ZigBee Module User Guide

Fit for CC2630 Serials ZigBee Module

DRF1609H (UART)
DRF2657C (RS232)
DRF2658C (USB)
DRF2659C (RS485)
DRF2670C (TCP/IP)

CONTENTS

Documentation and Module Firmware Release Notes:

Date	content
2017.02.23	This document was first published
2017.05.30	Module firmware version upgrade to V7.2 / V7.3: 1, increased the End Device node settings: (1), End Device is a node without routing function; (2), through the instructions, End Device can be found from their nearest three Router nodes, the function is compatible with CC2530 series positioning system; 2, increased the Router and End Device interrogation signal strength instructions; 3, increased the encryption and password enabled features; 4, increase the custom address addressing point to point transmission function; Instruction backward compatibility, V7.2 / V7.3 version of the module, you can still use the old configuration software (instruction); Data transfer, compatible with V7.2 version of the following modules (can communicate with each other) Firmware Version Description: Even version of the firmware (such as V7.2), can use onboard antenna and external antenna, odd version of the firmware (such as V7.3), usually suitable for products with a shell, can only use an external antenna.
2017.06.08	Manual (this document is modified): INS05, read the module parameters, X43-X48 modified to: X42-X47
2017.06.10	Module firmware version upgrade to V7.4 / V7.5: In the transparent transmission section has been added: Transparent transfer + custom address Transparent transfer + short address Transparent transfer + MAC address

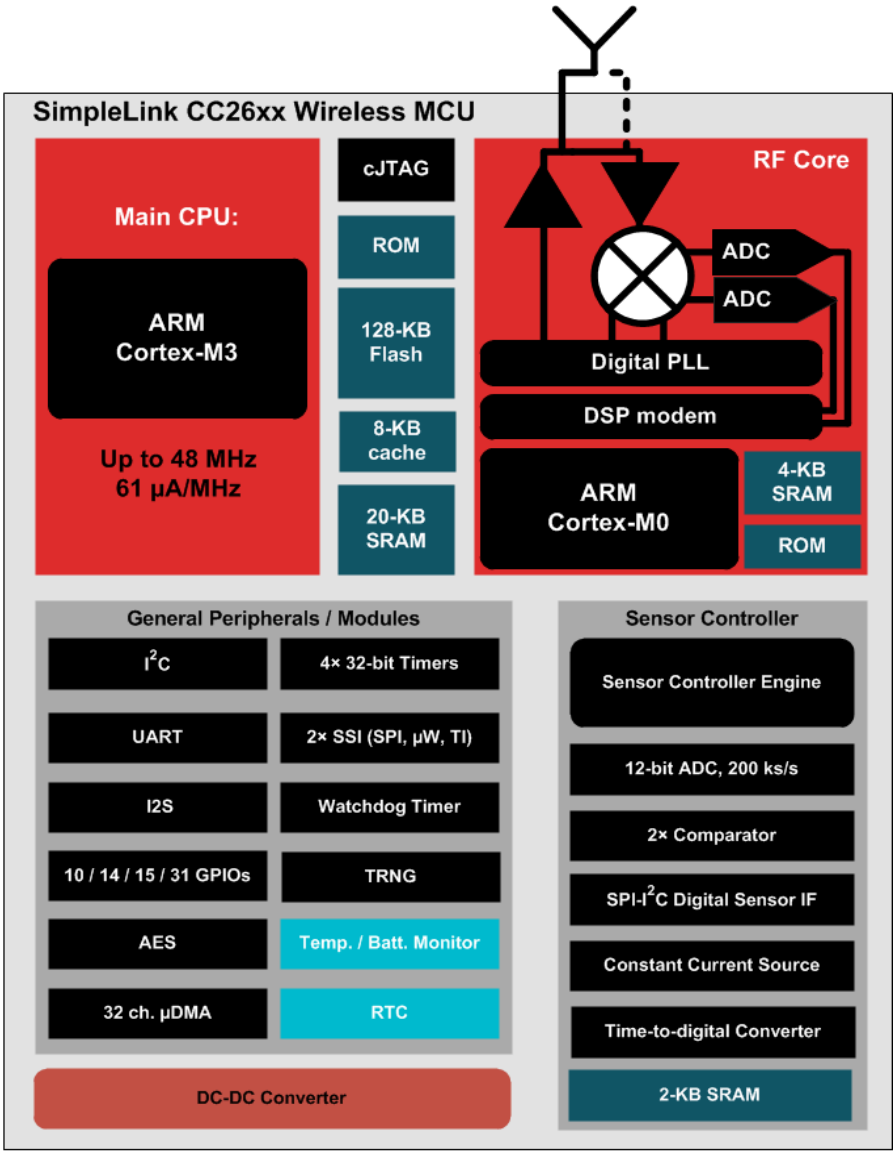
2017.06.28	Modify this document error: P52, P53: Destination address (short address) Destination address (custom address)
2017.08.02	Adjust the version release rules, each version consists of three small versions, such as X.1-X.3, X.4-X.6, X.7-X.9, V7.4: for the full-function version, the various parameters can be set, such as DRF1609H V7.5: for the shell with the version, the antenna selects the default for the external antenna, cannot be set, such as DRF2659C V7.6: for ZigBee gateway, node type = Coordinator, antenna selection = external antenna, baud rate = 115200, serial port format = 8-N-1, cannot set parameters such as DRF2670C Released the ZigBee gateway product, and added the use of instructions Released the ZigBee positioning system and positioning card products, and added the use of instructions Configuration software for the corresponding upgrade (increase the ZigBee gateway settings)
2017.08.23	Added addition to ZigBee positioning system: Positioning card, location reference point, data node The corresponding firmware versions are: V7.4 (DRF1609H), V7.5 (with shell), V7.6 (ZigBee gateway)

ZigBee Module Features

DTK new generation of ZigBee module, using TI's CC2630 chip.

CC2630 is a dual ARM core-32 bit CPU chip, Cortex-M3 is responsible for the processing of ZigBee protocol, and Cortex-M0 is responsible for wireless communication processing.
Is the fastest computing ZigBee module, compared with the first generation of products (CC2530, 8-bit 8051 chip), is tantamount to rocket and tractor comparison.

The new ZigBee module can form a larger network, a more stable network and transmit more capacity data.



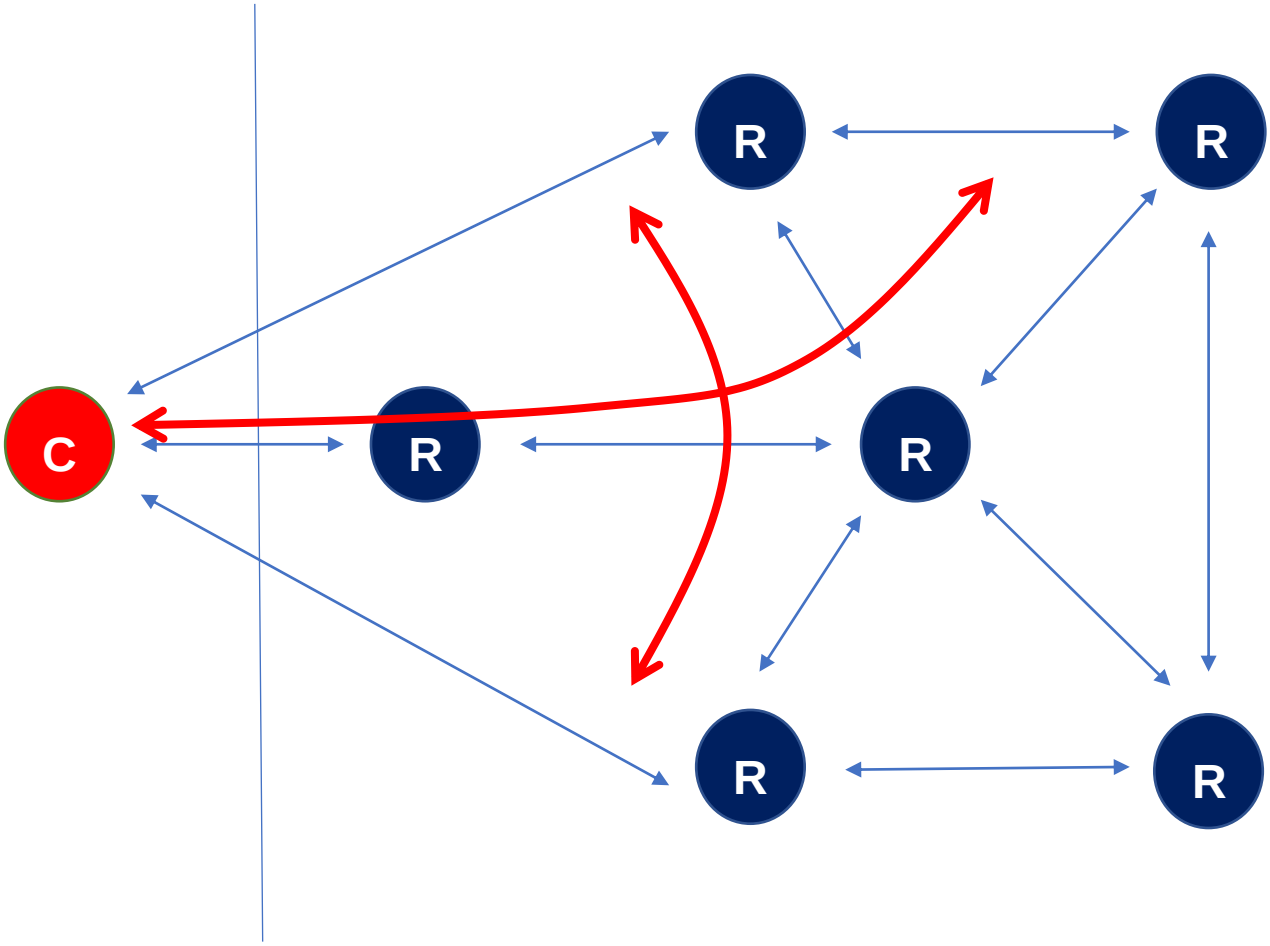
ZigBee module can set up a standard Mesh network for data transmission.

Automatically join the network (Router not need set, press the three function keys, can automatically find Coordinator to join the network).

Automatic routing, will automatically get the best routing path.

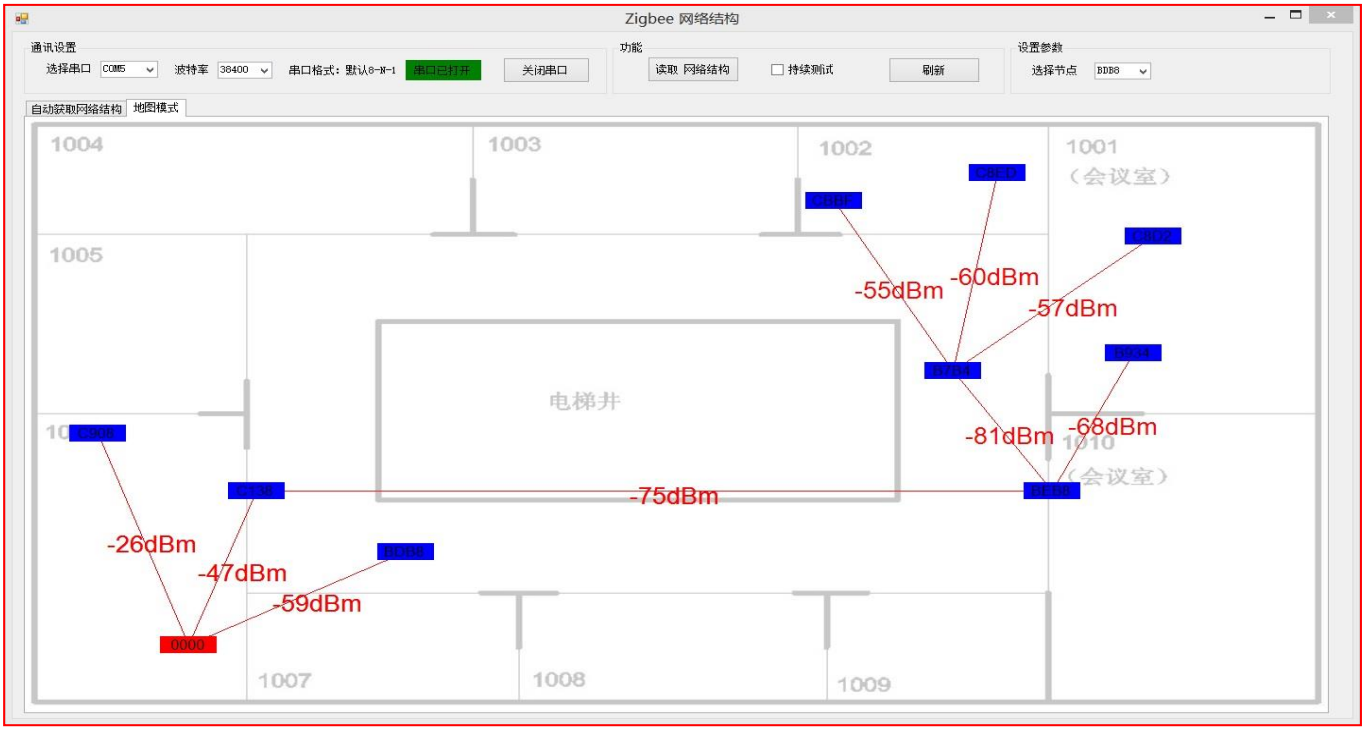
Dynamic routing maintenance, when a routing path is damaged, you can regain the best routing path.

Transparent transmission of data, and can also point to point to send to any node.

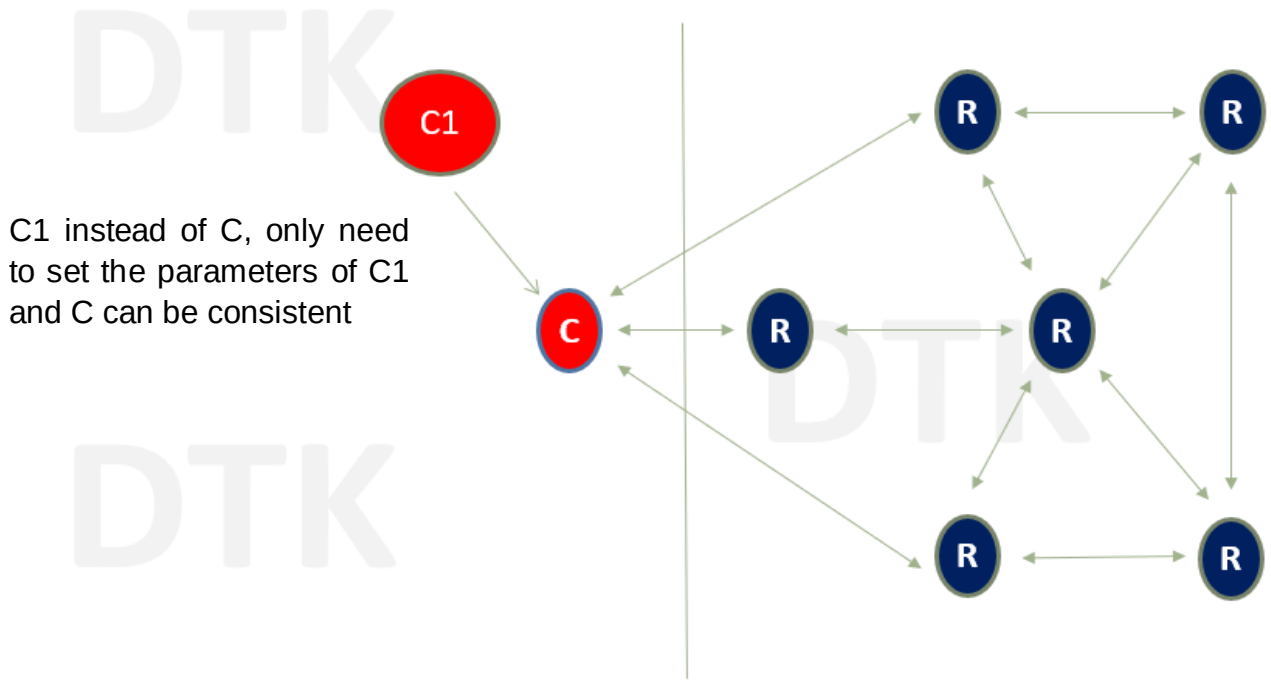


With the power of dual ARM-32-bit CPU, the module can support 200 automatic routing, if the application of different directions of street lighting control, a network can connect up to 500 lights (control lights on and off).

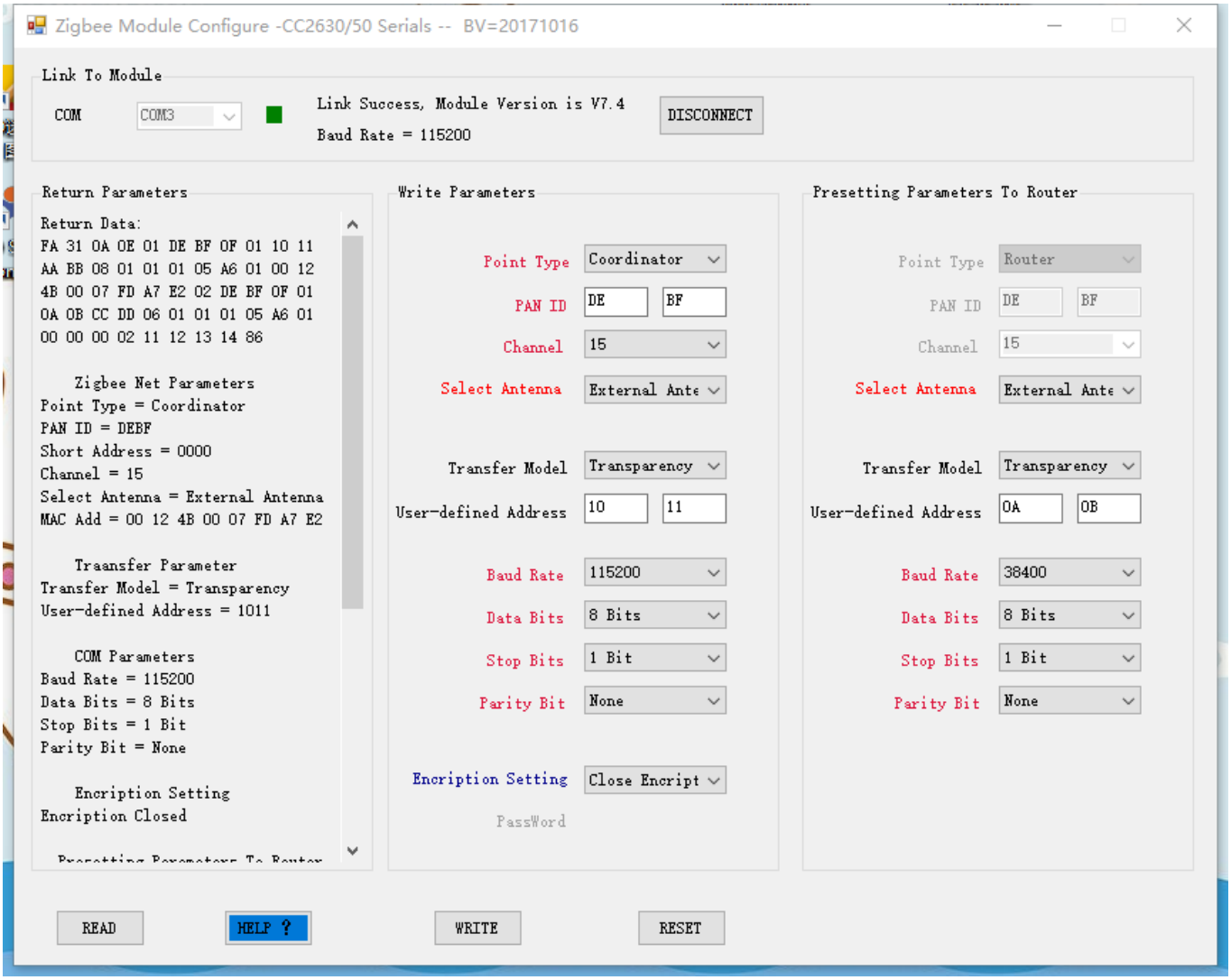
The ZigBee module, with the DTK application software, can clearly know the structure of the entire ZigBee network (all nodes of the routing relationship, and all nodes between the signal strength, greatly facilitate the user's debugging and networking.



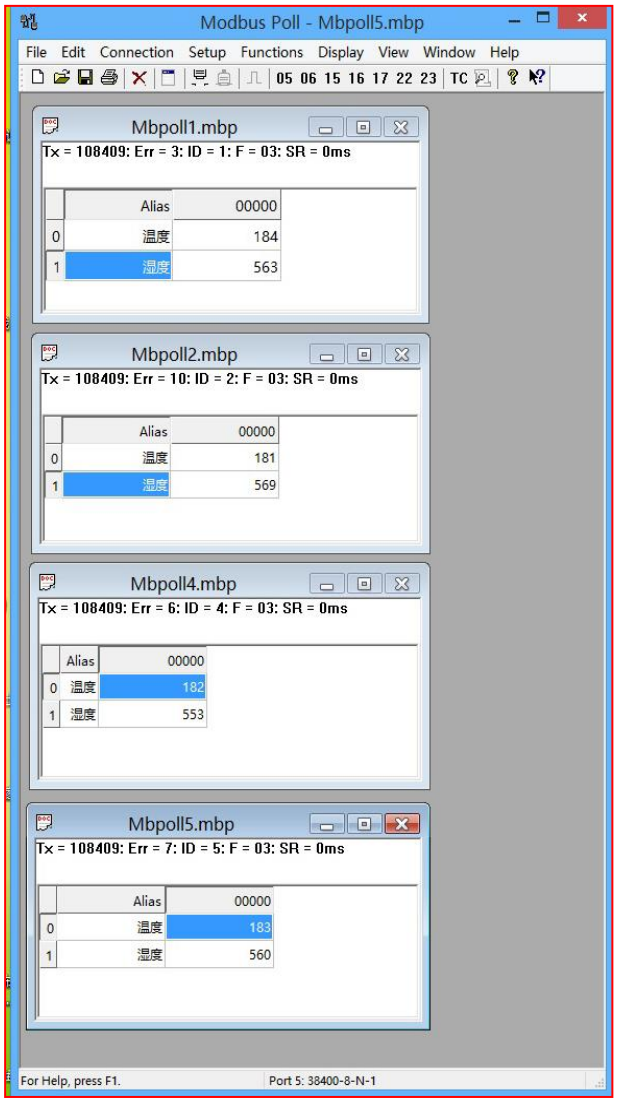
The ZigBee module solves the first generation of product replacement Coordinator problems, only need to set the new ZigBee module parameter with the old Coordinator parameters, that can replace the original Coordinator;

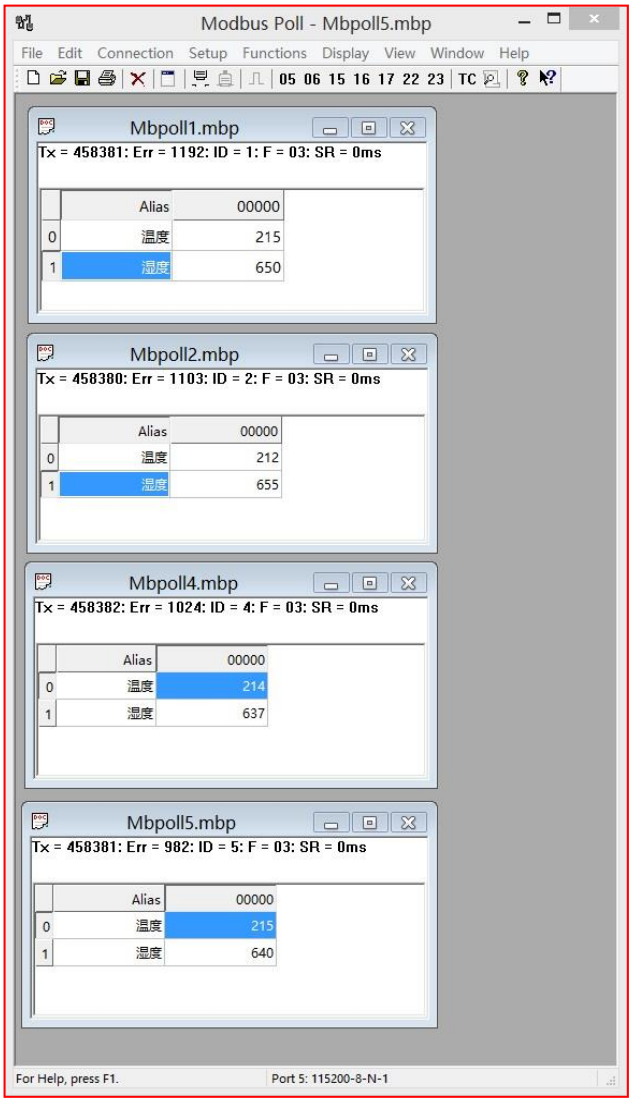


The parameters of the Router can be saved in the Coordinator. When the Router automatically joins the network (the function key of the Router is pressed three times), the parameter is automatically transferred to the Router (that is, it is not necessary to set up the Router, which greatly facilitates the construction).
Coordinator accepts all routers to join the network (up to 65530 Router), while the CC2530 module Coordinator can only assign addresses to 6 routers.



More stable data transmission:
Laboratory conditions, close-up test, the bit error rate of up to 0.0059% (5.9 per 100,000).
Measured conditions (separated from the room, more than 10 meters away, 20 WIFI interference), the bit error rate of up to 0.23% (2.3 per thousand).

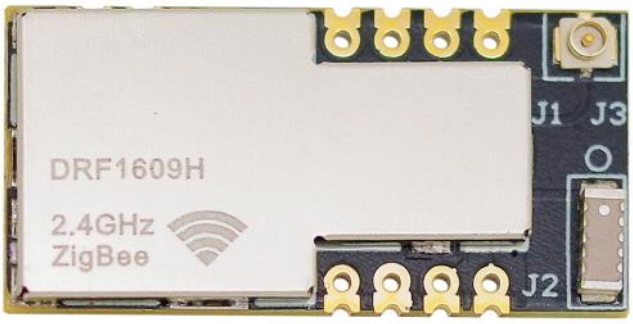


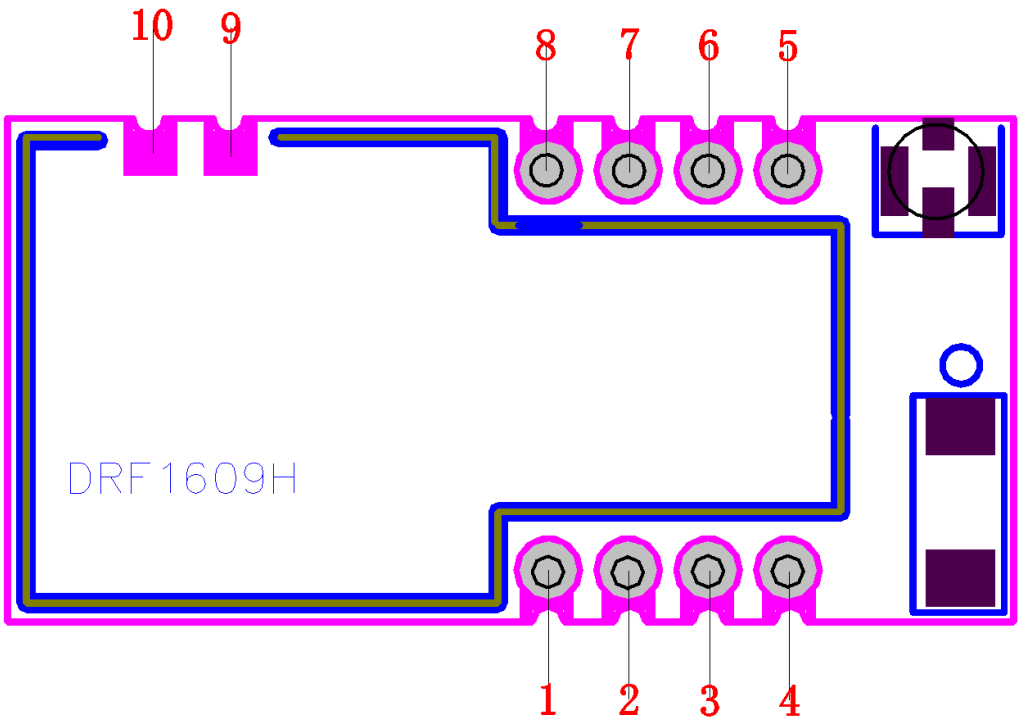


ZigBee Module Parameters

DRF1609H

Power	DC 3.3V
Temperature range	-40℃~85℃
Serial baud rate	38400bps (default) , 1200bps, 2400bps, 4800bps, 9600bps, 19200bps, 38400bps, 57600bps, 115200bps
Serial format	8-N-1 (default), 8-E-1, 8-O-1
Radio frequency	2.4GHz (2460MHz, default) , Users can change the channel through the serial command (2405MHz~2480MHz, step: 5MHz), the corresponding channel 11~26 optional
Transmission distance	Visual, open, transmission distance of 1600 meters
Working current	25mA (@3.3V) average
Receiving sensitivity	-98dBm
Main chip	TI CC2630F128
Configurable nodes	Coordinator, Router, End Device
Interface	3.3V UART





PIN	Name	Function
1	VCC	3.3V Power
2	GND	GND
3	RESET_N	Reset
4	KEY	Function Key
5	TX	UART TX
6	RX	UART RX
7	LED3	Indicates data transmission and reception
8	LED4	Indicates the state
9	TMS	JTAG TMS
10	TCK	JTAG TCK

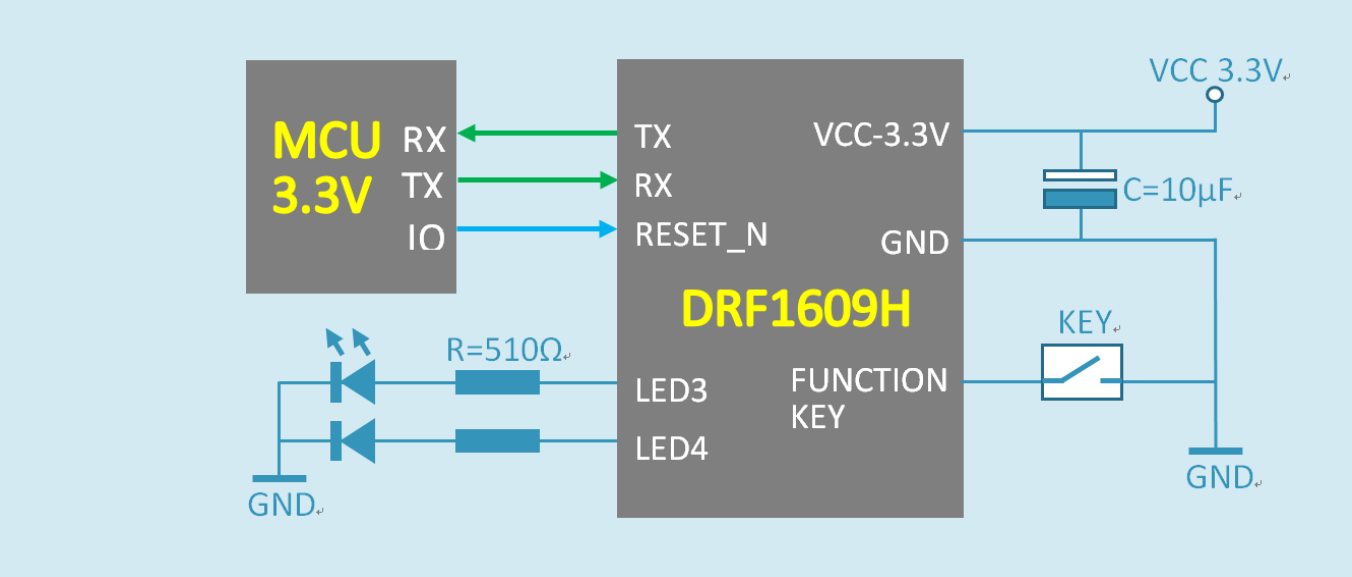
DRF1609H minimum application system:

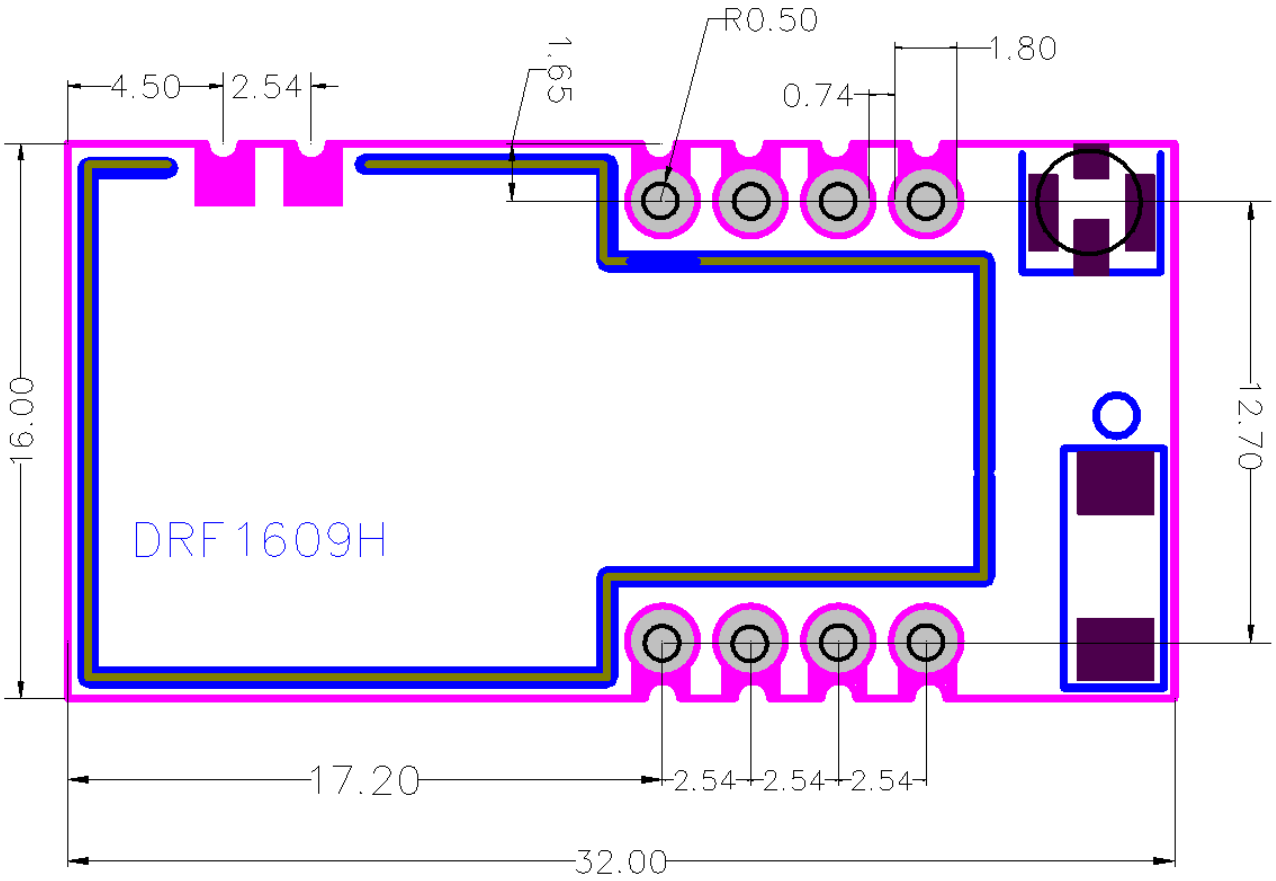
1. LED lights are not necessary, if you want to add LED lights, must be in series 510Ω resistor;
2. RESET_N is not required, can be controlled, low reset, reset time 5ms is sufficient, high level normal operation;

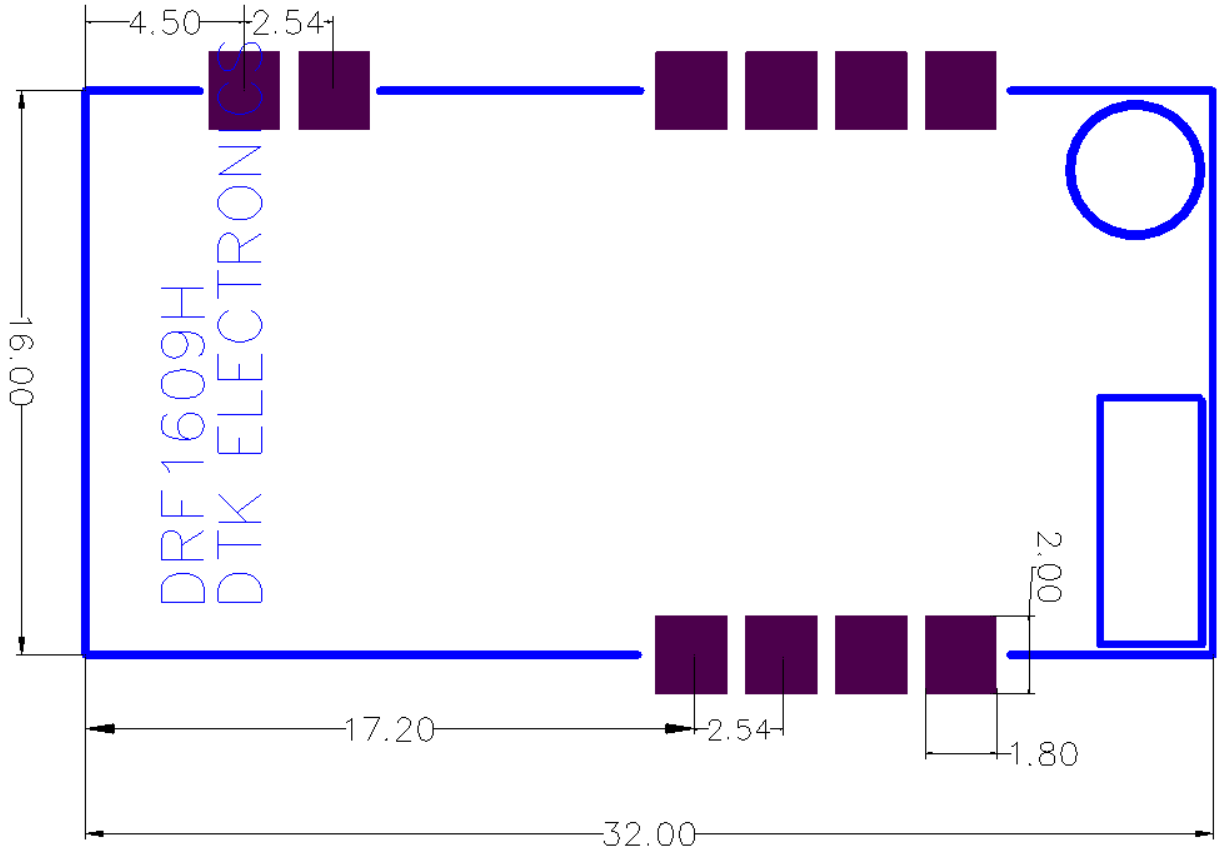
3. Power supply 10μF capacitor is not required;

4. FUNCTION KEY is not necessary, it is recommended to facilitate the node to find the network;

5. If the MCU is 5V operating voltage, please add the level conversion, or burn the module.

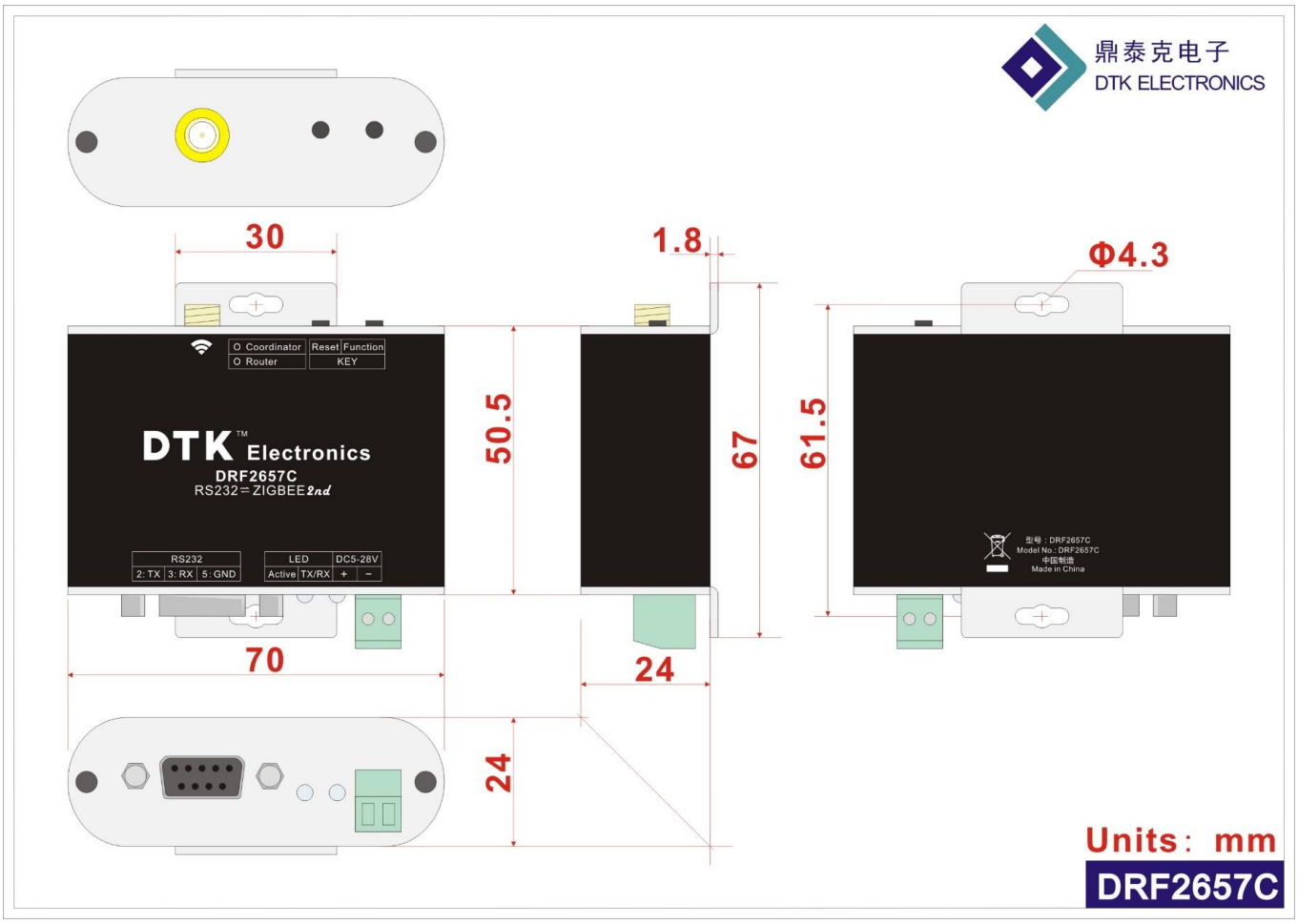



R0.50
1.80
4.50
2.54
1.65
0.74
19.00
12.70
DRF1609H
17.20
2.54
2.54
2.54
32.00


4.50
2.54
16.00
DRF1609H
DTK ELECTRONICS
2.00
17.20
2.54
1.80
32.00

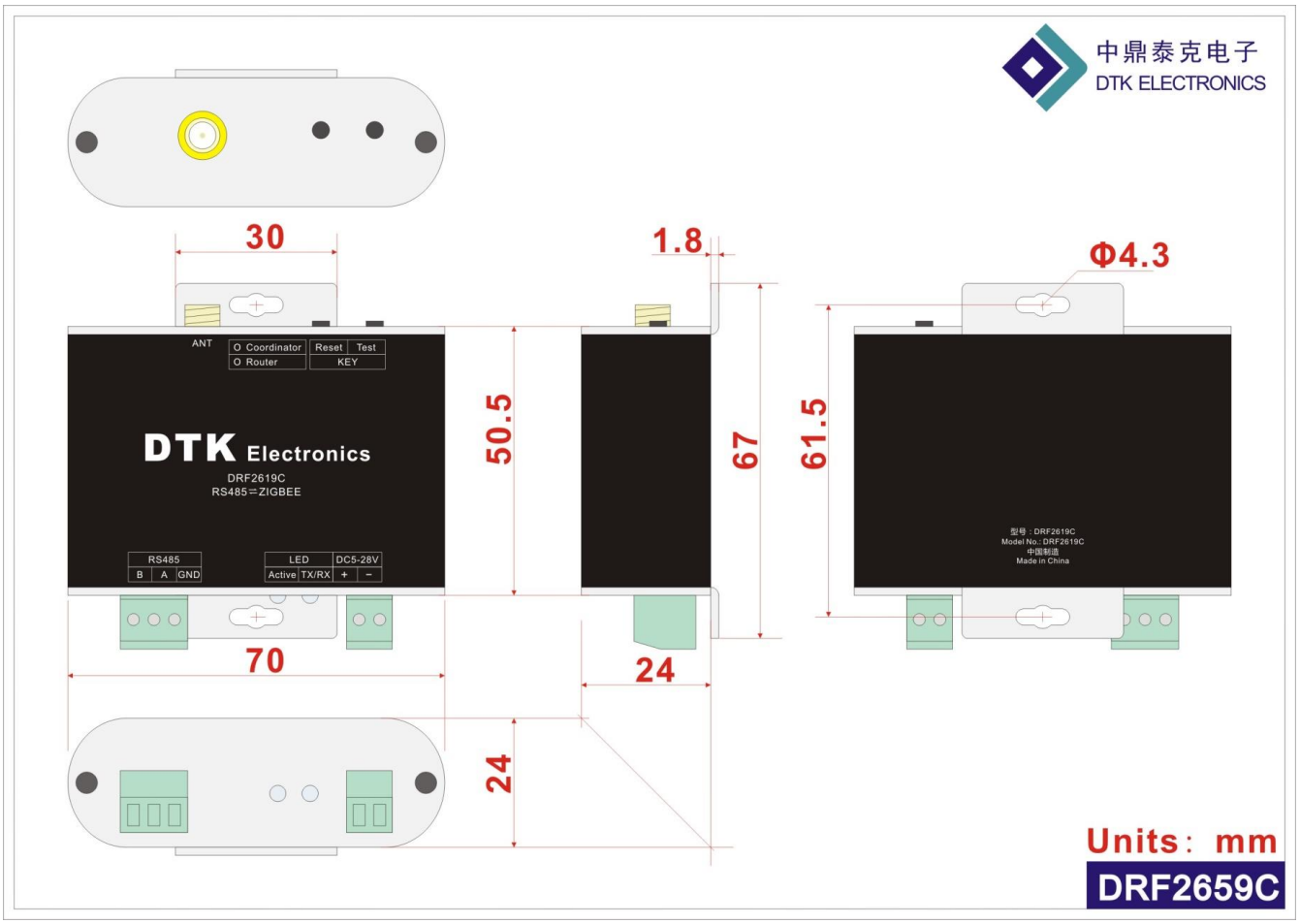
DRF2657C

Power	**DC 5 – 28V**
Temperature range	-40℃~85℃
Serial baud rate	38400bps (default), 1200bps, 2400bps, 4800bps, 9600bps, 19200bps, 38400bps, 57600bps, 115200bps
Serial format	8-N-1 (default), 8-E-1, 8-O-1
Radio frequency	2.4GHz (2460MHz, default), Users can change the channel through the serial command (2405MHz~2480MHz, step: 5MHz), the corresponding channel 11~26 optional
Transmission distance	Visual, open, transmission distance of 1600 meters
Working current	25mA (@3.3V) average
Receiving sensitivity	-98dBm
Main chip	TI CC2630F128
Configurable nodes	Coordinator, Router, End Device
Interface	RS232 (2: TX, 3: RX, 5: GND)


鼎泰克电子
DTK ELECTRONICS
30
1.8
Φ4.3
O Coordinator
O Router
Reset
Function
KEY
DTK™ Electronics
DRF2657C
RS232=ZIGBEE2nd
RS232
2: TX
3: RX
5: GND
LED
Active
TX/RX
DC5-28V
+
−
50.5
67
61.5
70
24
24
Units: mm
DRF2657C

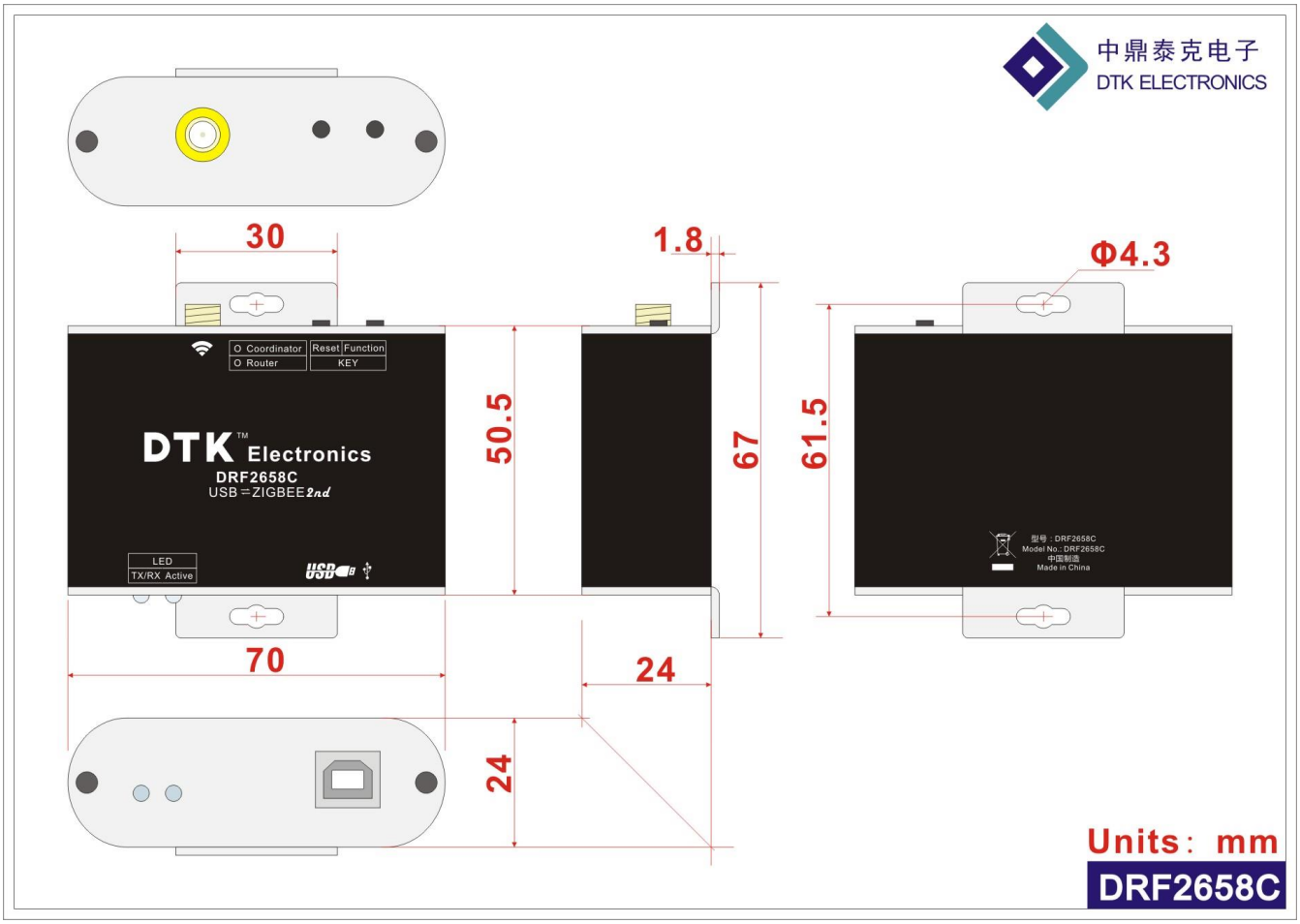
DRF2659C

Power	**DC 5 – 28V**
Temperature range	-40℃~85℃
Serial baud rate	38400bps (default), 1200bps, 2400bps, 4800bps, 9600bps, 19200bps, 38400bps, 57600bps, 115200bps
Serial format	8-N-1 (default), 8-E-1, 8-O-1
Radio frequency	2.4GHz (2460MHz, default) , Users can change the channel through the serial command (2405MHz~2480MHz, step: 5MHz), the corresponding channel 11~26 optional
Transmission distance	Visual, open, transmission distance of 1600 meters
Working current	25mA (@3.3V) average
Receiving sensitivity	-98dBm
Main chip	TI CC2630F128
Configurable nodes	Coordinator, Router, End Device
Interface	RS485


中鼎泰克电子
DTK ELECTRONICS
30
1.8
Φ4.3
ANT
O Coordinator
O Router
Reset
Test
KEY
DTK Electronics
DRF2619C
RS485=ZIGBEE
RS485
B A GND
LED
Active TX/RX
DC5-28V
+ -
50.5
67
61.5
70
24
24
型号：DRF2619C
Model No.: DRF2619C
中国制造
Made in China
Units: mm
DRF2659C

DRF2658C

Power	**DC 5 – 28V**
Temperature range	-40℃~85℃
Serial baud rate	38400bps (default) , 1200bps, 2400bps, 4800bps, 9600bps, 19200bps, 38400bps, 57600bps, 115200bps
Serial format	8-N-1 (default), 8-E-1, 8-O-1
Radio frequency	2.4GHz (2460MHz, default) , Users can change the channel through the serial command (2405MHz~2480MHz, step: 5MHz), the corresponding channel 11~26 optional
Transmission distance	Visual, open, transmission distance of 1600 meters
Working current	25mA (@3.3V) average
Receiving sensitivity	-98dBm
Main chip	TI CC2630F128
Configurable nodes	Coordinator, Router, End Device
Interface	USB (USB to UART, CP2102 chip inside)


中鼎泰克电子
DTK ELECTRONICS
30
1.8
Φ4.3
O Coordinator
O Router
Reset
Function
KEY
DTK Electronics
DRF2658C
USB=ZIGBEE2nd
LED
TX/RX Active
50.5
67
61.5
70
24
24
Units: mm
DRF2658C

DRF2670C (ZigBee Gateway)

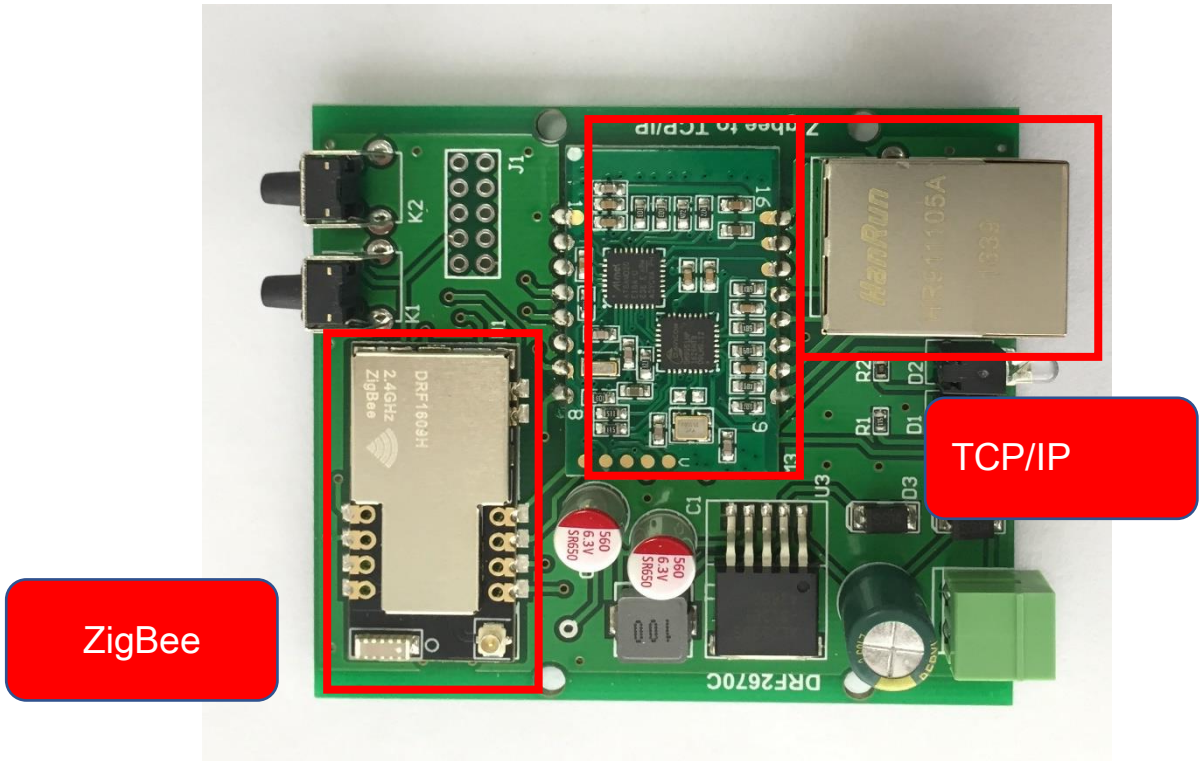
ZigBee gateway include the ZigBee part and network part inside, between the two through the serial (UART) connection.

ZigBee part active as Coordinator.

The data received from ZigBee wireless, through the serial port sent to the network part, and network part sent it to the target IP and port.

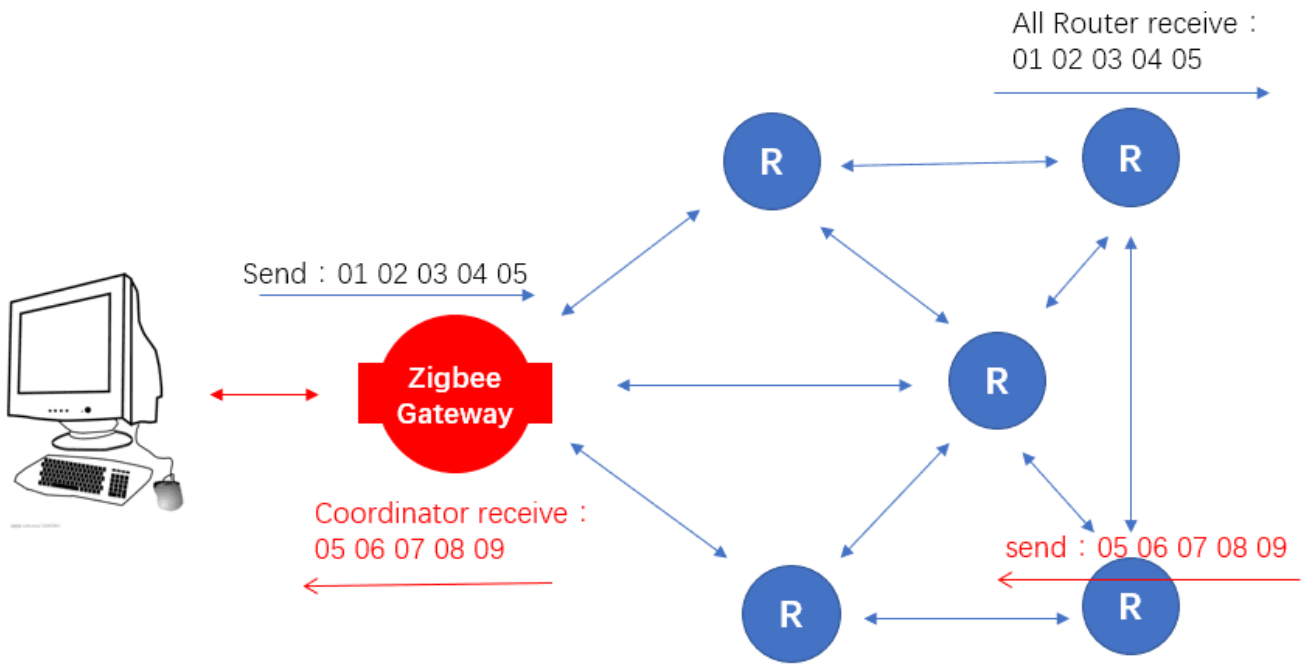
The data received from network, through the serial port sent to the ZigBee part, and ZigBee part sent it to Routers in this ZigBee net.

ZigBee and the network is completely transparent transmission.



ZigBee Gateway Works

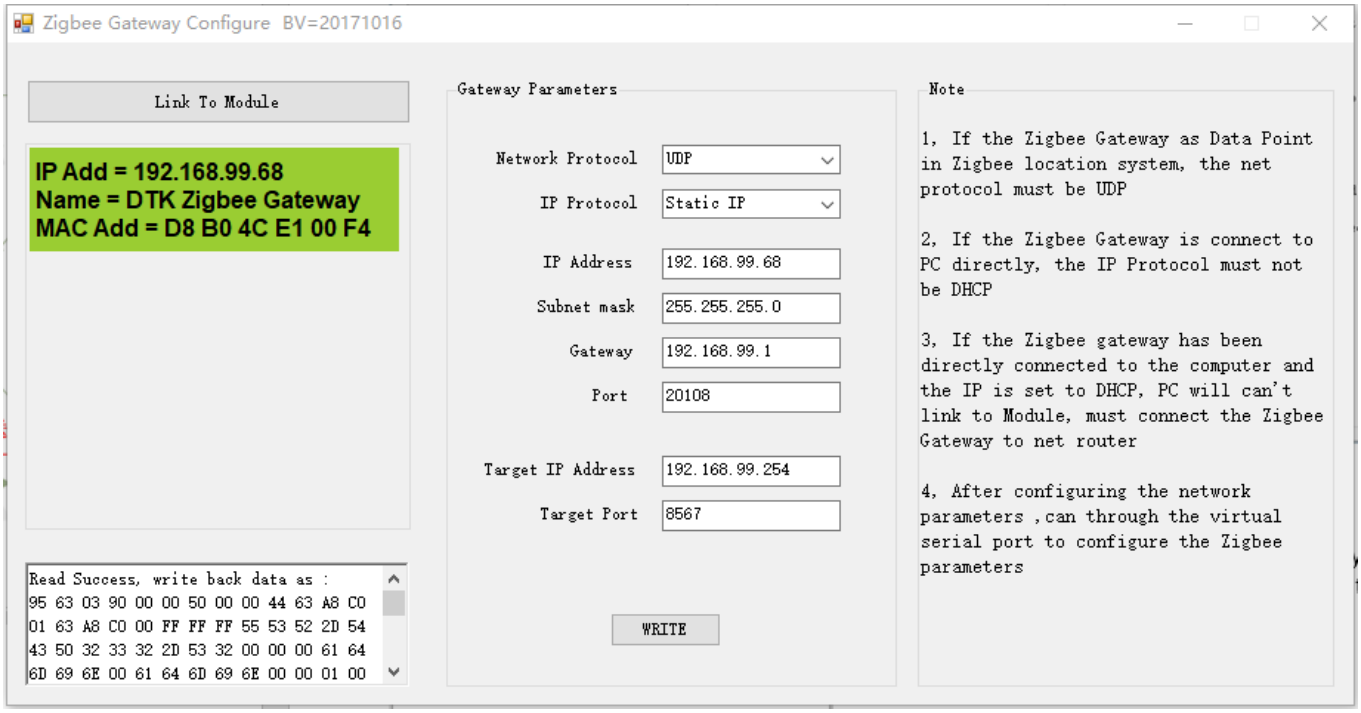
(1) directly connected to the computer:



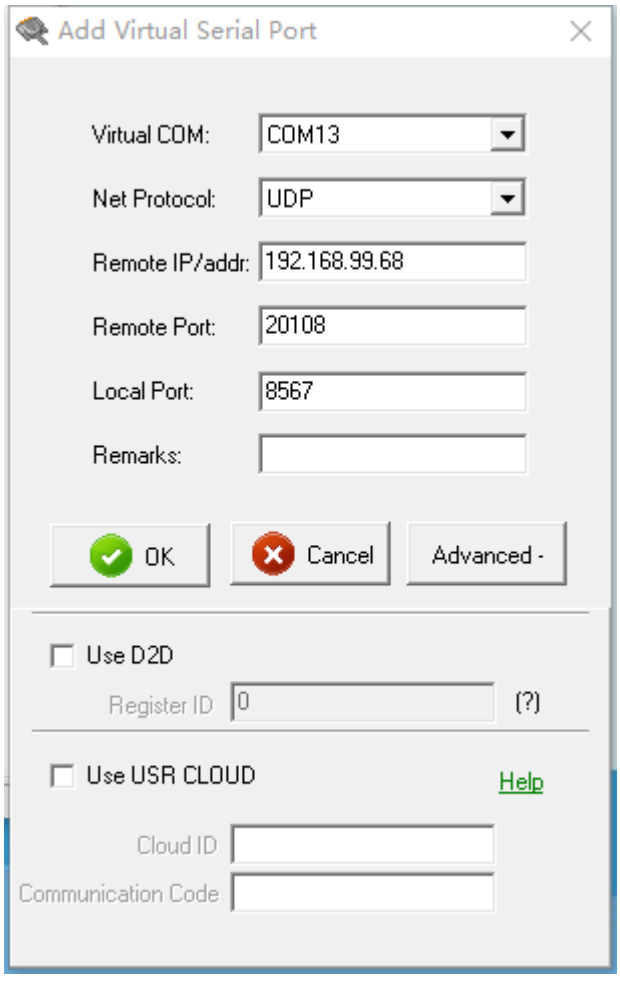
ZigBee gateway directly connected to the computer, the general configuration is:

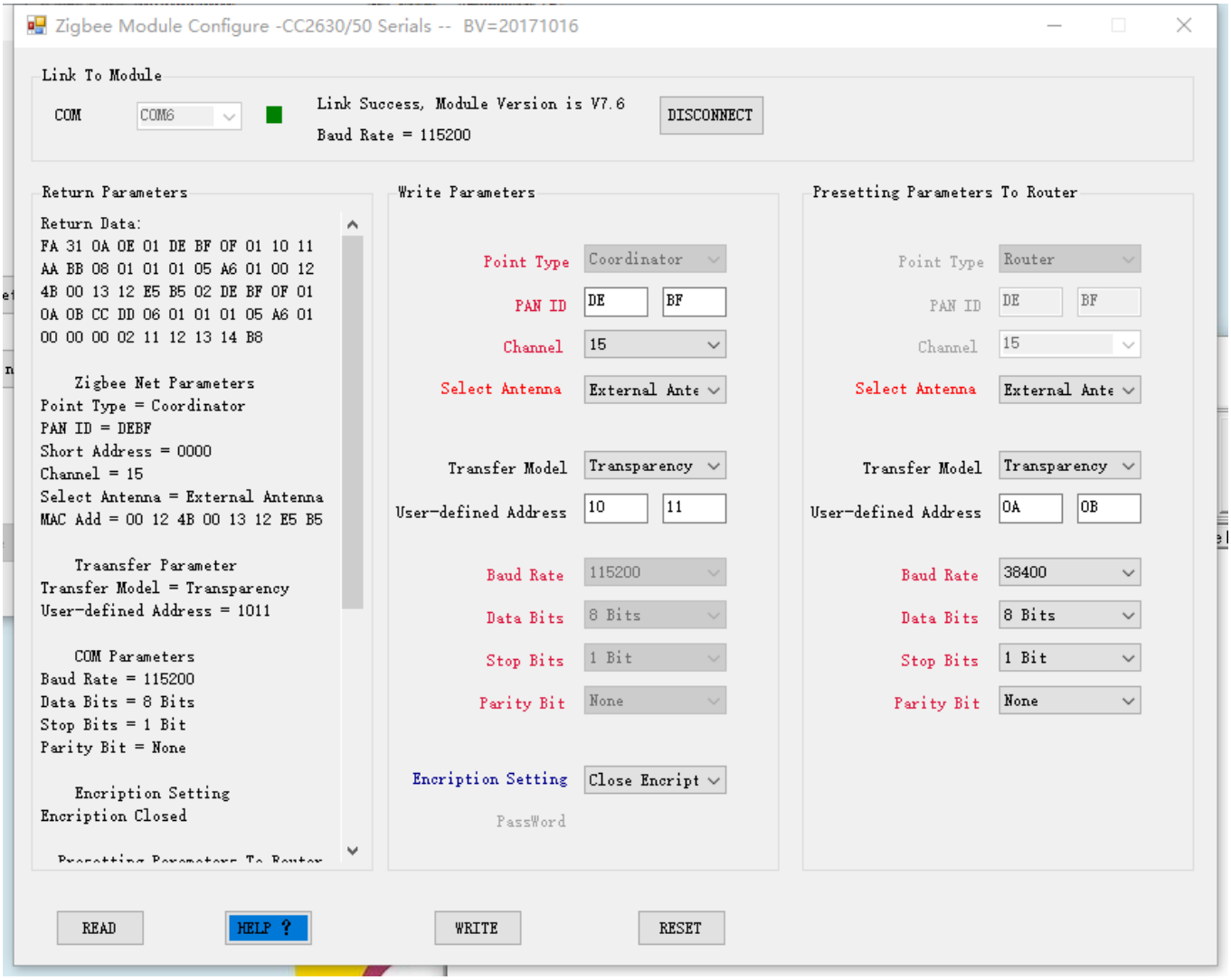
Module network protocol = UDP (do not configure TCP client)
IP mode = static IP (do not configure DHCP)

IP mode must not be configured for DHCP

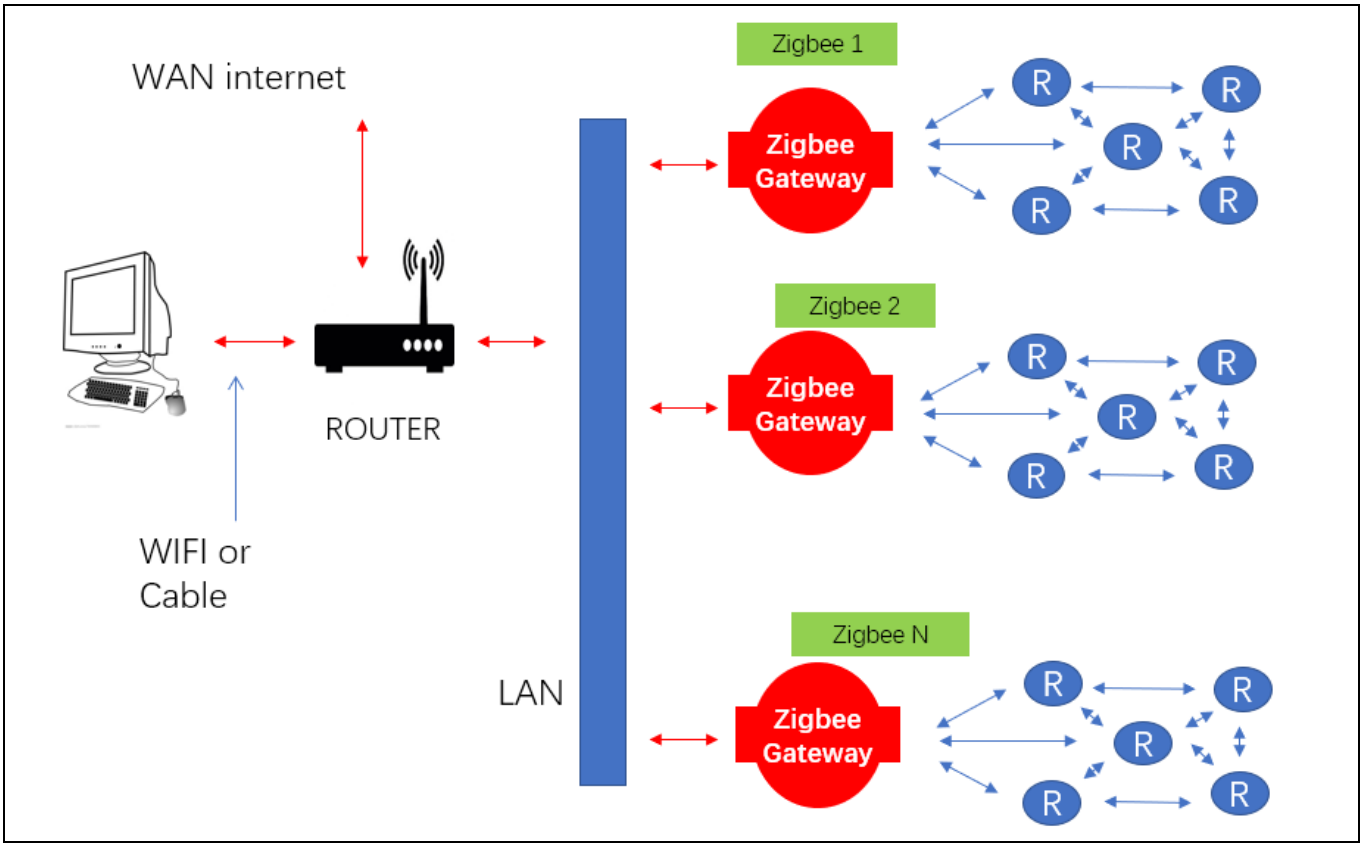


In the computer side to run the "virtual serial port" software, and this virtual port virtual port, you can operate the serial port to operate the network port, including the set ZigBee part of the parameters.

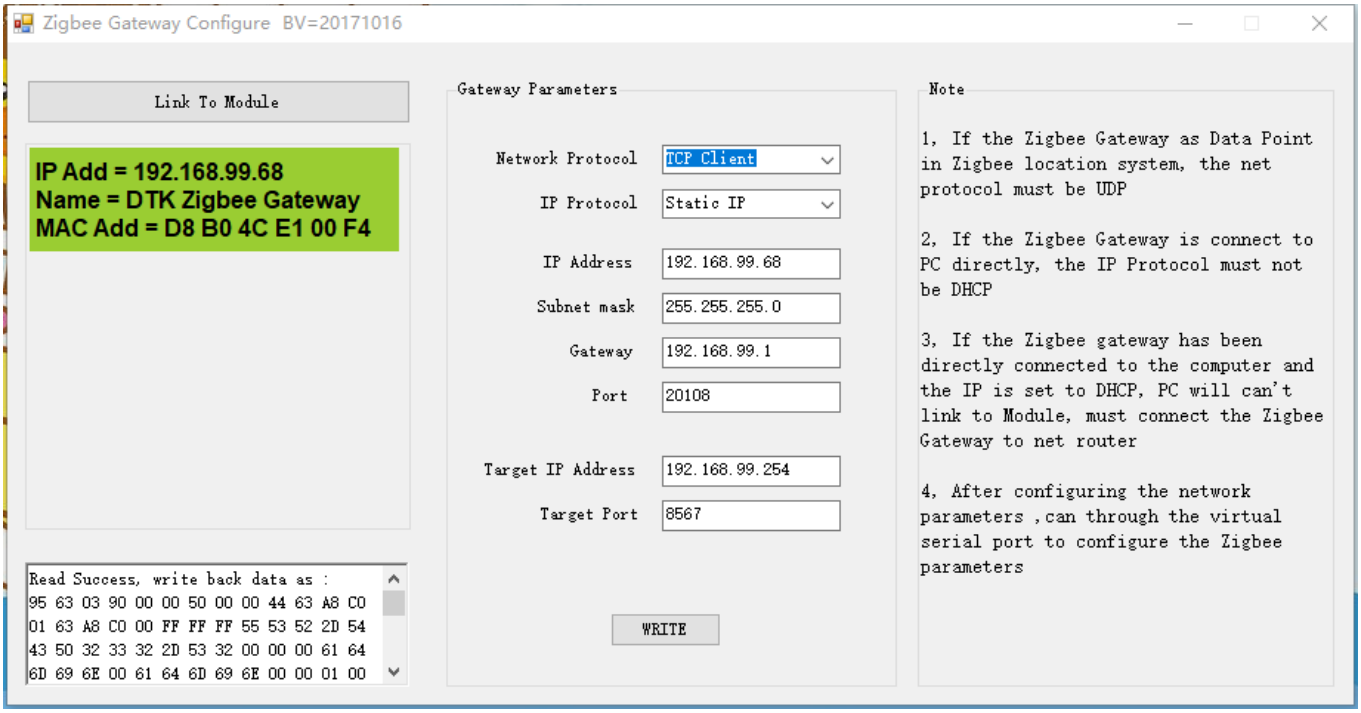



Zigbee Module Configure -CC2630/50 Serials -- BV=20171016
Link To Module
COM
COM6
Link Success, Module Version is V7.6
Baud Rate = 115200
DISCONNECT
Return Parameters
Return Data:
FA 31 0A 0E 01 DE BF 0F 01 10 11
AA BB 08 01 01 01 05 A6 01 00 12
4B 00 13 12 E5 B5 02 DE BF 0F 01
0A 0B CC DD 06 01 01 01 05 A6 01
00 00 00 02 11 12 13 14 B8
Zigbee Net Parameters
Point Type = Coordinator
PAN ID = DEBF
Short Address = 0000
Channel = 15
Select Antenna = External Antenna
MAC Add = 00 12 4B 00 13 12 E5 B5
Traansfer Parameter
Transfer Model = Transparency
User-defined Address = 1011
COM Parameters
Baud Rate = 115200
Data Bits = 8 Bits
Stop Bits = 1 Bit
Parity Bit = None
Encription Setting
Encription Closed
Write Parameters
Point Type
Coordinator
PAN ID
DE
BF
Channel
15
Select Antenna
External Ante
Transfer Model
Transparency
User-defined Address
10
11
Baud Rate
115200
Data Bits
8 Bits
Stop Bits
1 Bit
Parity Bit
None
Encription Setting
Close Encript
PassWord
Presetting Parameters To Router
Point Type
Router
PAN ID
DE
BF
Channel
15
Select Antenna
External Ante
Transfer Model
Transparency
User-defined Address
0A
0B
Baud Rate
38400
Data Bits
8 Bits
Stop Bits
1 Bit
Parity Bit
None
READ
HELP ?
WRITE
RESET

(2) Connected to the computer via LAN



ZigBee gateway through the router even when the computer, the general configuration:
Module Network Protocol = UDP, or TCP Client
IP mode = static IP, or DHCP



ZigBee Gateway Note:

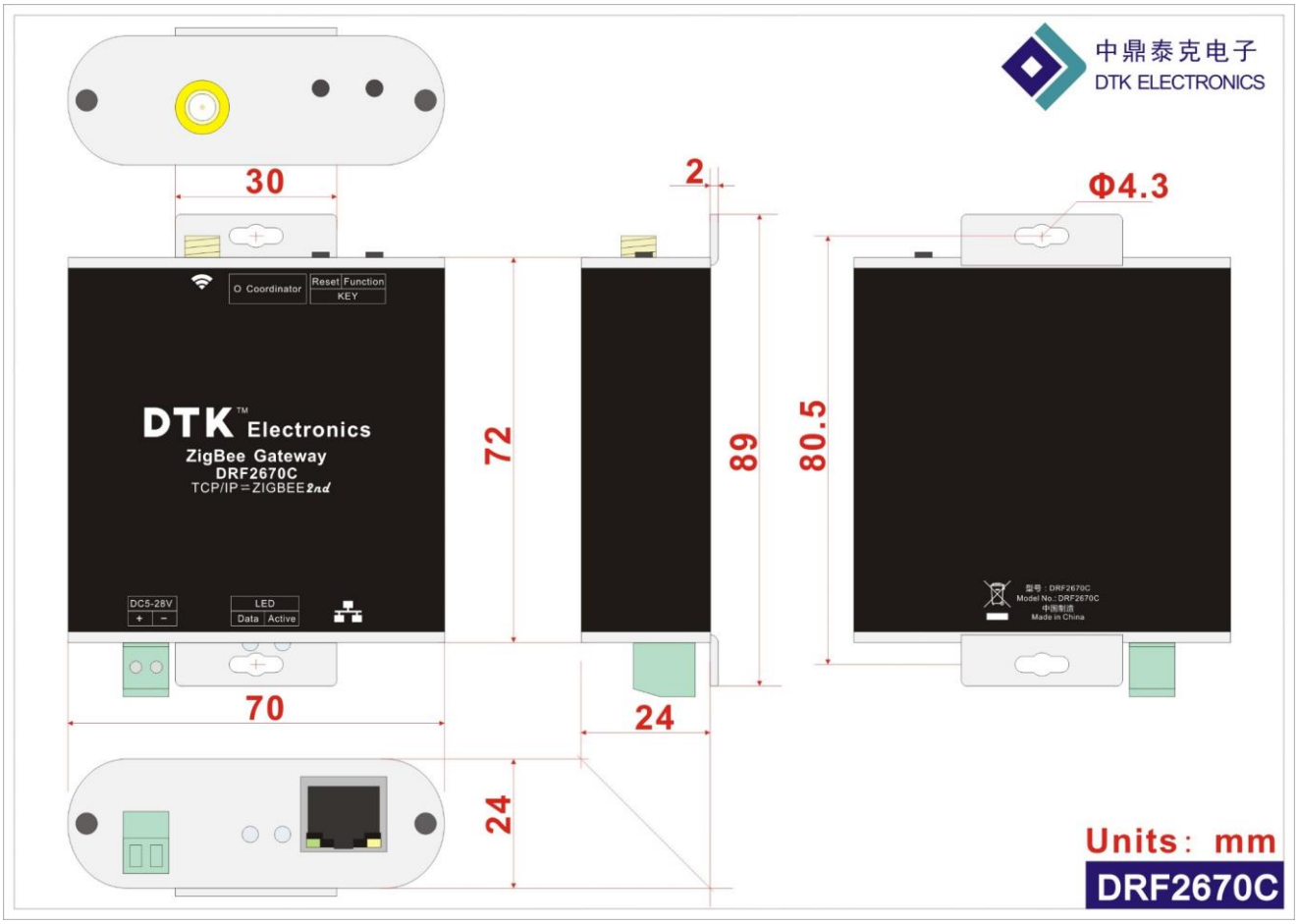
1, ZigBee gateway ZigBee parameters: node type = Coordinator, antenna selection = external antenna, baud rate = 115200, serial port format = 8-N-1, is not set;

2, if the ZigBee gateway is used as a data node for the positioning system, it needs to be set to: PAN ID = 0xDEBF, channel = 15;

3, ZigBee gateway, the use of third-party UART to TCP / IP module, the module can be set to TCP Server, or UDP Server, but taking into account the ZigBee gateway in the ZigBee network status, it is recommended that users only consider UDP and TCP Client Network mode

Parameters

Power	DC 5 – 28V
Temperature range	-40℃~85℃
Serial baud rate	115200bps
Serial format	8-N-1
Radio frequency	2.4GHz (2460MHz), the user can change the channel through the serial command (2405MHz~2480MHz, step: 5MHz), the corresponding channel 11~26 optional
Transmission distance	Visual, open, transmission distance of 1600 meters
Working current	200mA (@5V)
Receiving sensitivity	-98dBm
Main chip	TI CC2630F128
Configurable nodes	Coordinator
Interface	TCP/IP


中鼎泰克电子
DTK ELECTRONICS
30
2
Φ4.3
O Coordinator
Reset
Function
KEY
DTK™ Electronics
ZigBee Gateway
DRF2670C
TCP/IP=ZIGBEE2nd
DC5-28V
+
-
LED
Data
Active
72
89
80.5
70
24
24
Units: mm
DRF2670C

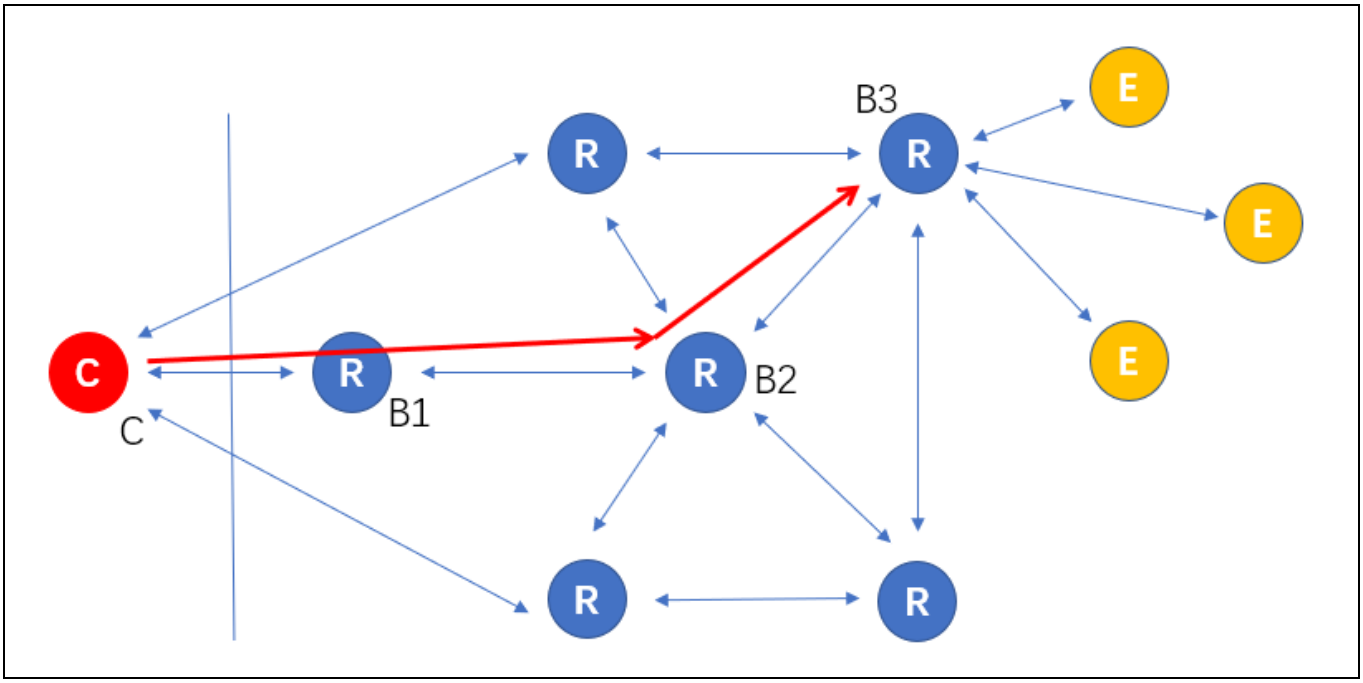
ZigBee Module Settings and Networking

Basic concept:

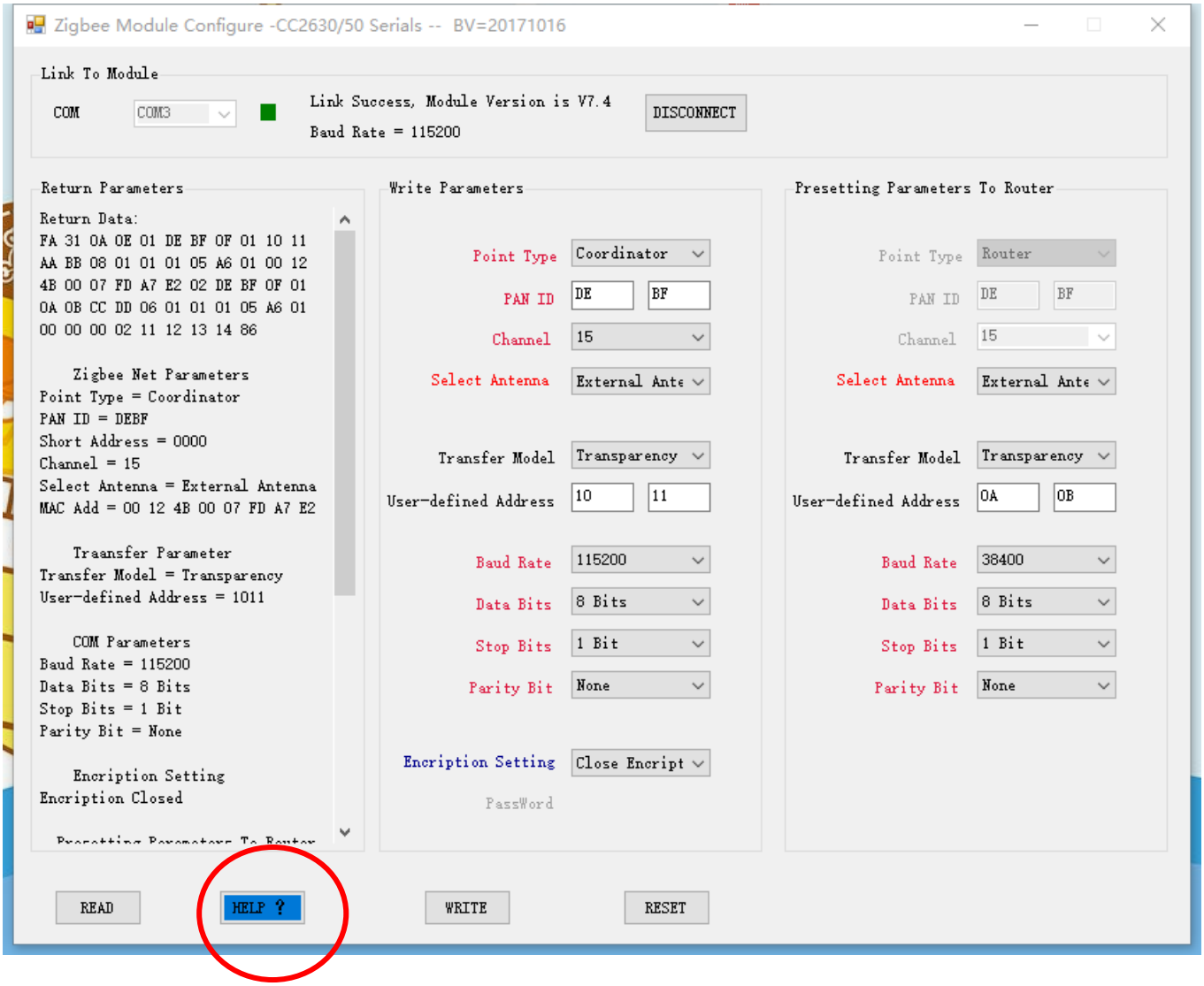
The ZigBee network is a MESH network. A network consists of a Coordinator (master) and N routers (routers, slave modules). All nodes have the same channel and PAN ID.

MESH network is the biggest characteristic of automatic routing and dynamic maintenance routing, such as C and B3 communication in the figure, if not directly reach, will automatically through B1, B2 routing data to B3, and, when B1 or B2 is damaged, will automatically find New routing path

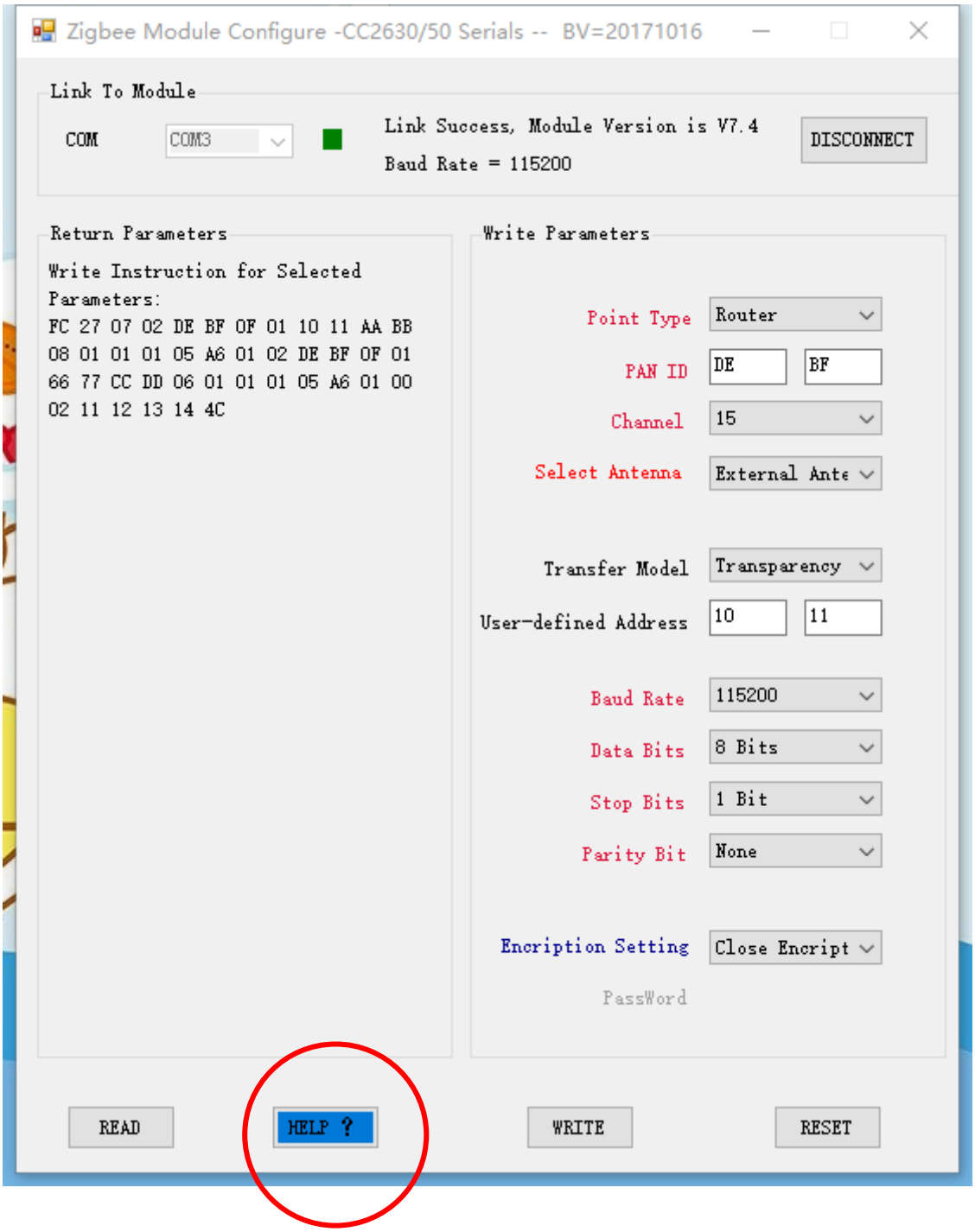
V7.2 / V7.3 Added the End Device node settings:
End Device node does not have the routing function, can send and receive data like Router;
End Device can query the signal strength of the last three routers, if Router is fixed Point, then End Device can be used as a positioning card;



1, first set a module to Coordinator. (If you do not want to set up a router separately, you can also set the parameters of the Router, and then press the function key on Router three times. Router will automatically find the Coordinator to join the network and get the default parameters.



2, the other module is set to Router, the module factory defaults to Router, you can not set the Router, press the function key three times Router, Router will automatically find the Coordinator to join the network, and from the Coordinator out of the default parameters, if different Router If you need different parameters (such as baud rate), you need to set up Router separately.

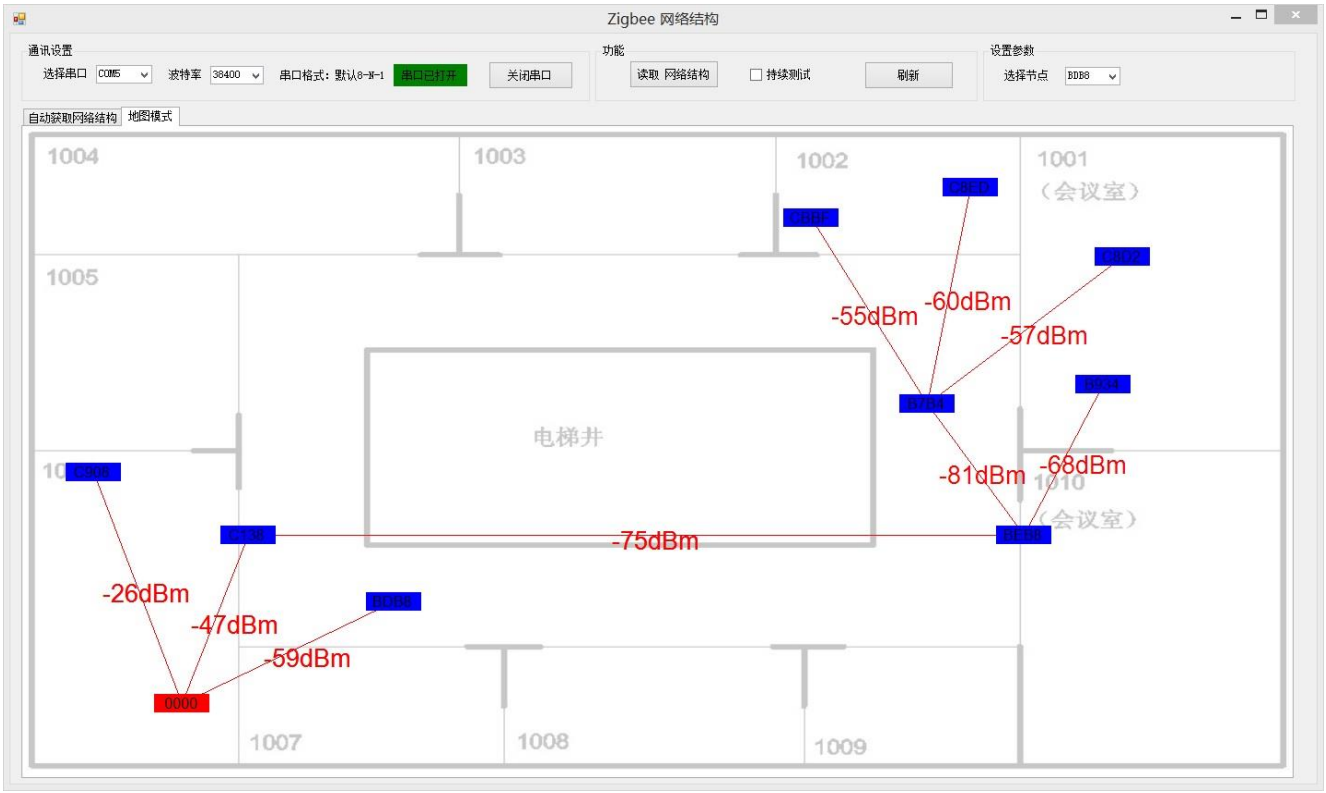


LED indicate:

Coordinator	
LED4	Long bright
LED3	When received wireless data, it will follow flash
Router	
LED4	Did not join the network (looking for the network), flashing After joining the network, slow flash Press the function key three times, start automatically join the network, and flash
LED3	When received wireless data, it will follow flash Press the function key three times, start automatically join the network, and flash

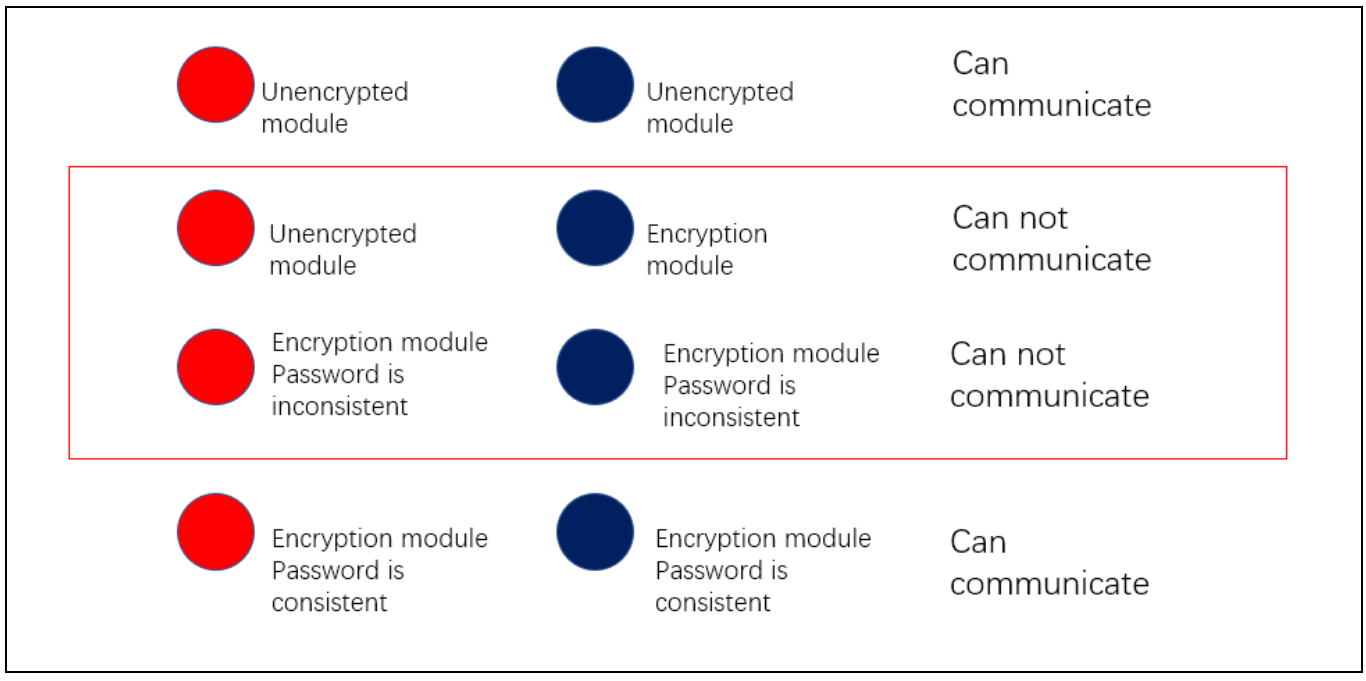
4, the network is completed, you can use DTK application software to observe the network structure:

Set the baud rate of the Coordinator to 115200 (or 57600, 38400)
Connect to the computer serial port
Run DTK CC2630 software, select ZigBee network
Select "map mode"
Click the right mouse button, select "switch map", select your own map file (such as jpg picture)
Point "connection module"
Point "read network structure"
Drag the read node to the corresponding place on the map



The ZigBee module can be set to use encryption and not use encryption, and can set 32-bit (4-byte encryption password)

For details, refer to the setting command (INS06). (Communication refers to data transmission and join the network)



Data Transfer for ZigBee Modules

ZigBee module has two kinds of data transmission methods:

1, transparent transmission (does not change the data, the module is equivalent to the serial line between):

(1), Coordinator data received from the serial port, will be sent to all the routers, and Output from the router serial port;

(2), Router received from the serial data, will be sent to the Coordinator intact, and Output from the Coordinator serial port.

2, point to point transmission:

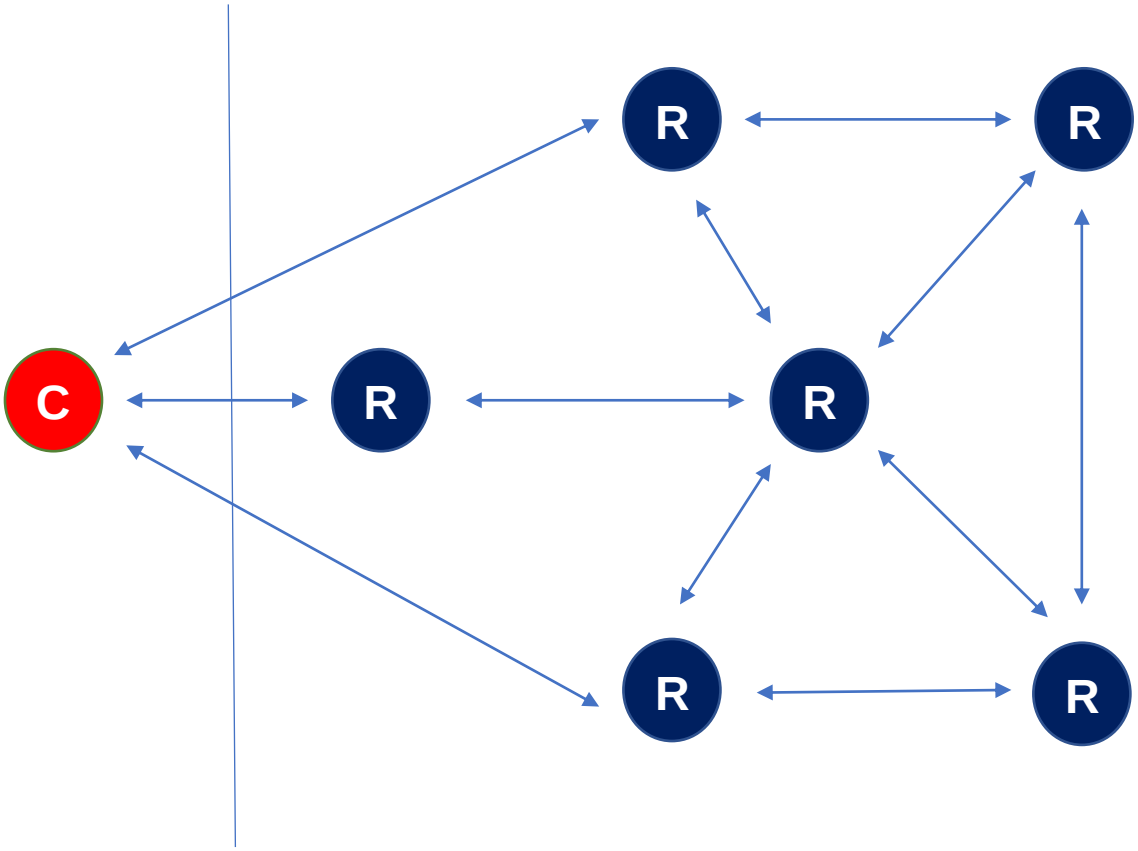
(1), can be sent to any node within a ZigBee network point to point;
You can use a short address as the destination address
You can use a custom address as the destination address

(2), or broadcast to all nodes within the ZigBee network.

1, transparent transmission:

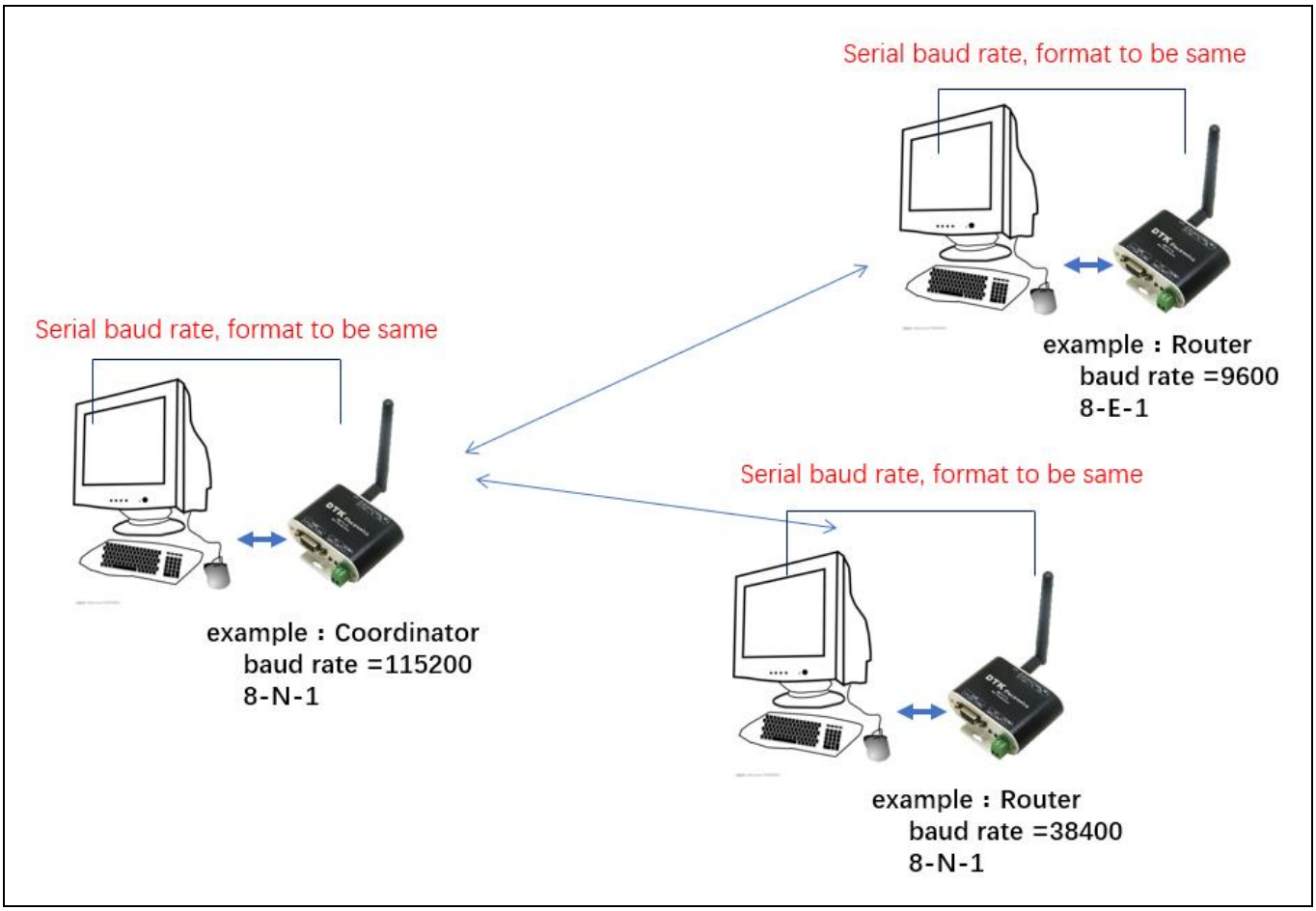
In this transmission process, Router will automatically find the best routing path for the data transmission automatically provides relay (no user settings, can be placed on demand).

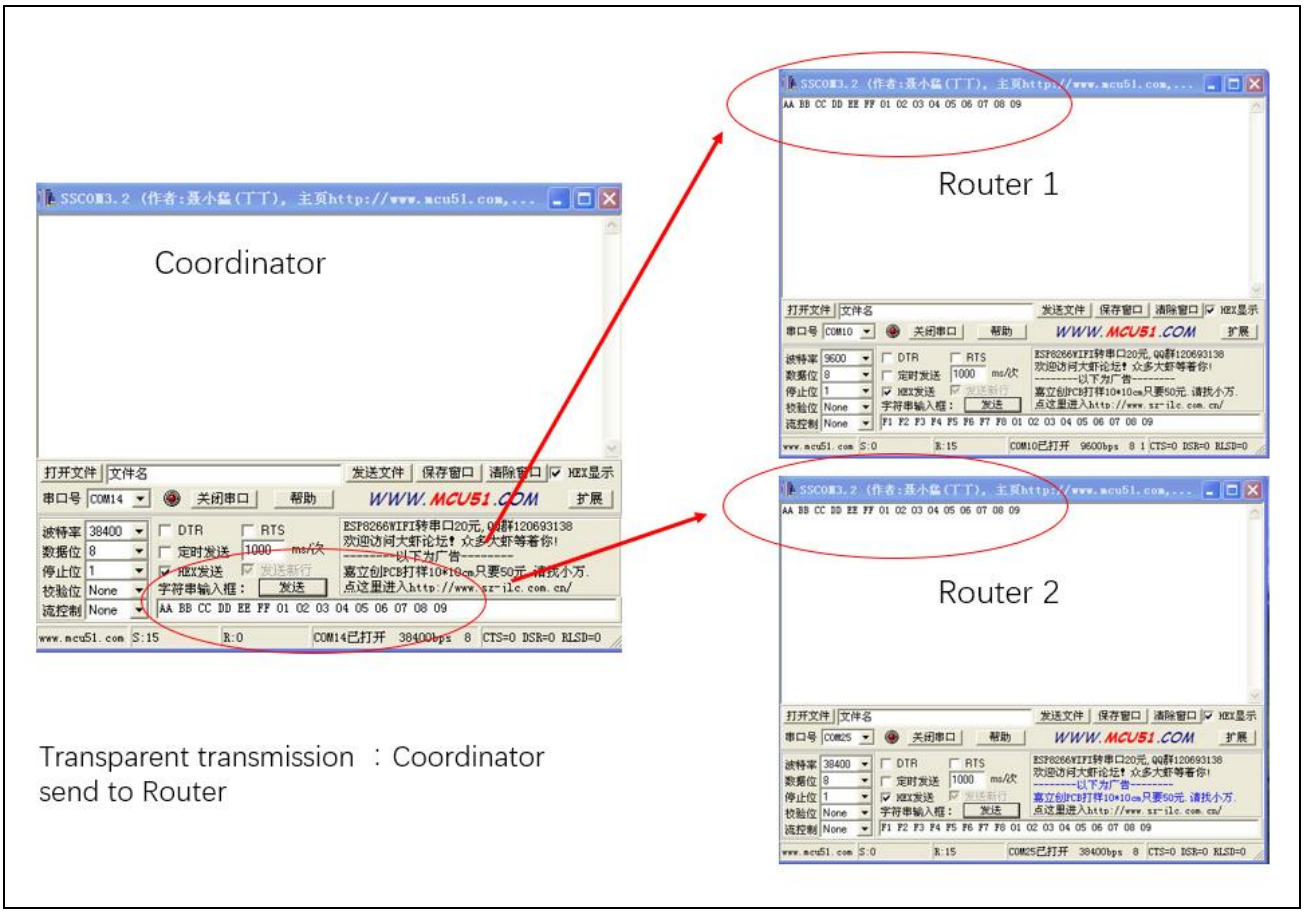
Transparent transmission between the Coordinator and Router, the equivalent of a serial line, that is, users do not need to modify the device or host computer software, cable can be converted into wireless transmission (and automatic routing).



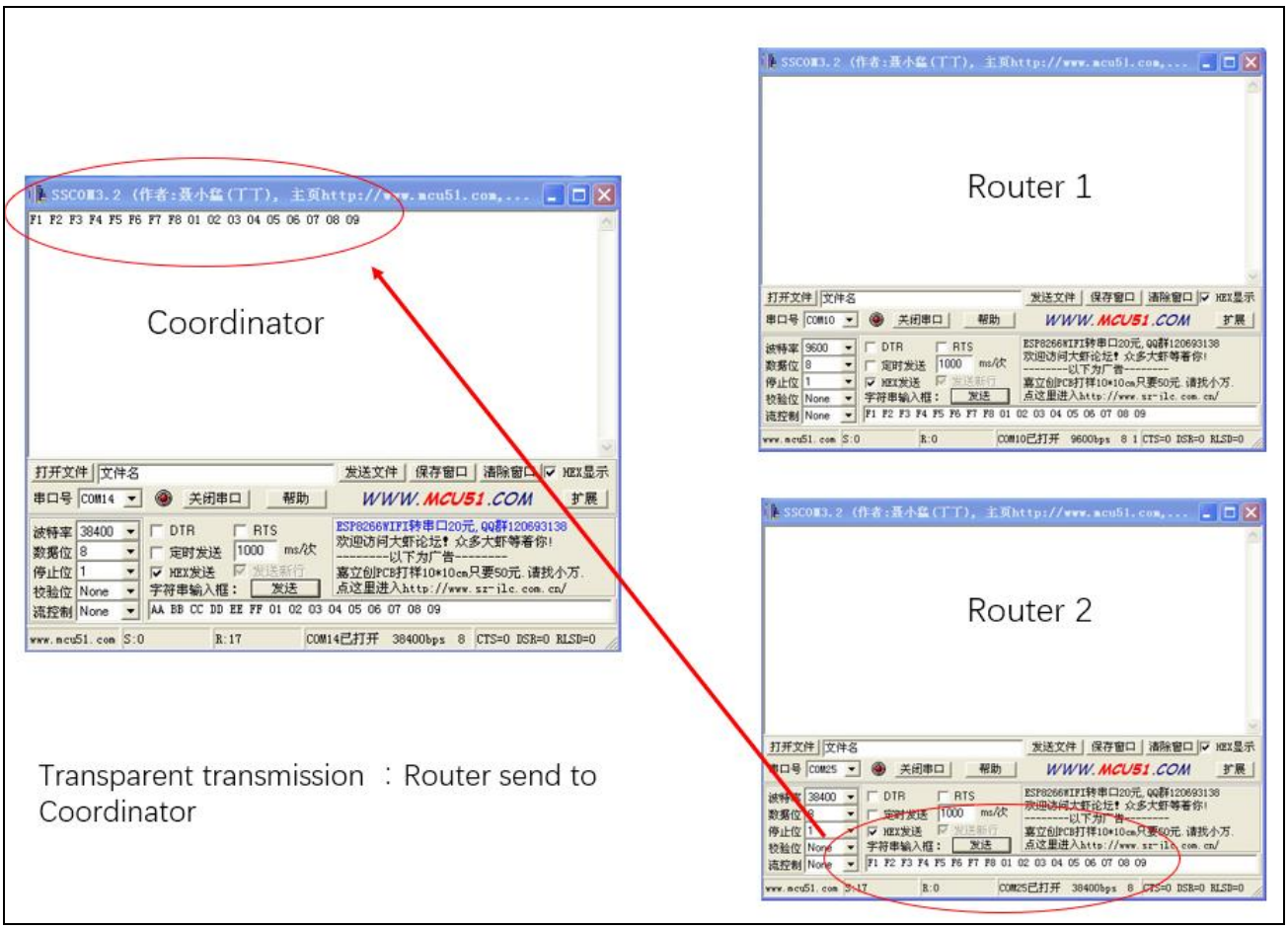
Transparent transmission test:

1 Coordinator connected to the computer
Routers connected to other computers (or other serial ports on the same computer)





Transparent transmission ：Coordinator send to Router



Transparent transmission ：Router send to Coordinator

2, point to point transmission (short address as the destination address):

Point-to-point is generally suitable for data transmission between Router and Router, can be sent to any node or broadcast to all nodes.

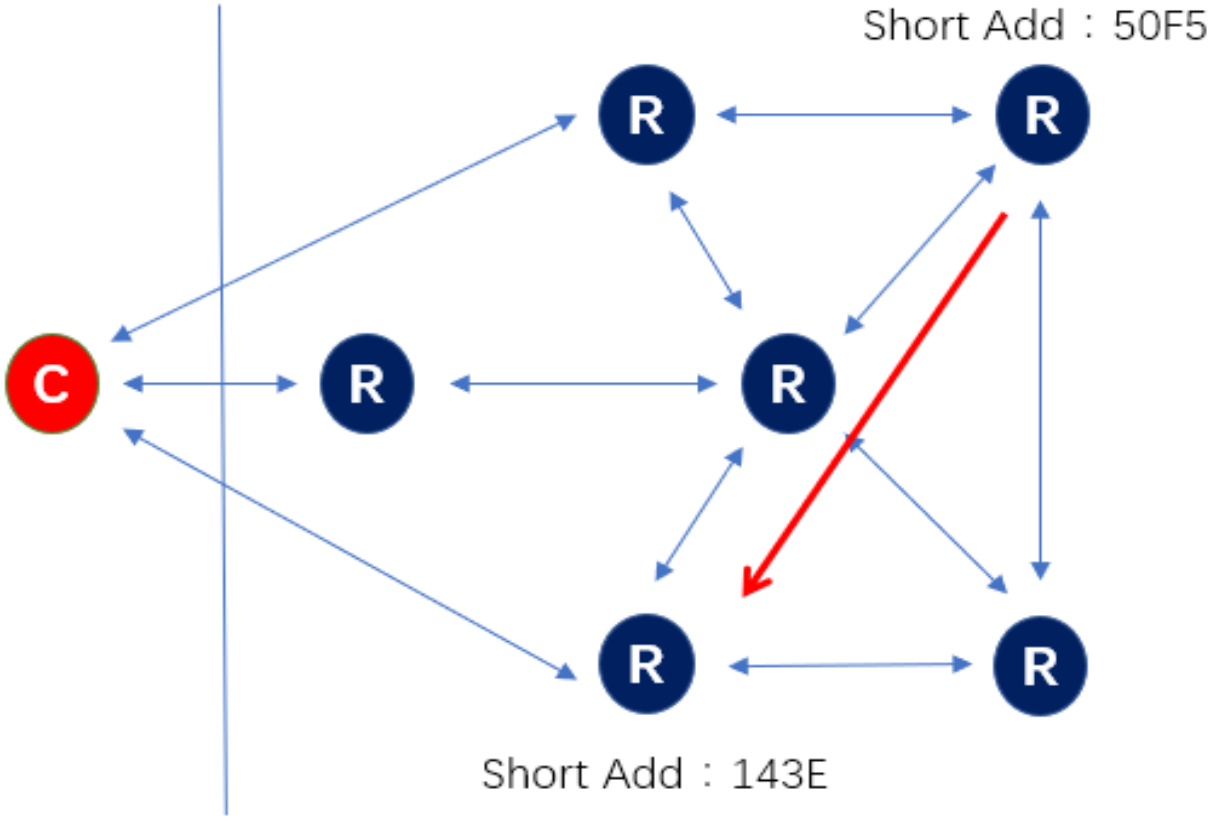
Send command format:
Data transfer instruction (0xFD) + data length + destination address (short address) + data (up to 92 Bytes)
The data length is longer in 92 bytes.

Example: Assuming data is transferred from 0x50F5 to 0x143E,

SEND： FD 0A 14 3E 01 02 03 04 05 06 07 08 09 10 (FD：Data transfer instruction, 0A：data length, 10 bytes, 14 3E：destination address, 01 02 03 04 05 06 07 08 09 10：data)

Received： FD 0A 14 3E 01 02 03 04 05 06 07 08 09 10 50 F5

If the destination address is 0xFFFF, than broadcast to all nodes



3, point to point transmission (custom address as the destination address):

Point-to-point is generally suitable for data transmission between Router and Router, can be sent to any node or broadcast to all nodes

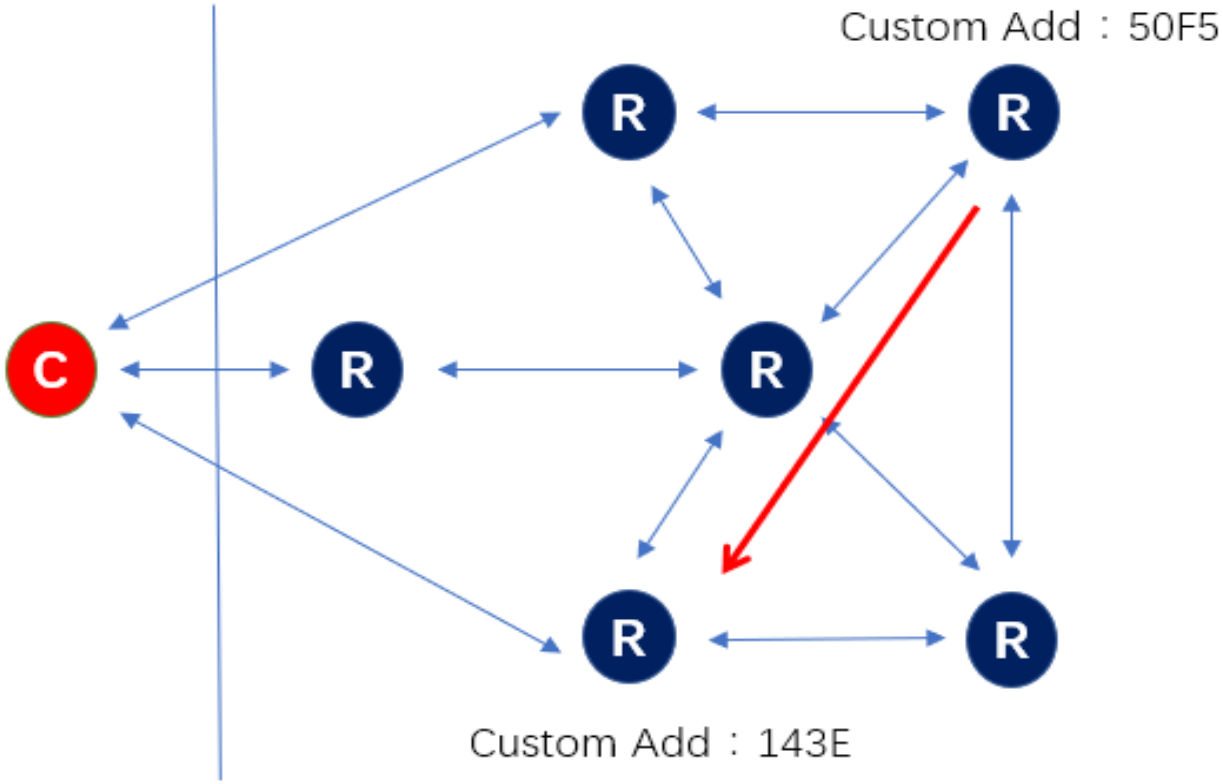
Send command format:
Data transfer instruction (0xED) + data length + destination address (custom address) + data (up to 92 Bytes)
The data length is longer in 92 bytes.

Example: Assuming data is transferred from 0x50F5 to 0x143E,

SEND： ED 0A 14 3E 01 02 03 04 05 06 07 08 09 10 (ED：Data transfer instruction, 0A：data length, 10 bytes, 14 3E：destination address, 01 02 03 04 05 06 07 08 09 10：data)

Received： ED 0A 14 3E 01 02 03 04 05 06 07 08 09 10 50 F5

If the destination address is 0xFFFF, than broadcast to all nodes



4, point to point transmission (custom address as the target address, remove the packet header):

Point-to-point is generally suitable for data transmission between Router and Router, can be sent to any node or broadcast to all nodes

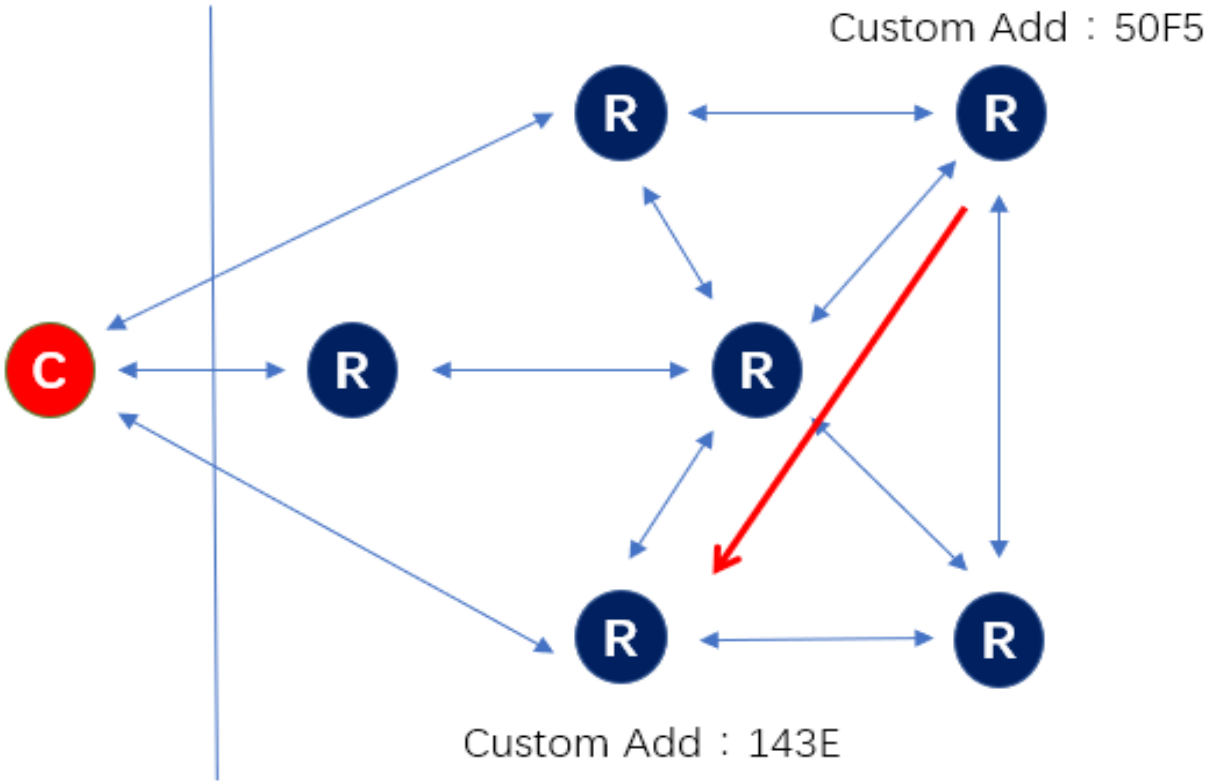
Send command format:
Data transfer instruction (0xEC) + data length + destination address (custom address) + data (up to 92 Bytes)
The data length is longer in 92 bytes.

Example: Assuming data is transferred from 0x50F5 to 0x143E,

SEND： EC 0A 14 3E 01 02 03 04 05 06 07 08 09 10 (EC：Data transfer instruction, 0A：data length, 10 bytes, 14 3E：destination address, 01 02 03 04 05 06 07 08 09 10：data)

Received： 01 02 03 04 05 06 07 08 09 10

If the destination address is 0xFFFF, the broadcast is sent to all nodes



5, transparent transmission + custom address:

(This is a transparent transmission)

Set the transfer mode of a module to: Transparent transfer + Custom address

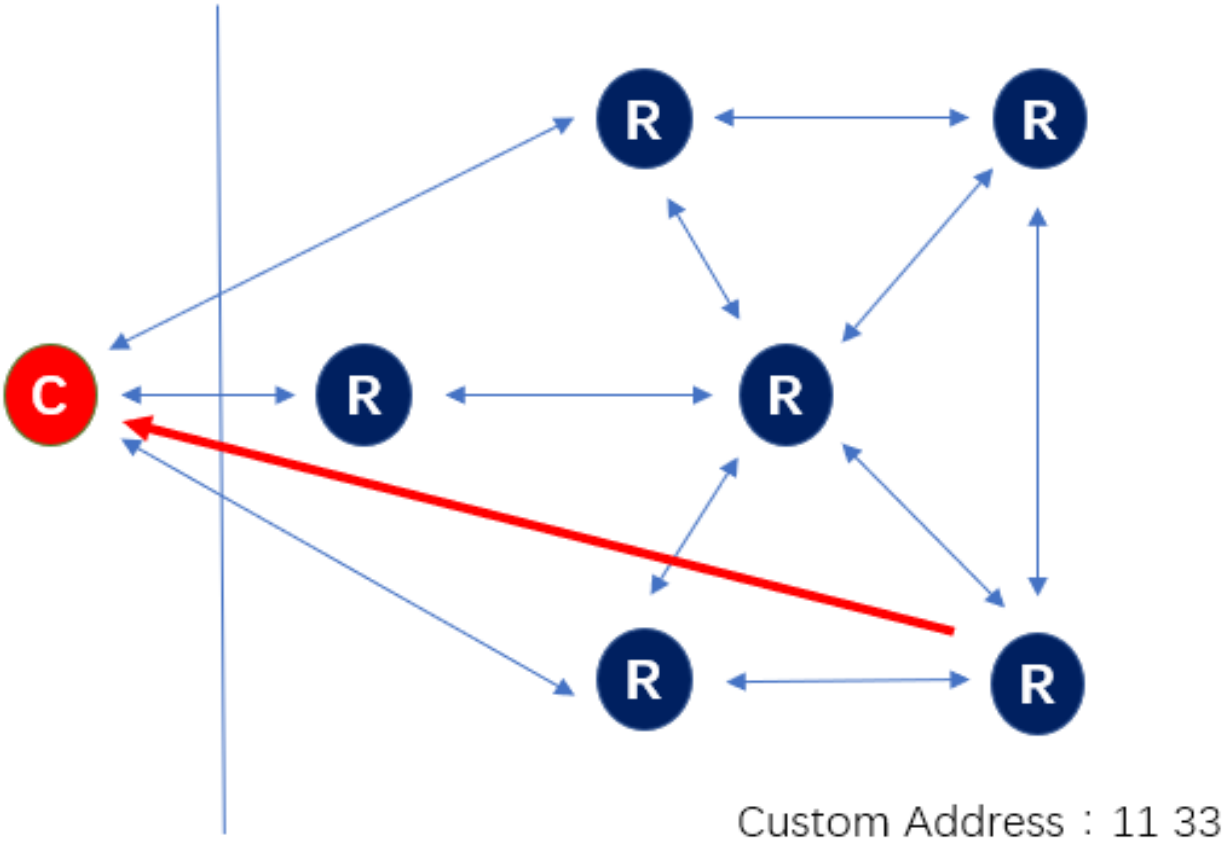
Then the module in the data transparent transmission, the data will be added at the end of their own custom address (2 bytes), sent together.

The data received by the receiver is: Data + Source node's custom address (2 bytes)

Send: 01 02 03 04 05 06 07 08 09 10

The data received is:
01 02 03 04 05 06 07 08 09 10 11 33
Data + Source node's custom address (2 bytes)

The maximum number of data sent is 259 bytes (plus the custom address is 261 bytes)



6, transparent transmission + short address:

(This is a transparent transmission

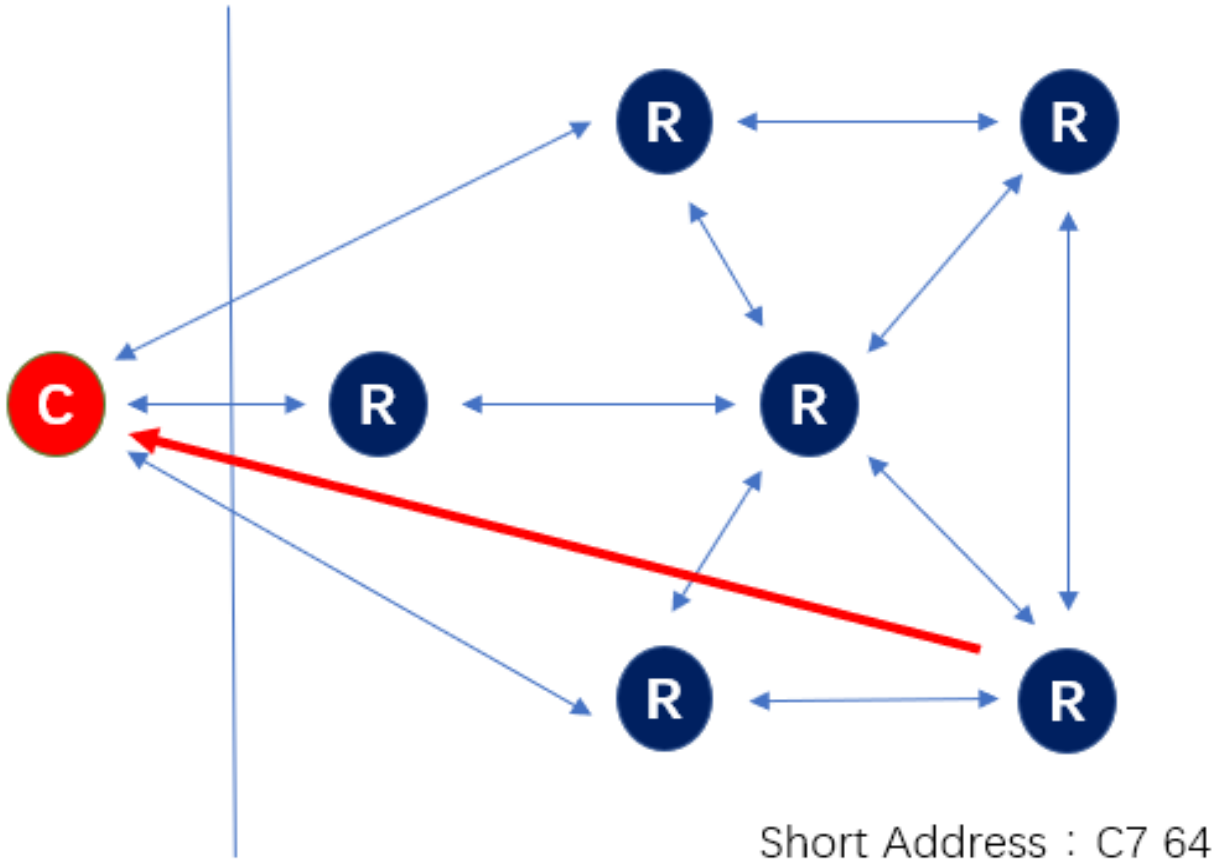
Set the transfer mode of a module to: Transparent transmission + Short address

Then the module in the data transparent transmission, the data will be added at the end of their own short address (2 bytes), sent together.

The data received by the receiver is: Data + Source node's short address (2 bytes)

Send: 01 02 03 04 05 06 07 08 09 10

The data received is:
01 02 03 04 05 06 07 08 09 10 C7 64
Data + Source node's short address (2 bytes)
The maximum number of data sent is 259 bytes (plus the short address is 261 bytes)



7, transparent transmission + MAC address:

(This is a transparent transmission)

Set the transmission mode of a module to: Transparent transfer + MAC address

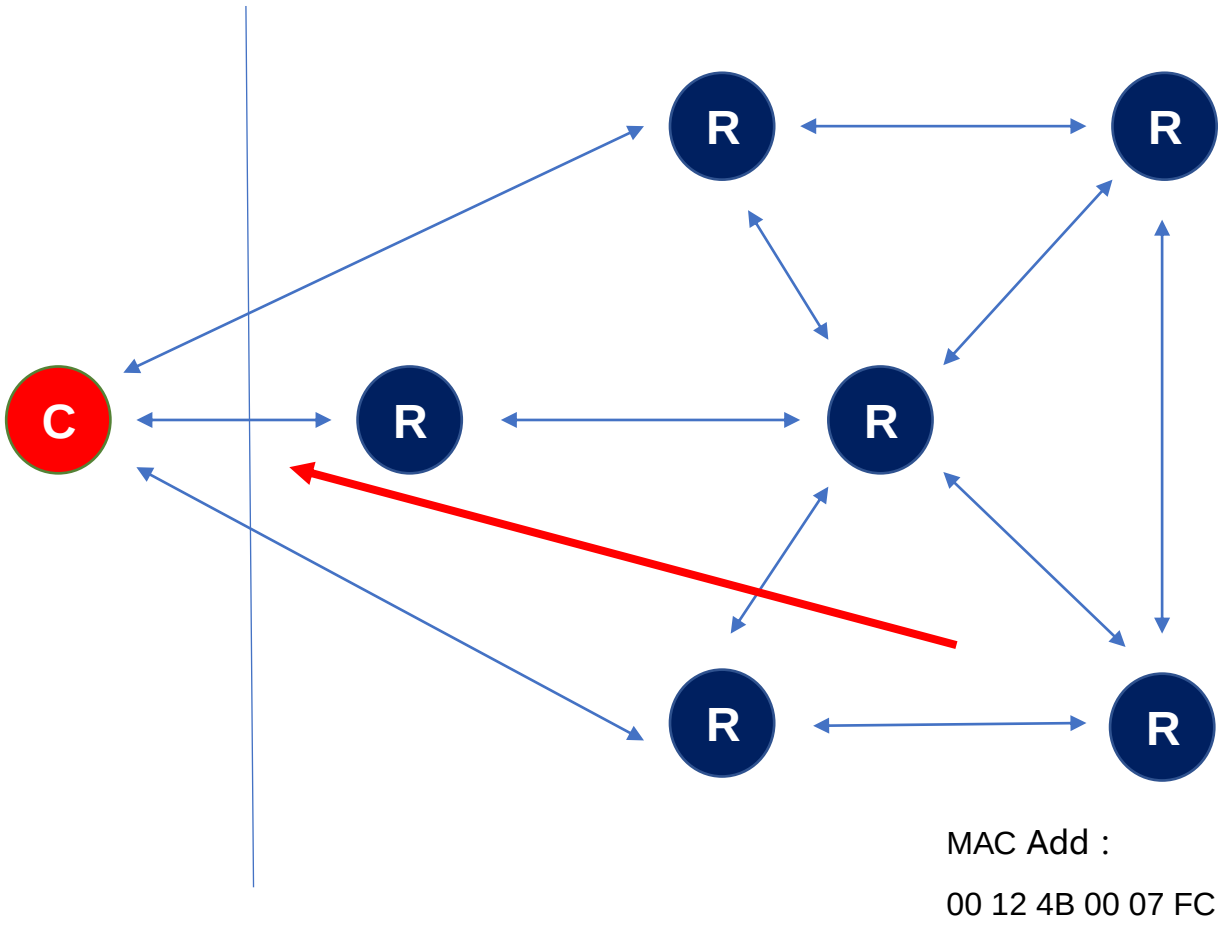
Then the module in the data transparent transmission, the data will be added to the final MAC address (8 bytes), sent together.

The data received by the receiver is: MAC address of the data + source node (8 bytes)

Send: 01 02 03 04 05 06 07 08 09 10

The data received is:
01 02 03 04 05 06 07 08 09 10 00 12 4B 00 07 FC C6 B0
Data + Source MAC address of the node (8 bytes)

The maximum number of data sent is 259 bytes (plus the MAC address of 267 bytes)
MAC addresses are globally unique

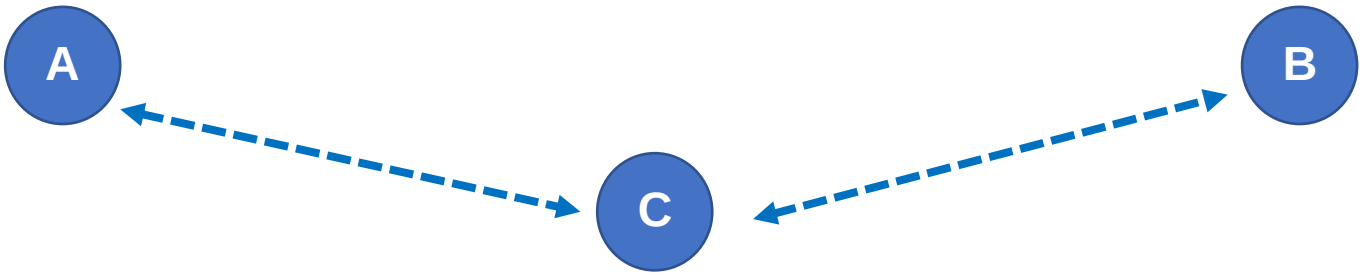


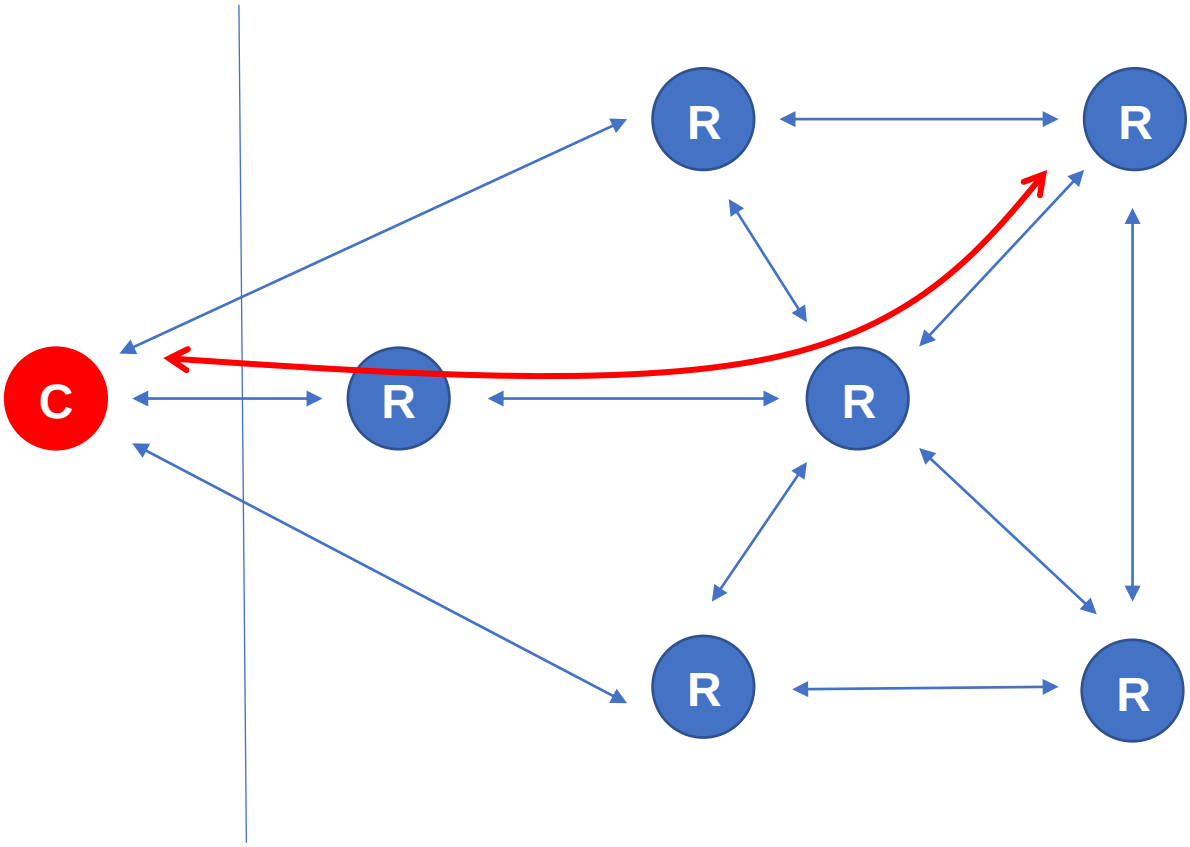
ZigBee module routing

ZigBee module routing is completely automatic, suitable for transparent transmission, point to point transmission.

Assuming that the distance between A and B modules is far away, it cannot communicate with A and B. Then, if there is a module C between A and B, if A, C, B and C can communicate with each other, then C Can automatically act as A, B between the routing.

C does not need special settings, just need to join the network.



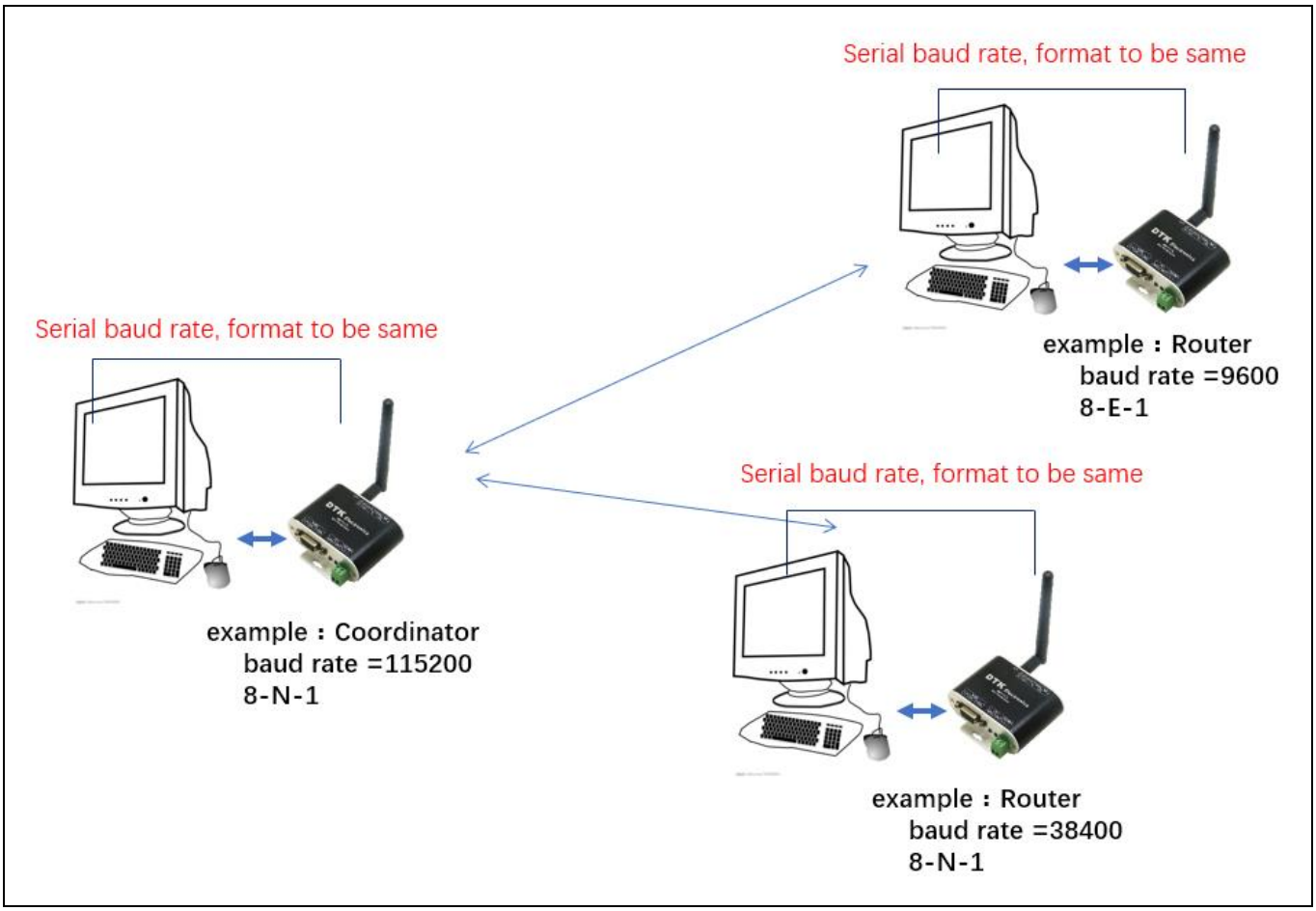


About baud rate:

Baud rate refers to: 2 hardware devices directly connected, the communication between them;

Users do not need to care about the so-called "ZigBee air baud rate";

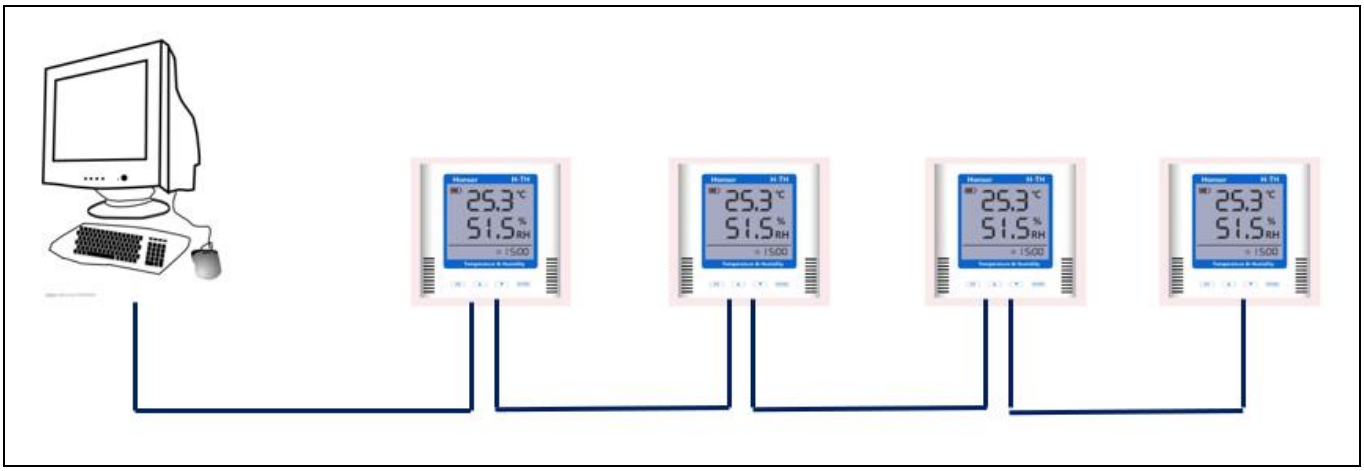
So: a ZigBee module connected with a device, the baud rate between them (and serial format) to be consistent, rather than requiring a ZigBee network ZigBee module baud rate to be consistent.



ZigBee Module Networking Example

Suppose there is a wired temperature and humidity measurement, transmission system. We use the ZigBee module to connect, transformed into a wireless ZigBee network temperature and humidity measurement system:

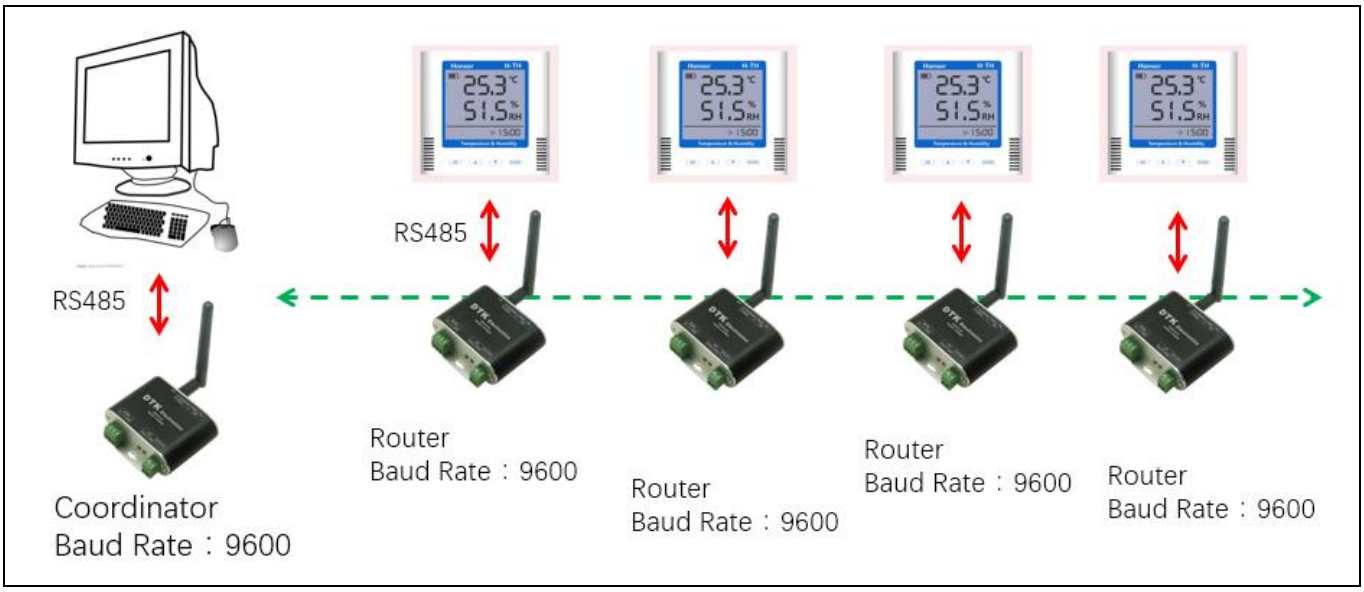
1 host computer through the RS485 bus connected to the four temperature and humidity measuring instrument (or temperature and humidity transmitter):
(Connected baud rate of 9600, MODBUS RTU protocol)



Renovation:

1, 1 module are set to Coordinator, connected to the host computer.

2, 4 modules are set to Router, connected to the temperature and humidity meter.
After the connection is complete, do not need to modify the host computer software, do not need to modify the device configuration, and wired use exactly the same.


RS485
Coordinator
Baud Rate：9600
RS485
Router
Baud Rate：9600
Router
Baud Rate：9600
Router
Baud Rate：9600
Router
Baud Rate：9600

ZigBee Module Instruction System

CC2630 series ZigBee module, the current shipments for the V7.4 / V7.5 / V7.6 version, instructions backward compatible.

Each version of the general instructions	Connection module (INS01)
	Reset module(INS02)
V7.0 /V7.1 instructions	Read module(INS03)
	Write module(INS04)
After V7.2 /V7.3 instructions	Read module (INS05)
	Write module (INS06)
	Query the End Device location (INS07)
	Query the point(Router, End Device) RSSI(INS08)

Note: All write instructions, write after the module needs to restart effective

Module received a connection instruction or read instruction, will enter the configuration state, prohibit the receipt of data for one minute

(INS01), Connection module instructions (Hexadecimal format)

Send	Head	Length	Instruction	Checksum
	FC	06	04 44 54 4B 52 46	81(In front of all bytes and, Keep the lower 8 bits)

	Head	Length	Status	Back instruction	Checksum
Back	FA	06	0A：Success 0B：Failed 0C：Disable	04 44 54 4B Software version (2 bytes) Software version = reply byte / 10 If the setting fails (or disable setting), only reply to 04, the instruction length is 02	In front of all bytes and, Keep the lower 8 bits

Note: After the connection is successful, the module enters the setting state, will prohibit the wireless data reception 1 minute

Example:
Send: FC 06 04 44 54 4B 52 46 81
Reply: FA 06 0A 04 44 54 4B 00 46 37 (connection successful),
Software version = 0x0046 / 10 = V7.0
FA 02 0B 04 0B (connection failed)

If the command is wrong, will be sent out as a data (of course, no reply)

(INS02), Reset module instruction (Hexadecimal format)

	Head	Length	Instruction	Checksum
Send	FC	06	06 44 54 4B AA BB	50 (In front of all bytes and, Keep the lower 8 bits)

	Head	Length	Status	Back instruction	Checksum
Back	FA	06	0A：Success 0B：Failed 0C：Disable	06 44 54 4B AA BB	58(In front of all bytes and, Keep the lower 8 bits)

Example:
Send: FC 06 06 44 54 4B AA BB 50
Received: FA 06 0A 06 44 54 4B AA BB 58 (module received reset command succeeded)
FA 06 0B 06 44 54 4B AA BB 59 (module receive reset command failed)

After the module receives a reset instruction, it restarts the module immediately.

(INS03), Read module instruction (Hexadecimal format)

Suitable for V7.0 / V7.1 firmware

	Head	Length	Instruction	Checksum
Send	FC	06	05 44 54 4B 52 46	82(In front of all bytes and, Keep the lower 8 bits)

	Head	Length	Status	Back instruction	Checksum
Back	FA	2B	0A：Success 0B：Failed 0C：Disable	05 + Read all the parameters of the module(42 Bytes)	In front of all bytes and, Keep the lower 8 bits

Example:

Send：FC 06 05 44 54 4B 52 46 82

Back：FA 2B 0A 05 01 5A 76 14 01 00 01 AA BB 06 01 01 01 05 A6 01 00 12 4B 00 07 FC C9 E2 02 5A 76 14 01 0A 0B CC DD 04 01 01 01 05 A6 00 00 00 97

If the command is wrong, will be sent out as a data (of course, no reply).

Note: After the success of the module, the module into the set state, will prohibit the wireless data reception 1 minute

Read all parameters of the module (hexadecimal, 42 Bytes):

X0	Point Type: 01 Coordinator, 02 Router
X1 X2	PAN ID: 0001-FF00
X3	Channel: 0B – 1A
X4	Transmission mode, Default write 01 Unchangeable
X5 X6	Self-address: Range: 0001 - FF00
X7 X8	Keep it, Default write AA BB
X9	Baud rate: 0x01：1200 0x02：2400 0x03：4800 0x04：9600 0x05：19200 0x06：38400 0x07：57600 0x08：1115200
X10	Data bits 01: default 8-bit data bits Unchangeable
X11	Stop bit 01: default 1 bit stop bit Unchangeable
X12	Parity 0x01: No parity 0x02: Even parity 0x03: Odd parity
X13 X14	Keep it, Default write 05 A6
X15	Antenna selection 00: Onboard antenna 01: External antenna
X16 – X23	MAC Address, 8 Bytes
Note	If the module is Coordinator, starting from X24 to X39, is the default to the Router parameters If the module is Router, starting from X24 to X39, read out the parameters meaningless
X24	Point Type: 01 Coordinator, 02 Router
X25 X26	PAN ID: 0001-FF00

X27	Channel: 0B – 1A
X28	Transmission mode, Default write 01 Unchangeable
X29 X30	Self-address: Range: 0001 - FF00
X31 X32	Keep it, Default write CC DD
X33	Baud rate: 0x01：1200 0x02：2400 0x03：4800 0x04：9600 0x05：19200 0x06：38400 0x07：57600 0x08：1115200
X34	Data bits 01: default 8-bit data bits Unchangeable
X35	Stop bit 01: default 1 bit stop bit Unchangeable
X36	Parity 0x01: No parity 0x02: Even parity 0x03: Odd parity
X37 X38	Keep it, Default write 05 A6
X39	Antenna selection 00: Onboard antenna 01: External antenna
X40 X41	Short address Such as the point address of the FF FE, Indicates that Router is not added to the network

(INS04), Write module instruction (Hexadecimal format)

Suitable for V7.0 / V7.1 firmware

	Head	Length	Instruction	Checksum
Send	FC	21	07 + Write all parameters of the module(32 Bytes)	In front of all bytes and, Keep the lower 8 bits

	Head	Length	Status	Back instruction	Checksum
Back	FA	01	0A：Success 0B：Failed 0C：Disable	07	In front of all bytes and, Keep the lower 8 bits

Example:
Send: FC 21 07 02 01 01 14 01 00 01 AA BB 06 01 01 01 05 A6 00 02 01 01 14 01 66 77 CC DD 06 01 01 01 05 A6 00 AA
Reply: FA 01 0A 07 0C

If the command is wrong, will be sent out as a data (of course, no reply)

Write parameters (hexadecimal, 32 Bytes) :

X0	Point Type: 01 Coordinator, 02 Router
X1 X2	PAN ID: 0001-FF00
X3	Channel: 0B – 1A
X4	Transmission mode, Default write 01 Unchangeable
X5 X6	Self-address: Range: 0001 - FF00
X7 X8	Keep it, Default write AA BB
X9	Baud rate: 0x01：1200 0x02：2400 0x03：4800 0x04：9600 0x05：19200 0x06：38400 0x07：57600 0x08：1115200
X10	Data bits 01: default 8-bit data bits Unchangeable
X11	Stop bit 01: default 1 bit stop bit Unchangeable
X12	Parity 0x01: No parity 0x02: Even parity 0x03: Odd parity
X13 X14	Keep it, Default write 05 A6
X15	Antenna selection 00: Onboard antenna 01: External antenna
Note	If the module is Coordinator, starting from X16 to X31, is the default to the Router parameters If the module is Router, starting from X16 to X31, read out the parameters meaningless
X16	Point Type: 01 Coordinator, 02 Router
X17 X18	PAN ID: 0001-FF00

X19	Channel: 0B – 1A
X20	Transmission mode, Default write 01 Unchangeable
X21 X22	Self-address: Range: 0001 - FF00
X23 X24	Keep it, Default write CC DD
X25	Baud rate: 0x01：1200 0x02：2400 0x03：4800 0x04：9600 0x05：19200 0x06：38400 0x07：57600 0x08：1115200
X26	Data bits 01: default 8-bit data bits Unchangeable
X27	Stop bit 01: default 1 bit stop bit Unchangeable
X28	Parity 0x01: No parity 0x02: Even parity 0x03: Odd parity
X29 X30	Keep it, Default write 05 A6
X31	Antenna selection 00: Onboard antenna 01: External antenna

(INS05), Read module instruction (Hexadecimal format)

Suitable for V7.2 / V7.3 firmware

Send	Head	Length	Instruction	Checksum
	FC	06	0E 44 54 4B 52 46	8B(In front of all bytes and, Keep the lower 8 bits)

Back	Head	Length	Status	Back instruction	Checksum
	FA	31	0A：Success 0B：Failed 0C：Disable	0E + Read all the parameters of the module(48 Bytes)	In front of all bytes and, Keep the lower 8 bits

Example:
Send: FC 06 0E 44 54 4B 52 46 8B
Reply: FA 31 0A 0E 01 5A 76 14 01 00 01 AA BB 06 01 01 01 05 A6 01 00 12 4B 00 07 FC C9 E2 02 5A 76 14 01 0A 0B CC DD 04 01 01 01 05 A6 00 00 00 01 01 11 12 13 14 E3

If the command is wrong, will be sent out as a data (of course, no reply)

Note: After the success of the module, the module into the set state, will prohibit the wireless data reception 1 minute.

Read all parameters of the module (hexadecimal, 48 Bytes):

X0	Point Type: 01 Coordinator, 02 Router
X1 X2	PAN ID: 0001-FF00
X3	Channel: 0B – 1A
X4	Transmission mode, Default write 01 Unchangeable
X5 X6	Self-address: Range: 0001 - FF00
X7 X8	Keep it, Default write AA BB
X9	Baud rate: 0x01：1200 0x02：2400 0x03：4800 0x04：9600 0x05：19200 0x06：38400 0x07：57600 0x08：1115200
X10	Data bits 01: default 8-bit data bits Unchangeable
X11	Stop bit 01: default 1 bit stop bit Unchangeable
X12	Parity 0x01: No parity 0x02: Even parity 0x03: Odd parity
X13 X14	Keep it, Default write 05 A6
X15	Antenna selection 00: Onboard antenna 01: External antenna
X16 – X23	MAC Address, 8 Bytes
Note	If the module is Coordinator, starting from X24 to X39, is the default to the Router parameters If the module is Router, starting from X24 to X39, read out the parameters meaningless
X24	Point Type: 01 Coordinator, 02 Router
X25 X26	PAN ID: 0001-FF00
X27	Channel: 0B – 1A

X28	Transmission mode, Default write 01 Unchangeable
X29 X30	Self-address: Range: 0001 - FF00
X31 X32	Keep it, Default write CC DD
X33	Baud rate: 0x01：1200 0x02：2400 0x03：4800 0x04：9600 0x05：19200 0x06：38400 0x07：57600 0x08：1115200
X34	Data bits 01: default 8-bit data bits Unchangeable
X35	Stop bit 01: default 1 bit stop bit Unchangeable
X36	Parity 0x01: No parity 0x02: Even parity 0x03: Odd parity
X37 X38	Keep it, Default write 05 A6
X39	Antenna selection 00: Onboard antenna 01: External antenna
X40 X41	Short address Such as the point address of the FF FE, Indicates that Router is not added to the network
X42	Internal use, meaningless
X43	Whether to enable encryption: A1: Enable encryption Others: Encryption is not enabled
X44 – X47	Password: 4 bytes password (32 bits) default is 11 12 13 14

(INS06), Write module instruction (Hexadecimal format)

Suitable for V7.2 / V7.3 firmware

	Head	Length	Instruction	Checksum
Send	FC	27	07 + Write all parameters of the module(38 Bytes)	In front of all bytes and, Keep the lower 8 bits

	Head	Length	Status	Back instruction	Checksum
Back	FA	01	0A：Success 0B：Failed 0C：Disable	07	In front of all bytes and, Keep the lower 8 bits

Example:
Send: FC 27 07 02 01 01 14 01 00 01 AA BB 06 01 01 01 05 A6 00 02 01 01 14 01 66 77 CC DD 06 01 01 01 05 A6 00 01 01 11 12 13 14 FC
Reply: FA 01 0A 07 0C

If the command is wrong, will be sent out as a data (of course, no reply).

Write parameters (hexadecimal, 38 Bytes)

X0	Point Type: 01 Coordinator, 02 Router
X1 X2	PAN ID: 0001-FF00
X3	Channel: 0B – 1A
X4	Transmission mode, Default write 01 Unchangeable
X5 X6	Self-address: Range: 0001 - FF00
X7 X8	Keep it, Default write AA BB
X9	Baud rate: 0x01：1200 0x02：2400 0x03：4800 0x04：9600 0x05：19200 0x06：38400 0x07：57600 0x08：1115200
X10	Data bits 01: default 8-bit data bits Unchangeable
X11	Stop bit 01: default 1 bit stop bit Unchangeable
X12	Parity 0x01: No parity 0x02: Even parity 0x03: Odd parity
X13 X14	Keep it, Default write 05 A6
X15	Antenna selection 00: Onboard antenna 01: External antenna
Note	If the module is Coordinator, starting from X16 to X31, is the default to the Router parameters If the module is Router, starting from X16 to X31, read out the parameters meaningless
X16	Point Type: 01 Coordinator, 02 Router
X17 X18	PAN ID: 0001-FF00
X19	Channel: 0B – 1A

X20	Transmission mode, Default write 01 Unchangeable
X21 X22	Self-address: Range: 0001 - FF00
X23 X24	Keep it, Default write CC DD
X25	Baud rate: 0x01：1200 0x02：2400 0x03：4800 0x04：9600 0x05：19200 0x06：38400 0x07：57600 0x08：1115200
X26	Data bits 01: default 8-bit data bits Unchangeable
X27	Stop bit 01: default 1 bit stop bit Unchangeable
X28	Parity 0x01: No parity 0x02: Even parity 0x03: Odd parity
X29 X30	Keep it, Default write 05 A6
X31	Antenna selection 00: Onboard antenna 01: External antenna
X32	Internal use, meaningless
X33	Whether to enable encryption: A1: Enable encryption Others: Encryption is not enabled
X34 – X37	Password: 4 bytes password (32 bits) default is 11 12 13 14

(INS07), Query the End Device location (Hexadecimal format)

Suitable for V7.2 / V7.3 firmware

Send	Head	Length	Instruction	Checksum
	FC	06	0B 44 54 4B 52 46	88 (In front of all bytes and, Keep the lower 8 bits)

Back	Head	Card Number (3B + Short Address)	Relative distance 1	Router1Short Address	Checksum
	FA	3B C9 22	49	CB F8	2C In front of all bytes and, Keep the lower 8 bits

	Head	Relative distance 2	Router2 Short Address	Relative distance 3	Router3 short address	Checksum
	FB	3E	CA 49	27	B9 34	B8 In front of all bytes and, Keep the lower 8 bits

Example:
Send: FC 06 0B 44 54 4B 52 46 88
Back: FA 3B C9 22 49 CB F8 2C FB 3E CA 49 27 B9 34 B8

If the command is wrong, will be sent out as a data (of course, no reply).

Explain:
FA 3B C9 22 49 CB F8 2C FB 3E CA 49 27 B9 34 B8

Card number: 3B C9 22 (C9 22 is the short address of End Device)
From the Router node CB F8, the relative distance is 49
From the node CA 49 second near the relative distance of 3E
From the Router node B9 34 third near the relative distance of 27

If the Router node is placed in a fixed, known location, the approximate location of the End Device can be estimated.

The relative distance is not the actual distance, there is no unit, and the actual distance does not correspond to the function. But the relative distance of the size of the value of the comparison is meaningful, according to the size of the relative distance to determine End Device in which Router near, is a simple and effective positioning method.

(INS08), Query the point (Router, End Device) RSSI (Hexadecimal format)

Suitable for V7.2 / V7.3 firmware

Send	Head	Length	Instruction	Checksum
	FC	06	0C 44 54 4B 52 46	89 (In front of all bytes and, Keep the lower 8 bits)

Back	Head	Length	Status	Back instruction	Checksum
	FA	04	0A：Success 0B：Failed 0C：Disable	How many Routers (1Byte) The last short address of the route (2 Bytes) Signal strength of the last route (1 Byte) (This is the relative signal strength, range: 0-100)	In front of all bytes and, Keep the lower 8 bits

Example:
Send: FC 06 0C 44 54 4B 52 46 89
Reply: FA 04 0A 02 C9 22 31 26

Send the query and receive a reply, said:
1, the node can communicate with the Coordinator,
2, the last time the strength of the signal communication is how much.

If the command is wrong, will be sent out as a data (of course, no reply)

ZigBee Module FAQ

How do I debug a ZigBee network?

A ZigBee network in the layout of the process, users often do not know whether a node signal is good, the following gives a few common methods of debugging:

1, continuous press 3 times on the Coordinator on the function keys, then Coordinator will continue to send test data, observe the Router or End Device on the Data light, if it is continuous, fast flashing, indicating that the node received data is good, if the light does not shine, Indicating that the node did not receive data, you can add a node in the node as an automatic relay test;

2, the Coordinator connected to the computer, by configuring the software "read the network structure" to see which nodes are not connected, and in the node before the addition of a Router node as an automatic relay test;

3. For a single Router or End Device, it can be determined by querying the signal strength command (if the instruction returns, then the node can communicate with the Coordinator and give the signal strength of the last route). This function is suitable for the node there are MCU + display, can be given on the display signal strength.

How do I use End Device?

End Device node function:

1, End Device can send and receive data like Router, but there is no routing data function:

If a relatively small space (about all nodes can communicate directly with the Coordinator), place A larger number of ZigBee nodes (such as more than 30) can be part of the node set to End Device, by In the End Device no routing function, to a certain extent, reduce the complexity of the entire network routing and routings expenses. (Usually set 10 Router almost).

2, through the command from the End Device from the nearest three routers between the signal strength, which roughly determine the End Device location: (i.e.: End Device as a location card)

This function is compatible with CC2530 positioning system V6.0 function, End Device node as a mobile node, if all the Router location is fixed, through the instructions, you can find out where the End Device.

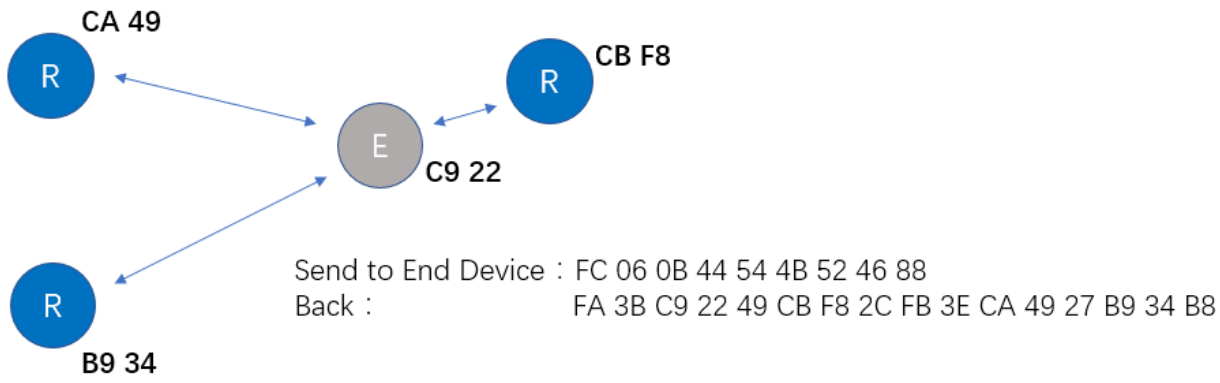
Thus, roughly determining the location of the End Device, which is not an accurate location, but for some relatively simple applications (such as mine lanes, hospitals, nursing homes, etc.), we need to know which room, and do not need to know which corner of the room, is still a simple, Low-cost positioning program.

How do I use End Device's location feature?

(This function requires End Device behind the MCU can be achieved)

The positioning function of the End Device is divided into two parts:
(1), End Device finds its own location (similar to autonomous navigation);
(2), the background monitoring End Device location (general mines, tunnels, etc. using the positioning system).

(1), End Device finds its own location (similar to autonomous navigation):



We can see that End Device is between three routers, closest to CBF8, with a relative distance (RSSI) of 49

(2), the background monitoring End Device location (general mines, tunnels and other use of the positioning system):

The whole system is a wireless solution, the routing level of Router is not more than 15, and the number of End Device is not more than 200 (assuming that a single End Device generates positioning data every 10 seconds)