PRODUCT APPLICATION NOTE



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

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

Module Network Distribution &Identification in HEX Command Mode

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

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

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

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

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

① Module reset

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

Receive asynchronous command "device startup notification" after successful reset

Asynchronous
De：55 0D 80 00 01 10 F3 4C 60 FE FF 14 43 0C 14 FW version Module MAC address
Description: Received device start, module reset completed

② Configure module A as the coordinator

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

③ Configure module B as a non-sleeping endpoint

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

④ Configure module B as a router

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

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

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

Second step：Module connected to network

① Module A starts to configure the network, and module A successfully establishes the network

Command	Response
55 03 00 02 02	55 04 00 02 00 02
Received 2 asynchronous Command	
Received <system notification-network status change>: 55 29 80 01 01 F3 4C 60 FE FF 14 43 0C 19 91 14 00 00 22 44 EA D4 CA FD 93 2D D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF F0 01 Indicates that the network has been established F3 4C 60 FE FF 14 43 0C is Module A (Coordinator) MAC 19 is channel 91 14 is PANID 00 00 is short address 22 44 EA D4 CA FD 93 2D is expand PANID D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF is network key Description: The coordinator establishes a network on channel 0x19=25, the PANID is 0x1491, and the short address is 0x0000	
Receive <system notification-network access time window notification>: 55 04 80 02 B4 36 Allow connecting network 180s Description: Module A has successfully established a network	

② Module B starts to configure the network, and module B joins the network

Command	Response
55 03 00 02 02	55 04 00 02 00 02
received asynchronous Command	
Received <system notification-network status change>: 55 29 80 01 02 E9 CE D6 FE FF 14 43 0C 19 91 14 2C 6A 22 44 EA D4 CA FD 93 2D D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF 9B 02 Indicates the first access to the network E9 CE D6 FE FF 14 43 0C Indicates module B (terminal node) MAC 19 is channel 91 14 is PANID 2C 6A is short address 22 44 EA D4 CA FD 93 2D is expand PANID D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF is network key Description: Module B joined the network successfully. Module B joined coordinator A as a terminal node. The channel, PANID, extended PANID, network key are the same as those of the coordinator, and the short address is 0x6A2C	

③Module A detects that module B is connected to the network

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

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

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

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

Precautions for the coordinator to detect node access to the network:
<System notification-node short address notification> is limited by the broadcast storm. When multiple modules enter the network at the same time, the message may not be broadcasted, resulting in the coordinator not receiving the message, so it cannot be used as a basis for detecting node network access. And <system notification-detecting node network access> is based on the coordinator detecting a module network access request as a judgment condition, and there is a risk of module network access failure. Therefore, it is recommended that if the coordinator needs to successfully detect the module's network access, it can send any request query command according to the short address of the network-connected module within 5 seconds after receiving the <system notification-node short address notification>, as long as there is a return message, that is It can be determined that the module has successfully entered the network.

The third step is to identify the network access node

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

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

Command	Response
Send <ZDO command-query node port number>:55 05 01 05 88 FC 70 Target short address **Analysis:** This command has no command parameters, only command ID and short address	55 05 01 05 00 02 06 Command valid Command number **Analysis:** The command input is valid, and the query number assigned by the module to this command is 0x02

Await async command……

Receive 2 asynchronous command
Wait for several milliseconds, receive <ZDO sending confirmation>: 55 07 8F 01 88 FC 02 00 F8 Target short address Command number Send successfully **Analysis:** The command is successfully sent, waiting for the target to reply with the execution result
Wait for several milliseconds, and receive <ZDO response-query node port number>: 55 0C 81 05 88 FC 02 00 04 01 02 03 04 F2 Short address of other side Command number Other side executed successfully Number of ports Port list **Analysis:** B has 4 application ports, namely port 1, port 2, port 3, and port 4

Coordinator A checks which are the 4 application ports of node B.
First look at port 1 of node B:

Command	Response
Send <ZDO command-query node port information>: 55 06 01 04 88 FC 01 70 Target short address Target ports **Analysis:** Query application port 1 of node B (short address 0xFC88)	55 05 01 04 00 03 06 Command is valid Command number Analysis: The input of this command is valid, and the query number assigned by the module to this command is 0x03

Received 2 asynchronous command
Receive <ZDO Send Confirmation>: 55 07 8F 01 88 FC 03 00 F9 Target short address Command number Send successfully Description: The coordinator establishes a network on channel 0x19=25, the PANID is 0x1491, and the short address is 0x0000
Received <ZDO Response - Query Node Port Information>: 55 21 81 04 88 FC 03 00 01 04 01 50 00 00 05 00 00 03 00 04 00 07 00 08 FC 04 03 00 06 00 08 00 08 FC AA 88 FC is short address of other side 03 is command number 00 is other side executed successfully 01 is target port 04 01 is apply port profile 50 00 is device ID 00 is device version 05 is the input cluster size 00 00 03 00 04 00 07 00 08 FC is the input cluster list 04 is the output cluster size 03 00 06 00 08 00 08 FC is the output cluster list Analysis: Query the information of port 1 of node B, the port profile is 0x0104 is a ZCL Home Automatic application, the device ID is 0x0050 corresponding to the "home gateway" device, the device version is 0, and the input cluster list has a total of 5 clusters, respectively { 0x0000, 0x0003, 0x0004, 0x0007, 0xFC08}, the 4 output clusters are respectively {0x0003, 0x0006, 0x0008, 0xFC08}. By looking up the table, we can analyze that port 1 of Node B supports "Basic Information (0x0000)", "Device Mark (0x0003)", "Group Management (0x0004)", "Switch Output (0x0007)", "Data Transmission (0xFC08)", a total of 5 local functions, and a total of 4 functions that can be output externally: "Device Mark (0x0003)", "Switch Control (0x0006)", "Brightness Control (0x0008)", and "Data Transmission (0xFC08)".

Precautions:
For some use Silicon

For some zigbee network access devices using Silicon Labs chips, <ZDO Send Confirmation> and <ZDO Response> may be reversed. This is a BUG of Silicon Labs' ZigBee series products and is a normal phenomenon. It is recommended to use it correctly. When using <ZDO Command> to query the target node on demand, wait for the timeout of <ZDO Response> for 18 seconds. The response message is treated as an invalid message.

Then look at port 2 of module B:

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

Command	**Response**
Send <ZDO command-query node port information>: 55 06 01 04 88 FC 02 70	55 05 01 04 00 04 01
Receive 2 asynchronous Command	
Received <ZDO Response - Query Node Port Information>: 55 19 81 04 88 FC 04 00 02 04 01 01 01 00 05 03 00 04 00 05 00 06 00 08 00 00 FB Target port Apply Port Profile Device ID Device version Input cluster size Input cluster list Output cluster size Description: The coordinator establishes a network on channel 0x19=25, the PANID is 0x1491, and the short address is 0x0000	
Received <ZDO Send Confirmation>: 55 07 8F 01 88 FC 04 00 FE Analysis: In this query, <ZDO Send Confirmation> and <ZDO Response> are reversed. Query the target port 2, whose profile is 0x0104 is also the ZCL Home Automatic application, and the device ID is 0x0101 corresponding to the device application of "dimming light". 5 input clusters {0x0003, 0x0004, 0x0005, 0x0006, 0x0008} indicate that they support "device flag (0x0003)", "group management (0x0004)", "scene snapshot (0x0005)", "switch control (0x0006)", "Brightness Control (0x0008)". The output cluster for port 2 is empty.	

A brief description of the functions of each cluster:
Basic information (0x0000): the function of recording and saving the factory information, version and production date of the device
Device mark (0x0003): The device switches mark status, which can be found by naked eyes and by other devices on the same network
Group management (0x0004): device group management function, you can receive multicast messages after grouping, and you can exit the grouping when you don't need to receive multicast messages
Scene snapshot (0x0005): Device settings save a complex physical state, and then you can quickly switch to this state with a Command
Switch Control (0x0006): The device outputs a state that can be switched between 0 and 1 states
Switch output (0x0007): The device simulates the function of a button or switch
Brightness control (0x0008): The device outputs a switching state between 0~255, such as PWM wave.
Data transmission (0xFC08): the device inputs and outputs data through the serial port

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

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

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

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

E72-2G4M20S1E (Link72) soft start:

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

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

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

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

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

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

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

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

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

Data reception	
Receive <system notification-device information notification>	55 28 80 05 00 01 4D 4D 60 FE FF 14 43 0C A7 B1 01 04 01 50 00 05 00 00 03 00 04 00 07 00 08 FC 04 03 00 06 00 08 00 08 FC F0 Termination Sign Virtual SN Short addressPort Number Port Profile Device ID Input cluster size Input cluster list Output cluster size Output Cluster List
Analysis: The port 1 information, port number and MAC address of the network access node are re-integrated into a virtual SN to facilitate cloud management. At the same time, the application profile, device ID, input cluster and output cluster of the application port can be obtained from the message, which is exactly the same as the previous example of viewing port 1. Port 1 of the network access node is a "home gateway" device, which supports "basic information (0x0000)", "device tag (0x0003)", "group management (0x0004)", "switch output (0x0007)", "data transmission (0xFC08)", a total of 5 local functions, and a total of 4 functions that can be output externally: "Device Mark (0x0003)", "Switch Control (0x0006)", "Brightness Control (0x0008)", and "Data Transmission (0xFC08)".	

Receive info from port 2:

Data reception

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

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

Receive info from port 3：

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

Receive info from port 4：

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

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

About us

Technical support: support@cdebyte.com

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

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

Official hotline:028-61543675

Web: https://www.cdebyte.com

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

Chengdu Ebyte Electronic Technology Co.,Ltd.

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