

T/SILA

上海浦东智能照明联合会团体标准

T/SILA 001—2022

代替 T/SILA 001—2020

电力线载波通信(PLC)全屋互联规范

Power Line Communication (PLC) smart home intercommunication specification

2022 - 07 - 06 发布

2022 - 07 - 06 实施

上海浦东智能照明联合会 发 布

电力线载波通信 (PLC) 全屋互联规范

1 范围

本文件规定了PLC全屋互联协议的PLC控制系统技术要求。
本文件适用于PLC控制系统的设计，制造与应用。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

控制设备 control device

是指连接到PLC总线上的设备，并用于发送指令控制其他连接到相同PLC总线上的设备。控制设备如控制面板、传感器等。

3.2

受控设备 controlled device

是指连接在电源和一支或若干支灯之间用来变换电源电压，限制灯的电流至规定值，提供启动电压和预热电流，防止冷启动，校正功率因数或降低无线电干扰的一个或若干个部件，如开关控制器、单色调光驱动器、双色调光驱动器、彩色调光驱动器、窗帘驱动器等。

3.3

中央协调节点 central coordinator

是指在 PLC-IoT 通信中的具体体现为头端通信模块，负责末端设备的接入以及数据的接受与发送。

3.4

终端节点 station

是指在 PLC-IoT 通信中的具体体现为尾端通信模块，接受与发送电力载波信号，为终端设备提供统一的接入 PLC-IoT 网络方式。

3.5

代理协调节点 proxy coordinator

是指在 PLC-IoT 通信中的具体体现为中间代理通信模块，接受与发送电力载波信号，为中央协调节点和终端节点之间提供代理协调功能。

4 缩略语

下列缩略语适用于本文件：

BPCS：信标帧载荷校验序列（Beacon Payload Check Sequence）

BTS：信标时间戳（Beacon Time Stamp）

CCO：中央协调节点（Central Coordinator）

CIFS：竞争帧间隔（Contention Inter Frame Space）

CIID：属性实例（Characteristic Instance Identification）

DTEI：目的终端设备标识（Destination Terminal Equipment Identifier）

ETMI：分集拷贝扩展模式（Extend Tone Map Index）

FC：帧控制（Frame Control）

FCCS: 帧控制校验序列 (Frame Control Check Sequence)
FL: 帧长 (Frame Length)
ICV: 完整性校验值 (Integrity Check Value)
LID: 链路标识 (Link Identifier)
MAC: 媒介访问控制 (Media Access Control)
MMTYPE: 网络管理封包类型 (Management Packet Type)
MPDU: MAC层协议数据单元 (MAC Protocol Data Unit)
MSDU: MAC层服务数据单元 (MAC Service Data Unit)
NID: 网路标识 (Network Identifier)
NNID: 邻近网路标识 (Neighbor Network Identifier)
ODA: 原始目的地址 (Original Destination Address)
ODTEI: 原始目的终端设备标识 (Original Destination Terminal Equipment Identifier)
OSA: 原始源地址 (Original Source Address)
OSTEI: 原始源终端设备标识 (Original Source Terminal Equipment Identifier)
PB: 物理块 (Physical Block)
PBB: 物理块 (Physical Block Body)
PBCS: 物理块校验序列 (Physical Block Check Sequence)
PBH: 物理块头 (Physical Block Header)
PCO: 代理协调节点 (Proxy Coordinator)
PLC: 电力线载波通信 (Power Line Communication)
PSS: 追随符号大小 (Pilot Step Size)
RIFS: 回应帧间隔 (Response inter frame space)
SACK: 选择确认 (Selective Acknowledgement)
SIID : 服务实例 (Service Instance Identification)
SOF: 帧起始 (Start of Frame)
STA: 终端节点 (Station)
TMI: 分集拷贝基本模式 (Tone Map Index)

5 系统组成与架构

5.1 系统架构

本系统由网关和子设备组成，网关和子设备之间基于PLC系统控制协议通信，系统架构如图1所示。

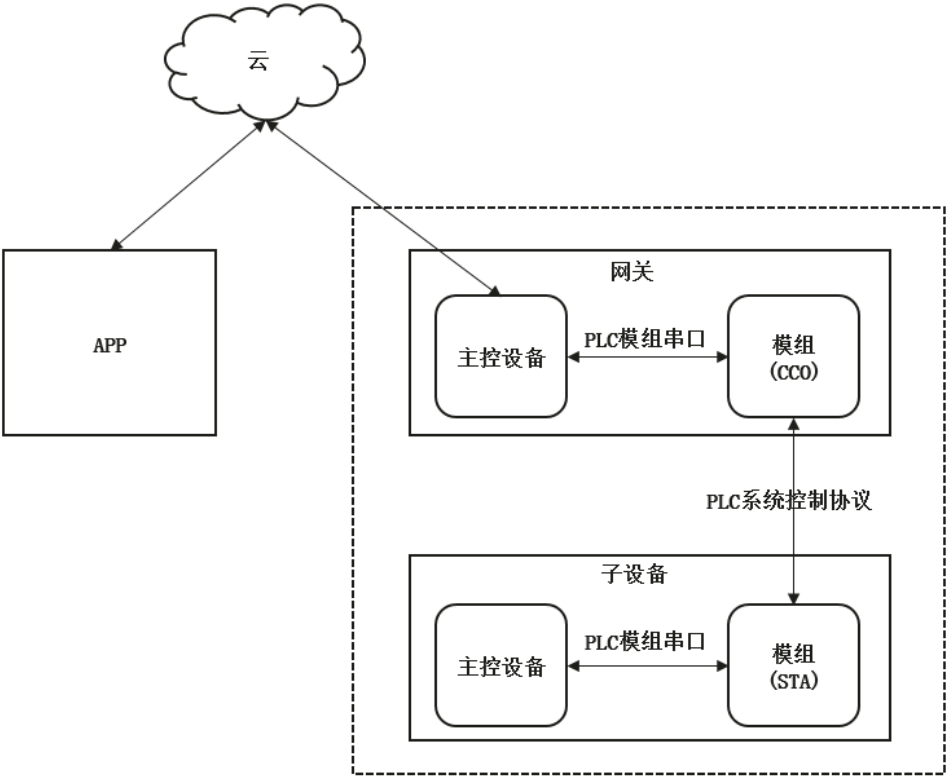


图1 系统架构

本系统基于PLC应用层构建全屋互联协议，实现通信单元之间业务数据交互，通过数据链路层完成数据传输，如图2所示。

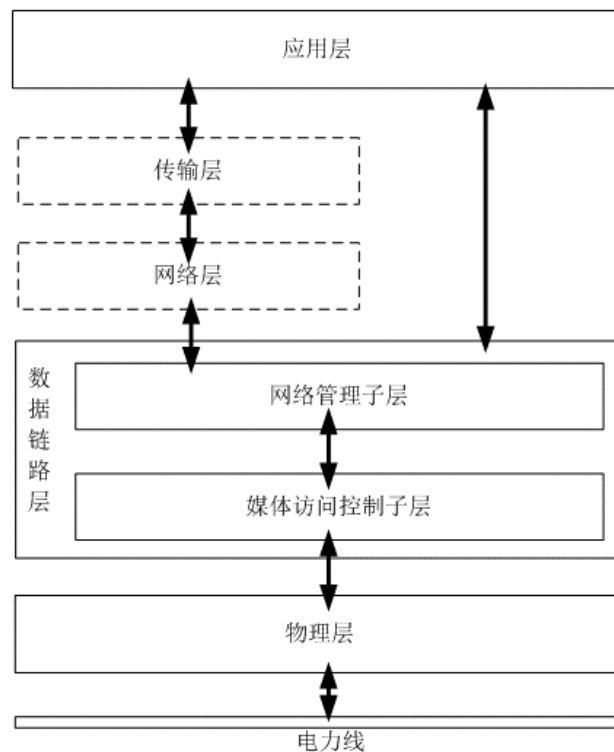


图2 PLC 分层

PLC 网络中有三种节点，以CCO（中心节点）、PCO（代理节点）、STA（终端）为组成的树形结构，如图3所示。其通信方式采用中央调度的方式，CCO 上电后会进行全网检测，确定PCO和STA，然后侦听STA的报文或者主动询问STA，通过CSMA/CA载波检测多址的方式进行传输管理和控制。

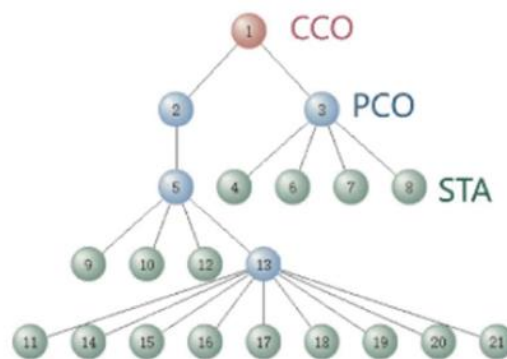


图3 PLC-IoT 树形组网及网络节点

所有STA站点向头端节点CCO发起关联入网请求，CCO确认后方可加入网络，网络建立可即可进行PLC通信。站点通信为CCO与STA站点的之间的相互通信，STA与STA不能直接通信，需要通过CCO来转发，PLC的自组网过程由芯片底层软件实现，无需应用层干预，芯片应用层互联规范应满足附件5要求。

入网过程：上电后和CCO之间能直接通信的STA站点，会首先入网，形成1级站点，并评估相互通信成功率，不能和CCO直接通信的站点若能和1级站点通信，就通过1级站点代理入网，以此类推逐级形成多层级网络，目前最大可以支持15层级。PCO站点非指定，由各站点自动形成。

PLC信道具有时变性，噪声也可能随着电器开闭时有时无，这意味着已经建立起来的路由网络可能

存在不通，PLC链路层需有路由评估机制，在路由周期内不断评估代理路由合理性，动态变化拓扑图，以确保通信可靠。路由评估需要时间，因此CC0坏掉或者站点拔掉，网络稳定需要一定时间，这个时间与网络规模或者层级深度有关系。

在PLC总线网络的每个设备，都有一个固定的物理地址（6字节MAC地址），MAC地址在PLC模块出厂时通过IANA或IEEE申请分配，使用过程不更改。使用MAC地址，在网络中可提供单播寻址（0~FF FF FF FF FF FE）方式或广播寻址（FF FF FF FF FF FF）方式进行通信。

5.2 系统组成

PLC系统一般由多个子系统组成，子系统通过PLC网关连接到局域网或云端服务器组成系统，移动终端通过云端连接系统。一个子系统由一个PLC网关、若干个控制设备和若干个受控设备组成。

PLC网关是集成控制、管理、计算和通信等功能的基础开放平台。网关包含PLC-CC0模组、MCU模块。特性如下：

- a) PLC 网关在系统中通过中央节点 CC0 进行协议转换与 STA 通信；
- b) 具备应用地址配置和管理；
- c) 具备场景配置与控制；
- d) 具备控制程序逻辑配置与控制；
- e) 具备系统设备状态监测功能；
- f) 具备通过网络把系统的指令同步传递到云端；
- g) 具备分组配置与控制。

场景可通过按键信号、时钟信号、传感器信号等进行触发，场景控制逻辑通过PLC网关进行配置，场景配置信息保存在每个受控设备内，当进行场景控制时，被寻址选中的受控设备可以实现同步响应。

5.3 系统要求

PLC 全屋互联系统的特性如下：

- a) 一个子系统至少含一个 CC0 中央节点；
- b) 任一个系统设备都可以主动发送事件上报信息；
- c) 一个子系统最多可独立寻址 1023 个的设备；
- d) 一个子系统最多可寻址 49150（2 个字节，除去预留的设备地址）个可寻址组，单个子设备至少支持 32 个分组；
- e) 一个子系统最多可支持 65535（2 个字节）个照明场景，单个子设备至少支持 32 个场景。

系统控制面板或传感器的事件信息发送到CC0，由CC0根据控制逻辑进行处理，并由CC0把处理完的控制信息发送到受控设备进行控制处理。

5.4 系统设备功能定义模型

设备profile是设备和其他子系统之间的交互数据定义能力和格式，用于描述设备所具备的能力和状态数据。设备的通过两种方式描述设备具备的特征，服务(service)和属性(characteristic)，设备由若干个服务及其属性组成。

设备service用来表示设备中用户可使用的功能函数，其中包含实现该函数输出/输入的数据以及实现该函数的行为。设备可以基于服务进行实例化，实例化后的名称称之为服务实例。

设备characteristic表示数据或相关行为的特征，名称称之为属性名，是Service的基本组成单元，如开关的开或关特性。如图4所示：

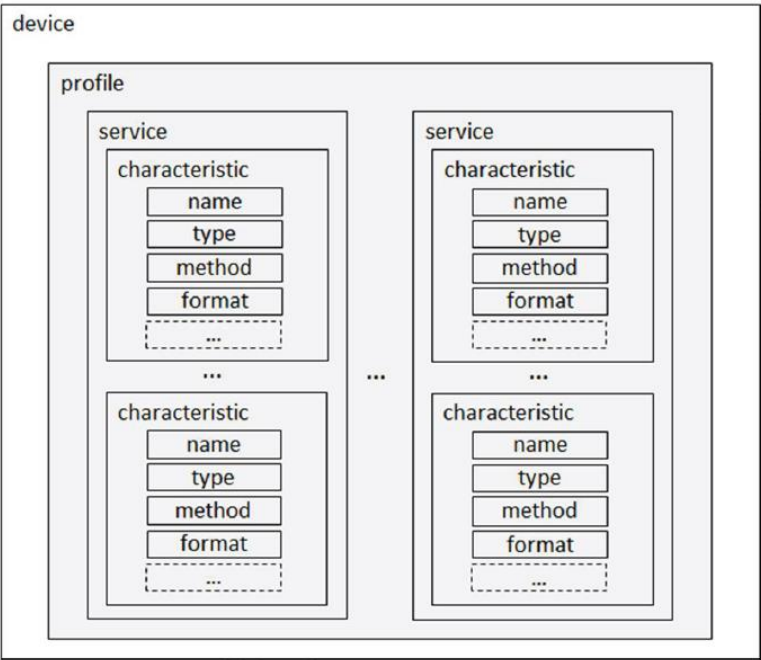


图4 设备功能定义模型

用户通过APP 控制设备执行场景时，云端到PLC-IoT网关设备的profile 数据的格式如图5：

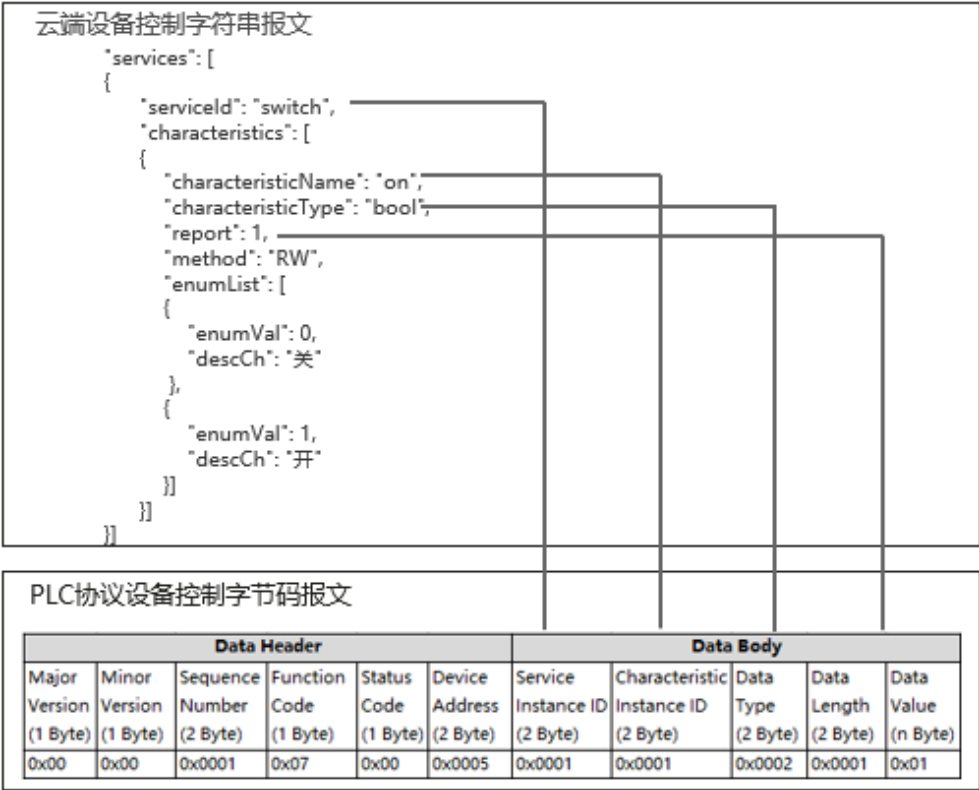


图5 PLC 协议设备控制报文转换

以下列举了几种典型的子设备器件物模型转换定义，用于示例PLC设备与物模型的映射，通过这种方式，可以无限扩展定义灯光控制的属性，例如新增灯光驱动控制器子设备的功率、故障信息，只要新增定义与调节亮度相似的服务属性即可传递到网关，并通过网关传递到云端。SIID和CIID使用两个字节编码，其中0x0001~0x1964用于定义通用范围段，0x1965~0x3FFF预留给团体标准定义范围段，x4000~0xFFFF预留给厂商定义私有不通范围段。

具体的物模型定义参见表1~表6：

表1 场景面板

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述
0x0041	scene	按键记录					
			0x008A	num	int	min:1 max:按键数量	场景按键键码编号上报
0x03F1	button1	按键(1)					
			0x008A	num	int	min:1 max:按键数量	按键编号
			0x0002	name	string	StringLength:32	按键名

表2 窗帘

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述
0x0013	mode	窗帘开合					
			0x0022	mode	enum	0-关 1-开 2-暂停	窗帘电机控制窗帘的开合
0x000B	opener	开合度					
			0x000E	current	int	min:0 max:100	当前的打开程度，100 为全开 单位：百分比；
			0x000F	target	int	min:0 max:100	目标的打开程度，100 为全开 单位：百分比；

表3 灯光驱动控制器

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述
0x0001	switch	开关					
			0x0001	on	bool	0-关 1-开	电源开关状态; 变化就上报
0x0007	brightness	亮度					
			0x0004	brightness	int	min:1 max:100 步长:1	亮度设置; 变化就上报
0x0005	colour	RGB 颜色					
			0x0007	red	int	min:0 max:255 步长:1	RGB 颜色 红色, 变化就 上报
			0x0008	green	int	min:0 max:255 步长:1	绿色 变化就上报
			0x0009	blue	int	min:0 max:255 步长:1	蓝色 变化就上报
			0x000A	white	int	min:0 max:255 步长:1	白色 变化就上报
0x0009	cct	色温					
			0x000D	colorTemperature	int	min:2700 max:6500 步长:1	灯的色温 变化就上报
0x0042	progressSwitch	开关渐变					
			0x008C	range	int	min:0 max:5	亮度变化时 长, 单位: 秒。默认值: 2 秒

表4 红外移动传感器

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述
0x0014	status	有无状态					
			0x0024	status	enum	0-无人 1-有人	有无持续的状态

表5 光照传感器

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述
0x0021	luminance	光亮度					
			0x0001	on	bool	0-关 1-开	电源开关状态
			0x000E	current	int	min:0 max:65535 步长:1	光照度, 单位 lx

表6 电源开关

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述
0x0001	switch	电源开关					
			0x0001	on	bool	0-关 1-开	电源开关状态 变化就上报

6 PLC 模组串口接口参考

6.1 范围

本协议规定了MCU与PLC CC0（主节点）之间串口通信数据传输的帧格式、数据编码及传输规则。

6.2 说明

本协议中所有保留字段都需要填0。

6.3 应用帧结构

6.3.1 字节格式

应用帧的基本单元为8位字节。链路层传输顺序为低位在前，高位在后；低字节在前，高字节在后。串口传输时：字节传输按异步方式进行，通信速率默认为115200 bps，基本单元包含1个起始位“0”、8个数据位、一个偶校验位P和1个停止位“1”，定义见表7。

表7 字节格式

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

6.3.2 帧格式定义

数据帧采用小端序，格式如表8所示。

表8 帧格式定义

长度 (byte)	1	1	2	2	2	L	2
含义	Head	Ctrl	Cmd	Seq	L	Data	CRC

说明：

Head：帧头，固定为 48H。

Ctrl: 控制域。

Cmd: 命令码。

Seq: 帧序列号, 用以匹配上下行报文的请求应答关系, 取值 0~65535, 循环使用。

L: 数据域 Data 的长度, 最长 496 字节。

Data: 数据域。

CRC: 报文的 CRC16 校验和, 从帧头开始到 Data 段结束。CRC 校验生成多项式采用 CRC16-CCITT(0x1021), $x^{16}+x^{12}+x^5+1$ 。

6.3.2.1 控制域 (Ctrl)

控制域 (Ctrl) 表示帧的传输方向、启动标志, 由1字节组成, 定义如表9所示。

表9 控制域

D7	D6	D5	D4	D3	D2	D1	D0
Dir	Prm	Rsv					

说明:

Dir: Dir=0 表示此帧报文是由主控设备发出的下行报文;

Dir=1 表示此帧报文是由通信模组发出的上行报文。

Prm: Prm=1 表示此帧报文来自启动站;

Prm=0 表示此帧报文来自从动站。

Rsv: 保留

6.3.2.2 命令码 (Cmd)

命令码 (Cmd) 见表10。

表10 命令码

Cmd	说明	命令类别
0001H	读取模组版本信息	本地通信命令
0002H	读取模组 MAC 地址	
0003H	读取模组通信地址	
0004H	设置模组通信地址	
0005H	模组重启	
0006H	传输文件	
0007H	读取模块上电时间	
0010H	读取白名单中节点数量	
0011H	读取白名单中节点信息	
0012H	添加节点到白名单	
0013H	删除白名单中节点	
0014H	清空白名单	
0015H	自组网功能开启	
0016H	设置白名单状态	
0017H	获取白名单状态	
0020H	读取拓扑中节点数量	
0021H	读取拓扑中节点信息	
0100H	发送数据	信道转发命令
0101H	接收数据	
0110H	远程发送命令	远程调测命令
0111H	远程接收命令	
0120H	总线数据通信命令	总线数据通信命令

6.3.3 本地通信命令详细说明

本地命令数据交互流程见图6。

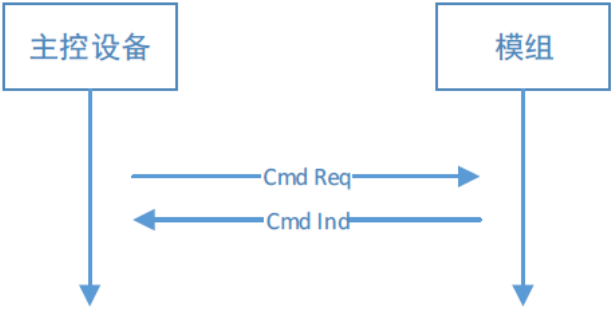


图6 本地命令数据交互流程

6.3.3.1 读取模组版本信息（0001H）

读取模组版本信息见表11。

表11 读取模组版本信息

方向	主控设备下发到模组	模组应答
Cmd	0001H	0001H
Data	空	厂商代码 (2bytes)
		芯片类型 (2bytes) 3921H
		软件版本号 (2bytes) BCD 格式
		保留 (2bytes) 0000H

6.3.3.2 读取模组 MAC 地址 (0002H)

读取模组MAC地址见表12。

表12 读取模组 MAC 地址

方向	主控设备下发到模组	模组应答
Cmd	0002H	0002H
Data	空	MAC 地址 (6bytes)
		保留 (2bytes) 0000H

6.3.3.3 读取模组通信地址 (0003H)

读取模组通信地址见表13。

表13 读取模组通信地址

方向	主控设备下发到模组	模组应答
Cmd	0003H	0003H
Data	空	通信地址 (6bytes)
		保留 (2bytes) 0000H

6.3.3.4 设置模组通信地址 (0004H)

设置模组通信地址见表14。

表14 设置模组通信地址

方向	主控设备下发到模组	模组应答
Cmd	0004H	0004H
Data	通信地址 (6bytes)	设置结果 (1byte) 0: 成功, 1: 失败
	保留 (2bytes) 0000H	失败原因 (1byte), 见 5.3.6
		Rsv (2bytes)
注: 模组通信地址保存在模组非易失性存储器中。		

6.3.3.5 模组重启 (0005H)

模组重启见表15。

表15 模组重启

方向	主控设备下发到模组	模组应答
Cmd	0005H	0005H
Data	Delay Time (1byte)	State (1Bte)
	Rsv (3bytes)	Rsv (3bytes)

说明：
 Delay Time：延时等待重启时间，单位：秒。0 代表立即重启。
 State：0-重启成功；1-重启失败。
 注：模组收到报文后，先应答再重启。

6.3.3.6 传输文件（0006H）

传输文件见表16。

表16 传输文件

方向	主控设备下发到模组	模组应答
Cmd	0006H	0006H
Data	Fn (1byte)	Fn (1byte)
	User Data	User Data

Fn 为功能码，不同功能码对应的 User Data 格式如下。

6.3.3.6.1 启动文件传输

启动文件传输见表17。

表17 启动文件传输

方向	主控设备下发到模组	模组应答
Fn	01H	01H
Data	File Attr (1bytes)	State (1byte)
	Segment Total (2bytes)	Reason (1byte)
	File Length (4bytes)	Rsv (1byte)
	File Crc (4bytes)	
	Trans Timeout (4bytes)	

说明：
 File Attr：0 表示清除下装；1 表示本地升级文件；2 表示全网升级文件；3 表示列表升级文件（升级部分 STA）。
 Segment Total：文件传输内容的总段数。
 File Length：文件的总长度，单位字节。
 File Crc：文件所有内容的 CRC32 校验和。
 Trans Timeout：文件传输超时时间，单位：分钟。
 State：0 表示成功；1 表示失败，失败原因见 Reason。
 Reason：取值含义请参见“异常状态代码”。

6.3.3.6.2 传输文件内容

传输文件内容见表18。

表18 传输文件内容

方向	主控设备下发到模组	模组应答
Fn	02H	02H
Data	Rsv (1byte)	State (1byte)
	Segment Num (2bytes)	Reason (1byte)
	Segment Size (2bytes)	Rsv (1byte)
	Segment Crc (2bytes)	
	Segment Data	

说明:

Segment Num: 文件内容的传输帧序号, 取值范围 0 至 n-1 (n 为总段数)。

Segment Size: 该帧文件内容的大小, 除最后一帧外, 其他帧必须为固定大小。

Segment Crc: Segment Data 的 CRC16 校验和。CRC 校验生成多项式采用 CRC16-CCITT (0x1021), $x^{16}+x^{12}+x^5+1$ 。

Segment Data: 该帧传输的文件内容, 长度为 L 字节。实际传输时, 不足 4 字节的倍数时通过末尾补 0x00 的方式补充为 4 字节的整数倍。

State: 0 表示成功; 1 表示失败, 失败原因见 Reason。

Reason: 取值含义请参见“异常状态代码”。

6.3.3.6.3 查询处理进度

查询处理进度见表19。

表19 查询处理进度

方向	主控设备下发到模组	模组应答
Fn	03H	03H
Data	Rsv (3byte)	State (1byte)
		Fail STAs (2byte)

说明:

State: 文件处理进度: 0 全部成功; 1 正在处理, 不能接收新文件; 2 未全部成功, 存在失败节点。

Fail STAs: 失败节点数。

6.3.3.6.4 配置升级列表

配置升级列表见表20。

表20 配置升级列表

方向	主控设备下发到模组	模组应答
Fn	04H	04H
Data	Mac Cnt (1bytes)	State (1byte)
	Mac List (6 * N Bytes)	Reason (1byte)
		Rsv (1byte)

说明：
Mac Cnt：升级列表个数；
Mac List：升级列表
State：0 表示成功；1 表示失败，失败原因见 Reason。
Reason：取值含义请参见“异常状态代码”。
注：此指令为在列表升级时用于配置 STA 升级列表，本地升级和全网升级时无效。

6.3.3.7 读取模块上电时间（0007H）

读取模块上电时间见表21。

表21 读取模块上电时间

方向	主控设备下发到模组	模组应答
Cmd	0007H	0007H
Data	本次查询报文序号（2byte）	MAC(6 byte)
		frame_index(2 byte)
		on_power_ms_time (4 byte)

说明：
MAC：本站点 MAC 地址。
frame_index 本次查询报文序号。
on_power_ms_time 站点 上电时间，单位 ms。

6.3.3.8 读取白名单中节点数量（0010H）

读取白名单中节点数量见表22。

表22 读取白名单中节点数量

方向	主控设备下发到模组	模组应答
Cmd	0010H	0010H
Data	空	节点数量（2bytes）
		保留（2bytes）0000H

6.3.3.9 读取白名单中节点信息（0011H）

读取白名单中节点信息见表23。

表23 读取白名单中节点信息

方向	主控设备下发到模组	模组应答
Cmd	0011H	0011H
Data	Start Seq (2Bytes)	Total (2Bytes)
		Start Seq (2Bytes)
	Req Cnt (2Bytes)	Ind Cnt (2Bytes)
		保留（2bytes）0000H
		Ind Data (6 * N Bytes)

说明：
Start Seq：起始序号，从 0 开始。
Req Cnt：本次查询的节点数量。
Total：白名单中节点总数量。

Ind Cnt: 本次应答的节点数量。

Ind Data: 本次应答的白名单数据, 每个节点 6 个字节 (大端)。

6.3.3.10 添加节点到白名单 (0012H)

添加节点到白名单见表24。

表24 添加节点到白名单

方向	主控设备下发到模组	模组应答
Cmd	0012H	0012H
Data	Req Cnt (2bytes)	State (1byte)
	Req Data (6 * N Bytes)	Reason (1byte), 见 5.3.6
		Rsv (2bytes)

说明:

Req Cnt: 本次设置的节点数量。

Req Data: 本次设置的白名单节点数据, 每个节点 6 个字节 (大端)。

State: 0 表示成功; 1 表示失败, 失败原因见 Reason。

Reason: 取值含义请参见“异常状态代码”。

6.3.3.11 删除白名单中节点 (0013H)

删除白名单节点见表25。

表25 删除白名单中节点

方向	主控设备下发到模组	模组应答
Cmd	0013H	0013H
Data	Req Cnt (2bytes)	State (1byte)
	Req Data (6 * N Bytes)	Reason (1byte), 见 5.3.6
		Rsv (2bytes)

说明:

Req Cnt: 本次删除的节点数量。

Req Data: 本次删除的白名单节点数据, 每个节点 6 个字节 (大端)。

State: 0 表示成功; 1 表示失败, 失败原因见 Reason。

Reason: 取值含义请参见“异常状态代码”。

6.3.3.12 清空白名单 (0014H)

清空白名单见表26。

表26 清空白名单

方向	主控设备下发到模组	模组应答
Cmd	0014H	0014H
Data	空	State (1byte)
		Reason (1byte), 见 5.3.6
		Rsv (2bytes)

说明:

State: 0 表示成功; 1 表示失败, 失败原因见 Reason。

Reason: 取值含义请参见“异常状态代码”。

6.3.3.13 自组网功能开启 (0015H)

自组网功能开启见表27。

表27 自组网功能开启

方向	主控设备下发到模组	模组应答
Cmd	0015H	0015H
Data	空	ret_code (1byte)
		reason (1 byte)
		reserved (2 byte)

注: 本命令只能在 CC0 端操作, 操作后需要重启生效, 自组网结束后自组网功能自动关闭。

Data 域字段说明:

ret_code: 清除结果。0 表示成功; 1 表示失败, 失败原因见 Reason。

Reason: 取值含义请参见“异常状态代码”。

reserved: 保留。

6.3.3.14 设置白名单状态 (0016H)

设置白名单状态见表28。

表28 设置白名单状态

方向	主控设备下发到模组	模组应答
Cmd	0016H	0016H
Data	Whitelist State (1byte)	State (1Bte)
	Rsv (3bytes)	Rsv (3bytes)

说明:

Whitelist State: 白名单状态, 0 表示关闭白名单, 1 表示开启白名单。

State: 0-表示成功; 1-表示失败。

6.3.3.15 获取白名单状态 (0017H)

获取白名单状态见表29。

表29 获取白名单状态

方向	主控设备下发到模组	模组应答
Cmd	0017H	0017H
Data	空	Whitelist State (1bte)
		Rsv (3bytes)

说明:

Whitelist State: 白名单状态, 0 表示白名单为关闭状态, 1 表示白名单为开启状态。

6.3.3.16 读取拓扑中节点数量 (0020H)

读取拓扑中节点数量见表30。

表30 读取拓扑中节点数量

方向	主控设备下发到模组	模组应答
Cmd	0020H	0020H
Data	空	节点数量 (2bytes)
		保留 (2bytes) 0000H

6.3.3.17 读取拓扑中节点信息 (0021H)

读取拓扑中节点信息见表31，应答的拓扑数据见表32。

表31 读取拓扑中节点信息

方向	主控设备下发到模组	模组应答
Cmd	0021H	0021H
Data	Start Seq (2Bytes)	Total (2Bytes)
		Start Seq (2Bytes)
	Req Cnt (2Bytes)	Ind Cnt (2Bytes)
		Rsv (2bytes) 0000H
		Ind Data (12 * N Bytes)

说明：

Start Seq：起始序号，从 1 开始，其中 1 为主节点，后续为从节点。每次查询必须从序号 1 起始查询。

Req Cnt：本次查询的节点数量。

Total：拓扑中节点总数量。

Ind Cnt：本次应答的节点数量。

Ind Data：本次应答的拓扑数据，每个节点 11 个字节。格式如表 32：

表32 应答的拓扑数据

数据内容	格式	字节数
MAC Addr	BIN	6
Tei	BIN	2
Proxy Tei	BIN	2
Node Info	BIN	1
Rsv	BIN	1

说明：

MAC Addr：6 字节，大端序。

Tei：本节点的节点标识，最大不超过 512。

Proxy Tei：本站点的代理站点节点标识

Node Info：节点信息，[3:0]代表本站点的网络层级，0 代表 0 层级，依次类推；[7:4]表示本站点的网络角色，0 无效，1 表示末梢节点 (STA)，2 表示代理节点，3 保留，4 表示主节点。

6.3.4 信道转发命令详细说明

信道转发命令通过模组转发数据到对端设备，数据交互流程见图7。

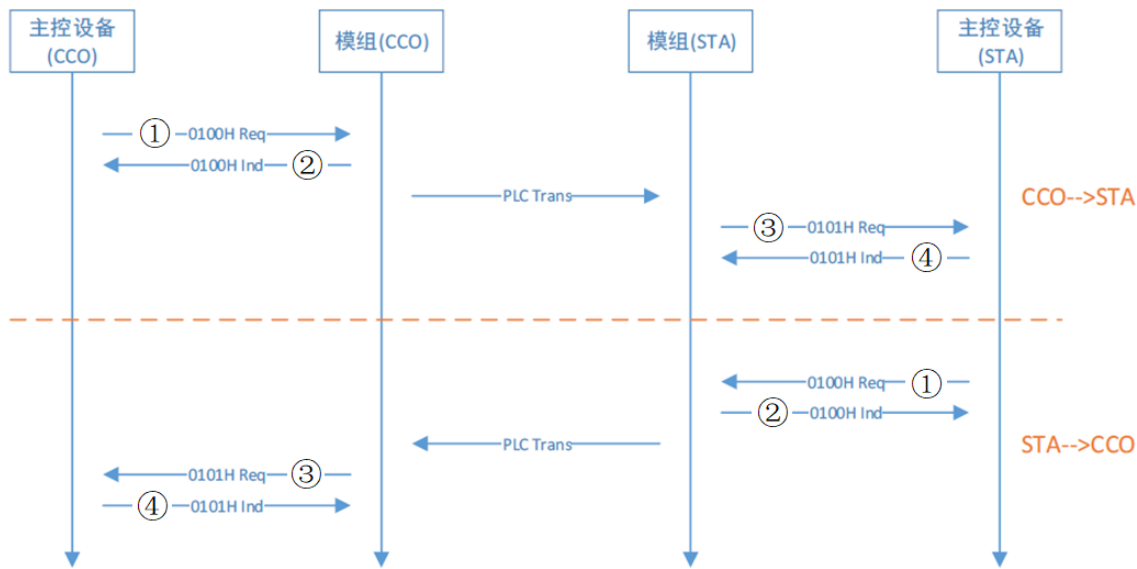


图7 信道转发命令数据交互流程

6.3.4.1 发送数据（0100H）

当主控设备需要发送报文给模组时，使用此格式，见表33。

表33 发送数据

方向	主控设备下发到模组	模组应答
Cmd	0100H ①	0100H ②
Data	Dest Addr (6bytes)	State (1byte)
	User Data Len (2bytes)	Reason (1byte)
	User Data	Rsv (2bytes)

说明：
Dest Addr：对端目的设备 MAC 地址；FF FF FF FF FF FF 表示全网广播。
User Data Len：User Data 数据长度，最大值为 488。
User Data：待发送的用户数据。
State：0 表示成功；1 表示失败，失败原因见 Reason。
Reason：取值含义请参见“异常状态代码”。

6.3.4.2 接收数据（0101H）

当模组需要发送报文给主控设备时，使用此格式，见表34。

表34 接收数据

方向	模组发送到主控设备	主控设备应答
Cmd	0101H ③	0101H ④
Data	Src Addr (6bytes)	State (1byte)
	User Data Len (2bytes)	Reason (1byte)
	User Data	Rsv (2bytes)

说明：
Src Addr：发送数据设备的 MAC 地址。

User Data Len: User Data 数据长度。
User Data: 待发送的用户数据。
State: 0 表示成功; 1 表示失败, 失败原因见 Reason。
Reason: 取值含义请参见“异常状态代码”。

6.3.5 远程调测命令

远程命令是通过中心节点转发本地命令到远程节点, 用于远程调试时通过CCO发送指令到STA。数据交互流程如图8所示。

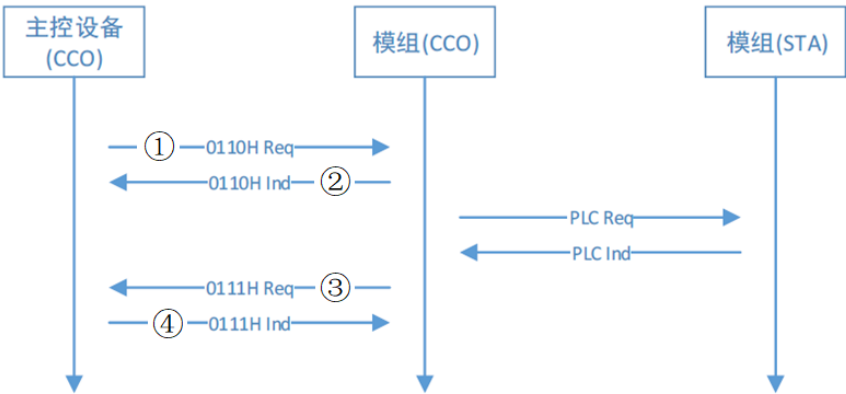


图8 远程调测命令数据交互流程

6.3.5.1 远程发送命令 (0110H)

远程发送命令见表35。

表35 远程发送命令

方向	主控设备下发到模组	模组应答
Cmd	0110H ①	0110H ②
Data	Dest Addr (6bytes)	State (1byte)
	User Data Len (2bytes)	Reason (1byte)
	User Data	Rsv (2bytes)

说明:
Dest Addr: 目的设备 MAC 地址; FF FF FF FF FF FF 表示全网广播。
User Data Len: User Data 数据长度。
User Data: 待转发的本地通信命令。
State: 0 表示成功; 1 表示失败, 失败原因见 Reason。
Reason: 取值含义请参见“异常状态代码”。

6.3.5.2 远程接收命令 (0111H)

远程接受命令见表36。

表36 远程接收命令

方向	模组发送到主控设备	主控设备应答
Cmd	0111H ③	0111H ④
Data	Src Addr (6bytes)	State (1byte)
	User Data Len (2bytes)	Reason (1byte)
	User Data	Rsv (2bytes)

说明：
Src Addr：发送数据设备的 MAC 地址。
User Data Len：User Data 数据长度。
User Data：待转发的本地通信命令应答。
State：0 表示成功；1 表示失败，失败原因见 Reason。
Reason：取值含义请参见“异常状态代码”。

6.3.5.3 调测支持的本地命令

调测支持的本地命令见表37。

表37 调测支持的本地命令

Cmd	说明
0001H	读取模组版本信息
0002H	读取模组 MAC 地址
0003H	读取模组通信地址
0004H	设置模组通信地址
0005H	模组重启
0006H	传输文件

6.3.6 系统控制数据通信命令

系统控制数据通信命令是在信道转发命令的基础上，简化其通信流程。数据交互流程如图9所示：

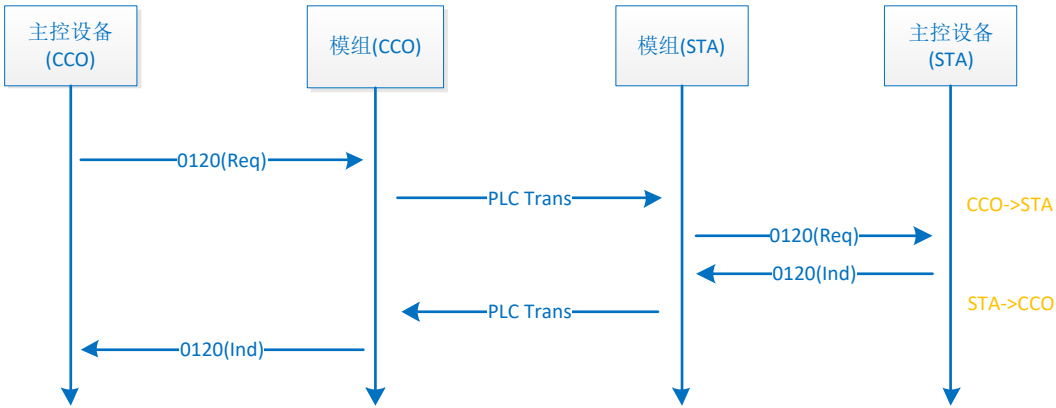


图9 系统控制数据通信命令数据交互流程

6.3.6.1 系统控制数据通信命令（0120H）

系统控制数据通信命令见表38。

表38 系统控制数据通信命令

方向	主控设备 (CC0) 到主控设备 (STA)	主控设备 (STA) 到主控设备 (CC0)
Cmd	0120H ①	0120H ②
Data	Dest Addr (6bytes)	Src Addr (6bytes)
	User Data Len (2bytes)	User Data Len (2bytes)
	User Data	User Data

说明：
Dest Addr：对端目的设备 MAC 地址；FF FF FF FF FF FF 表示全网广播。
User Data Len：User Data 数据长度。
User Data：待发送的用户数据。

6.3.7 异常状态代码

异常状态代码见表39。

表39 异常状态代码

取值	说明
00H	状态正常
01H	通信超时
02H	错误的格式
03H	节点忙
FFH	其它错误

6.4 PLC 应用报文

6.4.1 PLC ID

PLC ID见表40。

表40 PLC ID

取值	说明
50H	数据转发
51H	远程命令
55H	系统控制数据通信

6.4.2 报文格式

PLC应用报文格式如表41所示：

表41 PLC 应用报文格式

长度 (byte)	2	2	L
含义	CRC	L	User Data

说明：
CRC：User Data 的 CRC16 校验和，从帧头开始到 Data 段结束。CRC 校验生成多项式采用 CRC16-CCITT(0x1021)， $x^{16}+x^{12}+x^5+1$ 。
L：User Data 长度。

User Data：待发送的报文。

7 系统控制协议

7.1 数据交互流程

系统由受控设备和控制设备组成，以下以照明系统作为参考。PLC网关由主控处理器和PLC模组组成，主控处理器与PLC模组之间通过UART串口进行通信。其他控制设备的主控单元可以是PLC模组，也可以是PLC模组加外挂处理器。当控制设备的主控单元是PLC模组时，PLC模组需完成控制设备的全部通信和控制功能。当控制设备的主控单元是PLC模组加外挂处理器时，PLC模组通信数据通过UART接口与处理器进行通信，处理器完成数据处理和控制功能。

主控处理器与PLC模组之间的通信遵循“PLC模组接口协议”。照明系统PLC网关与STA控制设备之间的控制数据包采用协议“6.3.6总线数据通信命令”中的“6.3.6.1总线数据通信命令（0120H）”来完成。命令如图10所示：

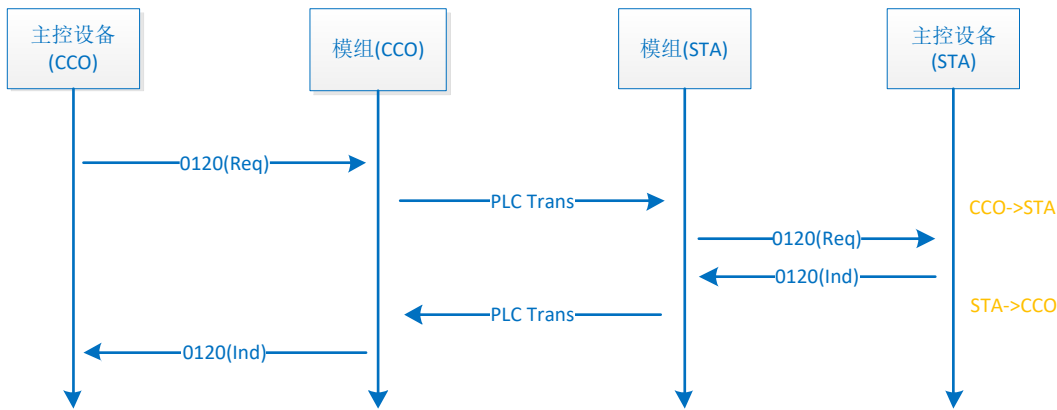


图10 总线数据通信命令数据交互流程

7.2 发送数据

当一个设备需要发送“控制报文”给远端设备时，使用此格式，见表42。

表42 发送数据

方向	主控设备下发到模组	
Cmd	0120H ①	
Data	Dest MAC Addr (6bytes)	
	UserData Len (2bytes)	
	UserData	PLC 协议主版本号 (1byte)
		PLC 协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code (1byte)
		Status Code (1byte)
		DEV Addr (2bytes)
		Data Body

7.3 接收数据

当模组需要转发远端设备发来“控制报文”给主控设备时，使用此格式，见表43。

表43 接收数据

方向	模组发送到主控设备		
Cmd	0120H ③		
Data	Src MAC Addr (6bytes)		
	UserData Len (2bytes)		
	UserData	PLC 协议主版本号 (1byte)	
		PLC 协议次版本号 (1byte)	
		Sequence Number (2bytes)	
		Func Code (1byte)	
		Status Code (1byte)	
		DEV Addr (2bytes)	
		Data Body	

说明:

Cmd: 0120H 是主控设备和模组直接的串口通信命令码。

Dest MAC Addr: 远端目的设备通信 MAC 地址; FF FF FF FF FF FF 表示全网广播。

当 CCO 给 STA 发送报文时, 目的设备通信地址指 STA 的 MAC 地址。

当 STA 给 CCO 发送报文时, 目的设备通信地址指 CCO 的 MAC 地址。

Src MAC Addr: 发送数据设备通信的 MAC 地址。

当 CCO 给 STA 发送报文时, 发送数据设备通信地址指 CCO 的 MAC 地址。

当 STA 给 CCO 发送报文时, 发送数据设备通信地址指 STA 的 MAC 地址。

UserDataLen: UserData 数据长度。

UserData: 待接收的用户数据。是模组 (CCO) 和模组 (STA) 通过 PLC 通信传输的系统控制协议报文。

PLC 协议主/次版本号: 用于 PLC 协议版本兼容性扩展预留, 需要根据 PLC 协议版本解析响应报文。当前分别为 1 和 0。

Sequence Number: 网关 CCO 向 STA 发送报文的递增序号, STA 在响应报文时返回此序号, 用于网关标识报文响应。

Fun Code: 功能码, 用于定义该指令的操作功能。

Status Code: 状态码, 用于定义该指令应答状态, 详见下文表 46。

State: 0 表示成功; 1 表示失败, 失败原因见 Reason。

Reason: 取值含义请参见“异常状态代码”。

DEV Addr: 设备应用地址。

Data Body: 功能命令数据。

7.3.1 功能码 (Func Code)

功能码见表44。

表44 功能码格式

B7	B6	B5	B4	B3	B2	B1	B0
F	x						

说明:

“F” 数据方向位:

“F” =0 表示数据帧来自发起设备。

“F” =1 表示数据帧来自响应设备。

“x” 表示功能代码。

功能码具体定义见表 45，Status Code 响应状态码定义见表 46。

表45 功能码具体定义

发起设备 Func Code	功能名称	响应设备 Func Code
0x01	查询设备信息	0x81
0x02	写入设备应用地址	0x82
0x03	读取设备应用地址	0x83
0x04	添加 N 个组地址	0x84
0x05	读取全部组地址	0x85
0x06	删除 N 个组地址	0x86
0x07	写入设备属性	0x87
0x08	读取设备属性	0x88
0x09	上报设备属性	0x89
0x0A	上报设备事件	0x8A
0x0B	N 个设备添加/删除 1 个组地址	0x8B
0x0C	设置场景	0x8C
0x0D	查询场景校验值	0x8D
0x0E	执行场景	0x8E
0x0F	删除场景	0x8F
0x10	获取心跳	0x90
0x11	重启设备	0x91
0x12	转发报文	不响应

表46 Status Code 响应状态码定义

Status Code	描述
0x00	成功
0x01	无法解析此请求
0x02	设备控制受限中
0x03	属性不可读
0x04	属性不可写
0x05	参数值错误
0x06	未定义

说明：

接收端按照上面的响应状态定义返回 Status Code 信息。

发送端的 Status Code 用于保留承载特殊指令，目前使用了 Bit0 和 Bit1。

Bit0：表示控制目标设备不响应报文，“1”不回应，用于避免批量设备响应导致信道拥塞；“0”回应，用于单设备控制；

Bit1：“1”表示控制目标设备收到指令后的静默时间内（5 秒）不主动上报设备属性变化，静默时间后，直到再次有属性变化才上报，用于避免批量设备同时上报属性变化导致信道拥塞，后续可以通过读设备 属性的命令码获取设备属性；“0”表示允许主动上报属性变化，用于单设备控制；

发送端的 Status Code 示例：

0x00 即 0b00000000（返回响应报文，允许上报属性变化）

0x01 即 0b00000001（不返回响应报文，允许上报属性变化）

0x03 即 0b00000011（不返回响应报文，此时不上报属性变化）

Data Type数据类型长度列表定义见表47，应用地址（DEV Addr）范围定义见表48。

表47 Data Type 数据类型长度列表定义

Data Type	数据类型	Data Value 长度值 (byte)	取值范围	描述
0x0001	int	4	-2147483648~2147483647	整数
0x0002	Bool	1	0, 1	布尔
0x0003	string	n 可变长度		字符串
0x0004	emun	1	0—255	枚举
0x0005	array	n 可变长度		数组

表48 应用地址（DEV Addr）范围定义

DEV Addr	应用地址定义
0x0000	保留
0x0001~0x000F	保留给 CCO 使用
0x0010~0x03FF	通过设备标识被分配使用的设备应用地址，
0x0400~0x07FF	无设备标识被分配使用的设备应用地址
0x0800~0x0BFF	设备标识冲突后被分配使用的设备应用地址
0x4000~0x40FF	组播地址（网关支持 256 个组，终端设备存储 32 个组）
0x4100~0xFFFFD	保留
0xFFFFE	出厂未分配应用地址时的值
0xFFFFF	广播地址

在 PLC 总线网络内每个设备需要一个应用地址（2 字节），不同于物理地址，应用地址对应用层提供可见的逻辑地址，方便设备的管理和数据的传输。在 PLC 设备处于应用状态时（非配置状态），使用 MAC 广播寻址方式，并通过使用应用地址在网络中提供单播、组播和广播的通信控制。

7.4 功能命令详解

7.4.1 查询设备信息（Func Code =0x01）

PLC网关（CCO）查询某个（STA）设备信息，低字节在前，高字节在后，见表49。

表49 查询设备信息

方向	主控设备MCU下发到CCO模组		
Cmd	0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (STA MAC Addr)
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x01
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	0x0000

（STA）设备响应，把应用地址(2BYTES)反馈给CCO。
查询设备信息响应见表50。

表50 查询设备信息响应

方向	设备MCU下发到STA模组		
Cmd	0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CC0 MAC Addr)
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x81
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr (2bytes)	xx xx
		Data Type (2bytes)	0x03 (String)
		Data Len (2bytes)	xx xx
		Dev Infor String (nbytes)	设备信息字符串，格式为： key:value,key:value

设备信息字符串

返回设备信息由ASCII字符串组成，格式为：key:value,key:value，key和value直接使用英文冒号分割，两组之间使用英文逗号分割，字符串总长度不超过476。

示例：

sn:12345678,prodId:1234,model:Model5,devType:075,manu:123,mac:00D8613E897B,hiv:1.0.0,fwv:1.0.0,hwv:1.0.0,swv:1.0.0,protType:1,subProdId:01,devCode:01

设备信息字段说明见表51。

表51 设备信息字段说明

设备信息 key 名称	设备信息 value 说明	是否必填	设备信息 value 示例
sn	设备唯一标识，比如 sn 号，长度范围 (0, 40]	是	12345678
prodId	设备产品 ID，即 ProductId，长度为 4	是	1234
model	设备型号，长度范围 (0, 32]	是	Model5
devType	设备类型 ID，长度为 3，详见附件 2	是	075
manu	设备制造商 ID，长度为 3，详见附件 3	是	123
mac	设备 MAC 地址，固定 12 字节	是	00D8613E897B
hiv	设备协议版本，长度范围 (0, 32]	是	1.0.0
fwv	设备固件版本，长度范围 [0, 64]	是	1.0.0
hwv	设备硬件版本，长度范围 [0, 64]	是	1.0.0
swv	设备软件版本，长度范围 [0, 64]	是	1.0.0
protType	设备协议类型，取值范围 [1, 3]	是	1
subProdId	设备子型号 ID，长度为 2，如果不支持则不返回此字段	可选	01
devCode	设备标识编码，长度为 4，范围 0001~FFFF，使用 Hex String 表示两个字节的四位，例如：0010 表示十进制的 16，如果不支持则不返回此字段	可选	0010

7.4.2 写入设备应用地址 (Func Code =0x02)

PLC网关（CC0）远程对设备（STA）写入应用地址DEV Addr（2bytes），低字节在前，高字节在后，写入设备应用地址见表52。

表52 写入设备应用地址

方向	主控设备MCU下发到CC0模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (STA MAC Addr)
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x02
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx

远程设备（STA）响应，把应用地址(2BYTES)反馈给CC0。写入设备应用地址响应见表53。

表53 写入设备应用地址响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CC0 MAC Addr)
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x82
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr (2bytes)	xx xx

7.4.3 读取设备应用地址（Func Code =0x03）

PLC网关（CC0）读取某个远程设备（STA）应用地址，低字节在前，高字节在后，读取设备应用地址见表54。

表54 读取设备应用地址

方向	主控设备MCU下发到CC0模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (STA MAC Addr)
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x03
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	0000

远程设备（STA）响应，把应用地址(2bytes)反馈给CC0。读取设备应用地址响应见表55。

表55 读取设备应用地址响应

方向	设备MCU下发到STA模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CC0 MAC Addr)
	UserData Len (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code (1byte)
		Status Code (1byte)
		DEV Addr (2bytes)

7.4.4 添加N个组地址（Func Code =0x04）

PLC网关（CC0）远程对单个设备（STA）写入N个组地址Group Addr（1个组地址2bytes）。添加N个组地址见表56。

表56 添加N个组地址

方向	主控设备MCU下发到CC0模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (STA MAC Addr)
	UserData Len (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code (1byte)
		Status Code (1byte)
		DEV Addr (2 bytes)
		Group Number (2bytes)
		Group Addr1 (2bytes)
		Group Addr2 (2bytes)
		
		Group AddrN (2bytes)

远程设备（STA）在写入组地址后，给CC0的响应报文。添加N个组地址响应见表57。

表57 添加 N 个组地址响应

方向	设备MCU下发到STA模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CC0 MAC Addr)
	UserData Len (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code(1bytes)
		Status Code (1byte)
		DEV Addr (2 bytes)

7.4.5 读取全部组地址 (Func Code =0x05)

PLC网关 (CC0) 远程读取某个设备 (STA) 全部组地址Group Addr (2bytes)。见表58。

表58 读取全部组地址

方向	主控设备MCU下发到CC0模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (STA MAC Addr)
	UserData Len (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code (1byte)
		Status Code (1byte)
		DEV Addr (2bytes)

说明：
远程设备 (STA) 给CC0的响应报文。
读取全部组地址响应见表59。

表59 读取全部组地址响应

方向	设备MCU下发到STA模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CC0 MAC Addr)
	UserDataLen (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code(1bytes)
		Status Code (1byte)
		DEV Addr (2 bytes)
		Group Number (2byte)
		Group Addr1 (2bytes)
		Group Addr2 (2bytes)
		
		Group AddrN (2bytes)

7.4.6 删除N个组地址 (Func Code =0x06)

PLC网关 (CC0) 删除某个远程设备 (STA) 的N个组地址, 低字节在前, 高字节在后, 删除N个组地址见表60。

表60 删除N个组地址

方向	主控设备MCU下发到CC0模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (STA MAC Addr)
	UserData Len (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code (1byte)
		Status Code (1byte)
		DEV Addr (2 bytes)
		Group Number (2byte)
		Group Addr1 (2bytes)
		Group Addr2 (2bytes)
		
		Group AddrN (2bytes)

远程设备 (STA) 给CC0的响应报文。
删除N个组地址响应见表61。

表61 删除 N 个组地址响应

方向	设备MCU下发到STA模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CC0 MAC Addr)
	UserDataLen (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code(1bytes)
		Status Code (1byte)
		DEV Addr (2 bytes)

7.4.7 写入设备属性 (Func Code =0x07)

PLC网关 (CC0) 单播或广播方式对设备写入多组属性参数，受控设备 (STA) 地址可以是单地址、组地址或广播地址，写入设备属性见表62。

表62 写入设备属性

方向	主控设备MCU下发到CC0模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	广播: FF FF FF FF FF FF 单播: xx xx xx xx xx xx (STA MAC Addr)
	UserData Len (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code (1byte)
		Status Code (1byte)
		DEV Addr (2bytes)
		SIID (2bytes)
		CIID (2bytes)
		Data Type (2byte)
		Data Len (2bytes)
		Data Value (n byte)
		...
		SIID (2bytes)
		CIID (2bytes)
		Data Type (2byte)
		Data Len (2bytes)
		Data Value (n byte)

说明:

SIID: 服务(service) ID, 用来表示设备中用户可使用的功能函数, 其中包含实现该函数输出/输入的数据以及实现该函数的行为。

CIID: 属性(characteristic) ID, 表示数据或相关行为的特征, 名称之为属性名, 是Service 的

基本组成单元，如开关的开或关特性。

远程设备（STA）给 CC0 的响应报文，写入设备属性响应见表 63。

表63 写入设备属性响应

方向	设备MCU下发到STA模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CC0 MAC Addr)
	UserDataLen (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code (1bytes)
		Status Code (1byte)
		DEV Addr (2 bytes)

7.4.8 读取设备属性（Func Code =0x08）

PLC网关（CC0）单播或广播方式读某个（DEV ADDR）设备多个属性参数到CC0，读取设备属性见表64。

表64 读取设备属性

方向	主控设备MCU下发到CC0模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes) ^a	
	广播：FF FF FF FF FF FF 单播：xx xx xx xx xx xx (STA MAC Addr)	
	UserData Len (2bytes)	
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code (1byte)
		Status Code (1byte)
		DEV Addr (2bytes)
		SIID (2bytes)
		CIID (2bytes)
		
		SIID (2bytes)
		CIID (2bytes)

注：Dest MAC Addr 目标地址可以是广播地址，也可以是 STA 的 MAC 地址。当不填写 SIID 和 CIID 时，表示要求返回所有服务和属性的值。

远程设备（STA）给 CC0 的响应报文。
读取设备属性响应见表 65。

表65 读取设备属性响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CC0 MAC Addr)
	UserDataLen (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x88
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr(2bytes)	xx xx
		SIID (2bytes)	
		CIID (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	
			
		SIID (2bytes)	
		CIID (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	

7.4.9 上报设备属性（Func Code =0x09）

STA设备（DEV ADDR）上报属性数据给CC0，上报设备属性见表66。

表66 上报设备属性

方向	主控设备MCU下发到STA模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CCO MAC Addr)
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x09
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr(2bytes)	0x00
		SIID (2bytes)	
		CIID (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (nbyte)	
			
		SIID (2bytes)	
		CIID (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (nbyte)	

CCO 给远程设备（STA）的响应报文，上报设备属性响应见 67。

表67 上报设备属性响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		FF FF FF FF FF FF
	UserDataLen (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x89
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr(2bytes)	xx xx

7.4.10 上报设备事件（Func Code =0x0A）

STA设备（DEV ADDR）上报事件数据给CCO，上报设备时间见表68。

表68 上报设备事件

方向	主控设备MCU下发到STA模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CC0 MAC Addr)
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x0A
		Status Code (1byte)	0x00
		DEV Addr(2bytes)	xx xx
		SIID (2bytes)	
		CIID (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	
			
		SIID (2bytes)	
		CIID (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	

CC0 给远程设备（STA）的响应报文，上报设备事件响应见表 69。

表69 上报设备事件响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		FF FF FF FF FF FF
	UserDataLen (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x8A
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr(2bytes)	xx xx

7.4.11 N 个设备添加/删除 1 个组地址 (Func Code =0x0B)

PLC网关（CC0）对远程N个设备（STA）添加或删除1个组地址Group Addr (2bytes)，N个设备添加/删除1个组地址见表70。

表70 N 个设备添加/删除 1 个组地址

方向	主控设备MCU下发到CCO模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	FF FF FF FF FF FF
	UserData Len (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		xx
		PLC协议次版本号 (1byte)
		xx
		Sequence Number (2bytes)
		xx xx
		Func Code (1byte)
		0x0B
		Status Code (1byte)
		0x00
		DEV Addr (2bytes)
		xx xx
		Group Mode (1byte)
		xx 操作模式 0x00: 表示添加组时需要持久化 0x01: 表示添加组时不需要持久化
		Group Action (1byte)
		xx 操作类型 0x01: 表示添加组 0x02: 表示删除组
		Group Addr (2bytes)
		xx xx (添加的组地址)
		Group Dev Number (2bytes)
		xx xx (包含的设备数量)
		DEV Addr1 (2bytes)
		xx xx (第1个设备地址)
		
		DEV AddrN (2bytes)
		xx xx (第N个设备地址)

如果设备数量多，可以通过多个报文设置。
 远程设备（STA）给 CCO 的响应报文，N 个设备添加/删除 1 个组地址响应见表 71。

表71 N 个设备添加/删除 1 个组地址响应

方向	设备MCU下发到STA模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)
	UserDataLen (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		xx
		PLC协议次版本号 (1byte)
		xx
		Sequence Number (2bytes)
		xx xx
		Func Code(1bytes)
		0x8B
		Status Code (1byte)
		0x00 ~ 0x06
		DEV Addr (2bytes)
		xx xx

7.4.12 设置场景 (Func Code =0x0C)

每个受控设备至少可配置多个个场景，场景可通过按键信号、时钟信号、传感器信号等进行触发，场景控制逻辑通过PLC网关进行配置，场景配置信息保存在每个受控设备内，当进行场景控制时，被寻址选中的受控设备可以实现同步响应。
 PLC网关（CCO）对某类型设备（STA）写入若干场景。对不同类型的设备，场景需要分开设置，设置场景见表72。

表72 设置场景

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x0C
		Status Code (1byte)	0x00
		DEV Addr(2bytes)	xx xx
		Scene ID(2byte)	xx xx
		SIID (2bytes)	
		CIID (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	
			
		SIID (2bytes)	
		CIID (2bytes)	
		Data Type (2byte)	
		Data Len (2bytes)	
		Data Value (n byte)	

SIID、CIID 是设备物模型定义中的服务和属性编码。
远程设备（STA）给 CCO 的响应报文，设置场景响应见表 73。

表73 设置场景响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CCO MAC Addr)
	UserDataLen (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code(1bytes)	0x8C
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr (2bytes)	xx xx

7.4.13 查询场景校验值 (Func Code =0x0D)

PLC网关（CCO）查询某个设备（STA）的全部场景校验值，插叙场景校验值见表74。

表74 查询场景校验值

方向	主控设备MCU下发到CC0模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx
	UserData Len (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code (1byte)
		Status Code (1byte)
		DEV Addr(2bytes)

远程设备（STA）给CC0的响应报文，查询场景校验值响应见表75。

表75 查询场景校验值响应

方向	设备MCU下发到STA模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CC0 MAC Addr)
	UserDataLen (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		PLC协议次版本号 (1byte)
		Sequence Number (2bytes)
		Func Code (1byte)
		Status Code (1byte)
		DEV Addr(2bytes)
		CRC 校验码 (2byte)

7.4.14 执行场景 (Func Code =0x0E)

PLC网关（CC0）控制设备（STA）执行某个场景（场景号），执行场景见表76。

表76 执行场景

方向	主控设备MCU下发到CCO模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	FF FF FF FF FF FF
	UserData Len (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		xx
		PLC协议次版本号 (1byte)
		xx
		Sequence Number (2bytes)
		xx xx
		Func Code (1byte)
		0x0E
	Status Code (1byte)	
	0x03 (不返回响应报文, 此时不上报属性变化)	
	DEV Addr(2bytes)	xx xx
	Scene ID(2byte)	xx xx

远程设备 (STA) 给 CCO 的响应报文, 执行场景响应见表 77。

表77 执行场景响应

方向	设备MCU下发到STA模组	
Cmd	0x0120H ①	0x0120
Data	Dest MAC Addr (6bytes)	xx xx xx xx xx xx (CCO MAC Addr)
	UserDataLen (2bytes)	xx xx
	UserData	PLC协议主版本号 (1byte)
		xx
		PLC协议次版本号 (1byte)
		xx
		Sequence Number (2bytes)
		xx xx
		Func Code(1bytes)
		0x8E
	Status Code (1byte)	
	0x00 ~ 0x06	
	DEV Addr (2bytes)	xx xx

7.4.15 删除场景 (Func Code =0x0F)

PLC网关 (CCO) 删除控制设备 (STA) 若干场景, 删除场景见表78。

表78 删除场景

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		FF FF FF FF FF FF
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x0F
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx
Scene ID (2byte)		场景ID, 如果填写0000则表示删除所有场景	

远程设备（STA）给 CCO 的响应报文，删除场景响应见表 79。

表79 删除场景响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		
	xx xx xx xx xx xx (CCO MAC Addr)		
	UserDataLen (2bytes)		
	xx xx		
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code(1bytes)	0x8F
Status Code (1byte)		0x00 ~ 0x06	
DEV Addr (2bytes)		xx xx	

7.4.16 获取心跳 (Func Code =0x10)

PLC网关（CCO）获取设备（STA）心跳信号，控制心跳见表80。

表80 控制心跳

方向	主控设备MCU下发到CC0模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		FF FF FF FF FF FF
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x10
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx
Mode (2byte)		xx xx	

远程设备（STA）给 CC0 的响应报文，获取心跳响应见表 81。

表81 获取心跳响应

方向	设备MCU下发到STA模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CC0 MAC Addr)
	UserDataLen (2bytes)		0x0006
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code(1bytes)	0x90
		Status Code (1byte)	0x00 ~ 0x06
		DEV Addr(2bytes)	xx xx

Mode 设备心跳响应模式：

0x00 00：即时响应，设备收到报文后立即返回响应报文，通常用于查询单个设备的心跳。

0x01 06：随机延时响应，第一个字节为 0x01 表示设备随机延时响应，第二个字节的值 x 乘以 10 表示随机延时的最大秒数，范围是[10, 2550]秒，例如：0x06 表示 x=6，6*10=60 秒，CC0 广播控制心跳报文，设备收到此报文之后，生成小于 1 的随机数*60，使所有设备在 0-60 秒范围内返回心跳结果，通过此方式减少 CC0 的心跳查询报文，同时分散设备的响应报文，避免同时响应导致网络拥塞。

7.4.17 重启设备（Func Code =0x11）

PLC网关（CC0）控制设备（STA）重启。可以单控、组控、广播，重启设备见表82。

表82 重启设备

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		FF FF FF FF FF FF
	UserData Len (2bytes)		xx xx
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x11
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx

远程设备 (STA) 给CCO的响应报文，重启设备响应见表83。

表83 重启设备响应

方向	设备MCU下发到STA模组			
Cmd	0x0120H ①		0x0120	
Data	Dest MAC Addr (6bytes)		xx xx xx xx xx xx (CC0 MAC Addr)	
	UserDataLen (2bytes)		xx xx	
	UserData	PLC协议主版本号 (1byte)		xx
		PLC协议次版本号 (1byte)		xx
		Sequence Number (2bytes)		xx xx
		Func Code(1bytes)		0x91
		Status Code (1byte)		0x00 ~ 0x06
DEV Addr (2bytes)		xx xx		

7.4.18 转发报文 (Func Code =0x12)

子设备A (STA) 通过CCO转发报文给予设备B (STA)，转发报文见表84。

表84 转发报文

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①	0x0120	
Data	Dest MAC Addr (6bytes)		
	FF FF FF FF FF FF		
	UserData Len (2bytes)		
	xx xx		
	UserData	PLC协议主版本号 (1byte)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x12
		Status Code (1byte)	0x00
		DEV Addr(2bytes)	xx xx
		Source DEV Addr (2bytes)	xx xx
		Dest DEV Addr (2bytes)	xx xx
Data Len (2bytes)		xx xx	
Data Value (n bytes)			

不支持返回响应报文。

附录 A
(规范性)
物模型表

附录 A 为各类设备的物模型编码表

- a) CIID 编码见表 A. 1;
- b) SIID 编码见表 A. 2;
- c) E01-05 驱动物模型见表 A. 3;
- d) 064 开关控制器物模型见表 A. 4;
- e) E0A 弱电干触点输出模块物模型见表 A. 5;
- f) 02C 开窗器物模型见表 A. 6;
- g) E31 单窗帘电机物模型见表 A. 7;
- h) E32 双窗帘电机物模型见表 A. 8;
- i) E33 窗帘干接点控制器物模型见表 A. 9;
- j) 075 场景面板物模型见表 A. 10;
- k) 11A 旋钮调光面板物模型见表 A. 11;
- l) E11 空调面板物模型见表 A. 12;
- m) E12 地暖面板物模型见表 A. 13;
- n) E13 新风面板物模型见表 A. 14;
- o) E21 光照度传感器物模型见表 A. 15;
- p) E22 移动型传感器物模型见表 A. 16;
- q) E23 存在型传感器物模型见表 A. 17;
- r) E24 空气质量传感器物模型见表 A. 18;
- s) E31PLC 空调网关物模型见表 A. 19。

表 A.1 CIID 编码表

sid_cid	ciid(HEX:十六进制)	ciid(DEC:十进制)	属性名称	数据类型
_on	0x0001	1	on	bool
_name	0x0002	2	name	string
_alarm	0x0003	3	alarm	bool
_brightness	0x0004	4	brightness	int
_saturation	0x0005	5	saturation	int
_volume	0x0006	6	volume	int
_red	0x0007	7	red	int
_green	0x0008	8	green	int
_blue	0x0009	9	blue	int
_white	0x000A	10	white	int
_bitWidth	0x000B	11	bitWidth	int
_hue	0x000C	12	hue	int
_colorTemperature	0x000D	13	colorTemperature	int
_current	0x000E	14	current	int
_target	0x000F	15	target	int
_level	0x0010	16	level	enum
_direction	0x0014	20	direction	enum
_state	0x0015	21	state	enum
_speed	0x0016	22	speed	int
_angle	0x0017	23	angle	int
_maximumSpeedRpm	0x0018	24	maximumSpeedRpm	int
_speedRpm	0x0019	25	speedRpm	int
_obstructionDetected	0x001F	31	obstructionDetected	bool
_currentState	0x0020	32	currentState	enum
_targetState	0x0021	33	targetState	enum
_mode	0x0022	34	mode	enum
_action	0x0023	35	action	enum
_status	0x0024	36	status	enum
_statusActive	0x0025	37	statusActive	bool
_gear	0x0026	38	gear	enum
_number	0x0027	39	number	int
_id	0x0028	40	id	string
_array	0x0029	41	array	array
_progress	0x002A	42	progress	int
_airQuality	0x0035	53	airQuality	enum
_model	0x003A	58	model	string
_time	0x003B	59	time	int

表A.1 CIID编码表（续）

sid_cid	ciid (HEX:十六进制)	ciid (DEC:十进制)	属性名称	数据类型
_timestamp	0x003C	60	timestamp	int
_dateTime	0x003D	61	dateTime	string
_timeZone	0x003E	62	timeZone	string
_formatter	0x003F	63	formatter	string
_length	0x0040	64	length	int
_width	0x0041	65	width	int
_height	0x0042	66	height	int
_weight	0x0043	67	weight	int
_area	0x0044	68	area	int
_average	0x0047	71	average	int
_instantaneousAccelerati	0x0048	72	instantaneousAcceleration	int
_odometer	0x004A	74	odometer	int
_rangeRemaining	0x004B	75	rangeRemaining	int
_type	0x004C	76	type	int
_longitude	0x004D	77	longitude	int
_latitude	0x004E	78	latitude	int
_altitude	0x004F	79	altitude	int
_accuracy	0x0050	80	accuracy	int
_total	0x0053	83	total	int
_maximum	0x0055	85	maximum	int
_voltage	0x0058	88	voltage	int
_totalConsumption	0x005A	90	totalConsumption	int
_savedConsumption	0x005B	91	savedConsumption	int
_lowPowerAlarm	0x005D	93	lowPowerAlarm	bool
_lowPowerThreshold	0x005E	94	lowPowerThreshold	int
_capacity	0x005F	95	capacity	int
_chargingState	0x0060	96	chargingState	enum
_actualcapacity	0x0062	98	actualcapacity	int
_version	0x0064	100	version	string
_introduction	0x0065	101	introduction	string
_bootTime	0x0067	103	bootTime	int
_intensity	0x0068	104	intensity	enum
_rssi	0x0069	105	rssi	int
_ssid	0x006A	106	ssid	string
_bssid	0x006B	107	bssid	string
_ip	0x006C	108	ip	string
_port	0x006D	109	port	int

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/726050115240010102>