

设备与服务器通讯协议

版本：V1.3

日期：2018 年 1 月

编辑：刘平

一、系统组成部分

系统由四部分组成：服务器、终端主机、手机 APP、接警中心平台

二、设备与服务器通讯描述

- 1、设备与服务器之间通过 TCP/IP (socket) 协议进行网络通讯，设备作为客户端与服务器的端口建立 TCP 连接并长期保持，即服务器随时可下发命令（待机模式下断开）。
- 2、设备每隔一段时间向服务器发送一次心跳数据，服务器以此数据来判断其是否在线，同时服务器收到心跳时应回复设备确认收到的信息（连接 AEP 平台的设备除外，平台自动回复）
- 3、设备有发送其它数据时服务器也应做相应的回复,否则设备会断开当前连接并重复建立 1-2 次连接再次发送数据，从而会加大设备耗电量（连接 AEP 平台的设备除外，平台自动回复）
- 4、具体数据协议见：“三、主机主动发送到服务器的相关数据”、“四、服务器主动发送到设备相关数据”

三、主机主动发送到服务器的相关数据

说明：

起始位：固定为“+c2s”

数据长度：从“起始位”至“校验码”（包括“校验码”）的字节个数； ≤ 1024 即 04 00（NB 版 ≤ 512 ）

类型：每种功能数据传输都有固定的字符

设备 ID：设备固定的独立身份代码（一般为设备二维码转换的结果）

校验码：“校验码”前面的所有位累加的结果（累加和，可设定一个 unsigned char 无符号字符类型变量自动累加，或者把所有位加起来然后 256 取模求余）

1、设备发送当前状态（同时也用作心跳功能,特殊情况时有变化也会发送）

内容详情	起始位				数据长度		类型	预留	设备 ID								总状态量	状态编号	内容长度	状态内容	 “取决于第 17 位的值”	校验码
值(16 进制)	+(2B)	C(63)	2(32)	S(73)	XX	XX	04	00														
位数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20+	(21+)	(21+)+1

说明：上电时所有数据都会发一遍，平时状态有变化才会发（比如信号强弱变化，开关状态），没变化的情况就固定时间发一次（可以当心跳，用来做离线判别）

长度：从“起始位”至“校验码”（包括“校验码”）的字节个数；≤1024 即 04 00（NB 版≤512）；例如：长度为 24 字节，则五六位分别是【0X00,0X18】

类型：固定为 0X04 【预留】用作存放设备 IMEI 的第 3 位字符（vre≧V5.4.8）

主设备 ID:前两位是机型(红外为:HW),后六位为设备二维码 ID 的后面 12 位数的转换结果(将 12 位字符串码转拼成 6 位的 16 进制数,例：061038955212 转后为【0X06,0X10,0X38,0X95,0X52,0X12】

总状态量：本次发送数据所包含的状态数量（每个状态量由后面的“状态编号”、“内容长度”、“状态内容”三个字段 组成）

状态编号：各状态有固定的编号，见下表

内容长度：当前状态所发内容的长度（字节），见下表

状态内容:当前状态编号所发的内容，见下表

状态项描述	编号 (10/16 进制)	长度(字节)	内容举例	支持机型[字符串]
NB/GPRS 信号强度	5【0X05】	1	0-5【10 进制】	HW
硬件版本号	8【0X08】	6-20	V1.0.0【ASCII 码】	HW
SIM 卡 CCID 号码	21【0X15】	15-20	SIM 卡上面对应的号码【ASCII 码】	HW
电池是否低压	42【0X2A】	1	1 表是正常，0 表示低压【10 进制】	HW
网络模块的硬件版本	63【0x3F】	x	【ASCII 编码】	HW
IMEI 号	64【0x40】	15	【ASCII 编码】	HW
防拆状态	65【0x41】	1	1 或 0（1 表是打开，0 表示压下）【10 进制编码】	HW
信号具体值(CSQ)	66【0x42】	1	0-255【10 进制】 CSQ 范围在 1-31 之间，不确定值时也会为 99，31 信号最好。 CSQ < 11，不容易附着网络。11 < CSQ < 18 在此区间网络不稳定会导致误码较多。CSQ > 18，能稳定通信。	HW
电压具体值（电量）	67【0x43】	2	0-65535mV【16 进制 unsigned short】例如 0X0bb8=3000mV，4.2V 电池电量计算： 【100%: ≧4.08】【90%: 4.06】【80%: 3.98】【70%: 3.92】【60%: 3.87】【50%: 3.82】【40%: 3.79】【30%: 3.77】【20%: 3.74】【10%: 3.68】【5%: 3.45】【0%: ≧3300】	HW
电压低压门阀值(推荐)	68【0x44】	2	0-65535mV【16 进制 unsigned short】例如 0X0DAC=3000mV	HW

温度 1 (环境)	70 【0x46】	2	0-65535℃ 【16 进制】 系数 0.1 例如 0x010E=270 =27℃ 大于 0x8000 为负温度 例如 0x810E-0X8000=270 =-27℃	HW
心跳时间	84 【0x54】	1	12/24 小时 【10 进制】	HW
红外探测区域有无	85 【0x55】	1	1 为有人，0 为无人	HW
烟感灵敏度	86 【0x56】	2	100-65534【0X00 ,0X64 】-【0XFF,0XFE】【16 进制 unsigned short】 YG:100 时灵敏度最高 450 最低	HW
报警消音时间	87 【0x57】	2	0-65534 【16 进制 unsigned short】（分钟） 0 表示不消音 65535 预留	HW
低压消音时间	88 【0x58】	2	0-65534 【16 进制 unsigned short】 分钟） 0 表示不消音 65535 永久消音	HW
故障消音时间	89 【0x59】	2	0-65534 【16 进制 unsigned short】（分钟） 0 表示不消音 65535 永久消音	HW
红外报警间隔时间	90 【0x5a】	2	2-6553 【16 进制 unsigned short】(单位：秒钟，实际值是设定值的 10 倍，例如设置为 2，则红外间隔的感应时间为 20 秒) 0 表示关闭 65535 表示无此功能(此数值由硬件决定，服务器无法设置)	HW
无人提示的判断时间	91 【0x5b】	2	1-65534 【16 进制 unsigned short】(单位： 分钟) 0 表示关闭 65535 表示无此功能	HW
红外探测器的灵敏度	92 【0x5c】	2	PB	HW
高温报警定值	93 【0x5d】	2	【16 进制 unsigned short】 26-85℃	HW
故障类型(时钟电路)	106	1	0 无故障	HW

AEP 平台的设备不用回复，脚本会自动处理，直连服务器必须返回成功（服务器必须正确返回，否则会影响设备进入睡眠的等待时间，从而加大功耗）

内容详情	超始位				数据长度		类型	预留	成功内容		校 验
值(16 进制)	+(2B)	C(63)	2(32)	S(73)	00	0B	04	00	O	K	
位数	1	2	3	4	5	6	7	8	9	10	11

回复代码举例（16 进制数）： 2b 63 32 73 00 0b 04 00 4f 4b dc 或者 直接返回字符 ： **received**

服务器返回失败（预留）

内容详情	超始位				数据长度		类 型	预 留	错误内容			代 码	校验码
值(16 进制)	+(2B)	C(63)	2(32)	S(73)	00	0D	04	00	E	R	R	00	
位数	1	2	3	4	5	6	7	8	9	10	11	12	13

2、设备发送实时报警

内容详情	超始位				数据长度		类型	预 留	主设备 ID								报 警 总 数	ACCT				MT	
值(16 进制)	+(2B)	C(63)	2(32)	S(73)	XX	XX	9(0x09)	00									1	0x31	0x32	0x33	0x34	0x31	0x38
位数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

内容详情	Q	XYZ			GG		CCC			S	时间						从设备 ID（APP、中心平台 ）								校验码
值(16 进制)	0x31	0x31	0x31	0x31	0x30	0x31	0x30	0x30	0x30	0	年	月	日	时	分	秒									
位数	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	(47+)+1

长度：起始位至校验码的字节数（如果只发一条报警时长度应为 48【0X00, 0x30】

类型：固定为 0X09 【预留】用作存放设备 IMEI 的第 3 位字符（vre≧V5.4.8）

主设备 ID: 前两位是机型（红外为：HW）,后六位为实际 ID(将 12 位字符串转拼成 6 位的 16 进制数，例 061038955212 【0X06 ,0X10, 0X38, 0X95, 0X52, 0X12】

报警总数、ACCT,MT,Q,GG,S,目前为固定内容（见上表）

CCC:报警防区（如果为 000 表示无防区或代表设备本身信息）

从设备 ID: 全为 0XFF 时表示主设备向所有从设备推送

时间：上传数据全为 0X00 时（取服务器上的时间为报警时间）

XYZ: 报警代码（见下表）

报警内容	报警代码【字符串】	支持机型【字符串】
低压报警	384	HW
红外报警	941	HW
高温报警(环境)	986	HW
报警测试	960	HW
温度短路(环境)	954	HW
温度开路(环境)	953	HW
自检正常	937	HW
开机（上电）	936	HW
探测区域已无人	935	HW
探测区域有人	934	HW
防拆报警	963	HW

AEP 平台的设备不用回复，脚本会自动处理！直连服务器必须返回成功（服务器必须正确返回，否则会影响设备进入睡眠的等待时间，从而加大功耗）

内容详情	超始位				数据长度		类型	预留	成功内容		校 验 码
值(16 进制)	+(2B)	C(63)	2(32)	S(73)	00	0B	09	00	O	K	
位数	1	2	3	4	5	6	7	8	9	10	11

回复代码举例(16 进制): 2b 63 32 73 00 0b 09 00 4f 4b e1 或者 直接返回字符：**received**

服务器返回失败（预留）

内容详情	超始位				数据长度		类型	预留	错误内容			代 码	校验码
值(16 进制)	+(2B)	C(63)	2(32)	S(73)	00	0D	09	00	E	R	R	00	
位数	1	2	3	4	5	6	7	8	9	10	11	12	13

3、设备已恢复出厂设置（仅按键复位后才发一次），

内容详情	超始位				数据长度		类型	预留	设备 ID								校验码
值(16 进制)	+(2B)	C(63)	2(32)	S(73)	00	17	01	00									
位数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

主设备 ID: 前两位是机型（红外为：HW ），后六位为实际 ID(将 12 位字符串转拼成 6 位的 16 进制数，例 061038955212 【0X06 ,0X10, 0X38, 0X95, 0X52, 0X12】

AEP 平台的设备不用回复，脚本会自动处理！直连服务器的设备才需要返回成功

内容详情	起始位				数据长度		类型	预留	成功内容		校验码
值(16 进制)	+(2B)	C(63)	2(32)	S(73)	00	0B	01	00	O	K	
位数	1	2	3	4	5	6	7	8	9	10	11

回复代码举例（每两位为一个 16 进制数）：2b 63 32 73 00 0b 01 00 4f 4b d9 或者 直接返回字符：**received**
服务器返回失败(预留)

内容详情	起始位				数据长度		类型	预留	错误内容			代码	校验码
值(16 进制)	+(2B)	C(63)	2(32)	S(73)	00	0D	01	00	E	R	R	00	
位数	1	2	3	4	5	6	7	8	9	10	11	12	13

四、服务器主动发送到设备相关数据（控制命令）

注意：起始位：固定为“+s2c”；其它说明见“三、主机主动发送到服务器的相关数据”开头描述

特别注意：连续发送数据时，每一条下发的数据中间要间隔 1s 以上！设备回复的数据起始位也为“+s2c”，与设备主动发送的起始位不一样!!!!!!!!!!!!!!

设置时必须先键将主机激活，才能收到下发指令：长按 3 秒测试报警键，会有一声蜂鸣提示，过几秒钟后听到第二声蜂鸣表示激活成功，主机会开放 30 秒时间等待指令
设置时也可以在设备上传数据的时间下发指令：设备每次上传数据后会等待 10 秒钟再断开连接

4、对设备进行一些功能设置

内容详情	起始位				数据长度		类型	预留	主设备 ID								控制设备 ID（用户自定义）								设置总项	设置类型	内容长度	设置内容	设置类型.....内容	校验码
值 (16 进制)	+	s	2	c	00	xx	02	00																					当总项>1才有此项	
位数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	27+	(27+)	(27+)+1

说明：主设备 ID:前两位是机型（烟感为：YG【0x59 0x47】）,后六位为设备二维码 ID 的后面 12 位数的转换结果(将 12 位字符串转拼成 6 位的 16 进制数，例：06103895212 转后为【0X06,0X10,0X38,0X95,0X52,0X12】)

设置项说明	设置总项	设置类型 10/16 进制	长度(10 进制)	设置内容	支持机型【字符串码】
设置主机连接的 IP 及端口	1	62【0x3e】	<40	【字符串编码】（"IP"+" ":"port"）例：192.168.1.100:25000 修改后可在设备本地复位恢复成为出厂默认的 IP（支持域名）	HW
心跳设置	1	75【0x4B】	1	12/24 小时【10 进制】只支持设置为 12、24 小时	HW

红外报警的间隔时间	1	98【0X62】	2(字节)	2-6553【0X00,0X00】-【0XFF,0XFE】(单位：秒钟，实际值是设定值的 10 倍，例如设置为 2，则红外间隔的感应时间为 20 秒) 0 表示关闭 65535 表示无此功能(此数值由硬件决定，服务器无法设置)	HW
设置红外感应灵敏度	1	99【0X63】	2(字节)	100-500【0X00,0X64】-【0X01,0XF4】 100 时灵敏度最高 500 最低 (暂无此功能)	HW
无人提示的判断时间	1	100【0X64】	2(字节)	1-65534【0X00,0X00】-【0XFF,0XFE】(单位：分钟) 0 表示关闭 65535 表示无此功能(此数值由硬件决定，服务器无法设置)	HW
修改 AEP 连接参数	1	111	10	【字符串编码】“产品 ID ”+“,”+“特征串”+“,”+“设备接入地址” 1 其中逗号为英文格式 2 修改后可在设备本地复位恢复成为出厂默认	HW

红外工作说明：

红外探测器：分“红外报警（941）”和“有人无人提示（934、935）”两种工作模式，建议用户二选一使用！（可远程或本地设置模式开关）

1 红外报警（941）是固定值：默认时间 10 分钟报警（适用于防盗场景 或者 服务器自己计时来判断有无人的方案）（此时间可设置修改，适用于服务器自己计时方案）

2 无人提示（935）是设备计时：默认连续 30 分钟没感应到人后提示。（此时间可设置修改，注意必须是连续时间没去到感应区域，否则会清 0 重新计时）

3 有人提示（934）：只要且必须设备发送过“935”后，任何时间进入探测区域都会立即触发一条“有人提示”（仅触发一条，想要再次触发必须等到下一个 935 之后）

短信设置功能（模块版本为：EC.....才有此功能）：

设置时必须先键将主机激活，才能收到短信指令：按一下测试键，会有一声蜂鸣提示，过几秒钟后听到第二声蜂鸣表示激活成功，主机会开放 30 秒时间等待指令

1.修改密码（密码出厂时默认为：123456）

设置密码短信格式：“旧密码” + “PW” + “新密码”

设置成功会回复短信到编辑指令查看的用户手机

例如：123456PW654321 可将密码改为 654321

注：修改密码后一定要记住该密码，设置任何指令都需要通过密码验证！

2. 短信设置所连接的服务器 IP、端口（此参数用于客户对接协议使用，修改错误会导致设备离线）

短信格式：“六位密码”+“TCPIP”+“所需设置的 IP 号”+“,”+“所需设置端口号”

设置成功会回复短信到编辑指令查看的用户手机

例如：123456TCPIP192.168.1.100,25000

在该例中“192.168.1.100”为所设置的 IP 号；“25000”为所设置的端口号

注：指令内容中“,”为英文格式下逗号，使用中文格式逗号不能被识别

3.短信指令设置 APN（选择中国以外的 GPRS 网络时必须设置）

短信格式：“主机密码” + “APN” + “ACCESS POINT NAME” +“,”+“USER NAME” +“,”+PASSWORD” ”

设置成功会回复短信到编辑指令查看的用户手机

例如：中国移动的 ACCESS POINT NAME 为：CMNET

USER NAME：无

PASSWORD：无

则短信指令为：123456APNCMNET,,

注：指令内容中“,”为英文格式下逗号，使用中文格式逗号不能被识别,

4、查看主机版本号

短信格式：“密码” + “VER”

设置成功会回复短信到编辑指令查看的用户手机

5、查看主机 IMEI 号

短信格式：“密码” + “RIMEI”

设置成功会回复短信到编辑指令查看的用户手机