



# **E18 Series Product Specification**

**CC2530 2.4GHz ZigBee3.0 Wireless Module**



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

# Contents

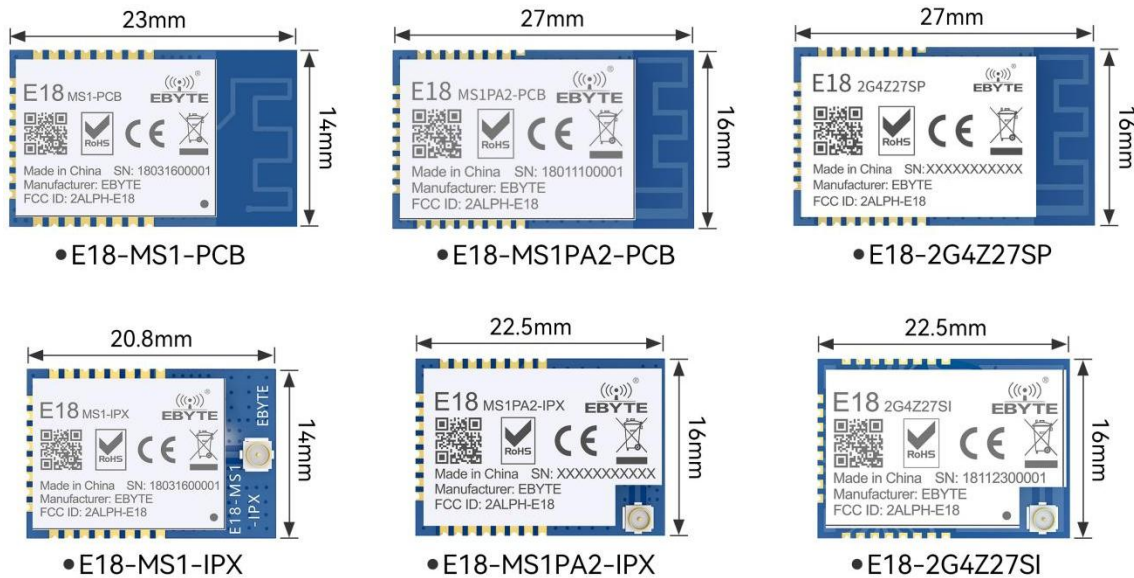
1. Introduction .....	2
1.1 Brief Introduction .....	2
1.2 ZigBee 3.0 Advantages .....	2
1.3 Features .....	3
1.4 Applications .....	4
2. Specification and parameter .....	5
2.1 Main parameter .....	5
2.2 Electrical parameters .....	5
2.3 Hardware parameters .....	6
2.4 Network System Parameters .....	6
3 Size and pin definition .....	8
4 Hardware Design .....	12
5. Software Design .....	13
6 FAQ .....	15
6.1 Communication range is too short .....	15
6.2 Module is easy to damage .....	15
6.3 BER(Bit Error Rate) is high .....	15
7 Production guidance .....	16
7.1 Reflow soldering temperature .....	16
7.2 Reflow soldering curve .....	16
8 E18 series .....	17
9 Antenna recommendation .....	17
10 Packaging .....	18
Revise History .....	19
About us .....	19

# 1. Introduction

## 1.1 Brief Introduction

E18 series is a 2.4GHz frequency band ZigBee communication protocol-to-serial wireless module designed and produced by Ebyte. The factory comes with self-organizing network firmware, ready to use, suitable for a variety of application scenarios (especially smart home).

The E18 series module adopts CC2530 RF chip imported from Texas Instruments. The chip integrates 8051 single-chip microcomputer and wireless transceiver. Some module models have built-in PA power amplifier to increase the communication distance. The factory-built firmware implements serial data transparent transmission based on the ZigBee3.0 protocol, and supports various commands under the ZigBee3.0 protocol. After actual measurement, it has very good compatibility with most ZigBee3.0 products on the market.



## 1.2 ZigBee 3.0 Advantages

E18 series module firmware is based on Z-Stack3.0.2 protocol stack (ZigBee 3.0), which is the best protocol stack for CC2530/CC2538 series chips, so our company has also made many optimizations on this basis to ensure long-term stable operation of the system.

The difference between ZigBee 3.0 and the previous version:

1. The networking method has changed: ZigBee 3.0 has banned the networking method as soon as the power is turned on, and networking is performed according to actual needs. Any device has no network in the factory state, the coordinator needs to run "formation" (call `bdb_StartCommissioning` (BDB\_COMMISSIONING\_MODE\_NWK\_FORMATION) ) to create a new network, and then run "Steering"

(call `bdb_StartCommissioning (BDB_COMMISSIONING_MODE_NWK_STEERING )` ) to open the network, the default time of opening the network is 180 seconds, the open network can be closed in advance by broadcasting "ZDP\_MgmtPermitJoinReq". During these 180 seconds, routers or end nodes also use "Steering" to trigger onboarding. "Steering" can be triggered by a button or a serial port. The coordinator and the devices that are not connected to the network are triggered in the same time period, and the networking can be realized as required.

2. Enhanced key security mechanism: After ZigBee 3.0 devices join the coordinator, the coordinator will remember the MAC address of each device and assign them a separate key, namely APS Key. This APS Key has the following purposes: ① When the coordinator's unified key (ie NWK Key) is leaked, the key can be replaced, and the replaced key is no longer encrypted by the well-known key "ZigBeeAlliance09", but It is issued to each network access device using the APS Key. ② When the coordinator performs OTA upgrade to the networked device, it can use the APS Key to encrypt the upgrade file to prevent the upgrade file from being tampered with.

3. Network management mechanism: ZigBee 3.0 improves the device management mechanism. First of all, the coordinator can know that the devices in the whole network join and leave, so that the management and control of the network devices can be completed only by operating on the coordinator.

4. Perfect ZCL protocol specification: By perfecting the ZCL protocol, the functions of ZigBee devices are more modular. The ZCL specification formats the functions supported by ZigBee devices, and even private functions customized by the device can be transmitted in the ZCL data format. Under the action of the ZCL data format, the functions supported by the ZigBee device can be flexibly increased or reduced, which avoids unnecessary troubles caused by the modification of the data format caused by the modification of the hardware function of the ZigBee device.

## 1.3 Features

- Role switching: The user can switch the device among the three types of coordinator, router and terminal through serial commands.
- Automatic networking: The coordinator automatically forms a network when it is powered on, and terminals and routers automatically search for and join the network.
- Network self-healing: if the intermediate node of the network is lost, other networks automatically join or maintain the original network (the isolated node automatically joins the original network, and the non-isolated node maintains the original network); if the coordinator is lost, there are non-isolated nodes in the original network, and the coordinator can restore the original network. The coordinator that joins the network or the original network PAN\_ID set by the same user joins the original network.
- Ultra-low power consumption: When the device is in the terminal state, it can be set to a low-power mode, and the sleep time of the device can be changed according to the user's usage time. In the low-power mode, the standby power consumption is less than 2.5uA; You can receive the messages you should receive within the time set by the user.
- Data retention time setting: When the device is in the coordinator and router state, the user can set the data retention time by himself, and cooperate with the terminal in sleep mode to save the data of the terminal device, and send the data to the terminal after the terminal wakes up from sleep. Terminal; save up to 4 pieces of data, if it exceeds, the first data will be automatically cleared; after the data saving time has passed, the data heap will be automatically cleared.
- Automatic retransmission: In the on-demand (unicast) mode, the device will automatically retransmit when it fails to send to the next node, and the number of retransmissions for each message is 2 times.
- Automatic routing: The module supports network routing function; routers and coordinators carry network data routing functions, and users can perform multi-hop networking.
- Encryption protocol: The module adopts AES 128-bit encryption function, which can change the network encryption and anti-monitoring; users can change the network key by themselves, and devices with the same network key can communicate normally in the network.
- Serial port configuration: The module has built-in serial port commands. Users can configure (view) the parameters and functions of the module through the serial port commands.

- Multi-type data communication: support the whole network broadcast, multicast and on-demand (unicast) functions; also support several transmission modes in broadcast and on-demand (unicast) mode.
- Channel change: Support 16 channel changes (2405-2480MHZ) from 11 to 26, and different channels correspond to different frequency bands.
- Network PAN\_ID change: Any switch of network PAN\_ID, users can customize PAN\_ID to join the corresponding network or automatically select PAN\_ID to join the network.
- Serial port baud rate change: Users can set the baud rate by themselves, up to 115200, the default number of bits is 8, the stop bit is 1 bit, and there is no parity bit.
- Short address search: Users can find the corresponding short address according to the MAC address (unique, fixed) of the module that has been added to the network.
- Command format switching: This module supports two modes of HEX command and transparent transmission, which can be easily configured and switched by users.
- Module reset: The user can reset the module through serial port commands.
- One-key restore baud rate: If the user forgets or does not know the baud rate, this function can be used to restore the default baud rate to 115200.
- Restore factory settings: Users can restore the module to factory settings through serial port commands.
- It has a national invention patent certificate, and its invention name is: a method of interconnection and interworking of wireless transparent modules based on ZigBee3.0 Patent No.: ZL 2019 1 1122430. X



## 1.4 Applications

- Smart home and industrial sensors, etc.;
- Security system, positioning system;
- Wireless remote control, drone;
- Wireless game remote control;
- Healthcare products;
- Wireless voice, wireless headset;
- Automotive industry applications.

## 2. Specification and parameter

### 2.1 Main parameter

Main Parameters	Unit	Model			Remark
		E18-MS1-PCB E18-MS1-IPX	E18-MS1PA2-PCB E18-MS1PA2-IPX	E18-2G4Z27SP E18-2G4Z27SI	
Working frequency	GHz	2.400 ~ 2.480			Support ISM band
Transmit power	dBm	4.0±0.5	20.0±0.5	27.0±0.5	
Blocking power	dBm	0 ~ 10.0			The probability of burning at close range is small
Receive sensitivity	dBm	-96.5±1.0	-98.0±1.0	-99.0±1.0	The air rate is 250kbps
Matched impedance	Ω	50			Equivalent impedance of PCB on-board antenna IPEX-1 interface antenna matching impedance
Minimum packet length	byte	4			
Measured distance	m	200	600	800	Clear and open, 2.5 meters high, air speed 250kBs. Note 1

Note 1: The gain of the on-board PCB antenna is -0.5dBi; the IPEX-1 interface is connected to an antenna with a gain of 3dBi, and the communication distance is increased by about 20%~30%.

### 2.2 Electrical parameters

Electrical parameters	Unit	Model			Remark
		E18-MS1-PCB E18-MS1-IPX	E18-MS1PA2-PCB E18-MS1PA2-IPX	E18-2G4Z27SP E18-2G4Z27SI	
Operating Voltage	V	2.0 ~ 3.6		2.5 ~ 3.6	≥3.3V can guarantee output power
Communication level	V	3.3			Risk of burnout with 5V TTL
Emission current	mA	28	168	500	Instantaneous power consumption
Receive current	mA	27	36	36	

Sleep current	uA	1.2	1.2	2.5	Software shutdown
Operating temperature	°C	-40 ~ +85			Industrial grade
Storage temperature	°C	-40 ~ +125			Industrial grade

## 2.3 Hardware parameters

Main parameters	E18-MS1-PCB	E18-MS1-IPX	E18-MS1PA2-PCB E18-2G4Z27SP	E18-MS1PA2-IPX E18-2G4Z27SI	Remark
Dimensions	14.1*23.0mm	14.1*20.8mm	16.0*27.0mm	16.0*22.5mm	
IC Full name	CC2530F256RHAT/QFN40				Factory built-in firmware, support secondary development
FLASH	256KB				
RAM	8KB				
Supporting protocol	ZigBee3.0				
Communication Interface	UART				TTL level
I/O interface	All I/O ports are led out				It is convenient for users to develop secondary.
Packaging method	SMD,stamp hole, pitch 1.27mm				The PCB package pins are the same, and each model can be replaced with each other.
PA+LNA	x	x	√	√	Module built-in PA+LNA
Antenna interface	PCB Antenna	IPEX-1	PCB天线	IPEX-1	

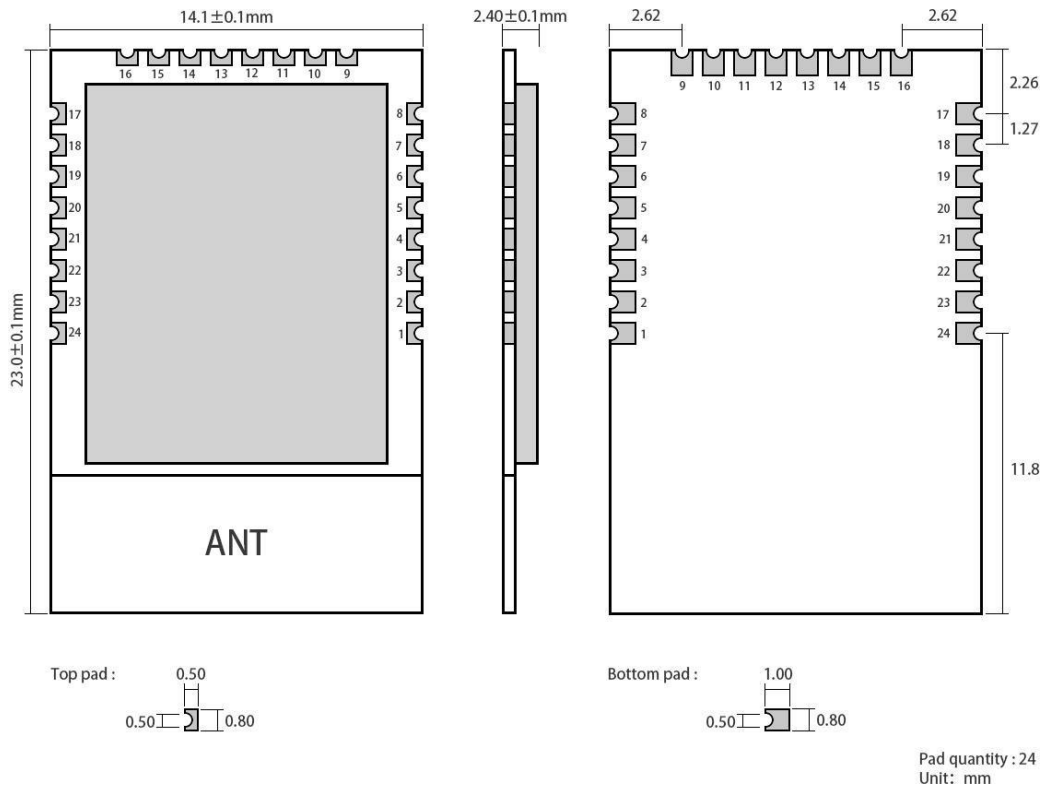
## 2.4 Network System Parameters

System parameters	Parameter value	Explanation
Total number of network devices	≤32	suggested value;
Network routing hierarchy	5 layers	System fixed value;
Number of concurrent data nodes in the network	≤7	suggested value; 7 nodes send data at the same time, each node sends 30 bytes without packet loss;
The maximum number of child devices connected to the parent device	10	System fixed value;
The length of time that the parent device saves the data of the dormant terminal child device.	7s	System fixed value;

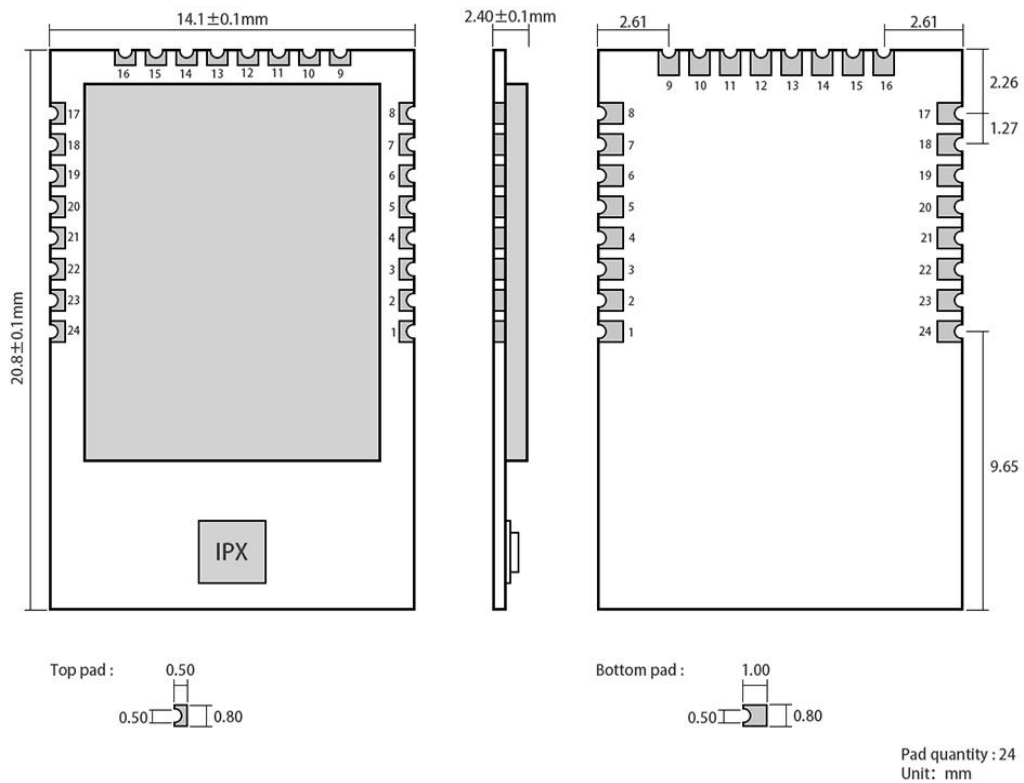
The parent device saves the maximum number of data of the dormant terminal and child devices	15	System fixed value;first in first out principle;
The parent device saves the maximum number of data of the same dormant terminal and child device	4	System fixed value; First in first out principle;
Dormant terminal Polling (periodic wake-up) duration	$\leq 7s$	System fixed value; fetch temporary data from the parent device after periodic automatic wake-up, and the period is generally less than "the parent device saves the data of the dormant terminal sub-device";
Broadcast interval in the network	$\geq 200ms$	Recommended value to effectively avoid network storms;
Number of retransmissions after fixed-point transmission (on-demand) data transmission fails	2 times	does not include the first transmission; If no feedback is received in the 6th second after the first transmission, re-send, if the feedback is not received in the 12th second, re-send, until the 18th second, no feedback is received, and the transmission is determined. fail;
Feedback data duration	$\leq 5s$	Generally, the feedback data can be received within 5 seconds, and if no feedback is received within 5 seconds, it can be determined that the transmission fails;



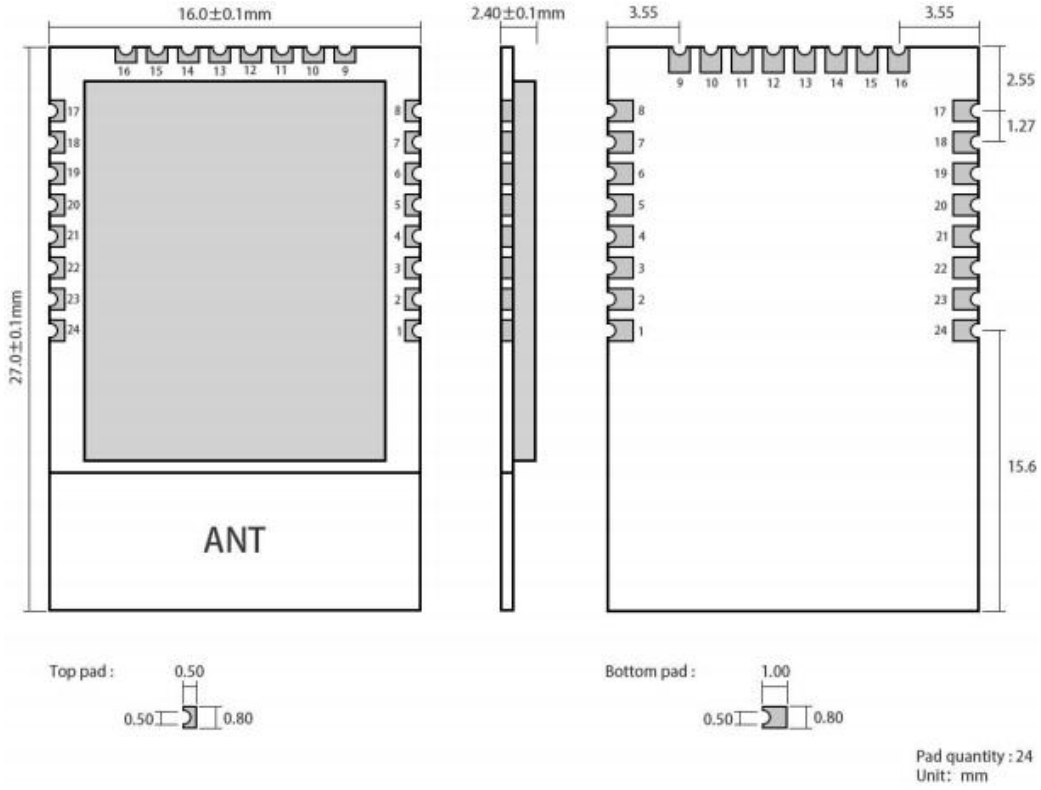
### 3 Size and pin definition



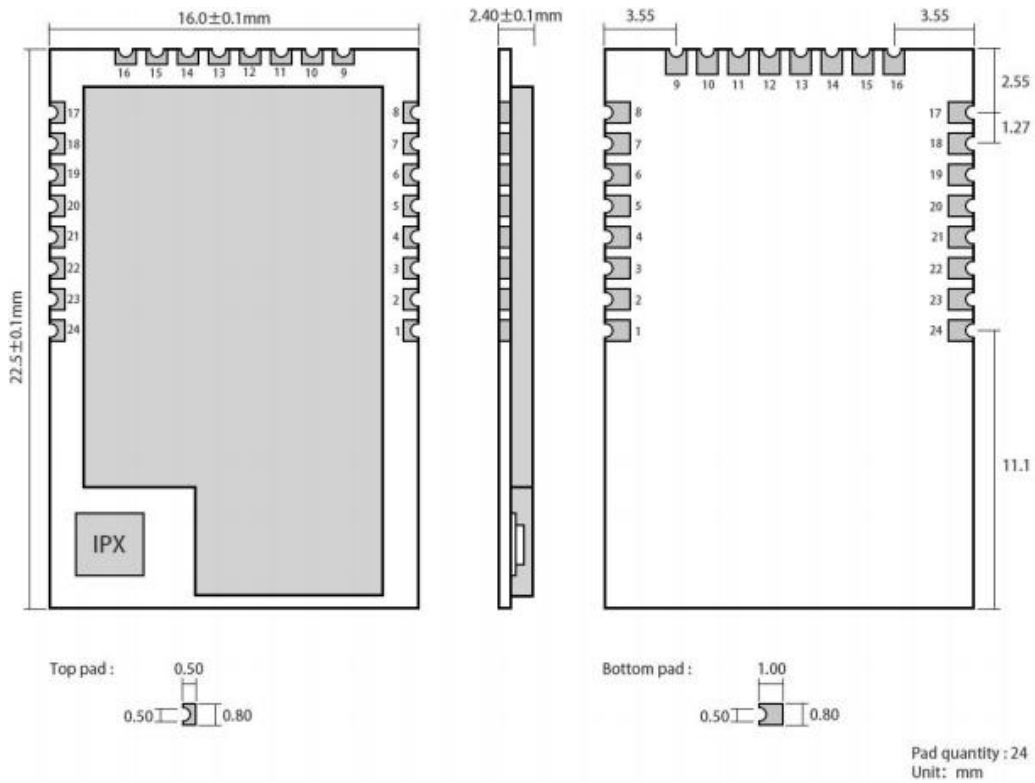
### E18-MS1-PCB Dimension



### E18-MS1-IPX Dimension



### E18-MS1PA2-PCB/E18-2G4Z27SP Dimension



**E18-MS1PA2-IPX/E18-2G4Z27SI Dimension**

Pin number	CC2530 Pin name	Module Pin name	Input/Output	Pin usage
1	GND	GND		Ground wire, connected to the power reference ground
2	VCC	VCC		Power supply, must be between 1.8 ~ 3.6V
3	P2.2	GPIO	I/O	DC-download program or Debug clock interface
4	P2.1	GPIO	I/O	DD-download program or Debug data interface
5	P2.0	GPIO	I/O	N/C
6	P1.7	NWK_KEY	I	Used for manual join, exit, and quick match keys. Not networked: Short press to join the network or create a network operation; Networked: Short press for quick match; Long press means to leave the current network; Note: Low level is valid, 100ms ≤ short press ≤ 3000ms, 5000 ≤ long press.
7	P1.6	GPIO	I/O	N/C
8	NC	NC		N/C
9	NC	NC		N/C
10	P1.5	UART0_TX	O	Serial port TX pin
11	P1.4	UART0_RX	I	Serial port RX pin
12	P1.3	RUN_LED	O	It is used to indicate the network access status of the module. Fast flashing 256 times (10Hz frequency) indicates that it is joining the network or creating a network, and slow flashing 12 times (2Hz frequency) indicates that the module has joined the network or successfully created the network; Low level lights up;
13	P1.2	NWK_LED	O	It is used to indicate the one key pairing status of the module,

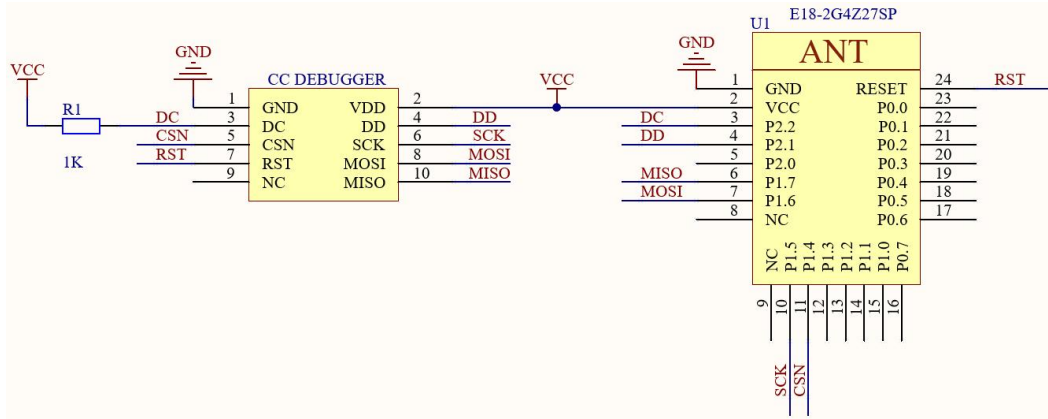
				provided that two modules need to join the same coordinator, and then one key pairing can be performed. In the transparent mode, mutual transparent transmission can be performed. Low level lighting;
14	P1.1	GPIO	I/O	The PA transmit control pin has been connected inside the module; There is no PA inside the E18-MS1-PCB/E18-MS1-IPX;
15	P1.0	GPIO	I/O	The PA receiving control pin has been connected inside the module; There is no PA inside the E18-MS1-PCB/E18-MS1-IPX;
16	P0.7	HGM	O	HGM pin of PA; E18-MS1-PCB/E18-MS1-IPX has no PA inside, so this pin is used as GPIO port;
17	P0.6	GPIO	I/O	N/C
18	P0.5	GPIO	I/O	N/C
19	P0.4	GPIO	I/O	N/C
20	P0.3	GPIO	I/O	N/C
21	P0.2	GPIO	I/O	N/C
22	P0.1	GPIO	I/O	N/C
23	P0.0	GPIO	I/O	N/C
24	RESET	RESET	I	Reset port

## 4 Hardware Design

- It is recommended to use a DC regulated power supply to supply power to the module, the power supply ripple coefficient should be as small as possible, and the module should be grounded reliably;
- Please pay attention to the correct connection of the positive and negative poles of the power supply, such as reverse connection may cause permanent damage to the module;
- Please check the power supply to ensure that it is between the recommended power supply voltages. If it exceeds the maximum value, the module will be permanently damaged;
- Please check the stability of the power supply, the voltage should not fluctuate greatly and frequently;
- When designing the power supply circuit for the module, it is often recommended to reserve more than 30% of the margin, so that the whole machine can work stably for a long time;
- The module should be kept as far away as possible from the power supply, transformer, high-frequency wiring and other parts with large electromagnetic interference;
- High-frequency digital traces, high-frequency analog traces, and power traces must avoid the underside of the module. If it is necessary to pass under the module, assuming that the module is soldered on the Top Layer, ground copper (all copper) is placed on the Top Layer of the contact part of the module. And well grounded), it must be close to the digital part of the module and routed on the Bottom Layer;
- Assuming that the module is soldered or placed on the Top Layer, it is also wrong to arbitrarily route wires on the Bottom Layer or other layers, which will affect the stray and receiving sensitivity of the module to varying degrees;
- Assuming that there are devices with large electromagnetic interference around the module, it will greatly affect the performance of the module. It is recommended to stay away from the module according to the intensity of the interference. If the situation allows, appropriate isolation and shielding can be done;
- Assuming that there are traces with large electromagnetic interference around the module (high-frequency digital, high-frequency analog, power traces), the performance of the module will also be greatly affected. It is recommended to stay away from the module according to the intensity of the interference. Proper isolation and shielding;
- If the communication line uses a 5V level, a 1k-5.1k resistor must be connected in series (not recommended, there is still a risk of damage);
- Try to stay away from some TTL protocols whose physical layer is also 2.4GHz, for example: USB3.0;
- The antenna installation structure has a great influence on the performance of the module. Make sure that the antenna is exposed and preferably vertically upward; when the module is installed inside the case, a high-quality antenna extension cable can be used to extend the antenna to the outside of the case;
- The antenna must not be installed inside the metal shell, which will greatly reduce the transmission distance.

## 5. Software Design

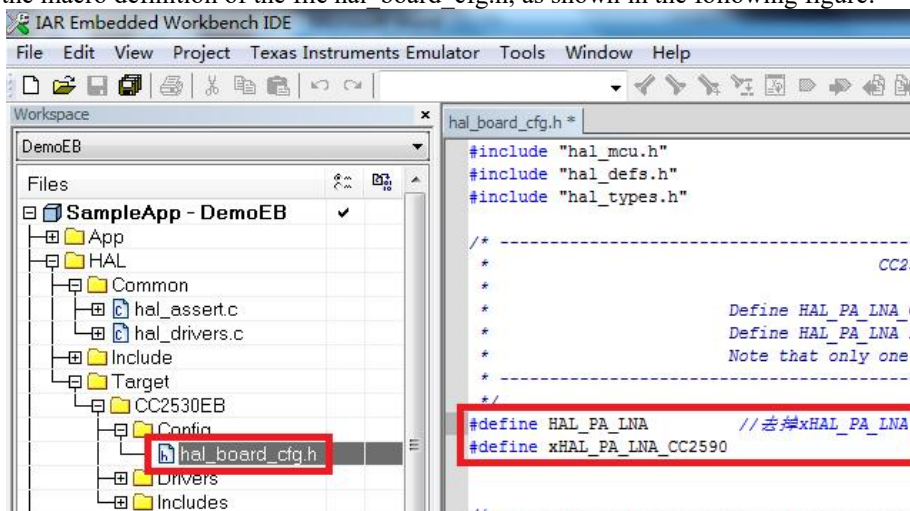
- The official CC DEBUGGER tool is required for programming or Debugging ([click to view the purchase link](#)). The wiring diagram is as follows:



- The PA power amplifier control information inside the module, applicable to E18-MS1PA2-PCB/E18-MS1PA2-IPX/E18-2G4Z27SP/E18-2G4Z27SI.
- The pins P1.0 and P1.1 of CC2530 are connected to LNA\_EN and PA\_EN of PA respectively, and the high level is effective.
- LNA\_EN is always high, the module is always receiving; PA\_EN is always high, the module is always transmitting.

Working mode	LNA_EN	PA_EN
Receive mode	1	0
Transmission mode	0	1
Sleep mode	0	0

- The software starts the PA power amplifier, and in the SDK protocol stack development package (Z-Stack 3.0.2), modify the macro definition of the file hal\_board\_cfg.h, as shown in the following figure:



- Modify the function to realize the automatic control of the PA power amplifier by the system. Find the macRadioTurnOnPower() function in the file mac\_radio\_defs.c and make changes. As shown below:

```
* Note that The register values are not retained during sleep.
*/
/* P1_1 -> PAEN */
RFC_OBS_CTRL0 = RFC_OBS_CTRL_PA_PD_INV;
OBSSEL1      = OBSSEL_OBS_CTRL0;

/* P1_0 -> EN (LNA control) */
RFC_OBS_CTRL1 = RFC_OBS_CTRL_LNAMIX_PD_INV;
OBSSEL0      = OBSSEL_OBS_CTRL1;
```

- Modify the power Different PA power amplifiers correspond to different transmit powers (unit: dBm).

E18-MS1PA2-PCB/E18-MS1PA2-IPX corresponds to 20dBm;

E18-2G4Z27SP/E18-2G4Z27SI corresponds to 27dBm;

Find the array static CODE const macPib\_t macPibDefaults in the file mac\_pib.c, and make changes as shown in the red box.

```
TRUE,
FALSE,

/* Proprietary */
#if defined (HAL_PA_LNA)
20,
#elif defined (HAL_PA_LNA_CC2590)
11,
#else
3,
```

## 6 FAQ

### 6.1 Communication range is too short

- The communication distance will be affected when obstacle exists;
- Data lose rate will be affected by temperature, humidity and co-channel interference;
- The ground will absorb and reflect wireless radio wave, so the performance will be poor when testing near ground;
- Sea water has great ability in absorbing wireless radio wave, so performance will be poor when testing near the sea;
- The signal will be affected when the antenna is near metal object or put in a metal case;
- Power register was set incorrectly, air data rate is set as too high (the higher the air data rate, the shorter the distance);
- The power supply low voltage under room temperature is lower than 2.5V, the lower the voltage, the lower the transmitting power;
- Due to antenna quality or poor matching between antenna and module.

### 6.2 Module is easy to damage

- Please check the power supply source, ensure it is 2.0V~3.6V, voltage higher than 3.6V will damage the module;
- Please check the stability of power source, the voltage cannot fluctuate too much;
- Please make sure antistatic measure are taken when installing and using, high frequency devices have electrostatic susceptibility;
- Please ensure the humidity is within limited range, some parts are sensitive to humidity;
- Please avoid using modules under too high or too low temperature.

### 6.3 BER(Bit Error Rate) is high

- There are co-channel signal interference nearby, please be away from interference sources or modify frequency and channel to avoid interference;
- Poor power supply may cause messy code. Make sure that the power supply is reliable;
- The extension line and feeder quality are poor or too long, so the bit error rate is high.

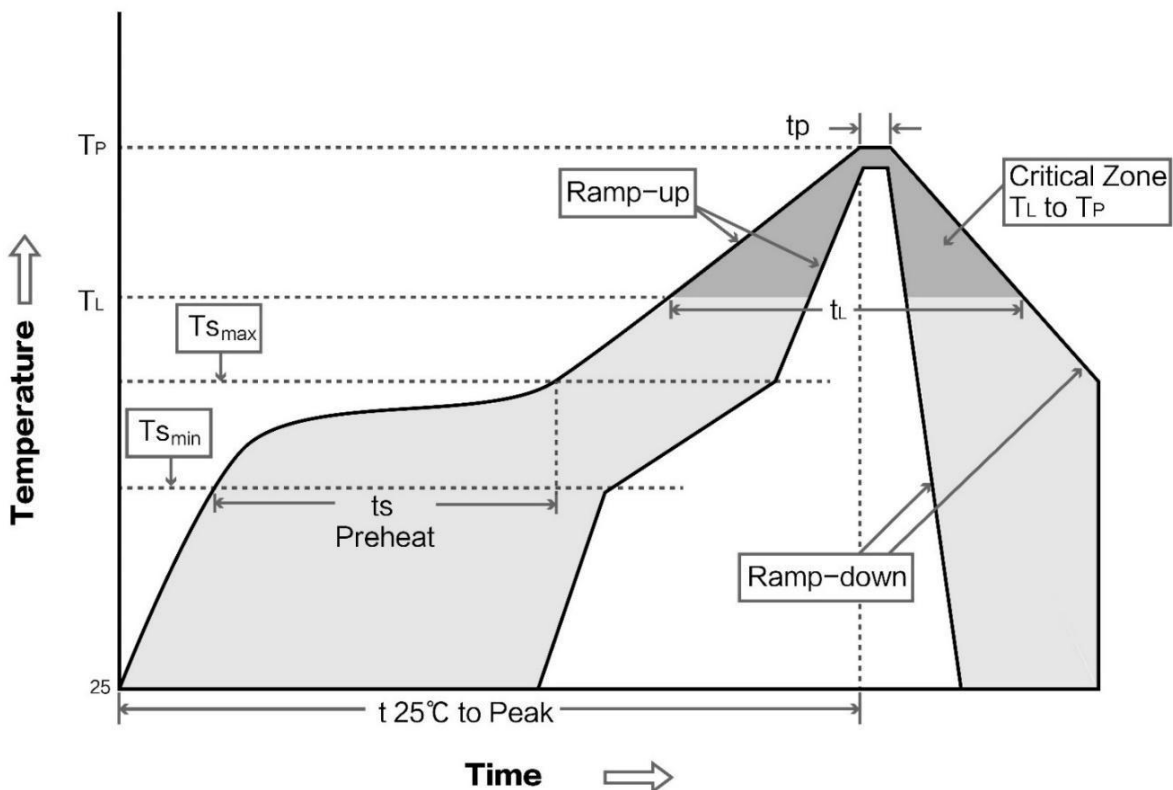


## 7 Production guidance

### 7.1 Reflow soldering temperature

Profile Feature	Curve feature	Sn-Pb Assembly	Pb-Free Assembly
Solder Paste	Solder paste	Sn63/Pb37	Sn96.5/Ag3/Cu0.5
Preheat Temperature min (T <sub>smin</sub> )	Minimum preheat temperature	100°C	150°C
Preheat temperature max (T <sub>smax</sub> )	Maximum preheat temperature	150°C	200°C
Preheat Time (T <sub>smin</sub> to T <sub>smax</sub> )(t <sub>s</sub> )	Preheat time	60-120 sec	60-120 sec
Average ramp-up rate(T <sub>smax</sub> to T <sub>p</sub> )	Average rate of ascent	3°C/second max	3°C/second max
Liquidous Temperature (T <sub>L</sub> )	Liquidus temperature	183°C	217°C
Time (t <sub>L</sub> ) Maintained Above (T <sub>L</sub> )	Time above liquidus	60-90 sec	30-90 sec
Peak temperature (T <sub>p</sub> )	Peak temperature	220-235°C	230-250°C
Average ramp-down rate (T <sub>p</sub> to T <sub>smax</sub> )	Average rate of descent	6°C/second max	6°C/second max
Time 25°C to peak temperature	Time from 25°C to peak temperature	6 minutes max	8 minutes max

### 7.2 Reflow soldering curve



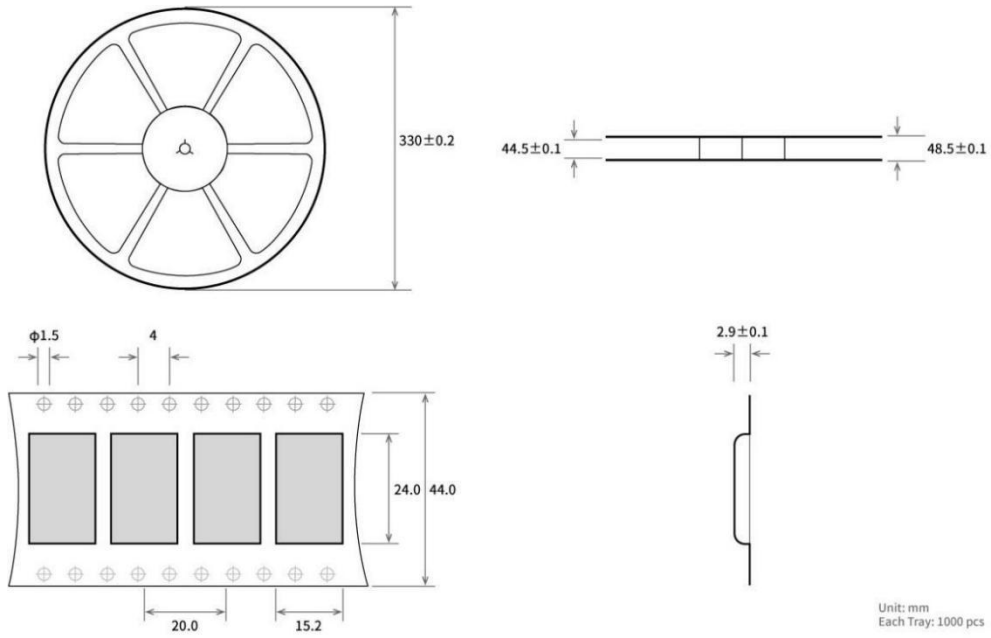
## 8 E18 series

Product module	Chip	Frequency	Power	Distance	Dimension	Package form	Antenna
		Hz	dBm	m	mm		
<a href="#">E18-MS1-PCB</a>	CC2530	2.4G	4	200	14.1*23	SMD	PCB
<a href="#">E18-MS1-IPX</a>	CC2530	2.4G	4	240	14.1*20.8	SMD	IPEX
<a href="#">E18-MS1PA2-PCB</a>	CC2530	2.4G	20	800	16*27	SMD	PCB
<a href="#">E18-MS1PA2-IPX</a>	CC2530	2.4G	20	1000	16*22.5	SMD	IPEX
<a href="#">E18-2G4Z27SP</a>	CC2530	2.4G	27	2500	16*27	SMD	PCB
<a href="#">E18-2G4Z27SI</a>	CC2530	2.4G	27	2500	16*22.5	SMD	IPEX
<a href="#">E18-2G4U04B</a>	CC2531	2.4G	4	200	18*59	USB	PCB

## 9 Antenna recommendation

Product module	Type	Frequency	Gain	Dimension	Feeder	Interface	Feature
		Hz	dBi	mm	cm		
<a href="#">TX2400-NP-5010</a>	Flexible antenna	2.4G	2.0	10x50	-	IPEX	Flexible FPC Soft Antenna
<a href="#">TX2400-JZ-3</a>	Glue stick antenna	2.4G	2.0	30	-	SMA-J	Ultra-short straight, omnidirectional antenna
<a href="#">TX2400-JZ-5</a>	Glue stick antenna	2.4G	2.0	50	-	SMA-J	Ultra-short straight, omnidirectional antenna
<a href="#">TX2400-JW-5</a>	Glue stick antenna	2.4G	2.0	50	-	SMA-J	Fixed bent, omnidirectional antenna
<a href="#">TX2400-JK-11</a>	Glue stick antenna	2.4G	2.5	110	-	SMA-J	Bendable glue stick, omnidirectional antenna
<a href="#">TX2400-JK-20</a>	Glue stick antenna	2.4G	3.0	200	-	SMA-J	Bendable glue stick, omnidirectional antenna
<a href="#">TX2400-XPL-150</a>	Sucker antenna	2.4G	3.5	150	150	SMA-J	Small suction cup antenna, cost-effective

# 10 Packaging



## Revise History

Version	Date	Description	Issued by
1.0	2022-7-8	Initial version	Ning
1.1	2022-8-5	Bug fixes	Yan
1.2	2022-9-26	Add Patent Certificate	Bin
1.3	2022-10-8	Error correction	Bin
1.4	2022-10-19	Error correction	Bin
1.5	2023-04-17	Error correction	Bin
1.6	2023-07-26	Format adjustment	Bin
1.7	2023-09-05	Error correction	Bin
1.8	2023-12-28	Error correction	Bin

## About us

Technical support: [support@cdebyte.com](mailto: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](mailto:info@cdebyte.com)

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

 **Chengdu Ebyte Electronic Technology Co.,Ltd.**