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

E72 V1.0 User Manual

(ZigBee3.0 Self-Networking Module)

目录

1. Module introduction 2
1.1 Introduction to ZigBee 2
1.2 Features 2
1.3 Support product family 5
2.Introduction functions and commands 6
2.1 Function pin table 6
2.2 Pin connection description 7
3 UART commands and configuration modes 7
3.1 Serial port command format 7
3.2 Command Type 9
3.3 Command code directory 10
3.4 AF Status Status Table 13
3.5 ZDO execution return status table 13
3.6 ZCL data type table 14
3.7 ZCL error status code 16
3.8 ZCL structure of data transmission module 17
3.9 Address format 18
4. User instruction set 20
4.1 Local configuration commands 20
4.2 System notification commands 37
4.3 Network management commands 44
4.4 Device Status Management and Control (ZCL Command) 58
5.User Notice 80
5.1 ZigBee network roles and precautions 80
5.2 network structure 82
5.3 Getting Started with Device Communication 82
6. Customized cooperation 91
7. About us 91

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

1. Module introduction

1.1 Introduction to ZigBee

ZigBee technology is a short-range, low-complexity, low-power, low-speed, low-cost two-way wireless communication technology.

There are three logical device types in ZigBee network: Coordinator (coordinator) , Router (router) and End-Device (terminal device) . A ZigBee network consists of a Coordinator , multiple Routers and multiple End_Devices .

The functions of each type of equipment are as follows:

(1) Coordinator (coordinator)

The coordinator is responsible for starting the entire network. It is also the first device of the network. The coordinator selects a channel and a network ID (also called PAN ID , or Personal Area Network ID) , and then starts the entire network.

The coordinator can also be used to assist in establishing bindings between the security layer and the application layer in the network .

Note that the role of the coordinator primarily involves the startup and configuration of the network. Once this is all done, the coordinator works like a router (or goes away) . Due to the distributed characteristics of the ZigBee network itself, the subsequent operation of the entire network does not depend on the existence of the coordinator.

(2) Router (router)

The main functions of the router are: to allow other devices to join the network, multi-hop routing and to assist in communication with its own battery-powered son terminal device.

Usually, a router is expected to be active all the time, so it must be powered by mains power. But when using the network mode of the tree group, the routing is allowed to operate once at a certain period of time, so that it can be powered by the battery.

(3) End-Device (terminal equipment)

The end device has no specific responsibility for maintaining the network structure, it can sleep or wake up, so it can be a battery powered device.

1.2 Features

No	Features	Feature description
1	Support ZigBee 3.0	The networking management module supports the ZigBee 3.0 specification and has powerful networking capabilities and interconnection capabilities. It supports networking of up to 200 ZigBee 3.0 devices, and supports networking of third-party ZigBee devices such as Tuya, Philips, and Myrock. (Note: This module can only be used as a coordinator and router device)
2	Network managemen	The module works in ZigBee coordinator mode, supports networking of other ZigBee devices, and manages all networking nodes. When the

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	t	device joins the network or exits the network, the network manager will generate corresponding messages.
3	On-demand networking	The networking manager can open network access when device access is required, close the network when no networking is required, or automatically close the network after 180 seconds.
4	Network self-healing function	The loss of a node does not affect the normal operation of the networking manager, and the lost node can be re-identified by the networking manager when it is powered on or moved back to its original spatial position. When the network manager is powered off or shut down, it does not affect the normal operation of the networked devices. After the networking manager is restored to the factory, a new network is created. If there are existing devices running on the original network, the devices of the old network and the new network can coexist in the same space without affecting each other.
5	Device identification function	Detect all networked devices, identify the device type (router, terminal node), identify the functions supported by the device (common data transmission modules, lights, switches), and extend the advanced SE authentication function (legal devices, illegal devices)
6	Concurrent communication	When sending data, the networking manager can send different messages to multiple targets at the same time , and wait for the targets to return asynchronously and in parallel. When one of the targets is abnormal, it will not affect the communication of other targets. The abnormal target will also return the corresponding message of the system and report to the upper computer. When receiving data, the serial port can output the address of each source device according to the messages received from multiple different targets.
7	Endpoint support	The networking manager supports direct connection of 48 terminal nodes and saves data for them.
8	Endpoint data retention	The network manager can save data for directly connected dormant terminals for 7 seconds, a single terminal can save up to 8 pieces of data, or at least 1 piece of data for 40 terminals at the same time , if it exceeds, the first data will be automatically cleared! After the data storage time has passed, the data heap is automatically emptied and a corresponding reminder message is sent to the upper computer to judge whether the dormant terminal is running normally.
9	Automatic resend function	In unicast (on-demand) mode, the automatic retransmission function can be enabled, and the device will automatically retransmit when it fails to send to the next node. The number of retransmissions for each message is 3 times, and the retransmission interval is 6 seconds. It can communicate with other nodes during the gap time waiting for retransmission.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

10	automatic routing	The module supports the network routing function. Routers and coordinators carry network data routing functions, and users can perform multi-hop networking.
11	Support encryption protocol	The module adopts AES 128 -bit encryption function, which can change the network encryption and anti-monitoring. Different networking managers use different keys to ensure that different networks do not interfere with each other. After the network manager is restored to the factory, the key can be recreated, and one network manager can create multiple networks that do not interfere with each other (coordinator-free network).
12	Support serial port configuration	The module has built-in serial port commands, and users can configure (view) the parameters and functions of the module through the serial port commands.
13	Multi-type data communication	Support network-wide broadcast, multicast and on-demand (unicast) functions.
14	channel detection	Channel detection can be used to detect other ZigBee networks that already exist in the space, and can be used as an automatic channel selection condition.
15	Automatically select channel	When the network manager creates a network, it supports the automatic selection of 16 channels (2405~2480MHZ), such as 11~26 . It can enable multiple channels at the same time, and automatically select the channel with the least interference.
16	Network PAN_ID change	The network PAN_ID can be selected from manual mode and automatic mode. In the automatic mode, the network manager actively searches the network access node by switching the window that allows access to the network. In the manual mode, the network access node and the network manager can set the same PANID to realize the specified network.
17	High-speed serial port baud rate	The serial port baud rate of the networking manager is as high as 230400 , which provides enough data bandwidth for sending and receiving data at the same time for multiple targets.
18	Real-time monitoring equipment access to the network	During networking, the networking manager can obtain the MAC address, short address, and all port information of the device (including the profile and cluster support information) of the connected device in real time, and can determine whether the device is connected to the network for the first time or the network is restored.
19	Network access device address	The networking manager can query the MAC address and short address of the networked devices on the module, and supports the networking and query of a maximum of 254 devices.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	management	
20	Device Information and Status Management	Detect the status of network access equipment, including but not limited to the baud rate, transparent transmission mode, and target of the data transmission module; the brightness and on-off status of the lighting equipment; the detection value of the sensor equipment, power consumption, etc.
21	Set up node-to-node direct communication (Bind)	Any network access node can be set to send messages to another network access node. The MAC address locking method will not be unlocked even if the target device is disconnected. At the same time, the locked target of each network access node can be queried.
22	single instruction multiple data	Using the transmission characteristics of ZigBee , one instruction can control multiple states, which greatly utilizes the transmission efficiency of ZigBee 250kbps
23	Communication Error Diagnosis	When the network manager fails to send any wireless message, there is a status feedback. Including the failure of communication in the on-demand mode, the broadcast storm in the broadcast mode, or the interference of the wireless channel, and the wireless transmission rate cannot keep up with the application delivery rate, an error message will be returned.

1.3 Support product family

No.	Product number	RF chip	Frequency (Hz)	Airspeed (bps)	Power (dBm)	Antenna
1	E72-2G4M20S1E	CC2652P	2.4G	250K	20	PCB

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

2.Introduction functions and commands

2.1 Function pin table

The network manager is based on the E72-2G4M20S1E module, and the pin package refers to the hardware description document " E72-2G4M20S1E_User Manual_CN_v1.0 ". The network manager firmware needs to use the following IO ports of this module.

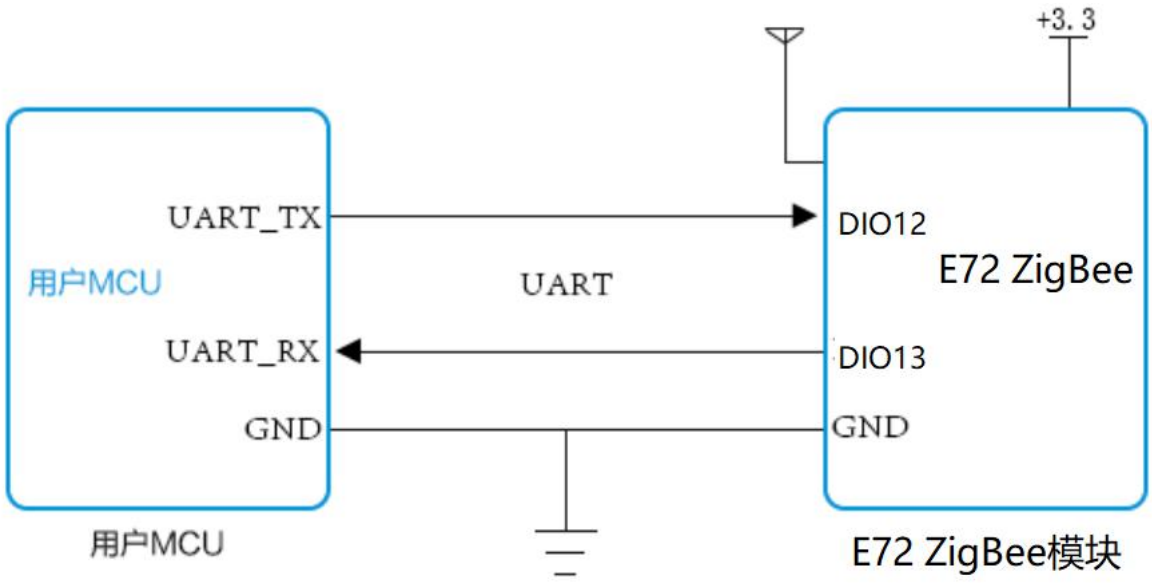
pin	function indication	Description (Alternate function pins can only be specified as the last modified function)	input / output
DIO12	UART_RX	Serial input signal pin	I
DIO13	UART_TX	Serial output signal pin	O
DIO15	BOOTLOADER	Enter the BootLoader signal interface, active low	I
DIO7	STATUS_LED	Status indicator, active low. Long light is in standby state, fast blinking means creating a new network or joining a network, 1S periodic blinking means allowing network access	O

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

2.2 Pin connection description

2.2.1 Serial port connection description



2.2.2 Pin Location Description

E72 ZigBee networking module adopts UART serial communication mode, users can connect to it through any MCU with UART function for data exchange. E72 DIO_12 and DIO_13 are the RX and TX pins of E72 internal serial port . The specific connection method is shown in the figure above.

3 UART commands and configuration modes

3.1 Serial port 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.

Command frame structure:

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Name	Frame header	Frame length	Frame payload
	SFD	JUST	payload
Number of bytes	1	1	lengthen

Frame header: starts with 0x55 as the command

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

Frame load: The frame load is the valid data of the serial port frame (including the checksum), when the module receives the frame load byte number equal to the frame length, that is, after receiving a complete command frame

Command mode :

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

Input command: The command frame input by the host computer to the module, when it is input, it is a complete command frame.

Feedback command: The module feeds back the command to the upper computer after receiving the input command, 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.

Frame payload structure and serial port commands :

name	frame payload			
	Payload			
	Command type	command code	command data	check code
	Cmd type	cmd code	Cmd data	check
number of bytes	1	1	0~252	1

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

Command code: The code of the execution command, 1 byte.

Command data: Incidental parameters of the command execution, minimum 0 bytes, maximum

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

252 bytes

Check code: The check code is an XOR8 check that does not contain the check code itself in the payload

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

3.2 Command Type

command mode	Command type	Descriptor	command type name
enter the command / feedback command	0x00	TYPE_CFG	local configuration commands
	0x01	TYPE_ZDO_REQ	network management commands
	0x02	TYPE_ZCL_SEND	Device Status and Control Commands
asynchronous command	0x80	TYPE_NOTIFY	system notification command
	0x81	TYPE_ZDO_RSP	network management back
	0x82	TYPE_ZCL_IND	Receiving device status and control
	0x8F	TYPE_SEND_CNF	send confirmation

The causal relationship between input commands and asynchronous commands :

The 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

The 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.

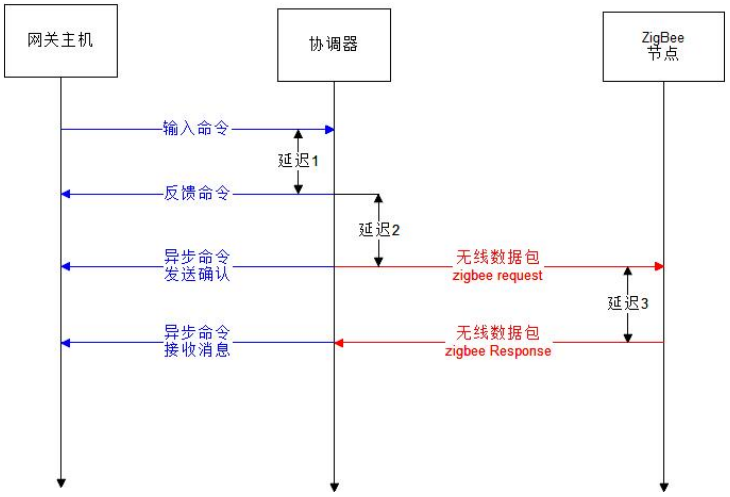
Each valid input TYPE_ZDO_REQ command or TYPE_ZCL_SEND command will generate TYPE_SEND_CNF , so TYPE_SEND_CNF can be used for task blocking or buffer release, especially useful when sending to multiple targets at the same time.

The 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.

Remote command flow chart (network management commands, device status and control commands **)**

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



3.3 Command code directory

Local configuration command :

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 mod type
0x06	CFG_CHANNEL	Query and set channel
0x07	CFG_GET_PANID	Query PANID
0x08	CFG_SET_PANID	set PANID
0x09	CFG_VIEW_GROUP	View Mods and Groups
0x0A	CFG_ADD_GROUP	add module
0x0B	CFG_REMOVE_GROUP	Module withdrawal
0x0C	CFG_RF_SCAN	Channel scan test
0x0D	CFG_TX_POWER	Set transmit power
0x20	CFG_GET_UTC	Get current UTC time
0x21	CFG_SET_UTC	set UTC time
0x22	CFG_GET_ADDRTABLE	read local address table
0x28	CFG_EZ_MODE	Retransmit device notification messages

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

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

Device Status and Control Commands (ZCL):

command code	Descriptor	command name
0x00	ZCL_READ_ATTR_REQ	read property
0x01	ZCL_WRTIE_ATTR_REQ	Modify properties
0x02	ZCL_READ_REPORT_REQ	Query attribute reporting rules
0x03	ZCL_WRITE_REPORT_REQ	Modify attribute reporting rules
0x04	ZCL_DISC_ATTR_REQ	View all properties
0x05	ZCL_DISC_ATTR_EX_REQ	View all properties (with extensions)
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

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

0x05	NOTIFY_DEVICE_JOIN	Device access information
0x06	NOTIFY_LEAVE	Module off-grid notification
0x0C	NOTIFY_SCAN_INFO	Scan result notification

Network management returns :

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

Receiver Status and Control (ZCL):

command code	Descriptor	command name
0x00	ZCL_READ_ATTR_RSP	read property returns
0x01	ZCL_WRTIE_ATTR_RSP	Modify property return
0x02	ZCL_READ_REPORT_RSP	Query attribute reporting rules return
0x03	ZCL_WRITE_REPORT_RSP	Modify the attribute reporting rule and return
0x04	ZCL_DISC_ATTR_RSP	View all properties back
0x05	ZCL_DISC_ATTR_EX_RSP	View all property returns (with extensions)
0x0A	ZCL_REPORT_IND	Active reporting of attributes
0x0B	ZCL_DEFAULT_RSP	The system returns the frame by default
0x0F	ZCL_CMD_IND	receive control commands

Send confirmation :

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

command code	Descriptor	command name
0x01	ZDO_SEND_CNF	Network management command sending confirmation
0x02	ZCL_SEND_CNF	Device Status Control Send Confirmation

3.4 AF Status Status Table

Error return status table: ACK return and general command feedback, proprietary command feedback, all fit into this table	
status value	status description
0x00	Successful operation
0x01	operation failed
0x02	Parameter error
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

3.5 ZDO execution return status table

ZDO Status Table		
State ID	Descriptor	Functional explanation
0x00	ZDP_SUCCESS	operate as
0x80	ZDP_INVALID_REQTYPE	invalid operation
0x81	ZDP_DEVICE_NOT_FOUND	device not found
0x82	ZDP_INVALID_EP	incorrect endpoint
0x83	ZDP_NOT_ACTIVE	endpoint does not exist
0x84	ZDP_NOT_SUPPORTED	Device does not support this

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

		command
0x85	ZDP_TIMEOUT	Device processing timed out
0x86	ZDP_NO_MATCH	Device processing match failed
0x88	ZDP_NO_ENTRY	This information does not exist on the device
0x89	ZDP_NO_DESCRIPTOR	The short address is not of the current device
0x8a	ZDP_INSUFFICIENT_SPACE	no storage space
0x8b	ZDP_NOT_PERMITTED	The current state does not support this operation
0x8c	ZDP_TABLE_FULL	Tablestore is full
0x8d	ZDP_NOT_AUTHORIZED	Operation not authenticated
0x8e	ZDP_BINDING_TABLE_FULL	The binding table is full

3.6 ZCL data type table

ZCL attribute data type table					
category	type of data	ID	number of bytes	invalid value	Report alignment
NULL	nodata	0x00	0		0
Ordinary data	data8	0x08	1		0
	data16	0x09	2		0
	data24	0x0a	3		0
	data32	0x0b	4		0
	data40	0x0c	5		0
	data48	0x0d	6		0
	data56	0x0e	7		0
	data64	0x0f	8		0
logical data	bool	0x10	1	0xff	0
binary data	bit8	0x18	1		0
	bit16	0x19	2		0
	bit24	0x1a	3		0
	bit32	0x1b	4		0
	bit40	0x1c	5		0
	bit48	0x1d	6		0
	bit56	0x1e	7		0

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	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	you8	0x28	1		4
	int16	0x29	2		4
	int24	0x2a	3		4
	int32	0x2b	4		4
	int40	0x2c	5		8
	you are 48	0x2d	6		8
	int56	0x2e	7		8
	int64	0x2f	8		8
enumerate	enum8	0x30	1	0xff	0
	enum16	0x31	2	0xffff	0
floating point	semi	0x38	2		4
	single	0x39	4		4
	double	0x3a	8		8
string	octstr	0x41	first byte	header is 0xff	0
	string	0x42	first byte	header is 0xff	0
	octstr16	0x43	first double byte	header is 0xffff	0
	string16	0x44	first double byte	header is 0xffff	0
serial type	uint8_array	0x48	2 + sum of content length	header is 0xffff	0
	struct	0x4C	2 + sum of content length	header is 0xffff	0

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

time	ToD	0xe0	4	0xffffffff	4
	date	0xe1	4	0xffffffff	4
	UTC	0xe2	4	0xffffffff	4
identifier	clusterID	0xe8	2	0xffff	0
	attriID	0xe9	2	0xffff	0
	bacOID	0xea	4	0xffffffff	0
other data	EUI64	0xf0	8	0xffffffff	0
	key128	0xf1	16		0

3.7 ZCL error status code

ZCL state table		
Value	describe	what happens
0x00	Successful operation	all commands
0x01	operation failed	all commands
0x7E	The operation is not authorized	When reading and writing Attribute
0x80	Incorrect command format	Send proprietary commands
0x81	This ZCL proprietary command is not supported	Send proprietary commands
0x82	This ZCL generic command is not supported	Send general command
0x83	Vendor-defined ZCL proprietary commands are not supported	Send specific commands with vendor ID
0x84	Vendor-defined ZCL common commands are not supported	Send 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	Configure active reporting

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	active reporting	or read configuration
0x8D	Invalid data type	Generic commands with data types
0x8E	Invalid option	Proprietary command
0x8F	Attribute write only	When reading Attitude
0x90	Inconsistent startup status	
0x91	Out Of Band	
0x92	inconsistency error	
0x93	deny this action	
0x94	time out	
0x95	Abort	OTA _
0x96	invalid image data	OTA _
0x97	waiting for data	OTA or other big data transfer
0x98	no image file	OTA _
0x99	need more image data	OTA _
0xc0	hardware error	
0xc1	software bug	
0xc2	Calibration error	

3.8 ZCL structure of data transmission module

project	value
Endpoint ID	1 (reserve endpoint=2 for serial port 2)
Profile ID	0x0104
Device ID	0x0500
In Cluster	0x0000 (Basic) 0x0003(Identify) 0xFC08 (data transparent transmission, manuCode =0x2000)
Out Cluster	0x0003 0xFC08 (data transparent transmission, manuCode =0x2000)

Module property parameters:

Cluster = 0xFC08， manucode = 0x2000				
property ID	Descriptor	name	type of data	operate
0x0000	Baud	baud rate	uint32	R
0x0001	targetAddr	Default	uint16	RW

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

		destination short address		
0x0002	targetEP	Default destination port	uint8	RW
0x0003	sendMode	Transparent mode	bool	RW
0x0004	LP Level	low power mode	Enum8	RW

ZCL control commands :

Command ID	command direction	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	return baud rate

3.9 Address format

3.9.1 IEEE address (MAC address)

The IEEE address of a ZigBee node is present at the factory, which is an 8 -byte address and is globally unique.

3.9.2 Short address and PANID

When the ZigBee coordinator creates a network, it will generate a PANID . The essence of the device networking is to obtain the same PANID as the coordinator . At the same time, the ZigBee device will also obtain a 16- bit short address, and the data transmission in the ZigBee mesh network needs to use the short address mode.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

3.9.3 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 . Port numbers from 1 to 240 are reference layers, port 0 is used for device network management, port 242 is used for green power device management, and port 255 is used for broadcast

3.9.4 Virtual address:

After a ZigBee device is networked, there will be a short address. The short address + port can be used as the address of the access control virtual device. The virtual address is a 24- bit address, which is composed of short address + port. In addition, if the coordinator sends a broadcast to control the device, it is recommended to fill in 0xFF for the target port , which is the broadcast port, so that multiple virtual devices on the same device can receive broadcast control. In addition, the port for multicast sending is also 0xFF .

3.9.5 Virtual device SN number :

The virtual address is an address management mechanism formulated by Ebyte according to the characteristics of the ZCL standard equipment to facilitate the device management of the ZCL standard. According to the 8 -byte IEEE address on each ZigBee device and the port number of each function and peripheral on the device, the combined 9 -byte (72bit) virtual device serial number. The format is "port number + IEEE address (8 -byte little endian mode)".

In the setting of " constant connection binding ", the binding can be set by setting the SN number of the source virtual device and the SN number of the target virtual device . Since this function can also specify the source device to be bound to the group, the ZigBee group can also be managed as a virtual device, and a virtual device SN number is assigned to it, the format is " 0xFF + group ID (low) + group ID (high) +0xFFFFFFFFFFFF (6 bytes)".

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

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

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

3.9.6 Group address and multicast:

The multicast mode of ZigBee operates at the APS layer, that is, ZigBee multicast is multicast for ports. The group address is 16bit , the range is 0~65535 . When using multicast, the port of the device needs to be added to the specified group, and multicast can only be controlled under the ZCL command. In multicast applications, a multi-port device can assign different ports to different groups. But if you want to control multiple ports on a device at the same time, you must first add these ports to the same group. For example , ZigBee multi-hole sockets can add different jacks to different groups.

4. User instruction set

4.1 Local configuration commands

4.1.1 Query the current status of the module

Command code: 0x00

Function:

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

input the command:

name	cmd data
	command data
	NULL
	null
number of bytes	0

Feedback command:

name	cmd data							
	command data							
	Net status	DevType	IEEE Addr	Channel	PAGE	ShortAddr	Ext PANID	NWK Key
	network status	Equipment type	MAC address	channel	PAGE	short address	Extended PANID	network key
number of bytes	1	1	8	1	2	2	8	16

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Network Status: 0x00 – Networked , 0xFF – Not Networked

Device Type: 0x00 - Coordinator, 0x01 - Router, 0x02 - End Node
MAC address : The module 's MAC address, fixed at the factory, unique in the world
Channel: The current channel of the module, not available when not networked
PANID : The current PANID of the module , not available when not networked
Short address: the current short address of the module, which is not available when the network is not connected
Extended PANID : None when not networked
Network key: no 0 when not networked

Command example: (purple: payload length red: command type + command code blue: check code)
Send command: 55 03 00 00 00
Receive instructions:
Not networked: 55 0D 00 00 FF (network status) 00 (device type) 28 EA E2 1A 00 4B 12 00 (MAC address) 9C
Networked: 55 2A 00 00 00 (network status) 00 (device type) 28 EA E2 1A 00 4B 12 00 (MAC address) 19 (channel) 93 61PANID 00 00 short address
28 EA E2 1A 00 4B 12 00 (extended PANID) C6 CD 93 B5 2F 37 9E F6 E9 A6 CE 3A 15 33 CF 55 (network key) B1

4.1.2 Module boot / soft start

Command code: 0x01
Function:

After the module is powered on, it is in a standby state, regardless of whether it has been networked before. In the standby state, no asynchronous commands will be issued to prevent the host computer from receiving a large amount of data during the power-on and startup process.
input the command:

name	cmd data
	command data
	AutoStart
	auto start
number of bytes	1

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

Feedback command:

name	cmd data

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	command data
	Status
	state
number of bytes	0

Status: 0 - Startup successful 2 - Startup passed 0xFF - Startup invalid

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 04 00 01 01 (automatic start) 00

receive instructions

Successful start: 55 04 00 01 00(Status) 01

The return command will be followed by an asynchronous feedback command of "network status change": 55 29 80 system notification 01 network status change 00 not networked 1A 1F 79 25 00 4B 12 00 00 MAC address FE FF FE FF 9A CD E6 F3 79 3C 1E 8F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 **17**

Already activated: 55 04 00 01 02 03

4.1.3 Open the network / start networking

Command code: 0x02

Function:

The coordinator opens the network to allow devices to join the network (a factory coordinator creates a new network), and routes and endpoints join the network. There will be delays when the coordinator creates the 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 router is connected to the network, which can prolong the time for the coordinator to open the network.

input the command:

name	cmd data
	command data
	NULL
	null
number of bytes	1

Feedback command:

name	cmd data

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	command data
	Status
	state
number of bytes	1

Status: 0x00 – operation valid, 0xFF – operation invalid. This command is valid only after soft start

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 0 3 00 02 02

Receive command parsing:

Feedback command: 55 04 00 02 00 (success) 02

Asynchronous notification 1 : 55 04 80 (system notification) 02 (open network notification) B4 (network window time) 36 **(0xB4=180 second network window)**

Asynchronous notification 2 : 55 29 80 (system notification) 01 (network status) 02 (network open) 1A 1F 79 25 00 4B 12 00 (MAC address) 0E (channel) A7 CE (PAN_ID) 00 00 (short address) 9A CD E6 F3 79 3C 1E 8F(Extended PANID) 86 BC 4D CE 83 8A 56 21 38 A8 78 8A 1D 59 8D EE(Network Key) F0

After waiting for 180 seconds, you will receive a system notification to close the network

55 04 80 (system notification) 02 (network notification turned on) 00 (network window closed) 82

Note: When the coordinator creates a new network, the LED light on the DIO7 of the E72 module will flash rapidly; within the time allowed for networking, the LED will continue to flash at a cycle of 1S until the network is automatically or manually turned off.

4.1.4 Close the network / stop networking

Command code: 0x03

Function:

Turn off the networking permission. If you run this command on routers and terminal nodes, subsequent devices may not be able to access the network.

input the command:

name	cmd data
	command data
	NULL
	null
number of bytes	0

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Feedback command:

name	cmd data
	command data
	Status
	state
number of bytes	0

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

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 0 3 00 03 03

Receive command parsing:

The network has been received as follows

Received feedback instruction: 55 04 00 03 00 (success) 03

Received asynchronous command: 55 04 80 (system notification) 02 (open network notification) 00 (network window close) 82

Not networked and received as follows

Received feedback command: 55 04 00 03 C2 (invalid) C1

Received asynchronous command: 55 04 80 (system notification) 02 (open network notification) 00 (network window close) 82

4.1.5 Restore factory settings

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:

name	cmd data		
	command data		
	mode	PAGE	Channel
	reset mode	Pan ID	channel
number of bytes	1	2	1

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Reset mode: 0x00 - reset; 0x01 - logout ; 0x02 - factory reset

PANID : The current PANID of the module. Fill in 0xFFFF when resetting. If you need to withdraw from the network or restore the factory when the network has been established, you need to fill in the current PANID of the module .

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

Feedback command:

name	cmd data
	command data
	Status
	state
number of bytes	0

Status: 0x00 - operation valid, 0xFF - operation invalid.

Command example: (purple: payload length red: command type + command code blue: check code)

reset mode

Send command: 55 07 00 04 00 (reset mode) FF FF (PAN_ID) FF (channel) FB

Received feedback instruction : 55 04 00 04 00 (success) 04

Asynchronous command received: 55 0D 80 00 (start notification) 06 (reset mode) 1C (software version) 1A 1F 79 25 00 4B 12 00 (MAC address) 9A

Exit mode

Sending command : 55 07 00 04 01 (off network mode) F5 8A (PANID) 0B (channel) 71

Received feedback command: 55 04 00 04 00 (operation successful) 04

Send and receive asynchronous commands: 55 0D 80 00 (start notification) 06 (watchdog reset) 1C (software version) 1A 1F 79 25 00 4B 12 00 (MAC address) 9A

Restore Factory

Send command : 55 07 00 04 02 (restore to factory mode) 93 86 (PANID) 0B (channel) 18

Feedback command : 55 04 00 04 00 (success) 04

If two 00s are received in a few seconds , the coordinator is clearing all networking and setting records in FLASH .

Send and receive asynchronous commands: 55 0D 80 00 (start notification) 06 (watchdog reset) 1C (software version) 26 30 79 25 00 4B 12 00 (MAC address) 85

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

4.1.6 Query and set channel

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:

name	cmd data	
	command data	
	Set	ChannelList
	set up	channel list
number of bytes	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:

name	cmd data	
	command data	
	status	ChannelList
	state	channel list
number of bytes	1	variable length N

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

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

Command example: (purple: payload length red: command type + command code blue: check code)

Query channel (channel list is empty)

Send command : 55 04 00 06 00 (disable) 06

Feedback received : 55 0B 00 06 00(success) 0B 0E 0F 13 14 18 19(channel list) 0A

disable channel

Send command : 55 06 00 06 00 (disable) 13 14 (channel list) 01

Feedback received : 55 09 00 06 00 (success) 0B 0E 0F 18 19 (channel list) 0D

coverage channel

Send command : 55 06 00 06 02 (override) 11 12 (channel list) 07

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Feedback received : 55 06 00 06 00 (success) 11 12 (channel list) 05

4.1.7 Query PANID

Command code: 0x07

Function:

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

input the command:

name	cmd data
	command data
	NULL
	null
number of bytes	0

Parameters: none

Feedback command:

name	cmd data	
	command data	
	status	PAGE
	state	Pan ID
number of bytes	1	2

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

PAN ID : Module PANID , default value 0xFFFF

Command example: (purple: payload length red: command type + command code blue: check code)

Send command : 55 03 00 07 07

Feedback received : 55 06 00 07 00 (query success) C1 BE(PANID) 78

Unnetworked feedback is : FF FF

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

4.1.8 Setting PANID

Command code: 0x08

Function:

The module specifies the PANID to establish a network in the coordinator mode , and this operation needs to be performed before establishing the network.

input the command:

name	cmd data
	command data
	PAGE
	Pan ID
number of bytes	2

PANID : Default PANID value

Feedback command:

name	cmd data
	command data
	status
	state
number of bytes	1

Status: 0 – setting valid, 1 – setting invalid

Command example: (purple: payload length red: command type + command code blue: check code)

Send instruction : 55 05 00 08 98 89(PANID) 19

Feedback received : 55 04 00 08 00 (success) 08

4.1.9 View the group added to this machine

Command code: 0x09

Function: View the group joined by the local machine. Only after the local machine joins the group can it receive the multicast messages of the group.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Input command format:

name	cmd data
	command data
	EP_idx
	Native Port Index
number of bytes	1

Native Port Index: The native port index defaults to 0x00

Feedback command:

name	cmd data		
	command data		
	Status	Group Num	Group List
	state	number of groups	add group list
number of bytes	1	1	2*N

Status: 0x00 - Query valid, with follow-up data, 0xFF - Query 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

Command example: (purple: payload length red: command type + command code blue: check code)
Send command : 55 04 00 09 00 (local port index) 09
Feedback received : 55 0B 00 09 00 (inquiry is valid) 03 (number of groups added) 0F 00 0E 00 0D 00 (there are 3 data in the group added list) 06

4.1.10 Adding groups to this machine

Command code: 0x0A
Function: Specify a port on the module to add a group
Input command format:

name	cmd data	
	command data	
	EP_idx	Group ID
	Native Port	group id

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	Index	
number of bytes	1	2

Feedback command:

name	cmd data
	command data
	Status
	state
number of bytes	1

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

Command example: (purple: payload length red: command type + command code blue: check code)

Coordinator joins group 0x0100

Send command: 55 06 00 0A 00 (port index) 00 10 (group ID) 1B

Feedback received : 55 04 00 0A 00(success) 0A

4.1.11 This machine withdraws from the group

Command code: 0x0B

Function: A port on the specified module exits the specified group

Input command format:

name	cmd data	
	command data	
	EP_idx	Group ID
	port index	group id
number of bytes	1	2

Port Index: Default 0

Group ID : The ID number of the group that needs to be exited

Feedback command:

name	cmd data

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	command data
	Status
	state
number of bytes	1

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

Command example: (purple: payload length red: command type + command code blue: check code)

The coordinator exits the 0x0100 group

Send command: 55 06 00 0B 00 (port index) 00 10 (group ID) 1B

Feedback received : 55 06 00 0B 00(success) 00

4.1.12 Scan channel

Command code: 0x0C

Function:

Scan the channel to determine which coordinators and routers are on the channel and whether it is clean. The command returns the result as an asynchronous command of "Scan Result Notification".

input the command:

name	cmd data		
	command data		
	ChannelList	Duration	Mode
	Scan channel list	Listening time per channel	scan mode
number of bytes	4	1	1

Scanning channel list: 32 -bit channel list, the corresponding channel enable is 1 , for example, when scanning 11~26 channels, fill in 0x07FFF800 , when the value is 0 , the default channel (11 , 14 , 15 , 19 , 20 , 24 , 25 total of 7 or "Philips channel").

Listening time per channel: Listening time per channel =(2^Duration)*15.36ms , the longer the time, the slower the scanning speed and the more devices scanned

Scanning mode: 0 - beacon scanning mode, this mode will return many beacons in "scan result notification", other - no effect

Feedback command:

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

name	cmd data
	command data
	Status
	state
number of bytes	0

Status: 0x00 - operation valid, 0xFF - operation invalid.

Note: If the previous scan is not completed and the next scan is performed, the operation will be invalid, and the completion of the scan is subject to the receipt of the "Scan complete" notification.

Command example: (purple: payload length red: command type + command code blue: check code)

Scan 7 default channels (Philips channels), each channel scans 2^7*15.36 milliseconds, and the estimated total time is 14 seconds

Send command: 55 09 00 0C 00 00 00 00 (scanning list is the default channel) 07 (frame listening time) 00 0B

Feedback received: 55 04 00 0C 00 (scanning valid) 0C

Received asynchronous command (valid beacon) : 55 12 80 0C 00 (scan successfully) 0E (channel) 83 CE (PANID) 1C 67 (short address) 45 5A 44 09 00 4B 12 00 (extended PANID) A3 (signal strength) 1C

Asynchronous command received (scan end): 55 09 80 0C 00 (scan successfully) FF FF FF FE FF (scan end) 72

4.1.13 Query / set transmit power

Command code: 0x0D

Function: Query or set the transmit power of the module

Input command format:

name	cmd data	
	command data	
	Mode	Power
	model	power
number of bytes	1	1

Mode: 0x00 - query, 0x01 - set

Power: The setting range is 0x0E~0x14 , corresponding to 14dbm~20dbm , and the default value of the coordinator is 14dbm .

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Feedback command:

name	cmd data
	command data
	Status
	state
number of bytes	1

Status: 0x00 - operation valid, 0xFF - operation invalid

Command example: (purple: payload length red: command type + command code blue: check code)

set power

Send command: 55 04 00 0D 01 (configuration mode) 14 (transmit power 20dbm) 18

Feedback received : 55 04 00 0D 00(success) 0D

Remarks : The power level is 0x0E~0x14 and the setting that exceeds the maximum value will not take effect and the previous setting power will be maintained

4.1.14 Get current UTC time

Command code: 0x20

Function:

Query the current UTC time of the coordinator

input the command:

name	cmd data
	command data
	null
	null
number of bytes	0

Parameters: none

Feedback command:

name	cmd data	
	command data	
	Status	UTC
	execution status	UTC time
number	1	4

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

of bytes		

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

UTC time: Coordinator's UTC32 time

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 03 00 20 20

Feedback received : 55 08 00 20 00 (success) E7 12 00 00 (UTC time) D5

4.1.15 Set UTC time

Command code: 0x21

Function:

Set the UTC time of the coordinator to enable the coordinator to provide UTC services to ZigBee devices .

Precautions:

Since the coordinator itself does not have an RTC clock, but the coordinator needs to provide time services for other networking devices, the host computer needs to periodically calibrate and set the UTC time of the coordinator. If the host computer does not support this function, the running time of the connected device may not match the real time.

input the command:

name	cmd data
	command data
	UTC
	UTC time
number of bytes	4

UTC time: the UTC time that needs to be set

Feedback command:

name	cmd data
	command data
	Status
	execution status
number	1

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

of bytes	

Execution status: 0x00 – Execution valid, 0xFF – Execution invalid

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 07 00 21 00 00 00 00 (UTC time) 21

Feedback received: 55 04 00 21 00 (success) 21

4.1.16 Read the network access address table

Command code: 0x22

Function:

Query the MAC addresses and short addresses of the nodes that have entered the network, one by one, for a total of 255 (0~254) entries. If the network access device is not ZigBee 3.0 and the parent node of the first network access is not the coordinator, it cannot be found. In addition, there may be zombie nodes in this table.

input the command:

name	cmd data	
	command data	
	addr_idx	mode
	address number	query mode
number of bytes	2	1

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

Query mode: 0x00 - normal query, 0x01 - query with flag bit

Feedback command:

name	cmd data				
	command data				
	status	addr_idx	short_addr	MAC	Flag
	state	address number	Node short address	Node MAC address	flag bit
number of bytes	1	2	2	8	1

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

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

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 legitimate device that has undergone the first network authentication, and less than 8 is a suspicious device

Command example: (purple: payload length red: command type + command code blue: check code)

common query

Send command : 55 06 00 22 00 00 (address number) 00 (inquiry mode) 22

Feedback received: 55 10 00 22 00 (success) 00 00 (address number) ED 1B (short address) 6A 90 B2 FE FF AC 33 BC (MAC address) BE

Query with flag bit

Send command : 55 06 00 22 00 00 (address number) 01 (inquiry mode) 23

Received feedback: 55 11 00 22 00 (success) 00 00 (address number) ED1B (short address) 6A 90 B2 FE FF AC 33 BC (MAC address) 0B (flag) B5

Notes: How to Make a Suspicious Device

- **MAC address can be read when reading the network address table**
- **When the terminal node is completely shut down or no signal is received, the coordinator deletes the terminal node according to the MAC address.**
- **Read the previous address code of the device from the network access address table, and find that the MAC address record is gone.**
- **Power cycle the end node and receive any information related to the end node at the coordinator**

Then read all the network access address table

Send command: 55 06 00 22 02 00 (address number) 01 (inquiry mode) 21

Feedback received: 55 11 00 22 00 (success) 02 00 (address number) 32 8C (short address) D0 27 47 0B 00 4B 12 00 (MAC address) 03 (suspicious device) 7F

Note : Query the address number saved by the coordinator, 0x0000~0x00FE is valid (that is, the maximum address number is FE 00), if the corresponding address has no device, the feedback command is all FF

4.1.17 Retransmit device notification message

Command code: 0x28

Function: The device information notification will only be available when the node accesses the network for the first time. If the message is missed, you can re-apply for the device to report it again, and it is valid only when the node is in normal operation.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

input the command:

name	cmd data
	command data
	MAC
	Node MAC address
number of bytes	8

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

Feedback command:

name	cmd data
	command data
	Status
	execution status
number of bytes	1

Execution status: 0x00 – operation valid, please wait for device upload, 0xFF – device does not exist

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 0B 00 28 13 B7 57 22 00 4B 12 00 (node MAC address) A0

Command feedback: 55 04 00 28 00 (success) 28

Asynchronous commands: 55 24 80 05 (device information notification) 01 (terminal marker) 01 13 B7 57 22 00 4B 12 00 (device SN number) BE 82 (short address) 01 (port number) 04 01 (device profile) 00 01 (device ID) 04 (number of input clusters) 0000 0300 0400 08FC (input cluster table) 03 (number of output clusters) 0000 0300 08FC (output cluster table) 37

4.2 System notification commands

4.2.1 Device startup notification

Command code: 0x00

Function:

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

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

module

Asynchronous command:

name	cmd data		
	command data		
	resetMode	Version	IEEE Addr
	reset mode	Software version	MAC address
number of bytes	1	1	8

Reset mode: 1 - Reset pin, 2 - VDDS power- down reset 4 - VDDR power- down reset 5- clock loss reset 6- soft reset (watchdog reset), 7- warm boot. This field can detect abnormal restart of the module.

MAC Address: The MAC address of the module

Command example: (purple: payload length red: command type + command code blue: check code)

For example, when reset using the command

Asynchronous command received: 55 0D 80 00 06 (soft reset) 10 (software version) 26 30 79 25 00 4B 12 00 (MAC address) 85

4.2.2 Network Status Change Notification

Command: 0x01

Function:

This asynchronous command will be generated when the module networking is successful, the module networking fails, and the connected module opens the network.

Asynchronous command:

name	cmd data						
	command data						
	Net status	IEEE Addr	Channel	PAGE	ShortAddr	Ext PANID	NWK Key
	network status	MAC address	channel	PAGE	short address	Extended PANID	network key
number of bytes	1	8	1	2	2	8	16

Network status: 0x00 — not networked, 0x01 — networked, 0x02 — network open

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

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Channel: the current channel of the module, 0 when the networking fails
PANID : The current PANID of the module , 0xFFFF when the networking fails
Short address: the current short address of the module, 0xFFFE when the networking fails
Extended PANID : All 0s when networking fails
Network key: all 0s when networking fails

Command example: (purple: payload length red: command type + command code blue: check code)
Coordinator open network notification: 55 29 80 01 02 (network open) C6 B4 E2 0A 00 4B 12 00 (MAC address) 14 (channel) 16 B3 (PANID) 00 00 (short address) C6 B4 E2 0A 00 4B 12 00 (Extended PANID) 1B F0 09 64 46 CB 73 77 A7 66 F8 CA 01 B7 80 F6 (Network Key) 0E

Coordinator restart notification: 55 29 80 01 01 (networked) C6 B4 E2 0A 00 4B 12 00 (MAC address) 14 (channel) 16 B3 (PANID) 00 00 (short address) C6 B4 E2 0A 00 4B 12 00 (Extended PANID) 1B F0 09 64 46 CB 73 77 A7 66 F8 CA 01 B7 80 F6 (Network Key) 0D

4.2.3 Turn on and off network notifications

Command code: 0x02
Function:

After the coordinator opens the network, this asynchronous command informs the window time to open the network. 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 to open the network 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 cut time becomes 0 .
Asynchronous command:

name	cmd data
	command data
	timeout
	window time
number of bytes	1

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

Command example: (purple: payload length red: command type + command code blue: check

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

code)

Send the command feedback to close the network access permission : 55 04 80 02 00 (window time) 82

Note : The coordinator has a 3 -minute window by default , and the coordinator will print a notification when the time is up.

4.2.4 Node Network Access Notification

Command code: 0x03

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 will lead to re-connection to the network. The host computer must pay attention to the first time the node is connected to the network. Usually, only the devices that have experienced the first time access to the network are legal devices.

Asynchronous command:

name	cmd data			
	command data			
	IEEE Addr	Nwk Addr	Parent Addr	Join mode
	MAC address	short address	parent node address	access mode
number of bytes	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)

Command example: (purple: payload length red: command type + command code blue: check code)

Detection node network access notification: 55 10 80 03 0F 4E 03 1C 00 4B 12 00 (MAC address) 2A 25 (network access node short address) 00 00 (parent node short address) 00 (first access to the network) 8B

Detection node re-entry (node restart) : 55 10 80 03 0F 4E 03 1C 00 4B 12 00 (MAC address) 2A 25 (network entry node short address) 00 00 (parent node short address) 01 (re-entry) 8A

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

4.2.5 Node short address update notification

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:

name	cmd data		
	command data		
	IEEE Addr	Nwk Addr	Node Type
	MAC address	short address	Node type
number of bytes	8	2	1

MAC address: The MAC address of the target node

short address: the short address of the target node

Node Type: 1 - Routed, 2 - Do Not Sleep End Node, 3 - Sleep End Node

Command example: (purple: payload length red: command type + command code blue: check code)

Short address update notification : 55 0E 80 04 0F 4E 03 1C 00 4B 12 00(MAC address) 2A 25(Short address) 02(Node type) 8E

4.2.6 Device Information Notification

Command code: 0x05

Function:

Detailed information on the network access node, including the Profile to which all ports (Endpoint) of the network access device belong and the supported clusters (cluster). Based on this information, you can determine what the network access device is and which functions it supports. The message is generated at the moment when the device newly joins the network, and a node may generate multiple messages. If the host computer loses the message, it can re-acquire the message through " Retransmit Device Notification Message ".

Asynchronous command:

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

name	cmd data									
	command data									
	EndFlag	DevSN	Shortaddr	Endpoint	ProfileID	DeviceID	In Cluster List		Out Cluster List	
	end marker	Device SN _	short address	The port number	equipment outline	Device ID	input cluster table		output cluster table	
							quantity	list	quantity	list
number of bytes	1	9	2	1	2	2	1	2*N	1	2*N

Termination flag: A single node will carry multiple ports when it enters the network. The flag is 1 to indicate that the port reporting of the node ends.
DevSN : Device virtual SN number, see Virtual SN
Short address: device short address
Port number: the port number of the device, the port number can be used in combination with the short address, as a 24- bit device address
Device profile: profile ID , the application layer only needs to pay attention to 0x0104
Device ID : Indicates the function of the device, determined by the ZCL protocol specification.
input cluster table: input clusters supported by the device
Output Cluster Table: Output clusters supported by the device

Command example: (purple: payload length red: command type + command code blue: check code)
Device Information Notification :
55 24 80 05 01 (terminator) 01 13 B7 57 22 00 4B 12 00 (device SN number) BE 82 (short address) 01 (port number) 04 01 (device profile) 00 01 (device ID) 04 (input cluster number) 00 00 03 00 04 00 08 FC (input cluster list) 03 (output cluster number) 00 00 03 00 08 FC (output cluster list) 37

4.2.7 Node Off-Grid Notification

Command code: 0x06
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:

name	cmd data

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	command data	
	IEEE Addr	
	MAC address	
number of bytes	8	

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

Command example: (purple: payload length red: command type + command code blue: check code)

Example of off-grid notification: 55 0B 80 06 0F 4E 03 1C 00 4B 12 00 (MAC address) 81

4.2.8 Scan result notification

Command code: 0x0C

Function:

Returns the channel scan result. In beacon scan mode, multiple beacons will be returned. Both the coordinator and the router will generate beacons. According to the number of beacons, you can roughly know how many coordinator routers are in the space, which channels are distributed, what are their PANIDs and short addresses, and how strong the signal strength is.

Asynchronous command:

name	cmd data					
	command data					
	Status	Channel	PAGE	nwkAddr	extPANID	LQI
	scan status	channel	PAGE	short address	Extended PANID	signal strength
number of bytes	1	2	2	2	8	1

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

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

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

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

Extended PANID : Scan to the extended PANID of the 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, the closer the distance, the stronger.

Command example: (purple: payload length red: command type + command code blue: check

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

code)

Feedback: 55 12 80 0C 00(success) 0E(channel) 83 CE(PANID) 1C 67(short address) 45 5A 44 09 00 4B 12 00(extended PANID) A3(signal strength) 1C

4.3 Network management commands

4.3.1 Analysis of network command format

Unified command header format:

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.

4.3.1.1 Input command format:

name	cmd data	
	command data	
	Nwk Addr	Cmd param
	short address	Command parameters
number of bytes	2	lengthen

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

4.3.1.2 Feedback command format:

name	cmd data	
	command data	
	status	handle
	execution status	command number
number of	1	1

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

bytes		

Execution status: 0x00 – Execution is valid, and a confirmation of sending will be generated subsequently. Other Values - Execution is invalid, see AF status table

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

4.3.1.3 Send confirmation format:

name	cmd data		
	command data		
	Nwk Addr	AF status	handle
	short address	send result	command number
number of bytes	2	1	1

Short address: The short address of the sending target

Sending result: wireless sending result, see AF status table

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

Remarks : Send acknowledgment and return E1 (channel interference), E9 (no ACK received), CD (terminal node not online) corresponding to 3.4 AF Status status table

4.3.1.4 Receive network management command and return:

name	cmd data			
	command data			
	Nwk Addr	handle	Zdo status	Cmd param
	short address	command number	Results of the	Command parameters
number of bytes	2	1	1	lengthen

Short address: Returns the short address of the device for the command

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

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

Execution result: The execution result of the command at the receiving end may return "Not supported", see ZDO status table

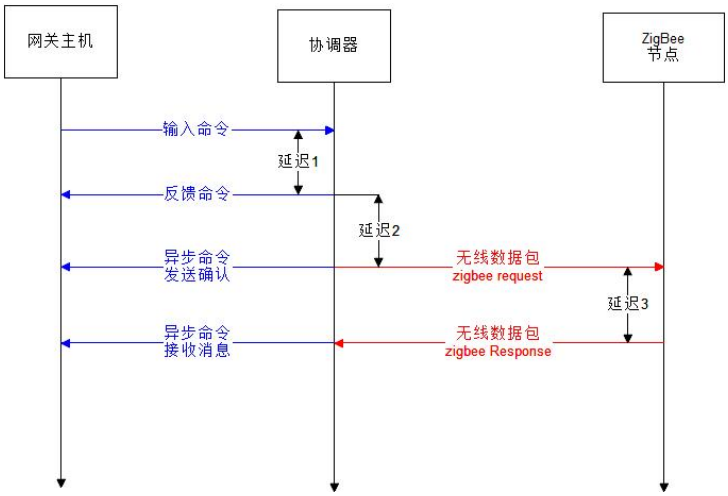
Command parameter: This parameter is valid only when the execution result is 0 .

Instructions for sending and receiving commands:

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

Precautions:

- status of any feedback command is 0 (successful), a sending confirmation will inevitably be generated, and no sending confirmation will be generated for other results.
- AF Status of the sending confirmation is unsuccessful, you can give up waiting for the return message and resend the request.
- For errors such as "full memory" (0x11), "channel interference" (0xE1), "no ACK received " (0xE9), etc., it may be caused by frequent network communication during this period, and you can choose to retransmit, as long as there is no continuous identical Errors are normal.
- For the "target device does not exist" (0xCD) error, it means that the device corresponding to the sending short address is invalid. First check whether the device corresponding to the short address exists, and then check whether the short address of the device has changed. You can use the method of "query node short address" to update the short address of the device



Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

4.3.2 Query node short address

Command code: 0x00

Function:

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

input the command:

name	cmd param
	Command content
	IEEE Addr
	MAC address
number of bytes	8

MAC address: the MAC address of the queried node

Return command:

name	cmd param	
	Command content	
	IEEE Addr	reserve
	MAC address	reserved bit
number of bytes	8	2

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

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 0D 01 00 FD FF (broadcast address) 3D 01 70 0F 00 4B 12 00 (target device MAC address) 19

Feedback command: 55 05 01 00 00 (status successful) 05 (command number) 04

Send confirmation: 55 07 8F 01 FD FF (broadcast address) 05 (command number) 00 (successfully sent) 89

Received and returned: 55 11 81 00 00 A0 (target short address) 05 (command number) 00 (execution successful) 3D 01 70 0F 00 4B 12 00 (target MAC address) B3 00 (reserved byte) 8D

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

4.3.3 Query Node MAC Address

Command code: 0x01

Function:

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

input the command:

name	cmd param
	Command content
	NULL
	null
number of bytes	0

Return command:

name	cmd param	
	Command content	
	IEEE Addr	reserve
	MAC address	reserved bit
number of bytes	8	2

MAC address: the MAC address of the queried node

Command example: (purple: payload length red: command type + command code blue: check code)

Send command : 55 05 01 01 7B 20 (target short address) 5B

Feedback command : 55 05 01 01 00 (status successful) 1A (command number) 1A

Send confirmation: 55 07 8F 01 7B 20 (target short address) 1A (command number) 00 (successfully sent) CF

Received and returned: 55 11 81 01 7B 20 (target short address) 1A (command number) 00 (successful execution) 3D 01 70 0F 00 4B 12 00 (target MAC address) AB 00 (reserved) 70

4.3.4 Query node network configuration information

Command code: 0x02

Function:

Query the network configuration information of a node

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

input the command:

name	cmd param
	Command content
	nwk_add
	short address
number of bytes	2

Return command:

name	cmd param						
	Command content						
	logicalType	freqBand	stackRev	manCode	maxBufSize	maxInSize	maxOutSize
	logical type	frequency band	ZigBee version	Manufacturer code	maximum command length	Max receive	max send
number of bytes	1	1	1	2	1	2	2

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

Frequency band: bitmap of the working frequency band of the node, bit1 - 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

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 05 01 02 27 84 (target short address) A0

Feedback command: 55 05 01 02 00 (status successful) 12 (command number) 11

55 07 8F 01 27 84 (target short address) 12 (command number) 00 (successfully sent) 3F

55 11 81 02 27 84 (target short address) 12 (command number) 00 (execution success) 02 (logic type) 08 (band) 15 (version) 00 20 (manufacturer code) 50 (maximum command length) A0 00 (maximum Receive length) A0 00 (maximum send length) 5D

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

4.3.5 Query node port information

Command code: 0x04

Function:

Queries information about a specified endpoint on a node. Including the profile to which it belongs and the supported cluster .

input the command:

name	cmd param
	Command content
	Endpoint
	The port number
number of bytes	1

Port number: the port number of the target device being queried

Return command:

name	cmd param							
	Command content							
	Endpoint	ProfileID	deviceID	device version	In Cluster List		Out Cluster List	
	The port number	equipment outline	Device ID	Device Information Version	input cluster table		output cluster table	
					quantity	list	quantity	list
number of bytes	1	2	2	1	1	2*N	1	2*N

Port number: the port number of the device being queried

Device profile: profile ID , the application layer only needs to pay attention to 0x0104

Device ID : Indicates the function of the device, determined by the ZCL protocol specification.

Device information version: the version number of the device description information , 0 is v1.0

input cluster table: input clusters supported by the device

Output Cluster Table: Output clusters supported by the device

Command example: (purple: payload length red: command type + command code blue: check code)

Send command : 55 06 01 04 27 84 (destination short address) 01 (destination port) A7

Feedback command : 55 05 01 04 00 (status successful) 15 (command number) 15

Send confirmation: 55 07 8F 01 27 84 15 (command number) 00 (successfully sent) 38

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Received and returned: 55 1D 81 04 27 84 15 (command number) 00 (successful execution) 01 (destination port) 04 01 (device profile) 00 01 (device ID) 00 (device version) 04 (input cluster number) 0000 0300 0400 08FC (input cluster list) 03 (output cluster number) 0000 0300 08FC (output cluster list) 35

4.3.6 Querying the Number of Node Ports

Command code: 0x05

Function:

Query all ports on a node

input the command:

name	cmd param
	Command content
	nwk_add
	short address
number of bytes	2

Return command:

name	cmd param	
	Command content	
	Endpoint Num	Endpoint List
	number of ports	port list
number of bytes	1	N

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

Port list: the port list of the queried node

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 05 01 05 27 84 (short address) A7

Feedback command: 55 05 01 05 00 (status successful) 1A (command number) 1E

Send confirmation: 55 07 8F 01 27 84 (short address) 1A (command number) 00 (successfully sent) 37

Receive and return: 55 09 81 05 27 84 (short address) 1A (command number) 00 (execution

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

success) 01 (port number) 01 (port list) 3D

4.3.7 Set node constant connection binding

Command code: 0x21

Function:

Use ZigBee Bind to set port constant connection binding on two nodes.

input the command:

name	cmd param		
	Command content		
	Src devSN	Cluster ID	Dst devSN
	Source virtual SN	Cluster ID	target virtual SN
number of bytes	9	2	9

Source virtual SN : The SN number of the source virtual device that is often connected , the virtual SN , and the source virtual SN can be obtained in the " Device Information Notification ".

Cluster ID : Cluster ID for constant connection communication

Target virtual SN : virtual SN number of the target device, virtual SN , the target can be a specific virtual device or a group, the target SN is filled with 9 bytes 0x00 and automatically replaced with the virtual SN of the coordinator .

Return command:

name	cmd param
	Command content
	NULL
	null
number of bytes	0

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

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 19 01 21 76 C2 (destination short address) 01 1A E7 45 0A 00 4B 12 00 (source virtual SN) 08FC (cluster ID) 01 49 71 F8 0A 00 4B 12 00 (destination virtual SN) 18

Feedback command: 55 05 01 21 00 (status successful) 05 (command number) 25

Send confirmation: 55 07 8F 01 76 C2 (target short address) 05 (command number) 00 (successfully

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

sent) 3F

Receive and return: 55 07 81 21 76 C2 (target short address) 05 (command number) 00 (execution successful) 11

Remarks : Before setting the normal connection, you need to set the target port of the corresponding terminal device to FE and set the target short address to FF FE to enter the bound Mac communication mode. Only one object is allowed to be set for the normal connection.

4.3.8 Cancel the node constant connection binding

Command code: 0x22

Function:

Release the existing constant connection binding, the format is the same as setting the constant connection binding

input the command:

name	cmd param		
	Command content		
	Src devSN	Cluster ID	Dst devSN
	Source virtual SN	Cluster ID	target virtual SN
number of bytes	9	2	9

Source Virtual SN : The SN number of the source virtual device that is often connected , see Virtual SN .

Cluster ID : Cluster ID for constant connection communication

Target virtual SN : the virtual SN number of the target device , see virtual SN , the target SN is filled with 9 bytes 0x00 and automatically replaced with the virtual SN of the coordinator .

Return command:

name	cmd param
	Command content
	NULL
	null
number of bytes	0

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

Command example: (purple: payload length red: command type + command code blue: check

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

code)

Send command: 55 19 01 22 76 C2 (destination short address) 01 1A E7 45 0A 00 4B 12 00 (source virtual SN) 08 FC (cluster ID) 01 49 71 F8 0A 00 4B 12 00 (destination virtual SN) 1B

Feedback command: 55 05 01 22 00 (status successful) 08 (command number) 2B

Send confirmation: 55 07 8F 01 76 C2 (target short address) 08 (command number) 00 (successfully sent) 32

Receive and return: 55 07 81 21 76 C2 (target short address) 08 (command number) 00 (execution successful) 1F

4.3.9 View the node constant connection binding

Command code: 0x33

Function:

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

Precautions:

Since the binding communication adopts the MAC address method, the source device will automatically search for the target according to the MAC address through the broadcast search method . The more non-existing MACs accumulate, a broadcast storm will be formed, affecting normal communication. Therefore, it is necessary to regularly maintain the network, and regularly check whether all devices in the network are bound to non-existing MAC addresses and delete them.

input the command:

name	cmd param
	Command content
	StartIdx
	start index
number of bytes	1

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

Return command:

name	cmd param					
	Command content					
	TotalNum	StartIdx	ListNum	List Data		
	Total number of records	start index	number of return	Frequent connection record		
				Source virtual SN	Cluster ID	target virtual SN
number of	1	1	1	20*N		
				9	2	9

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

bytes						

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 source virtual SN of the record
Cluster ID : The linked cluster ID of the record
target virtual SN : the recorded target virtual SN

Command example: (purple: payload length red: command type + command code blue: check code)
Send command: 55 06 01 33 76 C2 (target short address) 00 (start index) 86
Feedback command: 55 05 01 33 00 (status successful) 0C (command number) 3E
Send confirmation: 55 07 8F 01 76 C2 (target short address) 0C (command number) 00 (successful sending) 36
Receive and return: 55 1E 81 33 76 C2 (target short address) 0C (command number) 00 (successful execution) 01 (total number of records) 00 (start index) 01 (return number) 011AE745 0A004B1200 (source virtual SN) 08 FC (Cluster ID) 014971F80A004B1200 (Destination Virtual SN) 86

4.3.10 Delete Node

Command code: 0x34
Function:
Delete the specified node according to the MAC address. If the device to be deleted is a terminal node, the short address of this command should be sent to its parent node, fill in the short address of the parent node.
input the command:

name	cmd param		
	Command content		
	IEEE	rejoin	removechild
	MAC address	re-entry	delete child node
number of bytes	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
Return command:

name	cmd param
	Command

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	content
	NULL
	null
number of bytes	0

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

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 0F 01 34 00 00 (parent node short address) 13 B7 57 22 00 4B 12 00 (node MAC) 00 (re-entry) 00 (delete child node) BD

Feedback command: 55 05 01 34 00 (status successful) 09 (command number) 3C

Send confirmation: 55 07 8F 01 00 00 (parent node short address) 09 (command number) 00 (successfully sent) 87

Receive and return: 55 07 81 34 00 00 (parent node short address) 09 (command number) 00 (execution successful) BC

Wait a few seconds and then receive a module off-grid notification

55 0B 80 06 (off-grid notification) 13 B7 57 22 00 4B 12 00 (node MAC) 0E

Note : Since it is uncertain to delete the short address of the parent node of the device, you can use FD FF to broadcast the short address to delete

4.3.11 Channel Interference Detection

Command code: 0x38

Function:

Detect the quality of each channel and the 2.4G interference on each channel, and return the environmental LQI value of each channel. This command only supports on-demand and can be sent to the coordinator itself (ie short address =0x0000). Since scanning channels requires the target device to switch between multiple channels, if the target is a dormant terminal device, it may cause errors to transmit other data during the scanning process .

input the command:

name	cmd param		
	Command content		
	channel mask	duration	count
	channel list	Detection time	number of scans

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

number of bytes	4	1	1

Channel list: 32 -bit channel list, the corresponding channel enable is 1 , for example, when scanning channels 11~26 , fill in 0x07FFF800 , when the value is 0 , it is forced to scan channels 11~26 , and the recommended value is 0x07FFF800 .

Detection time: each channel listening time = (2^duration)*15.36ms , the longer the time, the slower the scanning speed, the maximum value is 5 , that is, each channel listens for 490ms .

Scan times: repeated scan times, range (1~5), it is recommended to fill in 0x01

Return command:

name	cmd param				
	Command content				
	channel mask	total transmit	total fails	channel count	energy list
	channel list	Cumulative sending	Cumulative sending failed	number of channels	Channel Quality List
number of bytes	4	2	2	1	lengthen

Channel list: 32 -bit channel list, the corresponding channel enable is 1 .

Cumulative sending: the cumulative number of data packets sent

Cumulative sending failures: The cumulative number of sending failures (this can be used to view the packet loss rate)

Number of channels: returns the number of scanned channels, combined with the returned channel list, can match the corresponding channels in the channel quality list

Channel quality list: The signal strength on the channel, represented by the LQI value, the maximum is 0xFF .

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 0B 01 38 00 00 (target short address) 00 F8 FF 07 (channel list) 05 (detection time) 01 (scan times) 3D

Feedback command: 55 05 01 38 00 (status successful) 12 (command number) 2B

Send confirmation: 55 07 8F 01 00 00 (target short address) 12 (command number) 00 (successfully sent) 9C

Receive and return: 55 20 81 38 00 00 (target short address) 12 (command number) 00 (execution success) 00 F8 FF 07 (channel list) C8 04 (cumulative sending) 00 00 (accumulating sending failed) 10 (number of channels) 7F BD AB 91 B9 99 CC BD 83 86 B6 E1 AB 66 66 B6 (channel quality list) 91

Notice:

- The channel signal strength list is the LQI value, and 0xFF is the strongest signal. You can use the

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

ratio obtained by dividing this value by 0xFF . If the ratio exceeds 80% , it is considered a very bad channel. The channel with the smallest signal is preferentially selected to create a network.

- From the time of receiving the sending confirmation to receiving the receiving return, the time to wait is at least (2^5)*15.36*16 = 7864.32ms , plus the serial port transmission delay and ZigBee command transmission delay, the actual need to wait 8~ 9 seconds.

4.4 Device Status Management and Control (ZCL Command)

4.4.1 ZCL protocol structure and related explanation

- ✧ Endpoint (port): There may be multiple application peripherals on a ZigBee device, and they may have the same and different functions. For example, each hole on the multi-hole socket has the same control function, which is located to the socket through the short address and MAC address, and is located to the jack through the port.
- ✧ Profile : used to mark the application protocol type of the port, the device side will refuse to execute commands from different profiles . Each Endpoint has a fixed Profile , a device with multiple ports, and can support multiple Profiles at the same time .
- ✧ Cluster : Cluster is used to describe the functional cluster supported by the device. Usually, a function will contain multiple control methods, multiple physical quantities or states, and there is a strong correlation between them. A port can support multiple clusters, indicating which functions it supports. The cluster is divided into two types : " Input " and " Output ". The input cluster indicates that the port of the device is the controlled party, and the output cluster indicates that the port is the party that initiates control. In principle, a port cannot be both a controller and a controlled person, otherwise it is easy to cause "self-locking".
- ✧ Attribute : In the ZCL protocol, each attribute represents a state parameter or physical quantity of the target device. The related states or physical quantities are usually compiled into the same cluster, and the commands to access attributes (read, modify, view, report) can carry multiple attribute parameters under the same cluster at the same time in one command, and all clusters have uniform attributes Access command structure format. If multiple identical attributes may exist on a single device, they are usually assigned to different ports. For example, the target device is a multi-hole socket. The opening and closing status and power consumption of each socket have their own independent parameters. They will use the same cluster ID and attribute ID , but the target ports are different. By setting different target ports to obtain the required corresponding The state parameter of the target.
- ✧ commands: Attributes and control commands are the means to operate the device provided in a cluster. Since attributes usually correspond to static variables in the device, the size is fixed and the data is short, so when sending a variable-length message to the controlled device, or the controlled device needs to return a variable-length message, it is all implemented through

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

control commands. Different from attribute access commands, control commands do not have a unified command structure, and different clusters have different control command structures. The parameters carried by the control command first change the physical state of the target device, and then synchronize to the corresponding attribute when the physical state changes. Therefore, some control commands cannot be used to control the target device by modifying the attributes, and the control commands can carry more Complex control parameters, and attributes must be fixed format data in Table 3.5 .

✧ The causality of ZCL control: a device with an output cluster (accurate to the port) sends a control command to a device (port) with an input cluster, causing one or more physical states of the input command to change, and the physical quantity of the change The value of is synchronized to the corresponding attribute under the cluster, causing any other device in the network to access the attribute corresponding to the physical state on the controlled device, which reflects the current physical state of the controlled device.

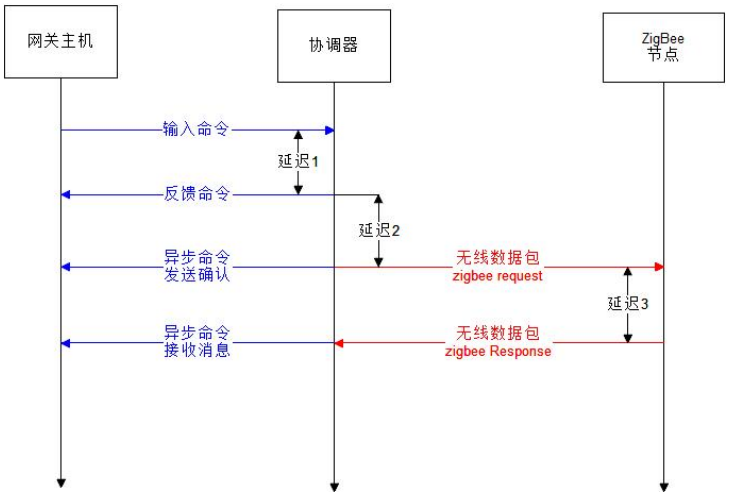
4.4.2 ZCL command format parsing

Unified command header format:

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 command", "feedback command", and two asynchronous commands, "send confirmation" and "receive command", with a total of 4 different formats . The access to the device adopts the 24- bit virtual address method of short address + port number .

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



① **command format:**

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

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

name	cmd data								
	command data								
	mode	shortAddr	Endpoint	SeqNum	Direction	ClusterID	ManuCode	AckMode	Ext data
	send mode	target short address	destination port	frame number	command direction	Cluster ID	Manufacturer code	Answer mode	Extended data
number of bytes	1	2	1	1	1	2	2	1	lengthen

Send Mode: 0x00 – Normal Mode, 0x40 – APS Encrypted, 0x80 – Route Forwarding Skip, 0xC0 – APS Encryption and Skip Route Forwarding

Target short address: send target short address, 0xFFFC~0xFFFF is broadcast (0xFFFE is invalid address)

Target port: the port of the sending target, fill in 0xFF and the short address is not broadcast, then use multicast sending

Frame serial number: The host computer generates the frame serial number. If the frame serial number and short address of the ZCL frame are received, and the port is equal to the sending, the message is the reply message of the target device.

Command direction: refer to the ZCL framework, 0 - C2S (attack- > accept), 1 - S2C (accept- > attack)

Cluster ID : The cluster ID that sent the message

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

Answer Mode: 0 - Answer with Default Response , 1 - Answer with APS Ack .

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

② **Feedback command format:**

name	cmd data	
	command data	
	status	SeqNum
	execution status	frame number
number of bytes	1	1

Execution status: 0 - Execution is valid, a confirmation of sending will be generated, other see AF status

Frame serial number: the frame serial number filled in when the host computer sends the corresponding command

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

③ **confirmation format:**

name	cmd data					
	command data					
	mode	shortAddr	Endpoint	SeqNum	Direction	AF status
	send mode	target short address	destination port	frame number	command direction	send result
number of bytes	1	2	1	1	1	1

Send mode: same as when sending

Destination Short Address: Send the destination short address, the same as when sending

Destination Port: The port to which the destination is sent, the same as when sending

Frame number: the same as when sending the command

Command direction: the same as when sending the command

Sending result: wireless sending result, see **AF status table**

④ **command "receive ZCL message" format:**

When the coordinator receives the ZCL message, it will convert it into the following unified header format

name	cmd data								
	command data								
	mode	shortAddr	Endpoint	SeqNum	Direction	ClusterID	ManuCode	Rssi	Ext data
	opponent mode	source short address	source port	command number	command direction	Cluster ID	Manufacturer code	signal strength	Extended data
number of bytes	1	2	1	1	1	2	2	1	lengthen

Peer mode: 0x00 - normal reception, 0x10 - broadcast received, 0x20 - signal strength valid, 0x30 - broadcast received and signal strength valid

Source short address: the short address of the other device

Source port: the port of the other device

Frame serial number: The frame serial number of the received message. If the received frame serial number, source address, and source port are the same as when sent, and the command direction is opposite, it is the return command of the sent command.

Command direction: refer to the ZCL framework, 0 - C2S (attack- > accept), 1 - S2C (accept- > attack)

Cluster ID : The cluster ID of the received message

Manufacturer Code: The manufacturer code of the received message, which needs to be supported by the source device.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Signal Strength: The RSSI value of the signal strength of the received message
Extended data: The extended data of different commands is different, and the subsequent command parsing will only analyze the extended data part

4.4.3 ZCL Command Type and Function List

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.

Function	command code	send	take over
read target properties	0x00	ZCL_READ_ATTR_REQ	ZCL_READ_ATTR_RSP
Modify target properties	0x01	ZCL_WRTIE_ATTR_REQ	ZCL_WRTIE_ATTR_RSP
Query attribute reporting rules	0x02	ZCL_READ_REPORT_REQ	ZCL_READ_REPORT_RSP
Modify attribute reporting rules	0x03	ZCL_WRITE_REPORT_REQ	ZCL_WRITE_REPORT_RSP
View all properties	0x04	ZCL_DISC_ATTR_REQ	ZCL_DISC_ATTR_RSP
View all properties (with extensions)	0x05	ZCL_DISC_ATTR_EX_REQ	ZCL_DISC_ATTR_EX_RSP
Active reporting of attributes	0x0A	none	ZCL_REPORT_IND
The system returns by default	0x0B	none	ZCL_DEFAULT_RSP
send control commands	0x0F	ZCL_CMD	none
receive control commands	0x0F	none	ZCL_CMD_IND

✧ "Query attribute reporting rules" and "Modify attribute reporting rules" require the target device to support this function. This wireless module only supports sending and receiving of this command, and there is no example command.

4.4.4 Read target properties

Command code: 0x00
Function: Read ZCL attribute parameters, you can read multiple parameters in a specified cluster on a port
Input command format:

name	ext data	
	Extended data	
	AttrNum	AttrID List
	number	List of

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	of properties	property IDs
number of bytes	1	2*N

Number of properties: The number of properties read at one time, the properties actually read can only be less than or equal to this value.
property list: a list of uint16 arrays consisting of property IDs

Feedback command format:

name	ext data				
	Extended data				
	AttrNum	Attr List * N			
	number of properties	property list			
		property ID	ZCL status	type of data	data value
number of bytes	1	2	1	1	lengthen

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

Command example: (purple: payload length red: command type + command code blue: check code)
Read all attributes under **Cluster ID 0xFC08** : (read 0x0000, 0x0001, 0x0002, 0x0003, 0x0004)
Send command: 55 19 02 00 00 (send mode) 7B 20 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) 00 (response mode) 05 (number of read attributes) 00 00 01 00 02 00 03 00 04 00 (attribute ID list) 2F
Feedback command: 55 05 02 00 00 (status successful) A2 (frame number) A0
Send confirmation: 55 0A 8F 02 00 (send mode) 7B 20 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 00 (successful transmission) 75
Receive and return: 55 2C 82 00 00 (peer mode) 7B 20 (source short address) 01 (source port) A2 (frame number) 01 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) FF (RSSI) 05(Number of attributes) 00 00(Attribute ID) 00(ZCL status) 23(Data type) 00 C2 01 00(Baud rate) 01 00(Attribute ID) 00(ZCL status) 21(Data type) FF FF(Transparently transmit the target short address) 02 00(attribute ID) 00(ZCL state) 20(data type) FF(transparent destination port) 03 00(attribute ID) 00(ZCL state) 10(data type) 00(serial port command mode) 04 00(attribute ID)

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

00(ZCL state) 30(Data type) 00(Low power level) 6F

Read all attributes under **Cluster ID 0x0000** : (read 0x0000, 0x0001, 0x0002, 0x0003, 0x0004, 0x0005, 0x0006, 0x0007)

Send command: 55 1F 02 00 40 (send mode) ED BD (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 00 00 (cluster ID) 00 00 (manufacturer code) 00 (response mode) 08 (number of attributes) 0000 0100 0200 0300 0400 0500 0600 0700 attribute list B9

Feedback command: 55 05 02 00 00 (status successful) A2 (frame number) A0

Send confirmation: 55 0A 8F 02 40 (send mode) ED BD (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 00 (successful transmission) 3E

Receive and return: 55 5F 82 00 00 (peer mode) ED BD (source short address) 01 (source port) A2 (frame number) 01 (command direction) 00 00 (cluster ID) 00 00 (manufacturer code) FF (RSSI) 08(Number of attributes) 00 00(Attribute ID) 00(ZCL status) 20(Data type) 01(ZigBee version) 01 00(Attribute ID) 00(ZCL status) 20(Data type) 10(Software version) 02 00 (attribute ID) 00(ZCL Status) 20(Data Type) 16(Protocol Version) 03 00(Attribute ID) 00(ZCL Status) 20(Data Type) 01(Hardware Version) 04 00(Attribute ID) 00(ZCL Status) 42(Data type string) 10(string length) 77 77 77 2E 45 62 79 74 65 2E 63 6F 6D 20 20 20(vendor name) 05 00(attribute ID) 00(ZCL status) 42(data type string) 10(String length) 45 31 38 2D 5A 69 67 62 65 65 2D 44 61 74 61 2E (product model) 06 00 (attribute ID) 00 (ZCL status) 42 (data type string) 08 (string length) 32 30 32 32 30 34 32 34 (compile date) 07 00 (Attribute ID) 00(ZCL status) 30(Data type) 01(Power mode) E7

Manufacturer Name: 10 (Data Length) 77 77 77 2E 45 62 79 74 65 2E 63 6F 6D 20 20 20 Convert to **ASCII** www.Ebyte.com

Product Model: 10 (Data Length) 45 31 38 2D5A 69 67 62 65 65 2D 44 61 74 61 2E Convert to ASIC **E18-Zigbee-Data.**

Compilation date: 08 (data length) 32 30 32 32 30 34 32 34 converted to **ASCII** 20220424

Remarks :

1. If the target short address is read in FD FF broadcast mode, all devices in the network except the coordinator will give feedback. It is not recommended to use broadcast mode to query and modify device information;

2. When reading multiple attributes at one time, the port index + sending mode in the sending command needs to be sent using " 0x40 ", otherwise the sending of the read command will fail;

3. The attributes under Cluster ID 0x0000 do not support the terminal device to read its own attributes, but the terminal device can read other devices;

4. Port index + sending mode: If you use ZCL command for data communication transmission, you need to use port index + sending mode: 0x40 mode to send.

4.4.5 Modify target properties

Command code: 0x01

Function: 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 consistent with

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

that in the target device. If the modification is invalid, which attributes will be invalidated in the returned command.

Input command format:

name	ext data			
	Extended data			
	AttrNum	Attr List * N		
	number of properties	property list		
		property ID	type of data	data value
number of bytes	1	2	1	lengthen

Number of attributes: The number of attributes that need to be modified

Attribute ID : The attribute ID that needs to be modified

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

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

Feedback command format:

name	ext data		
	Extended data		
	AttrNum	Attr List * N	
	number of properties	property list	
		property ID	ZCL status
number of bytes	1	2	1

Number of attributes: 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 .

property ID : Modified property ID

ZCL status: the cause of the error, see chapter 3.6 " ZCL Error Status Code "

Command example: (purple: payload length red: command type + command code blue: check code)

① the baud rate of the target device

Send command: 55 13 02 01 00 (send mode) 78 B8 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) 00 (response mode) 01 (attribute number) 00 00 (attribute ID) 23 (data type) 80 25 00 00 (baud rate) B4

Feedback command: 55 05 02 01 00 (status successful) A2 (frame number) A1

Send confirmation: 55 0A 8F 02 00 (send mode) 78 B8 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 00 (successful transmission) EE

Receive and return: 55 12 82 01 00 (peer mode) 78 B8 (source short address) 01 (source port) A2

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

(frame number) 01 (command direction) 08 (cluster ID) 00 20 (manufacturer code) FF (RSSI) 01 (Number of attributes) 00 00 (Attribute ID) 88 (ZCL error) 43

Note: Because modifying the baud rate of the device does not support direct modification, you need to use the send control command to modify it. Therefore, the direct use of the modify attribute command to set is unsuccessful, and the 0x88 error "read-only" is returned.

② the target short address of transparent transmission

Send command: 55 13 02 01 00 (send mode) 78 B8 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) 00 (response mode) 01 (attribute number) 01 00 (attribute ID) 21 (data type) FD FF (transparent target short address) 97

Feedback command: 55 05 02 01 00 (status successful) A2 (frame number) A1

Send confirmation: 55 0A 8F 02 00 (send mode) 78 B8 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 00 (successful transmission) EE

Received and returned: 55 0F 82 01 00 (peer mode) 78 B8 (source short address) 01 (source port) A2 (frame number) 01 (command direction) 08 (cluster ID) 00 20 (manufacturer code) FF (RSSI) 00 (number of attributes) CA

Remarks: If the modification is successful, the number of attributes that return the modification failure is 0

③ the target port of transparent transmission

Send command: 55 13 02 01 00 (send mode) 78 B8 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) 00 (response mode) 01 (attribute number) 02 00 (attribute ID) 20 (data type) 11 (transparent destination port) 86

Feedback command: 55 05 02 01 00 (status successful) A2 (frame number) A1

Send confirmation: 55 0A 8F 02 00 (send mode) 78 B8 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 00 (successful transmission) EE

Received and returned: 55 0F 82 01 00 (peer mode) 78 B8 (source short address) 01 (source port) A2 (frame number) 01 (command direction) 08 (cluster ID) 00 20 (manufacturer code) FF (RSSI) 00 (number of attributes) CA

④ the transparent transmission mode

Send command: 55 13 02 01 00 (send mode) 78 B8 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) 00 (response mode) 01(number of attributes) 03 00(attribute ID) 10(data type) 01(transparent mode) A7

Feedback command: 55 05 02 01 00 (status successful) A2 (frame number) A1

Send confirmation: 55 0A 8F 02 00 (send mode) 78 B8 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 00 (successful transmission) EE

Received and returned: 55 0F 82 01 00 (peer mode) 78 B8 (source short address) 01 (source port) A2 (frame number) 01 (command direction) 08 (cluster ID) 00 20 (manufacturer code) FF (RSSI) 00 (number of attributes) CA

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

⑤ Modify the low power consumption level

Send command: 55 13 02 01 00 (send mode) 78 B8 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) 00 (response mode) 01(number of attributes) 04 00(attribute ID) 30(data type) 01(power level) B7

Feedback command: 55 05 02 01 00 (status successful) A2 (frame number) A1

Send confirmation: 55 0A 8F 02 00 (send mode) 78 B8 (destination short address) 01 (destination port) A2 (frame number) 00 (command direction) 00 (successful transmission) EE

Received and returned: 55 0F 82 01 00 (peer mode) 78 B8 (source short address) 01 (source port) A2 (frame number) 01 (command direction) 08 (cluster ID) 00 20 (manufacturer code) FF (RSSI) 01 (number of attributes) 04 00 (attribute ID) 88 (ZCL error) 70

Note: To modify the low power consumption level of the device, you need to use the send control command to modify it.

4.4.6 Query attribute reporting rules

Command code: 0x02

Function:

Query the rules for automatic reporting of attributes, provided that the queried attributes support automatic reporting

enter:

name	ext data	
	Extended data	
	AttrNum	AttrIDList
	number of properties	List of property IDs
number of bytes	1	2*N

Number of properties: The number of properties queried.

property list: the ID of the property being queried

return:

name	ext data						
	Extended data						
	AttrNum	AttrList * N					
	number of properties	property list					
		property ID	ZCL status	minimum time	maximum time	type of data	variable
number of	1	2	1	2	2	1	align to lengthen

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

bytes							

Number of properties: Returns the number of properties for the query

property ID : the returned property ID

ZCL status: see " ZCL error status code ", only " operation successful " has the following data

Minimum time: The minimum interval for continuous reporting of this attribute, which can filter data reporting due to continuous jitter of the status value.

Maximum time: the maximum interval time reported by this attribute, which can be used as the heartbeat cycle

Data type: The data type of the variable value, see " ZCL Data Type Table "

Variable value: The change of the attribute value exceeds the variable value to trigger the report, and the value needs to be aligned by 4 bytes according to the size in " Report Alignment" in the " ZCL Data Type Table ".

Instruction example (not yet available)

4.4.7 Modifying property reporting rules

Command code: 0x03

Function:

Modify the automatic reporting rule of attributes, provided that the queried attribute supports automatic reporting, and the attribute that fails to be set will appear in the return command

enter:

name	ext data					
	Extended data					
	AttrNum	AttrList * N				
	number of properties	property list				
		property ID	minimum time	maximum time	type of data	variable
number of bytes	1	2	2	2	1	align to lengthen

Number of properties: the number of properties to set

property ID : The property ID of the setting

Minimum time: The minimum interval for continuous reporting of this attribute, which can filter data reporting due to continuous jitter of the status value.

Maximum time: the maximum interval time reported by this attribute, which can be used as the heartbeat cycle

Data type: The data type of the variable value, see " ZCL Data Type Table "

Variable value: The change of the attribute value exceeds the variable value to trigger the report, and the value needs to be aligned by 4 bytes according to the size in " Report Alignment" in the " ZCL Data Type Table ". If the alignment length is 0 , this property does not need to set the variable value.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

return:

name	ext data		
	Extended data		
	AttrNum	AttrList * N	
	number of properties	property list	
		property ID	ZCL status
number of bytes	1	2	1

Number of properties: This number only includes the number of properties that are not set

property id : set invalid property id

ZCL Status: Error reason, see " ZCL Error Status Code "

Instruction example (not yet available)

4.4.8 View all properties

Command code: 0x04

Function:

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

Input command format :

name	ext data	
	Extended data	
	AttrNum	AttrID
	number of properties	start attribute id
number of bytes	1	2

Number of properties: the number of properties expected to be queried 01

Starting attribute ID : start the search from the starting attribute ID

Feedback command format :

name	ext data			
	Extended data			
	End Flag	AttrNum	AttrList * N	
	end sign	number of attributes	query list	
			property ID	type of data

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

number of bytes	1	1	2	1

End flag: The returned query result includes the last attribute under the cluster
Number of attributes: The number of attributes returned by this query
property ID : the returned property ID
Data type: The data type corresponding to the attribute ID , see the data type table

Command example: (purple: payload length red: command type + command code blue: check code)

Send command: 55 11 02 04 00 (send mode) 6C 35 (destination short address) 01 (destination port) 95 (frame number) 00 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) 00 (response mode) 08 (number of read) 00 00 (start attribute ID) 17
Feedback command: 55 05 02 04 00 (status success) 95 (frame number) 93
Send confirmation: 55 0A 8F 02 00 (send mode) 6C 35 (destination short address) 01 (destination port) 95 (frame number) 00 (command direction) 00 (successful transmission) 40
Received and returned: 55 1F 82 04 20 (peer mode) 6C 35 (source short address) 01 (source port) 95 (frame number) 01 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) BD (RSSI)) 01(end flag) 05(attribute number) 00 00(attribute ID) 23(data type) 01 00(attribute ID) 21(data type) 02 00(attribute ID) 20(data type) 03 00(attribute ID)) 10 (data type) 04 00 (attribute ID) 30 (data type) 01

4.4.9 View all properties (with extensions)

Command code: 0x05
Function:

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

Input command format :

name	ext data	
	Extended data	
	AttrNum	AttrID
	number of properties	start attribute id
number of bytes	1	2

Number of properties: the number of properties expected to be queried
Starting attribute ID : start the search from the starting attribute ID

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Feedback command format :

name	ext data				
	Extended data				
	End Flag	AttrNum	AttrList * N		
	end sign	number of attributes	query list		
			property ID	type of data	operate
number of bytes	1	1	2	1	1

End flag: The returned query result includes the last attribute under the cluster
Number of attributes: The number of attributes returned by this query
property ID : the returned property ID
Data type: The data type corresponding to the attribute ID , see " Data Type Table "
Operation: bit0 - readable, bit1 - writable, bit2 - support active reporting

Command example: (purple: payload length red: command type + command code blue: check code)

Send to view the full status of the device (enhanced):

Send command: 55 11 02 05 00 (send mode) E9 8E (destination short address) 01 (destination port) 95 (frame number) 00 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) 00 (response mode) 08(Number of read attributes) 00 00(Start attribute ID) 28

Feedback command: 55 05 02 05 00 (status success) 95 (frame number) 92

Send confirmation: 55 0A 8F 02 00 (send mode) E9 8E (destination short address) 01 (destination port) 95 (frame number) 00 (command direction) 00 (successful transmission) 7E

Received and returned: 55 24 82 05 00 (peer mode) E9 8E (source short address) 01 (source port) 95 (frame number) 01 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) FF (RSSI) 01(end flag) 05(attribute number) 00 00(attribute ID) 23(data type) 01(operation read-only) 01 00(attribute ID) 21(data type) 03(operation can read and write) 02 00(attribute ID) 20(data type) 03(read/ write) 03 00(attribute ID) 10(data type) 03(operation read/write) 04 00(attribute ID) 30(data type) 01(operation read-only) 5F

Note: Since the attributes representing baud rate and low power consumption level are "read-only", the previous test of "modify attributes" was unsuccessful

4.4.10 Active status report

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.

take over:

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

name	ext data			
	Extended data			
	AttrNum	AttrList * N		
	number of properties	property list		
		property ID	type of data	data value
number of bytes	1	2	1	lengthen

Number of attributes: The number of attributes read. If the device supports some attribute IDs contained in the read command , the returned command also does not contain these attributes.
Attribute ID : The 16 -bit attribute ID read
Data type: data type, see " Data Type Table "
Data value: The state value corresponding to this attribute, the size is determined by the "bytes" item in the data type

Command example: (purple: payload length red: command type + command code blue: check code)
Receive the heartbeat packet of the data transparent transmission module: (The content of the heartbeat packet is the low power consumption level of the transparent transmission module)
Received command: 55 13 82 0A 20 (peer mode) 0F DC (source short address) 01 (source port) 08 (frame number) 01 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) 9C (signal strength) 01(number of attributes) 04 00(attribute ID) 30(data type) 01(data value) 0F

4.4.11 Default return frame

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

take over:

name	ext data	
	Extended data	
	ZCL status	Cmd ID
	ZCL status	Command ID
number of	1	1

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

bytes		

ZCL status: see 3.6 " ZCL Error Status Code "

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

4.4.12 Sending control commands

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.

Send control command format:

name	ext data	
	Extended data	
	Cmd ID	Cmd param
	Command ID	Command parameters
number of bytes	1	lengthen

Command ID : Command ID of the control command

Command parameters: the parameters carried by the control command, the content of the command parameters is determined according to the difference of cluster , cmd ID and manufacture Code

Receive control command format:

name	ext data	
	Extended data	
	Cmd ID	Cmd param
	Command ID	Command parameters
number of bytes	1	lengthen

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Command ID : Command ID of the received control command
Command parameters: the parameters carried by the received control command, the content of the command parameters is determined according to the difference of cluster , cmd ID and manufacture Code

Instruction example: Since the sending control command is related to the receiving control command, the example of combining the sending command in the receiving control command

4.4.13 Receive control commands

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.

take over:

name	ext data	
	Extended data	
	Cmd ID	Cmd param
	Command ID	Command content
number of bytes	1	lengthen

Command ID : Command ID of the received control command
Command content: The parameter content carried by the received control command is determined according to the difference of cluster , cmd ID and manufacture Code

Command example: (purple: payload length red: command type + command code blue: check code)
Control object: E18 wireless data transmission module

① control commands to modify the **baud rate** of the transparent transmission module :
Send command: 55 10 02 0F 00 (send mode) CB A6 (destination short address) 01 (destination port) AB (frame number) 00 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) 00 (response mode) 02 (command ID) 80 25 00 00 (command parameter = baud rate) B9
Feedback command : 55 05 02 0F 00 (status successful) AB (frame number) A6
Send confirmation: 55 0A 8F 02 00 (send mode) CB A6 (destination short address) 01 (destination port) AB (frame number) 00 (command direction) 00 (successful transmission) 4A

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Received and returned: 55 14 82 0F 20 (peer mode) CB A6 (source short address) 01 (source port) AB (frame number) 01 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) FC (RSSI) 02(command ID) 00(command parameter 1= execution successful) 80 25 00 00(command parameter 2= baud rate) E4

② Send **control commands to modify the low power consumption level** of the transparent transmission module :

Send command: 55 10 02 0F 00 (send mode) 2B DC (destination short address) 01 (destination port) AA (frame number) 00 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) 00 (response mode) 03(command ID) 03(command parameter = power level) 85

Feedback command: 55 05 02 0F 00 (successful status) AA (frame number) A7

Send confirmation: 55 0A 8F 02 00 (send mode) 2B DC (destination short address) 01 (destination port) AA (frame number) 00 (command direction) 00 (successful transmission) D1

Receive and return: 55 10 82 0F 20 (peer mode) 2B DC (source short address) 01 (source port) AA (frame number) 01 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) FC (RSSI) 03 (command ID) 00 (command parameter = execution successful) DB

③ Broadcast **control instructions** are used to **mark equipment** : (There may be interference or data congestion during broadcast control)

Send command: 55 11 02 0F 00 (send mode) FD FF (broadcast destination short address) FF (broadcast destination port) A1 (frame number) 00 (command direction) 03 00 (cluster ID) 00 00 (manufacturer code) 00(answer mode) 00(command ID) 00 00(command parameter = duration) 53

Feedback command: 55 05 02 0F 00 (status successful) A1 (frame number) AC

Send confirmation: 55 0A 8F 02 00 (send mode) FD FF (target short address) FF (broadcast destination port) A1 (frame number) 00 (command direction) 00 (broadcast success) D1

Note : The IDENTIFY cluster is used to mark the device. When the device is in the marked state, the indicator light of the E18 transparent transmission module will flash.

④ Receive " HelloWorld " sent by the **control command** module **through transparent data transmission**

Received command: 55 19 82 0F 20 (peer mode) CC 52 (source short address) 01 (source port) 10 (frame number) 01 (command direction) 08 FC (cluster ID) 00 20 (manufacturer code) DA (RSSI)) 00 (command ID) 48 65 6C 6C 6F 57 6F 72 6C 64 (command parameter =HelloWorld) 2D

4.4.14 ZCL properties and controls

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

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

4.4.14.1 Cluster=0x0000

Function: This cluster defines the factory information of the device, and almost all devices must support this cluster (BASIC 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 Identify	Product number	string	read only
0x0006	Date Code	compile date	string	read only
0x0007	Power Source	Power mode	enum8	read only

4.4.14.2 Cluster=0x0003

Function: 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 (IDENTIFY cluster)

Property sheet:

Cluster = 0003， Server				
AttrID	Descriptor	name	type of data	operate
0x0000	Identify Time	mark time	Win16	read and write

Send control commands:

Cluster = 0003， Client->Server			
cmdID	Descriptor	name	parameter
0x00	Identify	marking equipment	uint16 IdentifyTime : Mark Mode Duration

Receive control commands:

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Cluster = 0003， Sever->Client			
cmdID	Descriptor	name	parameter
0x00	IdentifyQueryresponse	Back to Query Marking Devices	uint16 timeout: remaining mark time

4.4.14.3 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 information	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 : The 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 does not need to be added, only the group ID is required . If you really need to add it, the header should not exceed 16 characters.
- When checking groups, fill in count with 0 to query all groups, and if it is not 0 , check whether the groups in the groupList exist on the device.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

- 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 a group. There is no corresponding return for this command, and only "default return" can be received during unicast.

Receive control commands:

Cluster = 0004， Sever->Client			
cmdID	Descriptor	name	parameter
0x00	AddGroupRsp	return equipment group	uint8 status: ZCL status 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 groups can be added uint8 count: The number of devices added to the group uint16 groupList [ ]: The group that the device joins
0x03	RemoveGroupRsp	remove a group return	uint8 status: ZCL status uint16 groupID : The group ID of the removed group

4.4.14.4 Cluster=0xFC08

Function: dedicated to Ebyte data transparent transmission

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

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

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Transparent transmission mode: 0- command mode, 1- transparent transmission mode
Low power mode: 0 - 1 second wake up (heartbeat packet 2 minutes), 1 - 3.33 seconds wake up (heartbeat packet 4 minutes), 2 - 5 seconds wake up (heartbeat packet 6 minutes),
3 - Sleep all the time (with 8 minute heartbeat packets)

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
0x04	Reset	Module restart	uint8 extAddr [8]: The MAC address of the module

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
The module cannot be broadcasted after restarting. It needs to fill in the correct MAC address. Even if it is broadcast, only one can be restarted.

Receive control commands:

Cluster = 0xFC08， manuCode=0x2000, Sever->Client			
cmdID	Descriptor	name	parameter
0x00	UartNotify	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

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

5.User Notice

5.1 ZigBee network roles and precautions

serial number	describe
1	This module adopts ZigBee network networking and only realizes the functions of coordinator and router.
2	The Zigbee network is a Mesh structure, which is not affected by the network depth. The more routing nodes are connected, the more sub-nodes are supported. (The total number of terminal child nodes is 48 , and the maximum number of networking is 200)
3	The coordinator can save data for 7 seconds for dormant terminals.
4	Broadcast performance: The maximum broadcast within 5 seconds does not exceed 100 packets, which actually depends on the broadcast receiving capability of the access device.
5	The coordinator is unique in the network, and the short address is fixed at 0000 .
6	If the on-demand address is FFFF , FFFD , FFFC , it corresponds to three broadcast modes respectively. If multicast transmission is required, the target port is set to 0 , and the target short address is set to the group ID .
7	When the network parameter PANID is FFFF , the PANID is automatically generated . If you need to manually set the PANID, you need to ensure that there is no coordinator and router with the PANID in the space, including the router that joined the coordinator last time.
8	All devices in the network have the broadcast function turned on. Simultaneous broadcasting by multiple devices or higher-frequency broadcasting by a single device may cause serious network congestion. Please try to avoid this situation.
9	All wireless commands will generate a sending confirmation, and the return time of the sending confirmation will be different for different sending targets, and even out of order. After sending a wireless command to a specific target, it is recommended to wait for an acknowledgment before sending the next command to that target. But sending commands to multiple different targets does not need to wait for a confirmation to send the command to the next target. For example, when there are routing nodes and sleeping nodes in the sending target, the routing node returns faster than the sleeping node.
10	In ZigBee network communication, the single-packet data transmission cycle cannot be too fast (generally recommended to be more than 1 second, or wait for the device to send confirmation or asynchronous return). Too fast may cause data loss. (Special attention, too many nodes in the network, too fast broadcast cycle may cause network instability.)
11	According to the node network access notification and device information notification, it is determined whether the network access node is the first time access to the network or the network is restored. A device with a first-time access record can be counted as a legitimate device. When deleting a node, if the node just shuts down or is offline, it can be considered that the device is illegal, and the next time it receives any information from the device (including the network access notification is not the first time to access the network), immediately send a delete command

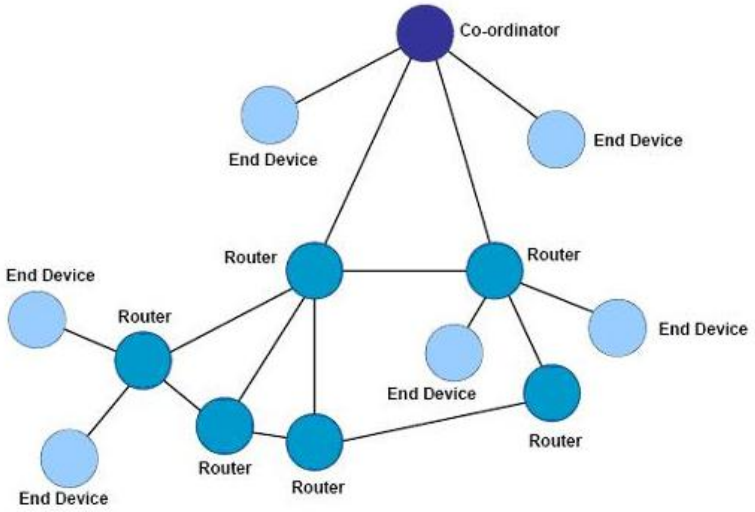
Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

5.2 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 hop"; this topology can also form a very complex network; the network also has self-organization and self-healing functions;
Network structure diagram 

5.3 Getting Started with Device Communication

5.3.1 Setting up the coordinator

The host computer software connects to the coordinator module:

1、Select the corresponding serial port;

2、Select the current module model (network manager)

3、Select the baud rate (the network manager is 230400);

4、Open the serial port;

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Figure 5-1

Configure Coordinator Mode

1、 Read the current module parameters and return a valid long address;

2、 Select the device type to be set (currently we choose the coordinator);

3、 Set the soft start mode (recommended to select "Auto")

4、 Write parameters (write the set device type into the module);

5、 configuration is completed, reset or re-power the network manager module



Figure 5-2

The coordinator creates a new network

1、 There are three ways to set the channel, enable, disable and overwrite. If you don't select it, it will read only the current enabled channel. It is recommended to select disable.

2、 Select the channel to be used, if you need to disable 11 channels, light 11

3、 Click the channel button to set the channel. It is currently in disable mode. After the channel is configured successfully, the enabled channel in the channel list will be lit.

4、 Click to open the network, and after the coordinator creates the network, it will display "Open the network successfully".

5、 Click to read the parameters, you will get the coordinator's PANID , short address, extension ID , current working channel, and the network status shows that the network has been established.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



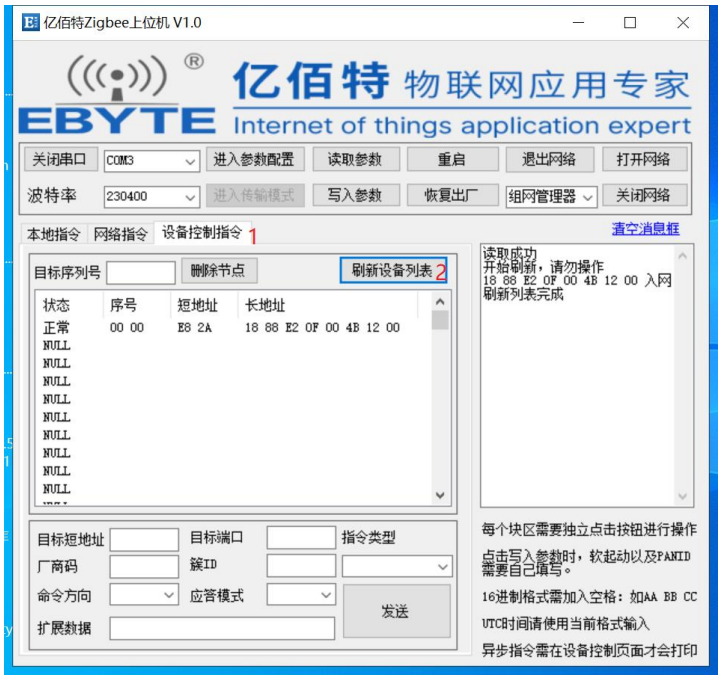
5.3.2 Device access and control

Device networking

1. Switch to the device control command interface within 180 seconds after the network is successfully opened .
2. Operate the network connection (button or control command) on the network access device, and then click to refresh the device list. The operation can be repeated until the device list displays the MAC address of the corresponding network access device. The message box will display the MAC address of the newly added device.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Send the Identify command to the network access device

1、 Enter the target short address

2、 Enter the target port, the target is E18 data transmission module, only port 1 is available

3、 The instruction type is control instruction

4、 The Identify command is a standard command, and the manufacturer code is 0 .

5、 The Identify command belongs to the command set of cluster 0x0003 , input little-endian mode, it should be 03 00

6、 Identify cluster is located at the input end of the target device, and the target device is the controlled end, so choose C2S

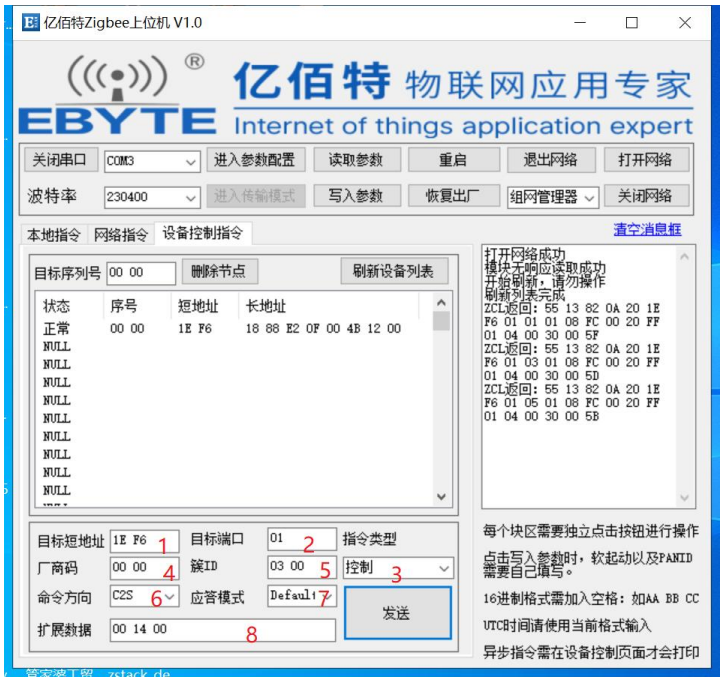
7、 Default as the answer mode

8、 The command ID of the Identify command is 0x00 , and the command parameter is the Identify time of 2 bytes (little endian mode) , so enter 00 14 00 , that is, the Identify lasts for 20 seconds

9、 Click Send, you can see that the LED of the E18 module is flashing, indicating that the E18 module has entered the Identify mode. In this mode, the E18 module can be seen by the naked eye and can also be found by other ZigBee nodes.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Query the parameters of the E18 module

1、 Enter the short address of the target E18 module

2、 Enter target port 01

3、 Enter the manufacturer code 0x2000 of the private protocol, and enter 00 20 in the little endian mode

4、 Enter the Ebyte transparent transmission cluster, the cluster ID of the cluster is 0xFC08 , and enter the little-endian mode 08 FC

5、 Instruction type selection read

6、 Command direction C2S

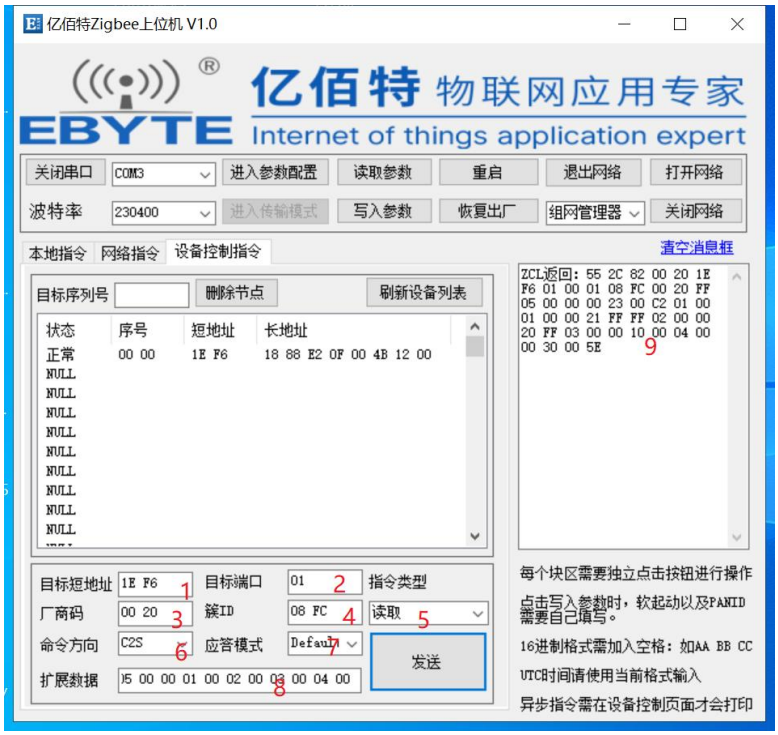
7、 Answer mode Default

8、 five attributes 0x0000, 0x0001 , 0x0002, 0x0003, 0x0004 under the Ebyte transparent transmission cluster , so enter 05 00 00 01 00 02 00 03 00 04 00

9、 Click send and receive a return message. The value of attribute 0x0000 under cluster 0xFC08 is 00 C2 01 00 , corresponding to the baud rate of 115200 ; the value of attribute 0x0001 is FF FF , and the corresponding target address of transparent transmission is 0xFFFF , which is broadcast transparent transmission; attribute The value of 0x0002 is FF , and the corresponding target port is 0xFF , that is, the broadcast port; the value of attribute 0x0003 is 00 , and the value of the corresponding transparent transmission mode is FALSE ; the value of attribute 0x0004 is 0 , and the corresponding low power consumption level is the fastest wake-up time in 1 second.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Set E18 as transparent transmission

1、 Enter the short address of the target E18 module

2、 Enter target port 01

3、 Enter the manufacturer code 0x2000 of the private protocol, and enter 00 20 in the little endian mode

4、 Enter the Ebyte transparent transmission cluster, the cluster ID of the cluster is 0xFC08 , and enter the little-endian mode 08 FC

5、 Instruction type selection write

6、 Command direction C2S

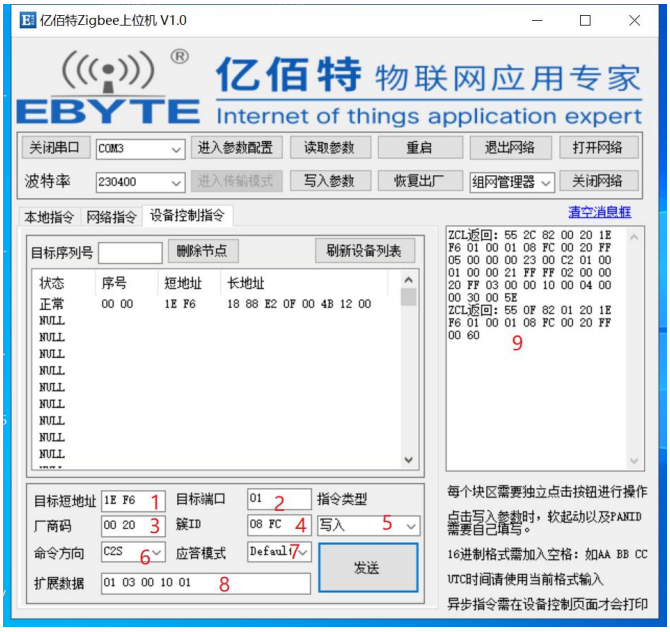
7、 Answer mode Default

8、 0x0003 corresponding to the transparent transmission mode . According to the read command, it is found that the data type of the attribute 0x0003 is 0x10 (BOOl type), and its value needs to be modified to TRUE , so enter 01 03 00 10 01 ,

9、 After clicking send, you will receive a return message. There are 0 attributes that failed to be modified, so it is considered that the modification of the transparent transmission mode is successful.

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



Send transparent data to E18 module

1、 Set the short address of the input target E18 module

2、 Enter target port 01

3、 Enter the manufacturer code 0x2000 of the private protocol, and enter 00 20 in the little endian mode

4、 Enter the Ebyte transparent transmission cluster, the cluster ID of the cluster is 0xFC08 , and enter the little-endian mode 08 FC

5、 Instruction type selection control

6、 Command direction C2S

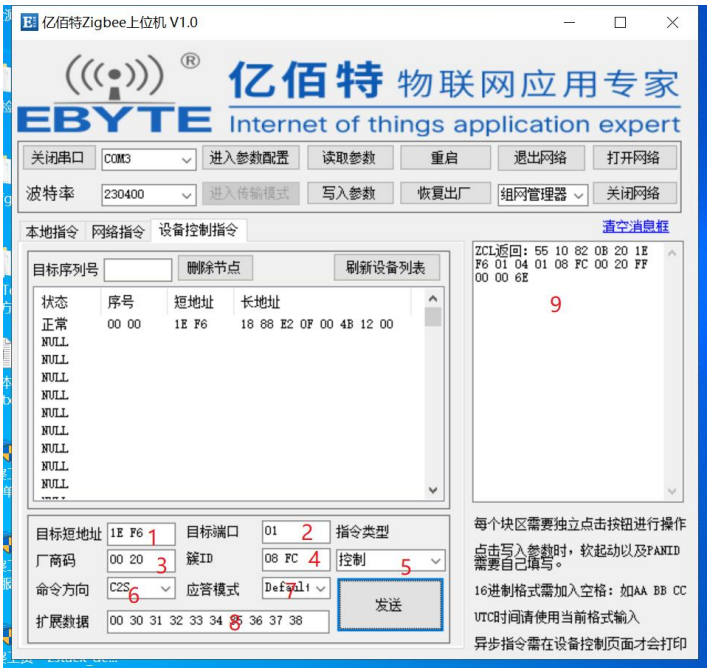
7、 Answer mode Default

8、 Enter the command ID 0x00 for transparent transmission, and the data to be transparently transmitted 31 32 33 34 35 36 37 38 , and then click Send

9、 The message box receives the default return frame, the status is 0x00 , which means that the E18 has received and executed the command correctly, and the command ID is 0x00 . At the same time , you can see the printed transparent string "12345678" at one end of the E18

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

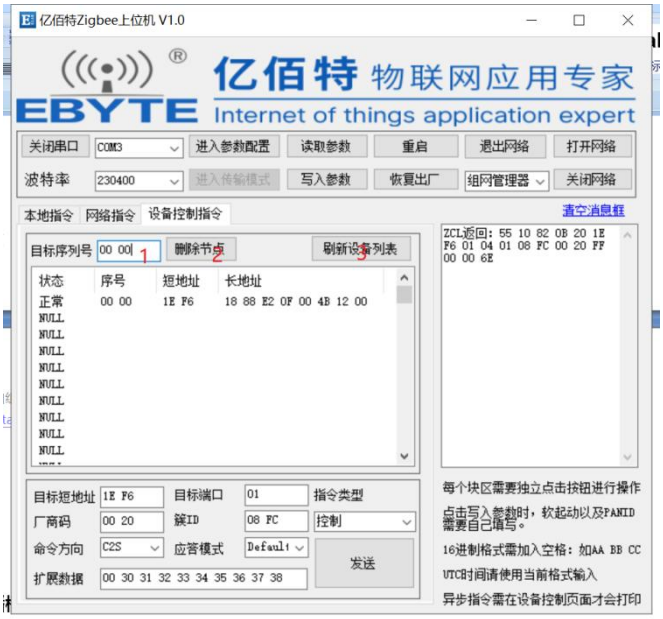


Delete a networked device

1, According to the serial number in the device list, enter the serial number of the device to be deleted in the target serial number

2, Click Delete Node

3, Then refresh the device list. If there is no display in the device list, the deletion is successful.



After deletion, the previously connected devices will no longer be displayed in the device list, and the deleted target device will also become "unnetworked"

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



5.3.3 Broadcast Mode

Differential table of data received by various types of devices in three broadcast modes:

broadcast mode	Equipment type		
	routing	terminal	dormant terminal
0xFFFF	Yes	Yes	Yes
0xFFFD	Yes	Yes	No
multicast	Yes	Yes	No
0xFFFC	Yes	No	No

Note: the user uses the broadcast mode communication steps

1、Set the target short address: 0xFFFF (received by all devices in the entire network), 0xFFFD (received by all devices except dormant terminals), 0xFFFC (received by all devices except dormant terminals and terminal devices);

2、Set the target port: the target port is set to " FF " by default;

3、After entering the transmission mode, the data broadcast can be started (the factory data transmission mode defaults to " 0xFFFF " mode broadcast);

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

6. Customized cooperation

★If corporate customers need to customize products, please contact our company.

★Ebyte has reached in-depth cooperation with many well-known enterprises.

7. About us



EBYTE is a company specializing in providing wireless data transmission solutions and products

- Independent research and development of hundreds of models of products and software;
- Multi-series wireless products such as wireless transparent transmission, WiFi , Bluetooth, Zigbee , PKE , digital radio, etc.;
- Has nearly 100 employees, tens of thousands of customers, and has sold millions of products;
- Business covers more than 30 countries and regions around the world;
- Passed ISO 9001 quality management system and ISO 14001 environmental system certification;
- Have a number of patents and software copyrights, and have passed international FCC/CE/ROHS and other authoritative certifications.

【Company Tel】028-61399028 【Company Fax】028-64146160
【Official Website】www.cdebyte.com 【Online Mall】cdebyte.taobao.com
【Technical Support】support@cdebyte.com 【Manager Li】raylee@cdebyte.com

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

【Company Address】 B333-D347 , Innovation Center, No. 4 , Xixin Avenue, High-tech West District, Chengdu, Sichuan Province

Copyright ©2012–2022, Chengdu Ebyte Electronic Technology Co.,Ltd.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000