 CE D6 FE EF 14 43 0C 88 FC 52 19 00 17	
	Note: Nodes access the network through routing, routers conforming to the zigbee 3.0 specification will submit two verification requests to the coordinator, and the coordinator will also receive the same node access information twice.	
	Received <system notification-node short address notification>: 55 0E 80 04 E9 CE D6 FE EF 14 43 0C 88 FC 02 59	
	E9 CE D6 FE EF 14 43 0C	Is module B MAC
	88 FC	Is the short address of module B
	02	Is a non-dormant endpoint

Precautions for the coordinator to detect node access to the network:

<System notification-node short address notification> is limited by the broadcast storm. When multiple modules enter the network at the same time, the message may not be broadcasted, resulting in the coordinator not receiving the message, so it cannot be used as a basis for detecting node network access. And <system notification-detecting node network access> is based on the coordinator detecting a module network access request as a judgment condition, and there is a risk of module network access failure. Therefore, it is recommended that if the coordinator needs to successfully detect the module's network access, it can send any

request query command according to the short address of the network-connected module within 5 seconds after receiving the <system notification-node short address notification>, as long as there is a return message, that is It can be determined that the module has successfully entered the network.

17.3 The third step is to identify the network access node:

When using E180-ZG120 series modules or E18 series modules as the coordinator:

The coordinator obtains the application port list of the network access node

Command	Response	
Send <ZDO command-query node port number>:		
55 05 01 05 88 FC 70	55 05 01 05 00 02 06	
Target short address	Command valid	Command number
Analysis: This command has no command parameters, only command ID and short address	Analysis: The command input is valid, and the query number assigned by the module to this command is 0 x 02	

Await async command...

Receive 2 asynchronous command				
Wait for several milliseconds, receive <ZDO sending confirmation>:				
55 07 8F 01 88 FC 02 00 F8				
Target short address	Command number	Send successfully		
Analysis: The command is successfully sent, waiting for the target to reply with the execution result.				
Wait for several milliseconds, and receive <ZDO response-query node port number>:				
55 07 8F 01 88 FC 02 00 04 01 02 03 04 F2				
Short address of other side	Command number	Other side executed successfully	Number of ports	Port list
Analysis: B has 4 application ports, namely port 1, port 2, port 3 and port 4				

Coordinator A checks which are the 4 application ports of node B.

First look at port 1 of node B:

Command	Response	
Send <ZDO command-query node port information>:		
55 06 01 04 88 FC 01 70	55 05 01 04 00 03 06	
Target short address	Target ports	Command is valid
		Command number
Analysis: Query application port 1 of node B (short address 0 x FC88).	Analysis: The input of this command is valid, and the query number assigned by the module to this command is 0 x 03.	

Received 2 asynchronous command		
Receive <ZDO Send Confirmation>:		
55 07 8F 01 88 FC 03 00 F9		
Target short address	Command number	Send successfully
Description: The coordinator establishes a network on channel 0 x 19 = 25, the PANID is 0 x 1491, and the short address is 0 x 0000		
Received <ZDO Response – Query Node Port Information>:		
55 21 81 04 88 FC 03 00 01 04 01 50 00 00 05 00 00 03 00 04 00 07 00 08 FC 04 03 00 06 00 08 00 08 FC AA		
88 FC	Is short address of other side	
03	Is command number	
00	Is other side executed successfully	
01	Is target port	
04 01	Is apply port profile	
50 00	Is device ID	
00	Is device version	
05	Is the input cluster size	
00 00 03 00 04 00 07 00 08 FC	Is the input cluster list	
04	Is the output cluster size	
03 00 06 00 08 00 08 FC	Is the output cluster list	
AA		
Analysis: Query the information of port 1 of node B, the port profile is 0 x 0104 is a ZCL Home Automatic application, the device ID is 0 x 0050 corresponding to the “home gateway” device, the device version is 0, and the input list has a total of 5 clusters, respectively {0 x 000, 0 x 003, 0 x 004, 0 x 007, 0 x FC08}, the 4 output clusters are respectively {0 x 0003, 0 x 0006, 0 x 0008, 0 x FC08}. By looking up the table, we can analyze that port 1 of Node B supports “Basic Information (0 x 0000)”, “Device Mark (0 x 0003)”, “Group Management (0 x 0004)”, “Switch Output (0 x 0007)”, “Data Transmission (0 x FC08)”, a lot of 5 local functions, and a total of 4 functions that can be output externally: “Device Mark (0 x 0003)”, “Switch Control (0 x 0006)”, “Brightness Control (0 x 0008)”, and “Data Transmission (0 x FC08)”.		

Precautions:

For some use Silicon.

For some zigbee network access devices using Silicon Labs chips, <ZDO Send Confirmation> and <ZDO Response> may be reversed. This is a BUG of Silicon Labs' ZigBee series products and is a normal phenomenon. It is recommended to use it correctly.

When using <ZDO Command> to query the target node on demand, wait for the timeout of <ZDO Response> for 18 seconds. The response message is treated as an invalid message.

Then look at port 2 of module B:

Port 3 and port 4 of module B are exactly the same as port 2.

Command		Response
Send <ZDO command-query node port information>:		
55 06 01 04 88 FC 02 70		55 05 01 04 00 04 01
Receive 2 asynchronous Command		
Receive <ZDO Response - Query Node Port Information>:		
55 19 81 04 88 FC 04 00 02 04 01 01 01 00 05 03 00 04 00 05 00 06 00 08 00 00 FB		
Target port	Apply Port Profile	Device ID
		Device version
		Input cluster size
		Input cluster list
		Output cluster size
Description: The coordinator establishes a network on channel 0 x 19 = 25, the PANID is 0 x 1491, and the short address is 0 x 0000		
Received <ZDO Send Confirmation>: 55 07 8F 01 88 FC 04 00 FE" to the upper line of Analysis.		
Analysis: In this query, <ZDO Send Confirmation> and <ZDO Response> are reversed Query the target port 2, whose profile is 0 x 0104 is also the ZCL Home Automatic application, and the device ID is 0 x 0101 corresponding to the device application of "dimming light". 5 input clusters {0 x 0003, 0 x 0004, 0 x 0004, 0 x 0005, 0 x 0006, 0 x 0008} indicate that they support "device flag (0 x 00003)", "group management (0 x 0004)", "scene snapshot (0 x 0005)", "switch control (0 x 0006)", "Brightness Control (0 x 0008)". The output cluster for port 2 is empty.		

A brief description of the functions of each cluster:

Basic information (0x0000): the function of recording and saving the factory information, version and production date of the device Device mark (0x0003): The device switches mark status, which can be found by naked eyes and by other devices on the same network Group management (0x0004): device group management function, you can receive multicast messages after grouping, and you can exit the grouping when you don't need to receive multicast messages Scene snapshot (0x0005): Device settings save a complex physical state, and then you can quickly switch to this state with a Command:

Switch Control (0x0006): The device outputs a state that can be switched between 0 and 1 States Switch output (0x0007): The device simulates the function of a button or switch

Brightness control (0x0008): The device outputs a switching state between 0~255, such as PWM wave. Data transmission (0xFC08): the device inputs and outputs data through the serial port.

Supplementary Tutorial: E72-2G4M20S1E(Link72) Automatically Identify Network Access Devices

Use the E72-2G4M20S1E (Link72) module as the coordinator, and the E180-ZG120A/B module to access the network as a router. E72-2G4M20S1E (Link72) has powerful parallel processing capability, and can automatically query all application ports of network-connected nodes while a large number of nodes are configured. E72-2G4M20S1E(Link72) needs to be soft-started before it can run. It is used to protect the host computer during startup. If the host computer does not need to be protected, it can start automatically.

Step 1: Start the E72-2G4M20S1E(Link72) and enter the network distribution mode

E72-2G4M20S1E (Link72) soft start:

Command	Response
55 04 00 01 01 00 autostart	55 04 00 01 00 01 Analysis: Wait for 3 seconds to receive feedback after sending the soft start, indicating that E72-2G4M20S1E (Link72) has created a network and is restarting the previous network.
Receive asynchronous command	
Received <system notification-network status change>: 55 29 80 01 01 ED 53 D1 26 00 4B 12 00 0B F6 E8 00 00 06 83 C1 60 B0 58 2C 16 E2 72 8B A2 7C D0 8E 20 26 A5 0E 9C FA 2F 56 72 28	

E72-2G4M20S1E(Link72) starts to connect to network:

At the same time, the module E180ZG120 is configured as a router and starts to configure the network

Command	Response
55 03 00 02 02	55 04 00 02 00 02
Received 2 asynchronous command	
Receive <system notification-allowed network access time window notification>: 55 04 00 02 B4 36	
Receive <system notification-network status change>: 55 29 80 01 02 ED 53 D1 26 00 4B 12 00 0B F6 E8 00 00 06 83 C1 60 B0 58 2C 16 E2 72 8B A2 7C D0 8E 20 26 A5 0E 9C FA 2F 56 72 2B	

Step 2: E72-2G4M20S1E (Link72) detects node access to the network

The coordinator detects that a new node has entered the network:

Data reception	
Receive <system notification-detection node network>	55 10 80 03 4D 4D 60 FE FF 14 43 0C A7 B1 00 00 00 AF time MAC address:short address Access network first
Receive <system notification-node short address notification>	55 0E 80 04 4D 4D 60 FE FF 14 43 0C A7 B1 01 A9 MAC address:short address Router node
Analysis: E72-2G4M20S1E (Link72) coordinator detects that the routing node with MAC address 4D 4D 60 FE FF 14 43 0C has entered the network, and the short address is 0xB1A7	

Step 3: E72-2G4M20S1E (Link72) automatically obtains network access node information

The coordinator automatically detects the information of the application port 1 of the network access node:

Data reception	
Receive <system notification-device information notification>	55 28 80 05 00 01 4D 4D 60 FE FF 14 43 0C A7 B1 01 04 01 50 00 05 00 00 03 00 04 00 07 00 08 FC 0A 03 00 06 00 08 00 08 FC F8 Termination Sign Virtual SN Short address:Port Number Port Profile Device ID Input cluster size Input cluster list Output cluster size Output Cluster List
Analysis: The port 1 information, port number and MAC address of the network access node are re-integrated into a virtual SN to facilitate cloud management. At the same time, the application profile, device ID, input cluster and output cluster of the application port can be obtained from the message, which is exactly the same as the previous example of viewing port 1. Port 1 of the network access node is a "home gateway" device, which supports "basic information (0x0000)", "device tag (0x0003)", "group management (0x0004)", "switch output (0x0007)", "data transmission (0xFC08)", a total of 5 local functions, and a total of 4 functions that can be output externally: "Device Mark (0x0003)", "Switch Control (0x0006)", "Brightness Control (0x0008)", and "Data Transmission (0xFC08)".	

Receive info from port 2:

Data reception

Receive notification-device information notification>	<system	55 20 80 05 00 02 4D 4D 60 FE FF 14 43 0C A7 B1 02 04 01 01 01 05 03 00 04 00 05 00 06 00 08 00 00 A5
Termination sign not end Virtual SN Device ID Input cluster size Input cluster list Output cluster size		
Analysis: Port 2 of the node uses a different virtual SN from port 1, and the device ID is "dimming light", which supports "group management (0x0004)", "scene snapshot (0x0005)", "switch control (0x0006)", "Brightness control (0x0008)" has a total of 5 application functions, no output control function		

Receive info from port 3:

Data reception		
Receive notification-device information notification>	<system	55 20 80 05 00 03 4D 4D 60 FE FF 14 43 0C A7 B1 03 04 01 01 01 05 03 00 04 00 05 00 06 00 08 00 00 A5
Analysis: The functions of port 3 and port 2 are exactly the same		

Receive info from port 4:

Data reception		
Receive notification-device information notification>	<system	55 20 80 05 01 04 4D 4D 60 FE FF 14 43 0C A7 B1 04 04 01 01 01 05 03 00 04 00 05 00 06 00 08 00 00 A4
Termination sign end		
Analysis: Port 4 has the same function as port 2 and port 3. Port 4 is the last application port of the network access node. There are 4 application ports in the network access node		

Note:

Zigbee 3.0 series modules in HEX mode not only meet the networking requirements between the modules themselves, but are also compatible with third-party Zigbee 3.0 products. The complete "network distribution -> identification" process is applicable to all Zigbee device networking. If it can be guaranteed that the devices participating in the networking are Zigbee 3.0 series modules in the use environment, the "identification" step can be skipped. You can also quickly configure the network by using AT commands.

18 Zigbee 3.0 Module Three Types of Serial Mode Switch

This section introduces how the Zigbee module judges the current Command mode and switches between several modes. E18 series modules and E180-ZG120A/B modules both support HEX Command and data transparent transmission modes, and E180-ZG120A/B also supports AT Command mode.

Preparation:

1. E18 series modules, E180-ZG120A/B modules.
2. Serial port debugging assistant tool: sscom or XCOM is recommended.
3. Hardware connection, open the serial port debugging assistant (baud rate: 115200, stop bit: 1, data bit: 8, Parity: None)

18.1 Query Current Mode and distribution network status

For details, see the current status of the module in Zigbee 3.0 Module HEX Command Standard Specification.

Command	Response	Current Mode	Network Status
55 03 00 00 00	55 2A 00 00 00 00 F3 4C 60 FE FF 14 43 0C 0F C6 19 00 00 8C 18 3B 14 41 E0 A2 2D 89 20 93 ED E8 05 4C 09 55 6C 25 10 78 9B 2F D3 1C Note: F3 4C 60 FE FF 14 43 0C is short address 0F is channel C6 19 is PANID 00 00 is short address 8C 18 3B 14 41 E0 A2 2D is expand ID 89 20 93 ED E8 05 4C 09 55 6C 25 10 78 9B 2F D3 is network key	HEX Command Mode	Connected
	55 0D 00 00 FF 01 4D 4D 60 FE FF 14 43 0C C4 Note: 4D 4D 60 FE FF 14 43 0C is MAC address	HEX Command Mode	Not connected
	OK Note: In the transparent transmission state, the return "OK" does not have a CR symbol, and in the transparent transmission state, in addition to returning to the above states, there are also "JAM" and "FAIL". JAM means that it is interfered and the sending fails; FAIL means sending failed.	Data Transparent Transmission Mode	Connected
	ERRO Note: In the transparent transmission state, the return "ERRO" does not have a CR symbol, and in the transparent transmission state, in addition to returning to the above states, there are also "JAM" and "FAIL". JAM means that it is interfered and the sending fails; FAIL means sending failed.	Data Transparent Transmission Mode	Not connected
	WRONG Note: \r\n means CRLF	AT Command Mode	-

18.2 Mutual Switch between three modes

18.2.1 HEX Command Mode to Transparent Transmission Mode

Command	Response
55 07 00 11 00 03 00 01 13	55 04 00 11 00 11
Note: Successfully enter Transparent Transmission Mode	

18.2.2 HEX Command Mode to AT Command Mode (for E180ZG120 only)

Command	Response
55 03 00 16 16	55 04 00 16 00 16
Note: Successfully enter AT Command Mode	

18.2.3 AT Command Mode to Transparent Transmission Mode (for E180ZG120A/B only)

Command	Response
AT + SEND	SEND_MODE\r\n
Note: Successfully enter Transparent Transmission Mode, \r\n means CRLF	

18.2.4 AT Command Mode to HEX Command Mode (for E180ZG120A/B only)

Command	Response
AT + EXIT	OK\r\n
Note: Successfully enter HEX Command Mode, \r\n means CRLF	

18.2.5 Transparent Transmission Mode to HEX Command Mode

Command	Response
+++	55 0D 80 00 00 10 D5 20 D9 FE FF 14 43 0C E6 Note: for E180-ZG120A/B module, E18 series has no response
Note: Successfully enter HEX Command Mode. Asynchronous Command, the module outputs this Command, indicating that the switch is successful (for E180-ZG120A/B); E18 series has no response. 10 is version info. D5 20 D9 FE FF 14 43 0C is MAC address	

18.2.6 Transparent Transmission Mode to AT Command Mode (for E180ZG120A/B only)

Command	Response
+AT	AT_MODE\r\n
Note: Successfully enter AT Command Mode, \r\n means CRLF	

Appendix:

1. Remotely set HEXCommand mode and transparent transmission mode

The HEXCommand mode and transparent transmission mode of the module are determined by a status parameter inside the module, which can be viewed and controlled remotely through the ZCL protocol.

According to the rules of the ZCL protocol, the module applies Cluster 0xFC08 on port 1, and Manufacture Code 0x2000. The value of Attribute 0x0003 can be read and written. The data type of this Attribute is a ZCL standard Bool data, 0 is the HEXCommand mode, and 1 is the data transparent transmission mode.

2. Module power-on default mode

The factory default value of the ZCL Attribute corresponding to the transmission mode is 0, and the default is HEX Command mode. When the Attribute is changed to 1 (can be modified locally or remotely), the module is E180-ZG120A/B and has not been configured with a network. When the module is powered on, it is in AT command mode, and the module is in transparent transmission mode when it is configured with a network. No matter whether the E18 series modules are configured with a network or not, the Attribute is always in the transparent transmission mode when the Attribute is 1. If the E18 modules without a network configuration are set to the transparent transmission mode, the network configuration operation cannot be performed through the serial port, and can only be triggered through the external Net pin. distribution network.

19 Range considerations

Ensure the antenna is not obstructed by radio shadowing during installation of the device. The product's range may be significantly reduced by:

- Walls and reinforced concrete ceilings
- Installation with the antenna inside a metal control cabinet
- Coated or metallised insulating glass, aluminium window frames, etc.
- Vehicles
- Trees, bushes, soil and rocks
- Proximity to metallic or conductive objects (e.g., railings, control cabinets, metal walls)
- Proximity to electric motors, transformers or power adapters
- Proximity to poorly shielded or openly operated computers or other electrical devices

20 Cleaning and care

Important:

- Never use aggressive detergents, rubbing alcohol or other chemical solutions, as these could damage the housing or even impair the functioning of the product.
- Do not submerge the product in water.

1. Disconnect the product from the power supply.
2. Clean the product with a dry, fibre-free cloth.

21 Disposal



This symbol must appear on any electrical and electronic equipment placed on the EU market. This symbol indicates that this device should not be disposed of as unsorted municipal waste at the end of its service life.

Owners of WEEE (Waste from Electrical and Electronic Equipment) shall dispose of it separately from unsorted municipal waste. Spent batteries and accumulators, which are not enclosed by the WEEE, as well as lamps that can be removed from the WEEE in a non-destructive manner, must be removed by end users from the WEEE in a non-destructive manner before it is handed over to a collection point.

Distributors of electrical and electronic equipment are legally obliged to provide free take-back of waste. Conrad provides the following return options **free of charge** (more details on our website):

- in our Conrad offices
- at the Conrad collection points
- at the collection points of public waste management authorities or the collection points set up by manufacturers or distributors within the meaning of the ElektroG

End users are responsible for deleting personal data from the WEEE to be disposed of.

It should be noted that different obligations about the return or recycling of WEEE may apply in countries outside of Germany.

22 Declaration of Conformity (DOC)

Conrad Electronic SE, Klaus-Conrad-Straße 1, D-92240 Hirschau hereby declares that this product conforms to the 2014/53/EU directive.

- Click on the following link to read the full text of the EU declaration of conformity:
www.conrad.com/downloads

Enter the product item number in the search box. You can then download the EU declaration of conformity in the available languages.

23 Technical data

23.1 Power supply

Power supply DC 8 - 28 V/DC, 12V/DC or 24 V/DC is recommended
Current consumption max. 78 mA at 20 dBm

23.2 RTU W/ 2 DI, 2 DO

Processor CC2530
Flash memory 256 KB
RAM memory 8 KB
Radio standard Zigbee® 3.0
Frequency range 2405 to 2480 MHz
Channel spacing 5 MHz
Modulation GFSK
Transmission mode duplex
Transmission power max. 20 dBm
Receiver sensitivity -98 ±1 dBm
Range max. 1.2 km (free space)
Antenna socket SMA-K socket (50 Ohm)
Antenna SMA-J, 5 dBi gain, omnidirectional
Interface RS485 (screw terminal block, 3.81 mm pitch, pluggable)
Serial interface baud rates 9600, 19200, 38400, 57600, 115200 bps (factory setting: 115200 bps)
Configurable as coordinator, router or end device

23.3 Configuration software

Operating system Windows 7, 10, 11

23.4 Other

Dimensions (W x H x D) approx. 68 x 66 x 21 mm (without plug)
Weight approx 64 g
Housing Aluminium

23.5 Ambient conditions

Operating/storage conditions -40 to +85 °C/ +40 to +125 °C, 5 – 95% relative humidity (non-condensing)



This is a publication by Conrad Electronic SE, Klaus-Conrad-Str. 1, D-92240 Hirschau (www.conrad.com).

All rights including translation reserved. Reproduction by any method, e.g. photocopy, microfilming, or the capture in electronic data processing systems require the prior written approval by the editor. Reprinting, also in part, is prohibited. This publication represent the technical status at the time of printing.

Copyright 2025 by Conrad Electronic SE.
