密　级：

编　号：ESDZMZ18010402

ES1667T 模块接口协议

青岛东软载波智能电子有限公司

版本信息

版本	修订日期	修改概要
V1.0	20180402	初版

1 术语

- 模块：ES1667T 通信模块。
- 设备：使用通信模块传输数据的设备。
- 用户网络口令：用来区分网络，两个或者多个模块配置成相同的用户网络口令，则可以相互透传通信及中继转发，并能接收到网络内模块发出的广播。
- 初始网络口令：出厂固定为 8 个字节的 eastsoft，不可修改。
- MAC 地址：模块出厂固化的唯一地址，6 字节，只可读，不可修改。
- 通信地址 Addr：模块在电力线网络上使用的寻址地址，由设备进行设置（出厂默认值为本模块 MAC 地址）。
- 请求：设备主动发起的报文。
- 确认：模块对设备请求的应答。
- 通知：模块主动上报给设备的报文。
- 响应：设备对模块通知的应答。
- 入网：模块配置过用户网络口令。
- 离网：模块未配置过用户用户网络口令，或者清除了用户网络口令。
- RSV：保留域，报文处理时，忽略其内容，但是在发送的报文中其对应的域必须存在。
- AES：高级加密标准（Advanced Encryption Standard，AES），是一种块加密标准。
- MD5：Message Digest Algorithm MD5，用于确保信息传输完整一致。

2 默认串口参数

2.1 通信速率

波特率	数据位	校验位	停止位
115200	8 位	无	1 位

2.2 字节格式

每字节含 8 位二进制码，传输时加上一个起始位（0）和一个停止位（1）共 10 位。其传输序列如下图，D0 是字节的最低有效位，D7 是字节的最高有效位。

0	D0	D1	D2	D3	D4	D5	D6	D7	1
起始位	8 个数据位								停止位

3 接口协议详细说明

设备给模块发送指令时，模块会进行应答，当指令格式正确时，模块回复正常应答报文；当格式错误时，则回复异常应答报文。本节只给出正常应答格式，关于异常应答格式，详见附录 A。

模块主动发起的指令或者通知给设备，设备可以按上述方式进行响应，但不是必须的要求。

3.1 帧格式

帧格式如下所示。

长度（byte）	1	2	1	1	变长	1	1
含义	79H	L	Ctrl	Cmd	Data	CSUM	CXOR

帧格式的各个域中，大于一个字节的域，均使用小端字节序传输。

- 79H：帧头。
- L：Data 域的长度。
- Ctrl：控制域。
- Cmd：指令字。
- Data：数据域。
- CSUM：和校验，是 L、Ctrl、Cmd、Data 所有字节算术和，不考虑溢出。
- CXOR：异或校验，初始值为 0，是 L、Ctrl、Cmd、Data 所有字节的异或。

3.1.1 控制域（Ctrl）

控制域由 1 字节组成，定义如图所示。

D7	D6	D5	D4 ~ D0
RSV	Prm	Respond	RSV

- Prm：该标志只对发送数据指令（指令字 14H）有效，标识发送的数据是该设备主动发起的，还是该设备对其他设备指令的回应。
  0：指令回应；1：主动发起。
  正确区分，有利于提高通信效率。
- Respond：标志模块回复给设备的应答是正常应答还是异常应答。
  0：正常应答；1：异常应答。

3.1.2 指令字列表（Cmd）

操作类别	指令值	说明
本地操作指令	01H	模块重启
	02H	读取模块版本信息
	03H	读取模块 MAC 地址
	06H	读取模块用户网络口令
	07H	设置模块用户网络口令
	0BH	读取模块通信地址
	0CH	设置模块通信地址
	0DH	读取模块网络参数
	0EH	设置模块网络参数
	40H	加密数据
	41H	解密数据
	42H	计算 MD5
信道操作指令	14H	发送数据

	15H	接收数据
	17H	发起设备搜索
	18H	停止设备搜索
	19H	上报搜索结果
	1AH	通知设备搜索
	1BH	响应设备搜索
	1CH	发起用户网络口令设置
	1DH	通知用户网络口令设置
	1FH	上报用户网络口令设置结果
远程调试指令	52H	远程读取版本信息
	53H	远程读取 MAC 地址
	5DH	远程读取网络参数

3.2 本地操作指令详细说明

3.2.1 模块重启

方向	设备下发到模块	模块正常应答
Cmd	01H	01H
Data	空	State（1 byte）
		RSV（1byte）

- State: 01H：重启成功；00H：重启失败。

注： 模块是先应答，再重启。

3.2.2 读取模块版本信息

方向	设备下发到模块	模块正常应答
Cmd	02H	02H
Data	空	厂商标识（2bytes） ES — 4553H
		芯片类型（2bytes） 1667 —1667H
		产品信息（1bytes） 固定为’T’，54H
		版本号（2bytes） BCD 格式

3.2.3 读取模块 MAC 地址

方向	设备下发到模块	模块正常应答
Cmd	03H	03H
Data	空	MAC 地址（6 bytes）

3.2.4 读取模块用户网络口令

方向	设备下发到模块	模块回应给设备
Cmd	06H	06H
Data	空	Len（1byte）

		PSK（Len bytes）

- Len：用户网络口令长度，有效范围 8~64，0 表示未设置用户网络口令；
- PSK：用户网络口令，长度 8 ~ 64 字节；

3.2.5 设置模块用户网络口令

方向	设备下发到模块	模块回应给设备
Cmd	07H	07H
Data	Len（1byte）	空
	PSK（Len bytes）	

- Len：用户网络口令长度，有效范围 8~64，当长度小于 8，执行用户口令清除操作；
- PSK：用户网络口令，长度 8 ~ 64 字节，当长度小于 8 时，忽略其内容。

3.2.6 读取模块通信地址

方向	设备下发到模块	模块正常应答
Cmd	0BH	0BH
Data	空	模块通信地址（6 bytes）

- 模块通信地址：长度固定为 6 字节。

3.2.7 设置模块通信地址

方向	设备下发到模块	模块正常应答
Cmd	0CH	0CH
Data	模块通信地址（6 bytes）	空

3.2.8 读取模块网络参数

方向	设备下发到模块	模块回应给设备
Cmd	0DH	0DH
Data	空	透传参数（1byte）
		串口参数（1byte）
		载波参数（1byte）
		RSV（4 bytes）

- 透传参数：

D0 ~ D3	D4 ~ D7
透传层级限制	RSV

  - 透传层级限制：透传发送数据的覆盖范围，直通的为 1，其他以此类推，0 表示设备不指定，由载波模块自身决定。设定范围 01H~0FH。
- 串口参数：

D0 ~ D1	D2 ~ D3	D4 ~ D7
停止位	校验位	波特率

  - 停止位：0 –1位停止位，1 –2位停止位；
  - 校验位：00 - 无校验，01 - 偶校验，02 - 奇校验；
  - 波特率：

    00 - 600

    01 - 1200

02 - 2400
03 - 4800
04 - 9600
05 - 14400
06 - 19200
07 - 38400
08 - 56000
09 - 57600
0A - 115200

- 载波参数：

D0 ~ D3	D4 ~ D7
子载波数	发送功率

  - 子载波数：0 – 131子载波，1 – 411子载波；
  - 发送功率：00 - 0档，01 - 1档，02 - 2档，03 - 3档；

3.2.9 设置模块网络参数

方向	设备下发到模块	模块正常应答
Cmd	0EH	0EH
Data	透传参数（1byte）	空
	串口参数（1byte）	
	载波参数（1byte）	
	RSV（4 bytes）	

含义参见读取模块网络参数。

3.2.10 加密数据

方向	设备下发到模块	模块回应给设备
Cmd	40H	40H
Data	RSV（4 字节）	RSV（4 字节）
	key（16 bytes）	Len（2 bytes）
	Len（2bytes）	密文数据（Len bytes）
	明文数据（Len bytes）	

- key：加密密钥，16 字节；
- Len：数据长度，必须为 16 的整数倍，最小 16，最大 2000。

3.2.11 解密数据

方向	设备下发到模块	模块回应给设备
Cmd	41H	41H
Data	RSV（4 字节）	RSV（4 字节）
	key（16 bytes）	Len（2 bytes）
	Len（2bytes）	明文数据（Len bytes）
	密文数据（Len bytes）	

- key：解密密钥，16 字节；
- Len：数据长度，必须为 16 的整数倍，最小 16，最大 2000。

3.2.12 计算 MD5

方向	设备下发到模块	模块回应给设备
Cmd	42H	42H
Data	RSV（4 字节）	RSV（4 字节）
	Len（2bytes）	MD5（16 bytes）
	数据（Len bytes）	

- Len：数据长度，最大 2000；
- MD5：计算结果，16 字节。

3.3 信道操作指令详细说明

3.3.1 发送数据

方向	设备下发到模块	模块正常应答
Cmd	14H	14H
Data	Data Ctrl（2bytes）	空
	Dst Addr（6bytes）	
	User Data Len（2bytes）	
	User Data（User Data Len bytes）	

- Data Ctrl： 数据控制域，各位含义如下表：

D0 ~ D10	D11	D12 ~ D15
RSV	网络口令类型	中继深度

  - 网络口令类型： 发送数据使用的网络口令类型 0 初始网络口令 1 用户网络口令。
  - 中继深度：发送数据的设备，到目的地址设备的跳数，直通的为 1，其他以此类推，0 设备不指定，由载波模块自身决定，只对广播有效。
- Dst Addr： 目的通信地址，也可以为 FFFFFFFFFFFFH，表示全网广播。
- User Data Len：User Data 的长度。
- User Data： 待发送的用户数据。

3.3.2 接收数据

当模块从电力线上接收需要本地设备处理的数据时，用此格式通知设备。

方向	模块发送到设备	设备正常应答
Cmd	15H	15H
Data	Data Ctrl（3bytes）	空
	Src Addr（6bytes）	
	User Data Len（2bytes）	
	User Data（User Data Len bytes）	

- Data Ctrl： 数据控制域，各位含义如下表：

D0 ~ D7	D8 ~ D11	D12 ~ D14	D15	D16 ~ D23
RSV	中继深度	RSV	网络口令类型	RSV

  - 中继深度：发送数据的设备到接收到数据的设备的跳数，直通的为 1。
  - 网络口令类型：数据发送方使用的网络口令类型 0 初始网络口令 1 用户网络

口令。

- Src Addr： 发送数据的设备的通信地址。
- User Data Len：User Data 的长度。
- User Data： 接收到的用户数据。

3.3.3 发起设备搜索

方向	设备下发到模块	模块正常应答
Cmd	17H	17H
Data	Data Ctrl（2bytes）	空
	Attribute Len（1byte）	
	Attribute（Attribute Len bytes）	

- Data Ctrl： 数据控制域，各位含义如下表：

D0 ~ D7	D8 ~ D11	D12 ~ D14	D15
RSV	深度	Search Rule	RSV

  - 深度：搜索半径，取值 1 ~ 15，1 表示直通，其他以此类推。0 按 15 处理。
  - Search Rule：搜索规则。

    00H：搜索所有设备，包含入网和离网的；

    01H：搜索与本设备用户网络口令相同的设备；

    02H：搜索未入网设备；

    03H-~07H：RSV。

- Attribute Len：设备层数据长度。
- Attribute： 设备层数据，满足搜索规则的模块，会将此信息上报给设备，设备用来决定是否参与本次搜索。

3.3.4 停止设备搜索

方向	设备下发到模块	模块正常应答
Cmd	18H	18H
Data	空	空

3.3.5 上报搜索结果

方向	模块发送到设备	设备正常应答
Cmd	19H	19H
Data	Dev Cnt（1byte）	空
	Dev0 Addr（6bytes）	
	Dev0 Ctrl（2 bytes）	
	Attribute Len0（1 byte）	
	Attribute0（Attribute Len bytes）	
	Dev1 Addr（6bytes）	
	Dev1 Ctrl（2 bytes）	
	Attribute Len1（1 byte）	
	Attribute1（Attribute Len bytes）	
	…	

- Dev Cnt：上报的设备个数，最大为 5。

- Dev Addr： 搜索到的设备通信地址。
- Dev Ctrl： 设备控制域，各位含义如下表：

D0 ~ D3	D4 ~ D7	D8 ~ D15
RSV	Net State	RSV

  - Net State： 网络状态。
    00H：不在网；
    01H：同属于自己网络；
    02H：属于其他网络；
    03H：未知；
    04H~0FH：RSV。
- Attribute Len：设备层数据长度。
- Attribute： 响应设备搜索的设备层数据，供发起设备搜索的设备使用，可用来做双向验证，决定后续是否让设备入网。

3.3.6 通知设备搜索

模块通知设备，本模块收到其他模块发起的设备搜索，格式如下：

方向	模块发送到设备	设备正常应答
Cmd	1AH	1AH
Data	RSV（2bytes）	空
	Src Addr（6bytes）	
	Task ID（1byte）	
	Attribute Len（1byte）	
	Attribute（Attribute Len bytes）	

- Src Addr：发起搜索的源通信地址，设备端在响应设备搜索时，返回给模块。
- Task ID：本次通知设备搜索的任务号，设备端在响应设备搜索时，返回给模块。
- Attribute Len：设备层数据长度。
- Attribute： 搜索发起端的设备层数据。

3.3.7 响应设备搜索

方向	设备下发到模块	模块正常应答
Cmd	1BH	1BH
Data	Data Ctrl（2bytes）	空
	Src Addr 地址（6bytes）	
	Task ID（1byte）	
	Attribute Len （1byte）	
	Attribute（Attribute Len bytes）	

- Data Ctrl： 数据控制域，各位含义如下表：

D0 ~ D7	D8	D9 ~ D15
RSV	State	RSV

  - State：回复状态。
    0：不参与搜索，其 Attribute Len = 0；

1：参与设备搜索，其 Attribute Len 按需添加。

- Src Addr： 搜索设备发起端通信地址。
- Task ID： 本次通知设备搜索的任务号。
- Attribute Len：设备层数据长度。
- Attribute： 被搜索设备层数据。

注：

- 无论是否参与搜索，设备端都要发送响应设备搜索指令给模块，若无响应，模块按不参与处理，模块等待回应时间为 180ms。
- 设备端响应设备搜索时，将通知设备搜索帧中的 Src Addr 和 Task ID 返回。

3.3.8 发起用户网络口令设置

方向	设备下发到模块	模块正常应答
Cmd	1CH	1CH
Data	RSV（2bytes）	空
	Dst Addr（6bytes）	
	Old Psk Len（1byte）	
	Old Psk（Old Psk Len bytes）	
	New Psk Len（1byte）	
	New Psk（New Psk Len bytes）	

- Dst Addr： 设置口令的目的地址。
- Old Psk Len： Old Psk 长度。
- Old Psk： 原始口令。
- New Psk Len：New Psk 长度。
- New Psk： 新口令。

注：

- 用户网络口令作为网络的区分，需要保证相邻网络不重复。
- 口令长度范围 8-64。
- 安全及可靠考虑，本指令不支持目的地址为全 FF 的广播。

3.3.9 通知用户网络口令设置

方向	模块发送到设备	设备正常应答
Cmd	1DH	1DH
Data	Data Ctrl（2bytes）	空
	Src Addr（6bytes）	
	New Psk Len（1 byte）	
	New Psk （New psklen bytes）	

- Data Ctrl：数据控制域，各位含义如下表：

D0 ~ D7	D08 ~ D11	D12 ~D15
RSV	中继深度	RSV

  - 中继深度：发起用户网络口令设置的设备到本设备的跳数，直通的为 1。

- Src Addr： 远程设置口令的源地址。
- New Psk Len： 新的用户网络口令长度。
- New Psk： 新的用户网络口令。

注：

该通知不需设备响应，只是通知设备模块自身用户网络口令修改了，新的用户网络口令为 New psklen 和 New psk。

3.3.10 上报用户网络口令设置结果

方向	模块发送到设备	设备正常应答
Cmd	1FH	1FH
Data	RSV（2bytes）	空
	Src Addr（6bytes）	
	State（1byte）	

- Src Addr：回复的源地址。
- State： 00H：修改失败；01H：修改成功。

4 附录

4.1 附录 A 异常状态代码

若模块接收到的报文格式存在问题，则应答一条异常报文，其中控制域（Ctrl）中的 Respond 置位，指令字为设备下发的指令字，数据域一个字节，Status，指明了异常原因，取值及说明如下：

取值	说明
00H	错误的格式
01H	错误的数据单元
02H	错误的长度
03H	指令字无效
04H	RAM 空间不足
05H	错误的状态
06H~FFH	保留

举例：

设置错误格式的通信地址。

设备发送：79 01 00 58 0C 01 66 54

模块应答：79 01 00 B8 0C 02 C7 B7

设备发送指令将模块的通信地址设置为“01”（1 字节错误格式），模块应答提示异常状态“错误的长度”。

4.2 附录 B 远程调试指令详细说明

远程调试指令在对应的本地指令基础上，设备下发到模块的格式都增加 Data Ctrl 和目的通信地址，模块回应给设备的报文，增加源通信地址，其他与本地操作指令格式相同，如表所示。

方向	设备下发到模块	模块正常应答
Cmd	5xH	5xH
Data	RSV（1byte）	Src Addr（6bytes）
	Dst Addr（6bytes）	
	本地操作指令对应格式	

- Dst Addr：目的模块通信地址。
- Src Addr：源模块，被操作的模块通信地址。

模块支持的远程调试指令及说明如下：

操作类别	指令值	说明
远程调试指令	52H	远程读取版本信息
	53H	读取 MAC 地址
	5DH	读取网络参数

注：

模块异常应答格式详见附录 A。