

WMRNET-IV 扩频无线水气表抄表网络 与上位机通讯协议 (VER 1.0)

深圳市安美通科技有限公司

2014-12-18

The information contained herein is the exclusive property of APPCON and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of APPCON.

上位机与集中器的通信命令格式说明

上位机与集中器的通信的所有命令都采用 ASCII 码进行传输，命令字符不分大小写，每个无线模块的 ID 与其嵌入的表 ID 相同，无线模块的 ID 由 4 个字节 16 进制组成，地址范围是从 0X00000000 到 0XFFFFFFF。其中 0X00000000 为集中器的地址，0X00000001 - 0XFFFFFFFE 为模块地址，0xFFFFFFFF 系统保留。

上位机基本命令格式

命令字符 _ 参数 1 _ 参数 2✓

例如:

上位机与无线模块模块通讯命令

CMD _ 无线模块 ID✓

集中器应答:A) OK 2 字节延时✓

经过 1 至 10 几秒

集中器再次应答:ANS _无线模块应答数据✓。如超时没有收到数据则集中器应答 NO ANS✓。

B) ERR * ✓

注 1: CMD 表示上位机与无线模块模块通讯命令.

注 2: _ 代表空格符(0X20), ✓代表回车换行(0X0D,0X0A).

注 3: 无线模块 ID 表示无线模块模块 ID, 用 16 进制表示不区分大小写, 以下均是合法输入: abc, 1, a, A ABCD7890, 123abCD, 0001234,12345.

注 4:无线模块应答数据:也将转为 ASCII 码形式输出, 例如无线模块应答数据为 16 进制:

0X68 0X01 0X23 0X45 0X67 0X89 0XAB 0XCD 0X68 0X02 0X02
转换形式后的为ASCII码字符串, 字符与字符之间用空格符分开.
ANS_68_01_23_45_67_89_AB_CD_68_02_02✓

上位机与集中器的通信命令

上位机与集中器的通信命令共计有 15 条，如下表：

序号	命令	说明
1	DELNET	删除网络命令。删除模块，路由器数据
2	CMD	上位机与无线模块模块通讯命令
3	TST	测试无线模块命令和控阀命令
4	RDNODE	读网络存在的无线表模块 ID 的命令
5	RDROUTER	读网络存在的无线路由模块 ID 的命令
6	FREQ	读写频率参数命令
7	NETID	读写网络 ID 命令
8	BATCH	组网即群表命令
9	STATUS	状态查询命令
10	RATE	读写集中器串口速率命令
11	MRATE	读写无线模块串口速率参数命令
12	VER	集中器软硬件版本命令
13	HELP	帮助命令
14	TXD	集中器与掌机通讯命令
15	SETID	集中器无线设置 ID 参数命令

1. 删除网络命令：

DELNET✓

集中器应答: A)OK✓

B)ERR * ✓

注:1)该命令删除所有已存模块的 ID 和网络数据。

2)删除网络后，系统不会重新组建网络。

3)*表示错误类型(以下相同) 1:不能识别的命令，或输入错误。

2:网络忙(正在执行上一条命令，以下相同)。

2. 上位机与无线模块模块通讯命令:

A) CMD _ 无线模块 ID ✓

B) CMD _ 无线模块 ID _ 应答字节数 _ 用户数据或命令(不大于 180 字节) ✓

集中器应答: A)OK 2 字节延时 ✓

经过 1 至几十秒

集中器再次应答:ANS _ 无线模块应答数据 _
电池电压 ✓。

如超时没有收到数据则集中器应答:

NO ANS ✓。

B)ERR * ✓

注:

- 1)2 字节延时, 应答的最大时间延时。
- 2)错误类型: 1:不能识别的命令, 或输入错误。 2:网络忙。 3:无线模块 ID 为空模块。
- 3) 应答字节数主要是用于网络延时, 不要求很准, 其代表模块应答集中器的大约字节数, 如模块将应答 100 个字节给集中器, 应答字节数就输入 100, 或略大于 100 的数字。
- 4)用户数据或命令的有效 16 进制数据不得大于 180 字节, 无线模块输出的是数据区的内容, 用 16 进制输出, 下位机应答也必须用 16 进制。下位机接收到无线模块输出数据后必须在 0.5 秒内作出应答, 且字节与字节间的间隙不能超过 20ms, 总的应答字节数也不能抄过 180 个字节。
- 5)对于接光电模块或单片机的模块, 如发送 A)命令, 模块收到命令后将 SGND 脚拉低, 10ms 后可以从串口接收数据, 要求的数据格式为 0x68+数据 (4 字节)。

模块收到 4 字节数据后, 在前后填入 1 字节状态信息, 1 字节的电池电压信息, 共计返回 6 个字节, 具体含义, 参见“上位机与集中器的通信命令”的命令 4: “读网络存在的无线模块模块 ID 的命

令”的注 8 说明。如等待 0.5 秒没有数据，或数据格式不对，则关闭串口，4 字节数据自动填充为 0xff，错误状态体现在 1 字节状态信息里。SGND 脚有 20mA 的灌电流能力，可用于给光电模块供电。

对于接双干簧管的模块，如发送 A)命令，由于数据是由模块采集的，不需要串口通讯，模块自动将 4 个字节计量表读数，加上 1 字节状态，1 字节的电池电压，返回给集中器。

6)对于接单片机的模块，如发送 B)命令，模块收到命令后将 SGND 脚拉低，10ms 后用户数据或命令从串口 TXD 脚输出，输出结束后，等待接收数据，等待的时间为 0.5S。如在 0.5S 内没有接收到任何数据，模块关闭串口，返回 4 个字节 ASCII 码‘ERR0’错误帧 + 1 字节的电池电压，共计 5 个字节，上传给集中器。如有数据，则在数据后加 1 字节的电池电压,返回给集中器。

3. 上位机测试无线模块命令和控阀命令:

A) 测试无线模块命令

TST _ 无线模块 ID _ 需要无线模块应答字节数✓

集中器应答: A)OK _ 2 字节延时✓

经过 1 至几十秒，

集中器再次应答:ANS _无线模块应答数据✓。

如超时没有收到数据则集中器应答:

NO ANS✓。

B)ERR * ✓

注:

1)2 字节延时，应答的最大时间延时。

2)错误类型: 1:不能识别的命令，或输入错误。 2:网络忙。 3:无线模块 ID 为空模块。

3)本条命令是用来测试无线模块的网络状态，需要无线模块应答字节数最大为 180，例如:

TST _ 12345678 _ 100✓

ID 为 123456789 无线模块则应答 0X00- 0X63 共计 100 个字节，集

中器则收到后输出:

ANS_00_01_02_03_04_05_06_07_08_09_0A_0B_0C_0D_0E_0F_
10_11_12_13_14_15_16_17_18_19_1A_1B_1C_1D_1E_1F_20_21
_22_23_24_25_26_27_28_29_2A_2B_2C_2D_2E_2F_30_31_32_3
3_34_35_36_37_38_39_3A_3B_3C_3D_3E_3F_40_41_42_43_44_
45_46_47_48_49_4A_4B_4C_4D_4E_4F_50_51_52_53_54_55_56
_57_58_59_5A_5B_5C_5D_5E_5F_60_61_62_63✓

4)A) 如输入 TST_ 无线模块 ID_ 0✓

集中器则收到后输出: ANS_24_24_24_ 电池空载电压 _ 无线发射
时电池电压✓

B) 控阀命令

TST_ 无线模块 ID_ 控阀指令✓

集中器应答: A)OK_ 2 字节延时✓

经过 1 至几十秒,

集中器再次应答: ANS_当前阀门状态✓。如超时没
有收到数据则集中器应答:

NO ANS✓。

B)ERR * ✓

注:

1)2 字节延时, 应答的最大时间延时。

2)错误类型: 1:不能识别的命令, 或输入错误。 2:网络忙。3:无线模
块 ID 为空模块。

3)控阀指令有 5 条:

控阀指令 = 192(0XC0) 查询阀门状态

控阀指令 = 193(0XC1) 阀门半开指令

控阀指令 = 194(0XC2) 阀门关闭指令

控阀指令 = 195(0XC3) 阀门打开指令

控阀指令 = 196(0XC4) 阀门防锈指令

应答当前阀门状态有 4 条:

ANS C0 状态不明或阀门正在执行动作中

ANS C1 阀门处于半开状态

ANS C2 阀门处于关闭状态

ANS C3 阀门处于打开状态

对于气表，阀门半开指令和阀门防锈指令无效。

- 4)开关阀过程是：如果当前记录的状态与控阀指令相同，则模块应答当前状态，并不再次执行动作(防锈指令除外)。如果当前记录的状态与控阀指令不相同，则模块应答 C0(阀门正在执行动作中)，并开始执行动作，当动作执行完毕模块切断马达电源并记录状态，但不主动上传状态。

执行动作时序是：首先启动阀门 1 秒，在这 1 秒内不做电流检测，1 秒后实时检测马达电流，当马达电流超过堵转电流，模块能在 100uS 内切断马达电源。如果马达电流没有超过堵转电流，但执行动作达到 20 秒，模块也立刻切断马达电源，堵转电流默认为 200mA。

- 5)如输入 TST _ 无线模块 ID _ 193✓，当前阀门状态为开。

模块首先应答 C0(正在执行动作)，紧接着关闭阀门，然后再打开三分之一的开阀时间。

- 6)控阀功能只针对某些定制机型，动作时间和堵转电流可定制。

- 7)控阀功能可定制成加密功能。

4. 读网络存在的无线表模块 ID 的命令：

RDNODE _ 模块 IDA _ 需读出模块数量✓

集中器应答:A)OK✓

模块 ID1 连接状况(1 字节) _ 模块 ID1 路由层数(1 字节) _ 模块 ID1(4 字节) _ 模块 ID1 数据(6 字节)✓

模块 ID2 连接状况(1 字节) _ 模块 ID2 路由层数(1 字节) _ 模块 ID2(6 字节) _ 模块 ID2 数据(6 字节)✓

... ..

END✓

B)ERR *✓

注:

1)集中器将从模块 IDA 开始按 ID 排序输出符合指定数量模块 ID，输入的模块 IDA 允许为空模块。

2)如符合模块 ID 数量不足或输出结束，在最后将填充 END✓。

3)错误类型: 1:不能识别的命令，或输入错误。 2:网络忙。

4)如输入为 RDNODE✓，及命令后不加参数，集中器将应答:

TOTAL_ XXXX✓,XXXX 代表所有模块的总数。

5)如输入为 RDNODE _ ID✓，及命令仅加 ID 参数，若 ID 在网内，集中器将应答: OK✓

模块 ID1 连接状况(1 字节)_ 模块 ID1 路由层数(1 字节)_ 模块 ID1(8 字节)_模块 ID1 数据(6 字节)✓

END✓

否则，应答:ERR 3✓。

6)模块连接状况如输出 G，代表最近一次组网找到了该模块。模块连接状况如输出 B，代表最近一次组网没有找到该模块。注意连续 9 次没有找到某模块，集中器将删除该模块。

7)模块路由层数代表最近一次组网该模块经过几级路由到达集中器。

8)模块数据有 6 个字节组成，1-4 个字节代表计量表读数，对于光电直读表这 4 个字节是光电表返回的数据；对于脉冲表这 4 个字节是无线模块自动计数的脉冲值，用 16 进制表示。

第 5 个字节代表模块状态，具体的含义见下表，第 6 个字节代表电池电压。

第 1-4 字节	4 个字节的数据	
第 5 字节	Bit 7	无线模块是否收到光电模块返回正确数据: 0 正确, 1 错误
	Bit 6	光电模块是否返回数据: 0 有, 1 无
	Bit 5	脉冲计数在两次组网期间是否受到磁攻击: 0 无, 1 有
	Bit 4	模块数据类型: 0 光电数据, 1 脉冲计数数据

	Bit 3	保留
	Bit 2	保留
	Bit 1-0	马达状态 00 状态不明 01 半阀状态 10 关阀状态 11 开阀状态
第 6 字节	电池电压 $\text{电池电压(V)} = \frac{\text{第 6 字节} + 200}{100}$ 例如: 第 6 字节是 0xA0, 十进制为 160, 则电池电压为 3.6V, 等于或低于 2V, 第 6 字节为 0x00, 等于或高于 4.55V, 第 6 字节为 0xff。	

5. 读网络存在的无线路由模块 ID 的命令:

RDROUTER _ 模块 IDA _ 需读出模块数量✓

集中器应答:A)OK✓

模块 ID1 连接状况(1 字节) _ 模块 ID1 路由层数(1 字节) _ 模块 ID1(4 字节) _ 模块 ID1 数据(2 字节)✓

模块 ID2 连接状况(1 字节) _ 模块 ID2 路由层数(1 字节) _ 模块 ID2(6 字节) _ 模块 ID2 数据(2 字节)✓

... ..

END✓

B)ERR *✓

注:

- 1)集中器将从模块 IDA 开始按 ID 排序输出符合指定数量模块 ID, 输入的模块 IDA 允许为空模块。
- 2)如符合模块 ID 数量不足或输出结束, 在最后将填充 END✓。
- 3)错误类型: 1:不能识别的命令, 或输入错误。 2:网络忙。
- 4)如输入为 RDNODE✓, 及命令后不加参数, 集中器将应答:

TOTAL _ XXXX✓, XXXX 代表所有模块的总数。

5)如输入为 RDNODE _ ID✓, 及命令仅加 ID 参数, 若 ID 在网内, 集中器将应答: OK✓

模块 ID1 连接状况(1 字节) _ 模块 ID1 路由层数(1 字节) _ 模块 ID1(8 字节) _ 模块 ID1 数据(2 字节)✓

END✓

否则, 应答:ERR 3✓。

6)模块连接状况如输出 G, 代表最近一次组网找到了该模块。模块连接状况如输出 B, 代表最近一次组网没有找到该模块。注意连续 9 次没有找到某模块, 集中器将删除该模块。

7)模块路由层数代表最近一次组网该模块经过几级路由到达集中器。

8)模块数据有 2 个字节组成, 第 1 个字节代表模块状态, 具体的含义见下表, 第 2 个字节代表电池电压。

第 1 字节	Bit 7	无线模块是否收到光电模块返回正确数据: 0 正确, 1 错误
	Bit 6	光电模块是否返回数据: 0 有, 1 无
	Bit 5	脉冲计数在两次组网期间是否受到磁攻击: 0 无, 1 有
	Bit 4	模块数据类型: 0 光电数据, 1 脉冲计数数据
	Bit 3	保留
	Bit 2	保留
	Bit 1-0	马达状态 00 状态不明 01 半阀状态 10 关阀状态 11 开阀状态
第 2 字节	电池电压 $\text{电池电压(V)} = \frac{\text{第 2 字节} + 200}{100}$ 例如: 第 2 字节是 0xA0, 十进制为 160, 则电池电压为	

	3.6V，等于或低于 2V，第 2 字节为 0x00，等于或高于 4.55V，第 2 字节为 0xff。
--	--

6. 读写频率参数命令:

A)读频率: `FREQ`✓

集中器应答:A)OK_XXXXXX✓

B)ERR *✓

B)写频率: `FREQ`_XXXXXX✓

集中器应答:A)OK✓

B)ERR *✓

注:

- 1)写频率命令只对集中器有效，并不会更改无线模块的参数。写频率命令确认后，**用户应执行删除网络命令，以重新组建网络。**
- 2)XXXXXX 是网络使用的频率，单位 KHz，如 490.000MHz，设置命令为: `FREQ`_490000✓
- 3)错误类型: 1:不能识别的命令，或输入错误。2:网络忙。

7. 读写网络 ID 命令:

A) 读网络 ID: `NETID`✓

集中器应答:A)OK_XXXX✓

B)ERR *✓

B) 写网络 ID: `NETID`_XXXX✓

集中器应答:OK✓

或 ERR *✓

注:

- 1)写网络 ID 命令只对集中器有效，并不会更改无线模块的参数。写网络 ID 命令确认后，**用户应执行删除网络命令，以重新组建网络。**
- 2) XXXX 是网络使用 ID，范围是 0x0000–0xfffe，0xffff 系统保留。
- 3)错误类型: 1:不能识别的命令，或输入错误。2:网络忙。

8. 组网并抄表命令:

BATCH✓

集中器应答:A)OK✓

B)ERR *✓

注:

- 1)网络在这种状况下,网络将处于活动状态开始维护网络并且按照约定格式抄表,是否维护结束可以通过查询命令 STATUS 读出。**维护网络时不能发送通讯命令,如 CMD 和 TST 命令。**
- 2)错误类型: 1:不能识别的命令,或输入错误。

9. 状态查询命令:

STATUS✓

集中器应答:A)BUSY✓

B)FREE✓

C)ERR *✓

注:

- 1)如网络处于维护状态集中器应答:BUSY✓,若维护结束将回答 FREE✓。
- 2)错误类型: 1:不能识别的命令或输入错误。

10. 写集中器串口速率命令:

RATE XXXX✓

集中器应答:A)OK✓

B)ERR *✓

注:

- 1)XXXX 可以是以下速率之一:
9600bps, 19200bps, 38400bps, 57600bps, 115200bps。
用户尽可能提高串口速率,以提高速度。
例如要将串口速率改为 115200bps 则命令为:
RATE 115200✓

集中器应答 OK✓ 后，立刻改变速率。

2)错误类型: 1:不能识别的命令，或输入错误。2:网络忙。

11. 读写无线模块串口速率参数命令:

A) 读参数 MRATE ✓

集中器应答:A)OK XXXX✓

B)ERR *✓

B) 写参数 MRATE XXXX✓

集中器应答:A)OK✓

B)ERR *✓

注:

1)此条命令目的是计算网络延时所用，并不能更改无线模块串口速率。此外对于脉冲计数模块此条命令无效。集中器设置的串口速率参数必须与实际网络内无线模块串口速率一致或者低于无线模块串口速率，否则通讯可能不正常。实际的无线模块串口速率可以通过本公司提供的 RF_MAGIC 软件进行设置。

2)XXXX 可以是以下速率之一： 1200bps, 2400bps, 4800bps, 9600bps, 19200bps, 38400bps, 57600bps。

例如要将串口速率参数改为 19200bps 则命令为:

MRATE 19200✓

3)错误类型: 1:不能识别的命令，或输入错误。2:网络忙。

12. 集中器软硬件版本命令:

VER✓

集中器应答:A)

* SHENZHEN APPCON TECHNOLOGIES CO.,LTD. *

* WIRELESS METER READ NETWORK *

* HARDWARE VERSION V1.5 *

* SOFTWARE VERSION V1.00 for GENERAL *

B)ERR *✓

注:

1)错误类型: 1:不能识别的命令, 或输入错误。2:网络忙。

13. 帮助命令:

HELP✓

集中器应答:A) 集中器将列出供客户使用的命令。

B)ERR *✓

注:

1)错误类型: 1:不能识别的命令, 或输入错误。2:网络忙。

14. 集中器与掌机通讯命令:

TXD_数据区✓

如格式正确集中器无应答, 否则集中器应答 ERR *✓

注:

1)错误类型: 1:不能识别的命令, 或输入错误。2:网络忙。 3:无线模块 ID 为空模块。

2)数据区的字节数不应超过 180 个字节, 字节用 ASCII 表示, 字节与字节间用空格隔开。

例如客户发送:

TXD_00_11_22_33_44_55_66_77_88_99_AA✓

掌机收到的数据将为: HEX 码的 0x00, 0x11, 0x22,
0x33, 0x44, 0x55, 0x66, 0x77, 0x88, 0x99, 0xaa。

14. 集中器无线设置 ID 参数命令:

SETID_口令(3 字节)_频率(3 字节)_网络 ID(2 字节)✓

集中器应答:A)OK_2 字节延时✓

经过 1 至几十秒,

集中器再次应答:ANS __频率(3 字节)_网络
ID(2 字节)✓

如超时没有收到数据则集中器应答:

NO ANS✓

B)ERR * ✓

注:

1)2 字节延时, 应答的最大时间延时。

2)错误类型: 1:不能识别的命令, 或输入错误。2:网络忙。 3:无线模块 ID 为空模块。

3)口令默认为 3 个字节的 0x00, 用户可定制。

掌机模块操作命令

掌机模块通讯用16进制表示，57600bps，无校验，55秒不操作，掌机模块进入休眠状态。当串口有数据时，模块被唤醒并相应命令，掌机模块操作如下：

- 1) 输入0xff(1字节唤醒字节)，则掌机模块则被唤醒，并切换至设置信道(默认488Mhz)，等待模块或路由器通过磁力触发上报数据，55秒没有再次输入0xff，或没有收到任何数据，掌机模块进入休眠。
- 2) 输入0xff(1字节唤醒字节)+频率(3字节，单位Khz)，则掌机模块则被唤醒，并切换至该频率，等待集中器通讯数据。55秒没有再次输入该命令，或没有收到任何数据，掌机模块进入休眠。
- 3) 输入0xff(1字节唤醒字节)+频率(3字节，单位Khz) + 0xXX(1字节命令) + 数据(可选，不等长)。掌机模块被唤醒，并执行相应的命令。

上述 3) 命令又分为四种类型：

A) 需要磁力触发模块操作的设置模块命令：

主要目的是为了近距离设置模块。具体操作是将磁铁靠近模块的磁力传感器约2秒以上，模块会在固定的默认频率(一般是488Mhz)自动发射模块的参数，格式如下：

0xa0(1字节命令头)+模块型号(1字节)+版本(1字节)+频率(3字节，单位Khz)+网络ID(2字节)+模块ID(2字节)+状态(1字节)+表底数(4字节)+模块物理ID(4字节)+RTC(6字节)。

其中：“模块物理ID”是固化在模块内部是唯一的并不可更改。“状态”是指阀门等的状态，如没有阀门则可忽略。“表底数”仅仅针对采集有模块完成的脉冲表有效，光电表则可以忽略。“RTC”实时时钟仅仅针对部分有客户定制的表。

磁力触发模块发射参数后，可以操作设置下列命令，模块收到正确命令后，会再次发射上述模块参数，执行该组命令，0xff后的发射频率无论是何值，都会在默认频率（一般是488Mhz）工作。

序号	命令	说明
1	0xff+频率+0x00+模块ID(4字节)	磁力触发后读模块参数
2	0xff+频率+0x01+模块物理ID或模块ID(4字节)+修改后频率(3字节)+修改后网络ID(4字节)	磁力触发后写模块频率和网络ID
3	0xff+频率+0x01+模块物理ID(4字节)+修改后频率(3字节)+修改后网络ID(2字节)+修改后模块ID(4字节)	磁力触发后写模块频率,网络ID和模块ID
4	0xff+频率+0x02+模块ID(4字节)+16进制表初值(4字节)	磁力触发后写模块的初值(仅仅针对脉冲表)
5	0xff+频率+0x03+模块ID(4字节)+RTC(6字节)	磁力触发后写模块的RTC(仅仅针对定制客户)

B) 掌机与模块通讯数据

掌机抄模块数据命令格式为:

0xff(1字节) + 频率(单位Khz,3字节) + 0x10 + ID地址(4字节)+数据(可选, 不等长).

本次命令将发送1.1-1.6秒左右, 发送完毕后。

如果发送ID地址后没有跟数据, 模块将应答:

0xa1 + 模块ID(4字节) + 数据(6字节)

如发送格式地址后有数据模块将输出数据给模块, 并返回模块应答的数据:

0xa1 + 模块ID(4字节) + 数据(模块应答的数据, 不等长)

注:1) 该命令类似“上位机与集中器的通信命令”中的 CMD 命令。

2) 模块应答的数据(6字节)格式, 参见“上位机与集中器的通信命令”的命令2:“读网络存在的无线模块模块ID的命令”的注8说明。

例如: 模块的频率为492.5Mhz, 网络ID是0x1234, 模块ID是0x11223344。

应发送命令: 0xff, 0x07, 0x83, 0xd4, 0x10, 0x11, 0x22, 0x33, 0x44

- 1) 掌机在发送完该条命令后，等待1秒接收数据，如有数据返回通过串口输出数据，如没有收到数据1秒过后模块将切换至默认设置频率(488Mhz) 接收，55秒后如串口或空中没有收到任何数据模块将休眠。如用户想保持在设置频率接收状态，需要每50-55秒向串口发送一个字节的0xff。

C) 掌机与集中器通讯命令

掌机与集中器通讯命令格式为：

0xff(1字节)+频率值(单位Khz，3字节)+ 0xff+用户的数据或命令(不大于180字节)。

注:1)集中器收到该命令后用ASCII码输出：

RCV_用户的数据或命令✓

- 2)此条命令对应与“上位机与集中器的通信命令”的命令 16: “集中器与掌机通讯命令”。

- 3)掌机在发送完该条命令后，将切换至接收状态，55秒后如串口或空中没有收到任何数据模块将休眠。

- 4)如用户想保持在一个固定的频率接收状态，不论模块休眠还是接收状态，需要每50-55秒向串口发送4个字节0xff(1字节)+频率值(单位Khz，3字节)。

D) 掌机批量修改模块参数命令：

该命令提供用途是无线批量修改无线模块的频率和网络ID，执行该组命令，掌机模块会扫描频率，保证无论何种设置的模块，在无线覆盖范围内都能收到。该命令执行时间约为8秒左右，命令格式如下：

0xff(1字节)+频率(单位Khz,3字节)+ 0x08 + 设置ID(1字节)+口令(3字节)+ 修改后频率(3字节)+ 修改后网络ID(2字节)+修改数量+ ID1(4字节)+ ID2(4字节)+ ID3(4字节)... .. 最大20个ID。

注:1)设置ID作用是区分本轮设置和前一次设置。模块收到该设置命令并在后面的ID号中包含自己的ID，则执行命令后，将同步该设置ID至模块，如下次再收到同样的设置ID的命令，

将不做出响应，如收到不一样的设置ID的命令，将响应命令，并同步设置ID。模块在48小时内没有收到该命令，则清零该设置ID，设置ID的范围是0x01至0x7f。

- 2) 口令默认为 3 个字节的 0x00，用户可定制。
- 3) 该条命令的修改数量是指后面的ID需要修改参数的个数。
例如，修改数量为10，ID个数为15个，那么前10个ID匹配的模块频率和网络ID将会被修改掉，同时同步该条命令设置ID，后面的5个ID，可能不是自己网络的模块不需要更改，那么这些模块仅仅同步该条命令设置ID，下次再接收到同样设置ID的这条命令将不再做出应答。

所有收到这条命令的模块，如果没有包含自己的ID，而同步过此次的设置ID，则不做任何操作。如果没有同步此次的设置ID，则在后面的1秒钟内随机上报自己的ID，格式是0xA8+ID(4字节)，1秒钟超时后，掌机模块自动应答一个空ID(0xA8, 0xff, 0xff, 0xff, 0xff)。用户可以通过这条命令发现和设置周边的模块。

- 4) 在有些情况下，用户仅仅想设置一只已知ID的模块，也可以通过这条命令，这是需要将设置ID设置为0xff，修改数量为1，ID的个数为一个即可。例如：

0xff+频率(3字节任意值)+ 0x08 + 设置ID(1字节0xff)+
口令(3字节)+ 修改后频率(3字节)+ 修改后网络ID(2字节)+ 修改数量(1字节0x01)+ ID1(4字节)

发出这条命令后，模块更改参数后，会应答：0xA8+ID(4字节)。并且收到这条命令的其他ID不匹配的模块，不做任何操作和应答。

在线设置模块命令

在线设置模块是通过模块的UART口完成的，设置采用HEX码，波特率为9600，无效验模式，设置命令有二条，格式如下：

1) 读设置命令：0xFF,0x56,0xAE,0x35,0xA9,0x55,0xF0。

应答：0x24，模块型号，版本号，频率，网络ID，模块ID，模块状态，表初值。

2) 写设置命令：0xFF,0x56,0xAE,0x35,0xA9,0x55,0x90频率，网络ID，模块ID，状态，表初值。

应答：0x24，模块型号，版本号，频率，网络ID，模块ID，模块状态，表初值。

其中参数表示用 HEX 表示，见下表

参数	字节数	说明
模块型号	1	APC340F-R代表路由器模块，模块代码为15，APC340F-N代表节点模块，模块代码为16，模块型号固化在FLASH内不可设置
版本号	1	当前版本，范围0-255，版本号固化在FLASH内不可设置
频率	3	单位KHz，如495.00MHz表示为0x07，0x8d，0x98
网络ID	2	网络使用ID，范围是0x0000–0xfffe，0xffff系统

		保留
模块ID	4	节点模块的 ID 范围是 0x00000001-0xfefffff. 路由器模块的 ID 范围是 0xff000000-0xffffffffe, 0x00000000 和 0xffffffff 系统保留。
模块状态	1	代表的是阀门当前状态, 用最低 2 位表示: 0x00: 状态不明, 0x01: 半阀状态, 0x02: 关阀 状态, 0x03: 开阀状态
表初值	4	16 进制表初值(4 字节)