M0M100P0 贴片式 WIFI 探针用户手册

版本 V1.0.1

浙江劢领智能科技有限公司

2018-5-28

版本信息

日期	版本	撰写人	修改说明
2018.05.04	V1.0.0	HuiHongmei	初稿，完成指令集、文档排版
2018.05.28	V1.0.1	HuiHongmei	增加新 AT 指令功能

目 录

1. 产品简介

1.1 概述

M0M100P0 是一款 WLAN 802.11 n IOT 模块，它内置 32 位微处理器，该模块完全兼容 IEEE 802.11 b/g/n 1T1R 2.4 GHz 标准，并且支持 802.11 e 服务质量(QoS)规范和 802.11 i 安全性规范，该模块支持无线网络连接速率高达 150 Mbps。

M0M100P0 天线封装方式可支持板载 PCB 天线；M0M100P0 可广泛应用于智能电网、智能交通、智能家具、手持设备、婴儿监控器、网络消费电子设备、工业控制等领域。

1.1.1 产品特性

（1）工作频率：2.4 GHz；

（2）工作速率：高达 150 Mbps；

（3）调制方式：BPSK，QPSK，16 QAM，64 QAM；

（4）硬件加密方式：WEP，TKIP，WPA，WPA2；

（5）模块上电后串口无乱码输出，可预防单机缓存溢出现象；

（6）支持丰富的 Socket AT 指令；

1.1.2 模块的封装

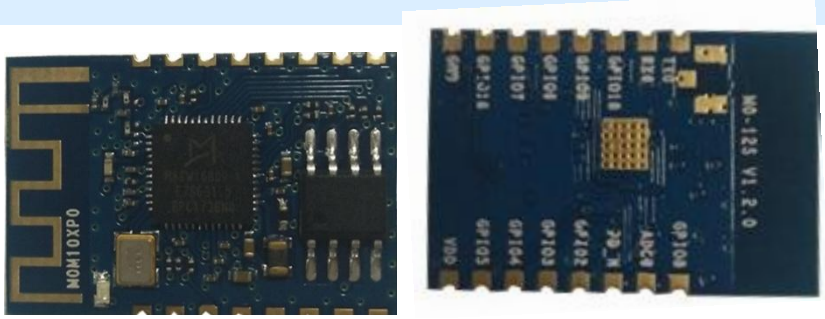

图 1-1：模块实物展示

1.1.3 模块的基本参数

模块	型号	M0M100P0
无线参数	无线标准	无线标准 IEEE 802.11b/g/n

	频率范围	频率范围 2.412GHz-2.484GHz
	数据传输速率（Mbps）	802.11b: 1, 2, 5.5, 11 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 802.11n HT20: MCS0~7 802.11n HT40: MCS0~7
	调制方式	BPSK/ QPSK/ 16-QAM/ 64-QAM
	展频技术	IEEE 802.11b: DSSS (Direct Sequence Spread Spectrum) IEEE 802.11g/n:OFDM (Orthogonal Frequency Division Multiplexing)
	工作模式	Soft-AP, Station & AP/Station modes
	工作通道	1-13
	安全机制	64/128 WEP, WPA, WPA2, WAPI
硬件参数	硬件接口	UART
	工作电压	3.0V--3.6V
	最大工作电流	408mA
	GPIO 驱动能力	Max：14ma
	输出阻抗	50Ω±10%
	工作温度	-20~70℃
	存储温度	-40~125℃
	尺寸	16mm*24mm*3mm

1.2 硬件介绍

M0M100P0 硬件接口丰富，可支持 UART，PWM，GPIO 等，适用于各种物联网应用场合。如图 1-2 所示模块管脚排列图。

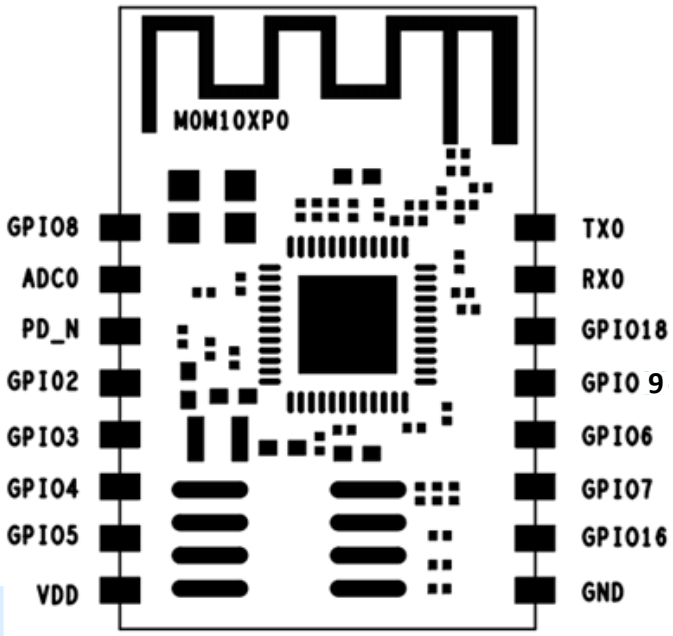

图 1-2：模块管脚排列图(BOTTOM VIEW)

模块管脚详细定义如下表格：

PIN	Function	Description
1	GPIO8	General Purpose Input/Output：GPIO8/PWM2；
2	ADC0	模拟量输入；
3	PD_N	模块使能功能： 高电平：模块正常工作 低电平：接地，模块关闭
4	GPIO2	General Purpose Input/Output：GPIO2；
5	GPIO3	General Purpose Input/Output：GPIO3；
6	GPIO4	General Purpose Input/Output：GPIO4；
7	GPIO5	General Purpose Input/Output：GPIO5；
8	VDD	电源，3.3V；
9	GND	接地；
10	GPIO16	General Purpose Input/Output：GPIO16；
11	GPIO7	General Purpose Output：GPIO7/PWM1；
12	GPIO6	General Purpose Output：GPIO6/PWM0；

13	GPIO9	General Purpose Input/Output：GPIO9/PWM3；
14	GPIO18	General Purpose Input/Output：GPIO18；
15	RXD	UART_RXD，串口接收；
16	TXD	UART_TXD，串口发送；

1.3 尺寸

M0M100P0 模块具有超小尺寸（16mm*24mm*3mm），如图 1-3 所示为模块尺寸图：

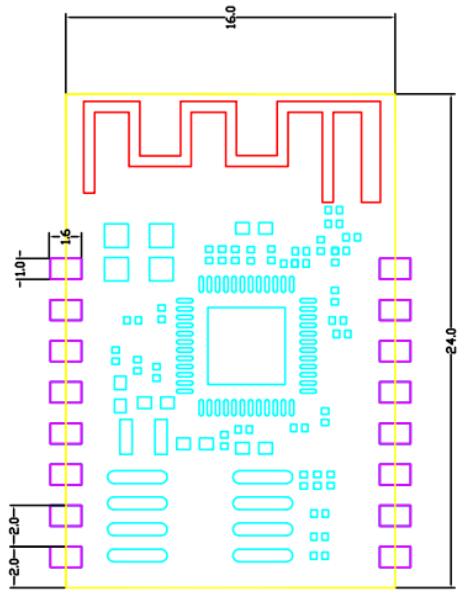

图 1-3：模块尺寸图（单位：mm）

1.4 参考设计电路

如图 1-4 所示，电源电路参考设计。

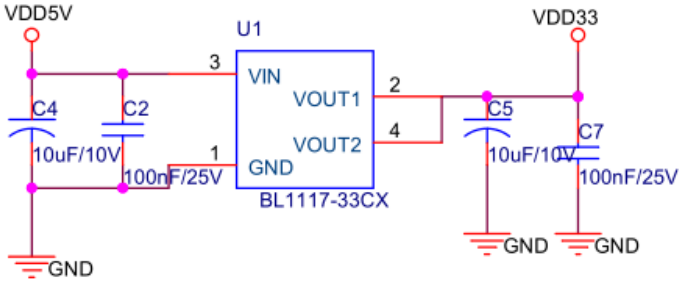

图 1-4：电源电路

如图 1-5，M0M100P0 模块的参考电路。

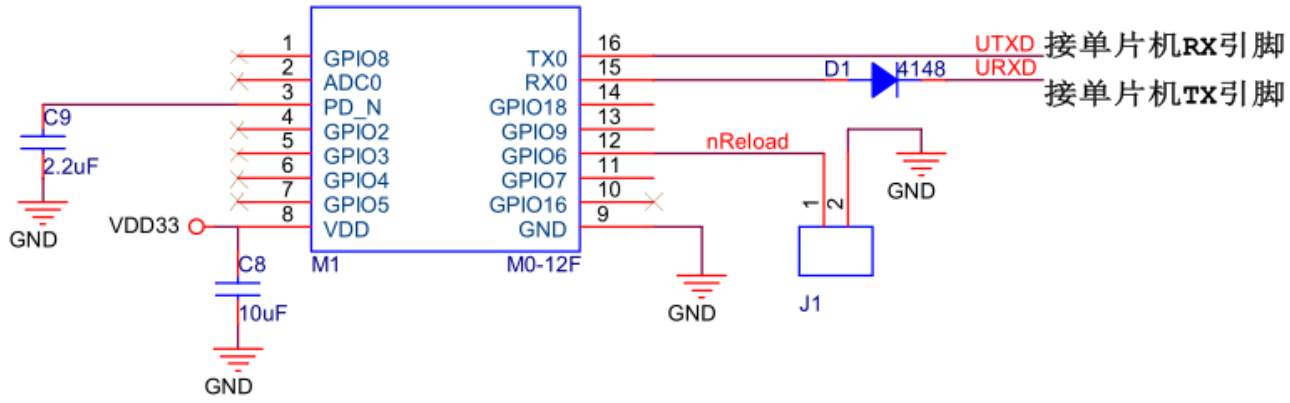

图 1-5：模块参考电路

1.5 产品编号规则

根据客户需求，M0M100P0 模块可以提供不同的配置版本，具体产品编号如图 1-6 所示。

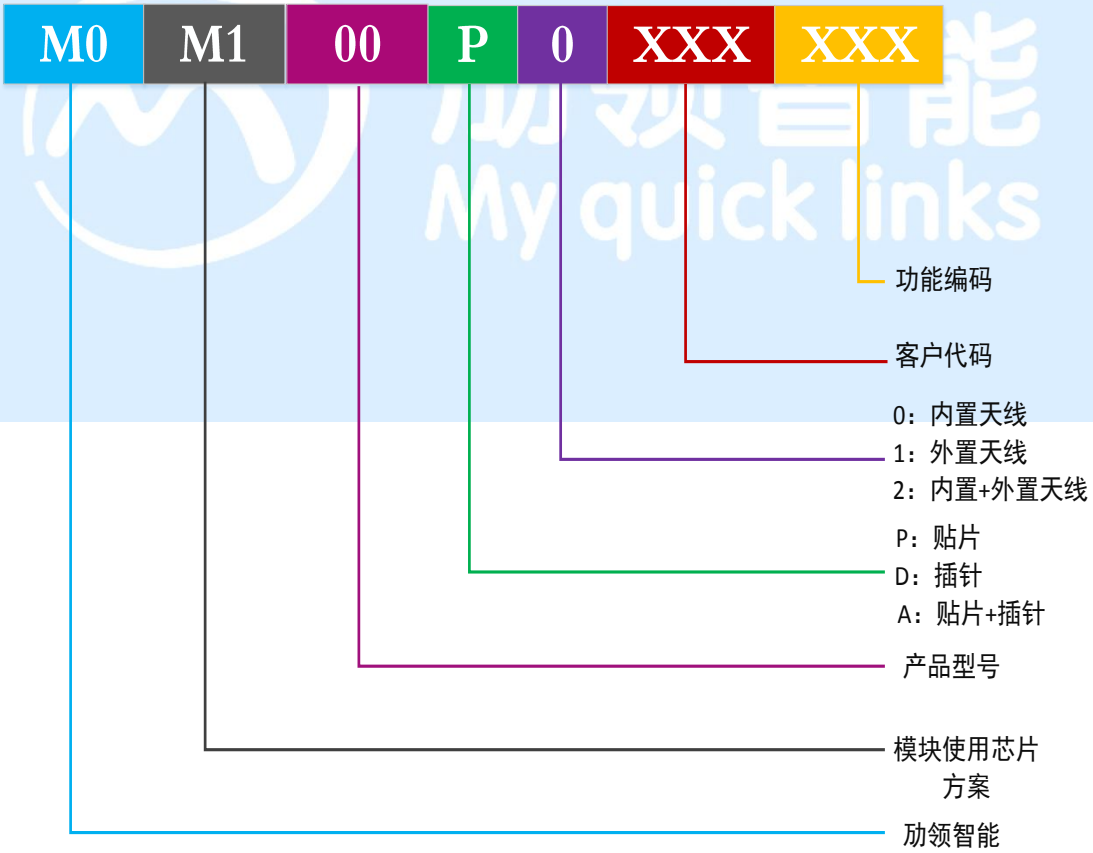

图 1-6：劢领产品编号规则

2. 功能描述

2.1 WIFI 探针技术

WIFI 探针技术是指基于 WIFI 探测技术来识别 AP（无线访问接入点）附近已开启 WIFI 的智能手机或者 WIFI 终端（笔记本、平板电脑等），无需用户接入 WIFI，WIFI 探针就能够识别用户的信息。

当我们走进探针信号覆盖区域内且我们的 WIFI 设备打开，我们的设备就能被探测出来，无论是 IOS 或者安卓系统都能够轻易检测到，并且获取设备的 MAC 地址。Wifi 探针模块可以探测周围的设备信息，包括目标 MAC、传输信道、帧类型、信号强度等等。

M0M1 系列 WIFI 探针模块具有以下特点：

1、即便手机没有连接 Wi-Fi，只要手机的 Wi-Fi 选项没有关闭，Wi-Fi 探针就能探测到手机发射出的信号进而能够做客流定位，手机品牌识别、新老顾客识别等数据分析；

2、 全频道、所有帧类型全抓取，自动探测区域内智能设备的 MAC 地址；

3、 从 Wi-Fi 模块设计、固件研发都是励领独自设计，我们方可提供全方位的技术支持和满足定制需求。

4、可设置波特率等串口参数。

5、设置探测的 WIFI 通道，可指定通道或者进行通道轮询。

2.1.1 实现原理

WIFI 是基于 IEEE802.11a/b/g/n 协议，在标准协议中，定义了 AP（无线接入点）何 STA（站或者客户端）的两种工作模式；协议中规定了 BEACON、ACK、DATA、PROBE 等多种无线数据帧类型，在站（STA）连接到无线接入点（AP）时进行交互的就是数据帧何应答帧、同时 AP 周期性发送 BEACON。

在站点（SAT）没连接到无线接入点（AP）上，手机客户端等站点（STA）也会发送 PROBE 帧进行探测询问哪个 AP 是可以接入的，WIFI 探针就是基于各种无线数据帧来抓获手机等 WIFI 客户端的 MAC 地址信息。

因此，要一个 WiFi 设备在 WiFi 探针的侦听范围内，当这个 WiFi 设备（无论是终端、路由器或者其他 WiFi 设备）发送任何一帧（Frame）时，不管是发给谁，探针都能截获，并分析出此

帧 MAC 层与物理层的一些信息，比如发送与接收设备的 MAC 地址、帧类型、信号强度等。对于周围的 WiFi 设备来说，探针是透明的。探针不需要与周围的设备有任何交互，其本身不需要发出任何 WiFi 信号。

2.1.2 应用领域

1、 客流统计：实时客流的统计及分析，掌握线下人群数据；

2、 精准营销：利用探测数据与用户信息对接，实现线下精准营销；

3、 公共安全业务：公安局侦测、公共安防、家庭安防

4、 考勤：员工考勤，员工定位；

5、借助第三方媒体类、咨询类、新闻类、生活类平台，将商家需要投放的广告更加精准地、智能地传播到顾客的手机屏幕，做到线下的千人千面。

6、 VIP 提醒：贵宾客户提醒，访问轨迹。

2.2 工作模式：透明传输模式

M0M100P0 模块支持串口透明传输模式。这一模式的优势在于可以实现串口即插即用，从而最大程度的降低用户使用的复杂度。M0M100P0 探针模块不需要与周围的设备有任何交互，其本身不需要发出任何 WiFi 信号。就可以实现串口透明传周围信息内容：包括设备的 MAC 地址、帧类型、信号强度等参数。

简而言之，将模块作为无线收数据的串口看待，无需任何改变即可轻松收发无线数据。

3. AT 指令说明

M0M100P0 探针模块是本公司自主研发的 WIFI 探针模块，可以通过 AT 指令进行设置。

3.1 WIFI 探针特点

- 全频段 1-13 个信道探测；
- 可通过 AT 指令设置波特率等串口参数；
- 可通过 AT 指令设置过滤探测到的 MAC 地址的周期；
- 可通过 AT 指令 设置探测的 WIFI 通道，可以指定通道或者进行通道轮询；
- 串口透传模式。

3.2 模块波特率选择

M0M100P0 上电后，默认的波特率为：115200，用户可以通过串口AT指令来设置WIFI探针模块的波特率参数。模块的缺省 UART 口参数配置如图3-1：

图 3-1：M0M100P0 缺省 UART 参数

用户可以通过 AT+指令利用 UART 口对模块进行置。

<说明>： AT 命令调试工具推荐使用 UartAssist 软件工具，以下介绍均使用 UartAssist 工具。

3.3 AT+指令集概述

AT+指令可以直接通过超级终端等串口调试程序进行输入，也可以通过编程输入。如下图 3-2 所示，通过 UartAssist 工具，列出 WIFI 探针模块探测到附近所有的 MAC 地址。

图3-2：列出探测到所有MAC等参数示意图

3.3.1 命令格式

AT+指令采用基于 ASCII 码的命令行，指令的格式如下：

格式说明

< >: 表示必须包含的部分

[ ]: 表示可选的部分

命令消息 ： AT+<CMD>[op][para-1,para-2,para-3,para-4…]<CR>	
AT 指令解析	说明
AT+	命令消息前缀；
CMD	指令字符串，如 UART 等字符串；详细请参考 3.3.3 节
op	指令操作符，由用户指定是参数设置或查询； 其中“=” ：表示参数设置，“” ：表示查询
para-n	参数设置时输入，若是查询时，则不需要，即为空即可；
CR	结束符，回车，ASCII 码 0x0a 或 0x0d；
说明：输入命令时，AT+<CMD> 字符自动回显成大写，参数部分保持不变。	

而 M0M100P0 模块返回值说明如下：

响应消息 ： +<RSP>[op] [para-1,para-2,para-3,para-4…]<CR><LF><CR><LF>	
AT 指令解析	说明
+	响应消息前缀；
RSP	响应字符串，包括：“ok” ：表示成功，“ERR”：表示失败；
op	指令操作符，查询时：返回“=” ，参数设置：返回“”；
para-n	查询时返回参数或出错时错误码；
CR	ASCII 码 0x0d；
LF	ASCII 码 0x0a。

错误码表示含义：

Table 2 错误码列表

错误码	说明
-1	无效的命令格式
-2	无效的命令
-3	无效的操作符

-4	无效的参数
-5	操作不允许

3.3.2 AT 指令的使用

在 AT 指令使用过程中需注意以下几点：

1、M0M101D0 模块 AT 指令集出厂默认波特率为：115200；

2、 ⟶ 表示：串口输入； ⟵ 表示：模块响应。

3、本节只是举一个简单 AT 指令使用实例，方便用户使用理解，用户可根据 4.2.3 节选择所需的 AT 指令进行参数配置或查询。

查询指令使用		
⟶	AT＋UART	查询 WIFI 探针模块 UART 参数
⟵	＋ok=	查询成功；（若出现“+ERR=”表示错误，用户需根据3.3.1节中“Table 2 错误码列表”查找原因）
	115200,8,1,NONE,NFC	参数值，表示模块 UART 的波特率为：115200。
	CR LF	结束符，回车，ASCII 码 0x0a 或 0x0d；

设置指令使用		
⟶	AT＋UART=115200,8,1,NONE,NFC	设置 WIFI 探针模块的 UART 参数
⟵	＋ok	设置成功；（若出现“+ERR=”表示错误，用户需根据3.3.1节中“Table 2 错误码列表”查找原因）

3.3.3 指令集

Table 3 AT+指令列表

指令	描述
<null>	空指令

串口指令	
UART	设置/查询串口UART参数
管理指令	
RELD	恢复出厂设置
Z	保存用户设置并重启模块
DLY	设置/查询信道切换周期
CHN	设置/查询模块当前工作的信道号
INTERVAL	设置/查询模块一个采集周期完成后停止采集的时间间隔
MAC	直接抓取指定的MAC地址的帧
TYPE	启动第二套格式输出采集内容

注意：

1、用户在配置 WIFI 探针模块的串口 UART 参数时，必须使用 AT＋Z 指令进行参数保存，方可生效；否则，所配置参数无效。

2、WIFI 探针模块出厂默认波特率为：115200。

3、WIFI 探针模块出厂默认的数据传输模式：透传模式。

3.3.3.1 AT＋UART

功能:设置/查询串口 UART 的参数	
查询指令格式: AT+UART<CR>	响应: +ok=<baudrate,data_bits,stop_bit,parity,flowctrl><CR><LF><CR><LF>
	参数：请参考设置参数
设置指令格式: AT+UART=<baudrate,data_bits,stop_bit,parity,flowctrl> <CR>	响应: +ok<CR><LF><CR><LF>
	参数: baudrate：波特率，2400、4800、9600、19200、38400、57600、115200、230400等 data_bits：数据位 8 stop_bits：停止位 1,2 parity：检验位 NONE（无检验位） EVEN（偶检验） ODD（奇检验） flowctrl：硬件流控（CTSRTS） NFC：无硬件流控 FC：有硬件流控

3.3.3.2 AT+Z

功能:保存用户设置参数	
指令格式: AT+Z<CR>	响应: +ok<CR><LF><CR><LF>
	参数：无
说明：用户所设置的参数，必须使用AT＋Z指令进行参数保存，才能生效；否则用户所设置的参数无效。	

3.3.3.3 AT+RELD

功能:恢复出厂设置	
指令格式: AT+RELD<CR>	响应: +ok=rebooting… <CR><LF><CR><LF>
	参数：无
说明：该命令恢复模块的出厂设置参数。	

3.3.3.4 AT＋DLY

功能: 设置/查询信道切换周期	
查询指令格式: AT+DLY <CR>	响应: +ok=< time ><CR><LF><CR><LF>
	参数: 请参考设置参数
设置指令格式: AT+DLY=<time > <CR>	响应: +ok<CR><LF><CR><LF>
	参数: time:信道的切换时间间隔,最小取值为:100ms;单位为毫秒。
说明：模块默认的信道切换时间间隔为：2000ms。	

3.3.3.5 AT＋CHN

功能：设置/查询模块当前工作的信道号	
查询指令格式： AT+CHN <CR>	响应： +ok=< channel ><CR><LF><CR><LF>
	参数：请参考设置参数
设置指令格式： AT+CHN=< channel > <CR>	响应： +ok<CR><LF><CR><LF>
	参数： channel：传输信道号。取值范围：1~13。
说明：若想设置多个信道号时，即AT+CHN=1,3,5,9 中间只需“,”隔开即可。其中1、3、5、9为信道号。	

3.3.3.6 AT＋INTERVAL

功能：设置/查询模块一个采集周期完成后停止采集的时间间隔	
查询指令格式： AT+INTERVAL<CR>	响应： +ok=< time_interval ><CR><LF><CR><LF>
	参数：请参考设置参数
设置指令格式： AT+ INTERVAL =< time_interval > <CR>	响应： +ok<CR><LF><CR><LF>
	参数： time_interval:时间间隔，单位为秒。
说明：模块出厂默认周期停止采集时间为0。 当AT+INTERVAL=5，也就是一个周期后间隔5秒后再采集数据。	

3.3.3.7 AT+MAC

功能：直接抓取指定的 MAC 地址的帧	
指令格式： AT+MAC =<mac><CR>	响应： +ok<CR><LF><CR><LF>
	参数： mac：指定MAC地址。

3.3.3.8 AT+ TYPE

功能:启动第二套格式输出采集内容	
指令格式: AT+ TYPE =1<CR>	响应: +ok=< ADDR1|ADDR2|ADDR3|FRAME 大类|FRAME 小类| CHN|RSSI ><CR><LF><CR><LF>
	参数: ADDR1~ADDR3：mac 802.11的mac地址; FRAME大类、FRAME小类：指WiFi信号的类别，其中，“大类”分为“管理”、“控制”、“数据”三类,其值分别为“0”、“1”、“2”; CHN：指WiFi信号所在的传输信道，取值在1~13之间; RSSI：信号强度，最小值为“-100”。
说明：模块默认的输出格式为：$MAC,ECD9D1C86040,RSSI,-58,CHN,03， 即：MAC、RSSI、CHN三个参数值。	