ICS 33.040.50
CCS K 74

T/SILA

上海浦东智能照明联合会团体标准

T/SILA 013—2024

电力线载波通信（PLC）道路照明互联规范

Power Line Communication (PLC) Intercommunication Specification for Road Lighting

2024－01－25 发布　　2024－01－25 实施

上海浦东智能照明联合会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的职责。

本文件由上海浦东智能照明联合会提出并归口。

本文件主要起草单位：上海浦东智能照明联合会、深圳市电力线载波互联技术协会、青岛东软载波科技股份有限公司、厦门市致创能源技术有限公司、北京智芯微电子科技有限公司、海思技术有限公司、杭州联芯通半导体有限公司、中国建筑上海设计研究院有限公司、康体佳智能科技（深圳）有限公司、永林电子（上海）有限公司、深圳市朴联技术有限公司、广州和光同行信息科技有限公司、苏州市高事达科技股份有限公司、浙江感同智联科技有限公司、江苏芯云电子科技有限公司、深圳市力合微电子股份有限公司、上海鸣志电器股份有限公司、深圳微自然创新科技有限公司、威凯检测技术有限公司、佛山市中昊光电科技有限公司、利尔达科技集团股份有限公司、深圳市尚为照明有限公司、深圳市同一方光电技术有限公司、上海时代之光照明电器检测有限公司、上海屹店智能科技有限公司、中智德智慧物联科技集团有限公司、鹤山市耀能路灯管理有限公司、江门市新会区广汇路灯管理有限公司、佛山电器照明股份有限公司、上海物喜智能科技有限公司、上海亚明照明有限公司、广东南方电信规划咨询设计院有限公司、惠州市西顿工业发展有限公司、欧智通科技股份有限公司。

本文件主要起草人：贺海斌、王晓辉、代照亮、洪极慧、陈聪敏、屈佳伟、代洪光、盖宇、康永恒、徐生杰、杨立、陈志辉、况东、王桂光、刘道坤、杨志超、高洋、范金良、郑维杰、程晨、吴丽文、余志铭、朱永、王佳、赖毅平、项逢智、谢毅、刘泳海、刘诗蔚、王孟源、陈晓嘉、庄晓波、安波、张成良、冯朋、张桂春、陈杰明、马焰琳、黄熙、武玉豪、朱华荣、朱晓、张海辉、郑春凌、刘欢、马小平。

电力线载波通信（PLC）道路照明互联规范

1 范围

本文件规定了PLC道路照明互联协议的PLC控制系统技术要求。

本文件适用于道路照明应用中PLC设备之间以及PLC设备与控制设备之间数据交换。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

T/SILA 001 — 2022 电力线载波通信（PLC）全屋互联规范

IEEE Std 1901.1 — 2018 IEEE智能电网应用中频（小于12 MHz）电力线通信标准（IEEE Standard for Medium Frequency (less than 12 MHz) Power Line Communications for Smart Grid Applications）

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

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。控制设备如路灯控制器、集中控制器主机等。

3.2

受控设备 controlled device

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，如单色调光驱动器、双色调光驱动器、彩色调光驱动器等。

3.3

中央协调节点 central coordinator

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

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

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。

3.6

城市路灯控制管理系统主站 urban street light control system

采用物联网通信和宽带电力载波技术进行数据传输和控制，实现城市路灯照明智能控制的管理系统。

3.7

漏电值 leakage value

指电气设备或电路中由于绝缘破损、漏电等原因而流出的非正常电流值。

3.8

MQTT 消息中心 MQTT message center

MQTT消息服务用于路灯控制管理系统对所有智能控制终端设备进行远程控制指令下发、执行回复的消息执行服务。

3.9

MQTT数据服务中心 MQTT data service center

MQTT数据服务中心用于接收智能终端设备的数据采集上报存储、数据挖掘分析。

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：导频符号大小（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

PLC控制系统由主站层、控制管理层、路灯控制层组成，其中路灯控制层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，系统架构见图1。

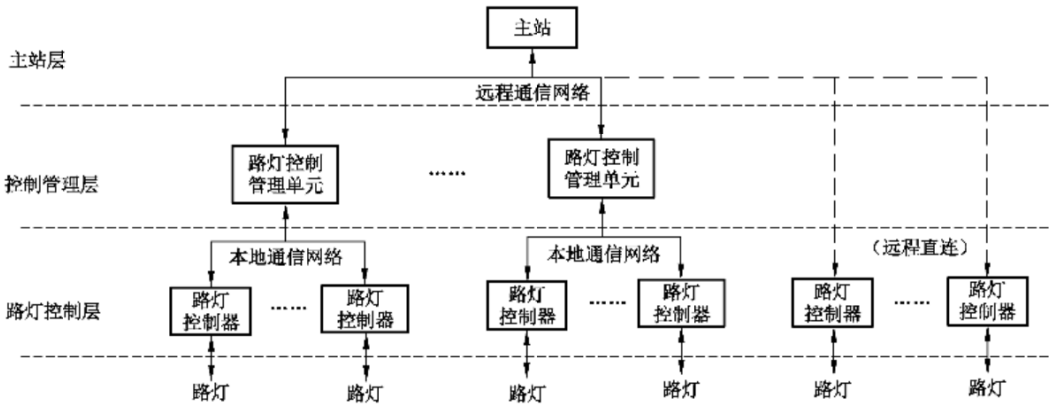


图1　系统架构

本系统基于北向接口规范给出了基于PLC通信技术的城市路灯接入城市路灯控制管理系统主站的协议结构，规定了应用于城市路灯接入城市路灯控制管理系统主站的协议技术要求。

本系统基于PLC应用层构建道路照明互联协议，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，通过物理层发送到电力线载波信道上进行报文通信，网络协议栈层级划分见图2。

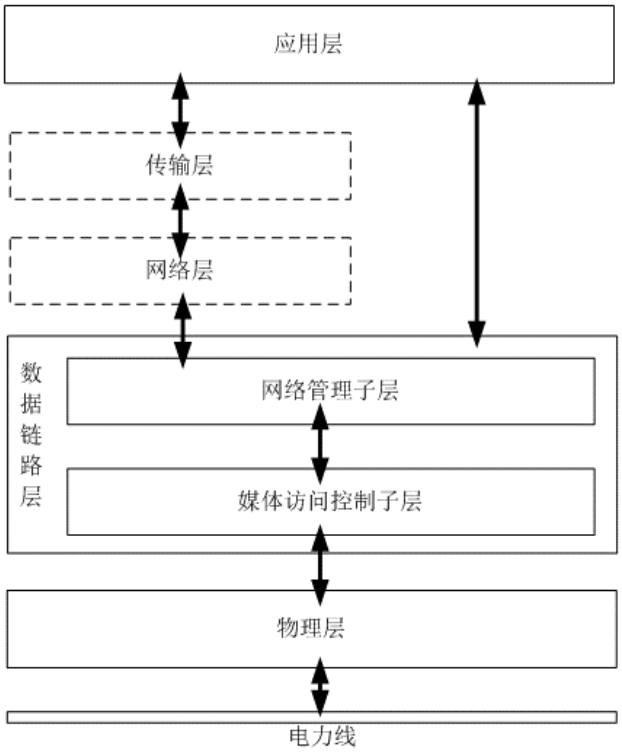


图2　PLC 网络协议栈层级划分图

PLC网络中有三种节点，以CCO（中央协调节点）、PCO（代理协调节点）、STA（终端节点）组成的树形结构，见图3。其通信方式采用中央调度方式，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。

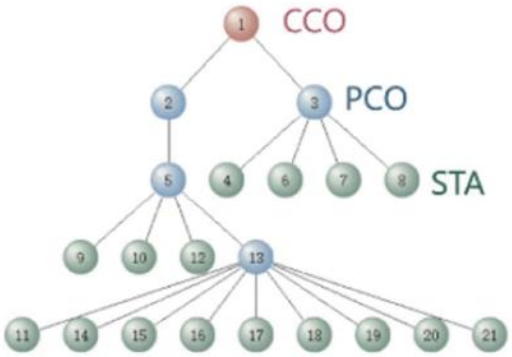


图3　PLC-IoT 树形组网及网络节点

所有STA向CCO发起关联入网请求，CCO确认后方可加入网络，网络建立即可通过PLC通信进行报文传输。站点通信为CCO与STA站点之间的相互通信，STA与STA不能直接通信，需要通过CCO来转发，PLC的自组网过程依据物理层和数据链路层协议实现，无需应用层干预，芯片物理层与链路层互联规范应满足附录D要求。

入网过程：上电后和CCO能直接通信的STA，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代理协调节点非指定，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CCO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即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，用户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-CCO模组、MCU模块。特性如下：

a)　PLC 网关在系统中通过中央协调节点 CCO 进行协议转换与 STA 通信；
b)　具备应用地址配置和管理功能；
c)　具备调光策略配置与控制功能；
d)　具备控制程序逻辑配置与控制功能；
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功能。

调光策略可通过系统时间、传感器信号等进行触发，策略逻辑可在管理系统平台进行编辑，存储于PLC网关，再由PLC网关进行逻辑处理后在规定的条件下控制受控设备进行状态执行。

5.3　系统要求

PLC互联系统的特性如下：

a)　一个子系统至少含一个 CCO 中央协调节点；
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；
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CCO，由CCO根据控制逻辑进行处理，并由CCO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。通过两种方式描述设备具备的特征，服务和属性，设备由若干个服务及其属性组成。

设备服务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。

设备属性表示数据或相关行为的特征，称之为属性名，是service 的基本组成单元，如开关的开或关特性。

5.4.1 实时检测

路灯控制器能对灯开关灯状态、电流值、电压值、功率、功率因数、用电量、漏电值等参数进行监测。

5.4.2 定时开关与调光

路灯控制器能预先设定定时开关灯时间、定时调光、动态调光规则参数，根据设定规则自动开关灯和调光控制管理。

5.4.3 故障检测

路灯控制器能在出现灯源故障、镇流器故障、线路故障等导致灯具不亮实现报警检测与漏电报警，将故障相关数据上传给集中控制器上报平台。设备功能定义模型见图4。

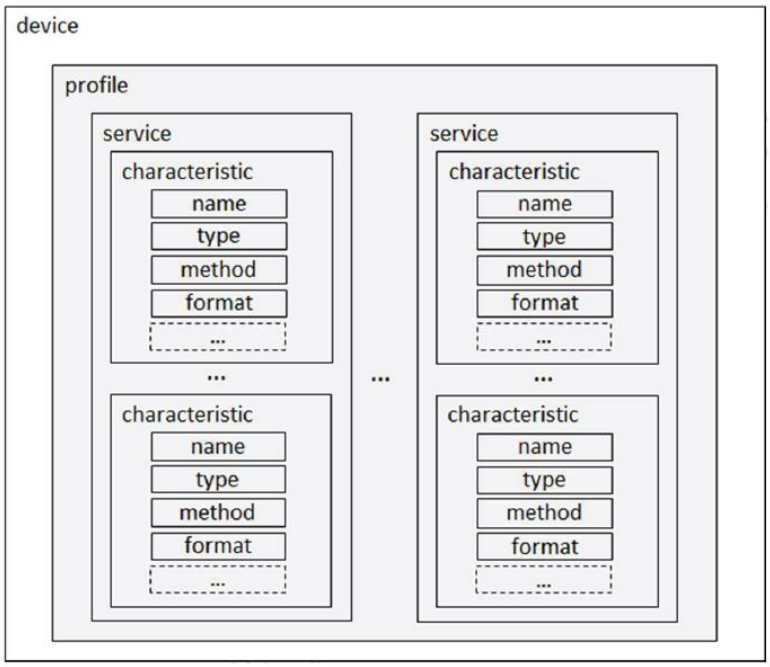


图4 设备功能定义模型

用户通过APP控制设备执行场景时，云端到网关设备的profile数据的格式应按照图5所示格式要求。

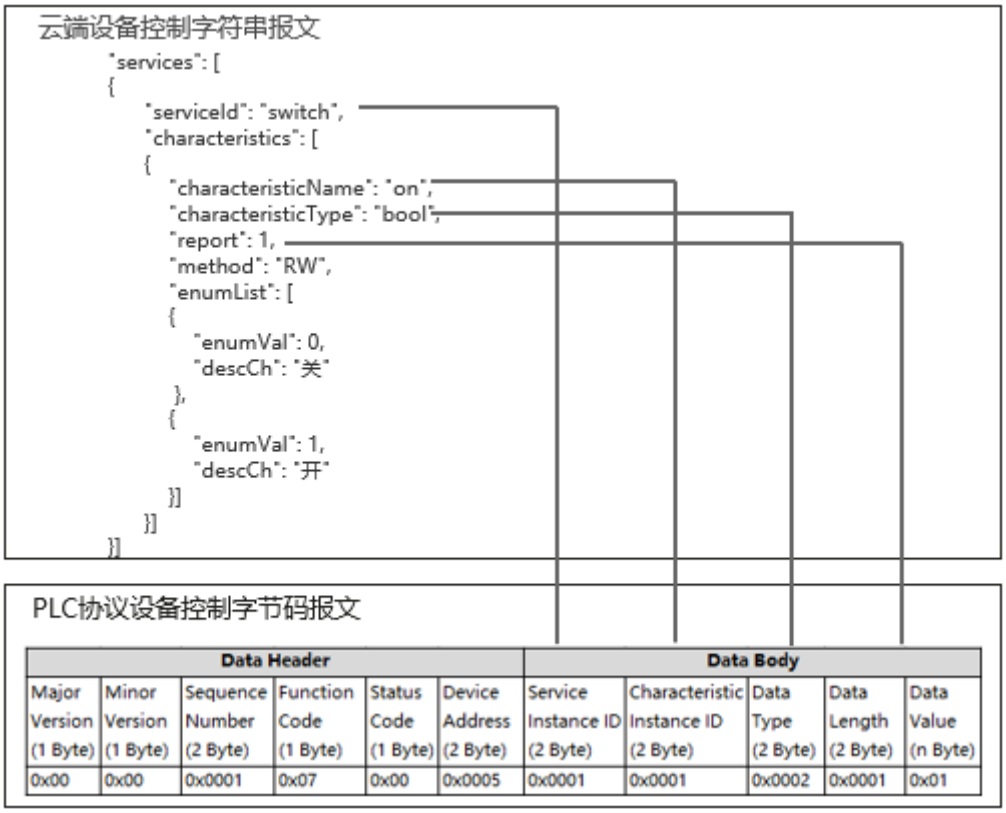


图5　PLC 协议设备控制报文转换

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，0x4000 ～ 0xFFFF 预留给厂商定义私有不通用范围段。

具体的物模型定义参见附录 A。

当 PLC 设备为单灯控制器时，其物模型表见表 1。

表1　单灯控制器

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B59	s_switch	单灯开关	0x1B59	onoff	bool	0-关 1-开	电源开关状态变化上报	必选
0x1B5A	s_dimming	单灯调光	0x1B5A	brightness	int	min:0 max:100 步长：1	亮度值 变化上报	必选
			0x1B5B	color_temperature	int	min:0 max:100 步长：1	色温值 变化上报	可选
0x1B5B	s_realtime_data	单灯实时数据	0x1B59	onoff	bool	0-关 1-开	电源开关状态	必选
			0x1B5A	brightness	int	min:0 max:100	亮度值	必选
			0x1B5B	color_temperature	int	min:0 max:100	色温值	可选

表1　单灯控制器（续）

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B5B	s_realtime_data	单灯实时数据	0x1B5D	voltage	int	min:0 max:10000	总电压 单位0.1V	必选
			0x1B5E	current	int	min:0 max:20000	总电流 单位1mA	必选
			0x1B5F	leak_current	int	min:0 max:20000	总漏电流 单位1mA	必选
			0x1B60	power	int	min:0 max:100000	总功率 单位0.1W	必选
			0x1B61	power_effect	int	min:0 max:1000	总功率因素 单位0.001	必选
			0x1BBC	volt_frequency	int	min:0 max:1000	电压频率 单位0.1Hz	可选
			0x1B62	running_time	int	min:0 max:99999999	总运行时长 单位min	可选
			0x1B63	lighting_time	int	min:0 max:99999999	总亮灯时长 单位min	可选
			0x1B64	asix_x	int	min:-1800 max:1800	x轴倾角 单位0.1°	可选
			0x1B65	asix_y	int	min:-1800 max:1800	y轴倾角 单位0.1°	可选
			0x1B66	asix_z	int	min:-1800 max:1800	z轴倾角 单位0.1°	可选
			0x1BBD	water_det	bool	0-没进水 1-进水	水浸检测	可选
			0x1B67	version_hw	string	长度范围[0,64]	硬件版本号	必选
			0x1B68	version_sw	string	长度范围[0,64]	软件版本号	必选
0x1B5C	s_alarm_threshold	单灯告警阈值	0x1B69	over_volt_threshold	int	min:0 max:10000	过压阈值 单位0.1V 过压上报	可选
			0x1B6A	under_volt_threshold	int	min:0 max:10000	欠压阈值 单位0.1V 欠压上报	可选
			0x1B6B	over_current_threshold	int	min:0 max:20000	过流阈值 单位1mA 过流上报	可选
			0x1B6C	leak_current_threshold	int	min:0 max:20000	漏电流阈值 单位1mA 漏电上报	可选

表1　单灯控制器（续）

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B5C	s_alarm_threshold	单灯告警阈值	0x1B6D	under_power_threshold	int	min:0 max:100000	欠功率阈值 单位0.1W 功率过低上报	可选
			0x1B6E	dip_angle_threshold	int	min:-1800 max:1800	倾角阈值 单位0.1° 倾斜上报	可选

当 PLC 设备为双灯控制器时，其物模型表见表 2。

表2　双灯控制器

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B5F	d_switch	双灯开关	0x1B74	ch1_onoff	bool	0-关 1-开	通道1开关状态变化上报	必选
			0x1B75	ch2_onoff	bool	0-关 1-开	通道2开关状态变化上报	必选
0x1B60	d_dimming	双灯调光	0x1B76	ch1_brightness	int	min:0 max:100 步长：1	通道1亮度值变化上报	必选
			0x1B77	ch1_color_temperature	int	min:0 max:100 步长：1	通道1色温值变化上报	可选
			0x1B78	ch2_brightness	int	min:0 max:100 步长：1	通道2亮度值变化上报	必选
			0x1B79	ch2_color_temperature	int	min:0 max:100 步长：1	通道2色温值变化上报	可选
			0x1B74	ch1_onoff	bool	0-关 1-开	通道1开关状态	必选
			0x1B76	ch1_brightness	int	min:0 max:100	通道1亮度值	必选
			0x1B77	ch1_color_temperature	int	min:0 max:100	通道1色温值	可选
			0x1B75	ch2_onoff	bool	0-关 1-开	通道2开关状态	必选
			0x1B78	ch2_brightness	int	min:0 max:100	通道2亮度值	必选
			0x1B79	ch2_color_temperature	int	min:0 max:100	通道2色温值	可选

表2　双灯控制器（续）

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B61	d_realtime_data	双灯实时数据	0x1B7B	ch1_voltage	int	min:0 max:10000	通道1电压 单位0.1V	可选
			0x1B7C	ch1_current	int	min:0 max:20000	通道1电流 单位1mA	可选
			0x1B7D	ch1_leak_current	int	min:0 max:20000	通道1漏电流 单位1mA	可选
			0x1B7E	ch1_power	int	min:0 max:100000	通道1功率 单位0.1W	可选
			0x1B7F	ch1_power_effect	int	min:0 max:1000	通道1功率因素 单位0.001	可选
			0x1B80	ch1_running_time	int	min:0 max:99999999	通道1运行时长 单位min	可选
			0x1B81	ch1_lighting_time	int	min:0 max:99999999	通道1亮灯时长 单位min	可选
			0x1B82	ch2_consumption	int	min:0 max:99999999	通道2用电量 单位0.01kwh	可选
			0x1B83	ch2_voltage	int	min:0 max:10000	通道2电压 单位0.1V	可选
			0x1B84	ch2_current	int	min:0 max:20000	通道2电流 单位1mA	可选
			0x1B85	ch2_leak_current	int	min:0 max:20000	通道2漏电流 单位1mA	可选
			0x1B86	ch2_power	int	min:0 max:100000	通道2功率 单位0.1W	可选
			0x1B87	ch2_power_effect	int	min:0 max:1000	通道2功率因素 单位0.001	可选
			0x1B88	ch2_running_time	int	min:0 max:99999999	通道2运行时长 单位min	可选
			0x1B89	ch2_lighting_time	int	min:0 max:99999999	通道2亮灯时长 单位min	可选
			0x1B64	asix_x	int	min:-1800 max:1800	x轴倾角 单位0.1°	可选
			0x1B65	asix_y	int	min:-1800 max:1800	y轴倾角 单位0.1°	可选

表2　双灯控制器（续）

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B61	d_realtime_data	双灯实时数据	0x1B66	asix_z	int	min:-1800 max:1800	z轴倾角 单位0.1°	可选
			0x1BBD	water_det	bool	0-没进水 1-进水	水浸检测	可选
			0x1B67	version_hw	string	长度范围[0,64]	硬件版本号	必选
			0x1B68	version_sw	string	长度范围[0,64]	软件版本号	必选
0x1B62	d_alarm_threshold	双灯告警阈值	0x1B69	over_volt_threshold	int	min:0 max:10000	总过压阈值 单位0.1V 过压上报	必选
			0x1B6A	under_volt_threshold	int	min:0 max:10000	总欠压阈值 单位0.1V 欠压上报	必选
			0x1B6B	over_current_threshold	int	min:0 max:20000	总过流阈值 单位1mA 过流上报	必选
			0x1B6C	leak_current_threshold	int	min:0 max:20000	总漏电流阈值 单位1mA 漏电上报	必选
			0x1B6D	under_power_threshold	int	min:0 max:100000	总欠功率阈值 单位0.1W 功率过低上报	必选
			0x1B8A	ch1_over_volt_threshold	int	min:0 max:10000	通道1过压阈值 单位0.1V 过压上报	可选
			0x1B8B	ch1_under_volt_threshold	int	min:0 max:10000	通道1欠压阈值 单位0.1V 欠压上报	可选
			0x1B8C	ch1_over_current_threshold	int	min:0 max:20000	通道1过流阈值 单位1mA 过流上报	可选
			0x1B8D	ch1_leak_current_threshold	int	min:0 max:20000	通道1漏电流阈值 单位1mA 漏电上报	可选
			0x1B8E	ch1_under_power_threshold	int	min:0 max:100000	通道1欠功率阈值 单位0.1W 功率过低上报	可选

表2　双灯控制器（续）

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B62	d_alarm_threshold	双灯告警阈值	0x1B8F	ch2_over_volt_threshold	int	min:0 max:10000	通道2过压阈值 单位0.1V 过压上报	可选
			0x1B90	ch2_under_volt_threshold	int	min:0 max:10000	通道2欠压阈值 单位0.1V 欠压上报	可选
			0x1B91	ch2_over_current_threshold	int	min:0 max:20000	通道2过流阈值 单位1mA 过流上报	可选
			0x1B92	ch2_leak_current_threshold	int	min:0 max:20000	通道2漏电流阈值 单位1mA 漏电上报	可选
			0x1B93	ch2_under_power_threshold	int	min:0 max:100000	通道2欠功率阈值 单位0.1W 功率过低上报	可选
			0x1B6E	dip_angle_threshold	int	min:-1800 max:1800	倾角阈值 单位0.1° 倾斜上报	可选

当 PLC 设备为四灯控制器时，其物模型表见表 3。

表3　四灯控制器

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B64	f_switch	四灯开关	0x1B74	ch1_onoff	bool	0-关 1-开	通道1开关状态变化上报	必选
			0x1B75	ch2_onoff	bool	0-关 1-开	通道2开关状态变化上报	必选
			0x1B96	ch3_onoff	bool	0-关 1-开	通道3开关状态变化上报	必选
			0x1B97	ch4_onoff	bool	0-关 1-开	通道4开关状态变化上报	必选
0x1B65	f_dimming	四灯调光	0x1B76	ch1_brightness	int	min:0 max:100 步长：1	通道1亮度值 变化上报	必选
			0x1B77	ch1_color_temperature	int	min:0 max:100 步长：1	通道1色温值 变化上报	可选
			0x1B78	ch2_brightness	int	min:0 max:100 步长：1	通道2亮度值 变化上报	必选
			0x1B79	ch2_color_temperature	int	min:0 max:100 步长：1	通道2色温值 变化上报	可选

表3　四灯控制器（续）

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B65	f_dimming	四灯调光	0x1B99	ch3_color_temperature	int	min:0 max:100 步长：1	通道3色温值 变化上报	可选
			0x1B9A	ch4_brightness	int	min:0 max:100 步长：1	通道4亮度值 变化上报	必选
			0x1B9B	ch4_color_temperature	int	min:0 max:100 步长：1	通道4色温值 变化上报	可选
0x1B66	f_realtime_data	四灯实时数据	0x1B74	ch1_onoff	bool	0-关 1-开	通道1开关状态	必选
			0x1B76	ch1_brightness	int	min:0 max:100	通道1亮度值	必选
			0x1B77	ch1_color_temperature	int	min:0 max:100	通道1色温值	可选
			0x1B75	ch2_onoff	bool	0-关 1-开	通道2开关状态	必选
			0x1B78	ch2_brightness	int	min:0 max:100	通道2亮度值	必选
			0x1B79	ch2_color_temperature	int	min:0 max:100	通道2色温值	可选
			0x1B98	ch3_onoff	bool	0-关 1-开	通道3开关状态	必选
			0x1B99	ch3_brightness	int	min:0 max:100	通道3亮度值	必选
			0x1B9E	ch3_color_temperature	int	min:0 max:100	通道3色温值	可选
			0x1B97	ch4_onoff	bool	0-关 1-开	通道4开关状态	必选
			0x1B9A	ch4_brightness	int	min:0 max:100	通道4亮度值	必选
			0x1B9B	ch4_color_temperature	int	min:0 max:100	通道4色温值	可选
			0x1B5C	consumption	int	min:0 max:99999999	总用电量 单位0.01kwh	必选
			0x1B5D	voltage	int	min:0 max:10000	总电压 单位0.1V	必选
			0x1B5E	current	int	min:0 max:20000	总电流 单位1mA	必选
			0x1B5F	leak_current	int	min:0 max:20000	总漏电流 单位1mA	必选
			0x1B60	power	int	min:0 max:100000	总功率 单位0.1W	必选
			0x1B61	power_effect	int	min:0 max:1000	总功率因素 单位0.001	必选
			0x1BBC	volt_frequency	int	min:0 max:1000	电压频率 单位0.1Hz	可选
			0x1B62	running_time	int	min:0 max:99999999	总运行时长 单位min	可选

表3　四灯控制器（续）

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B66	f_realtime_data	四灯实时数据	0x1B63	lighting_time	int	min:0 max:99999999	总亮灯时长 单位min	可选
			0x1B7A	ch1_consumption	int	min:0 max:99999999	通道1用电量 单位0.01kwh	可选
			0x1B7B	ch1_voltage	int	min:0 max:10000	通道1电压 单位0.1V	可选
			0x1B7C	ch1_current	int	min:0 max:20000	通道1电流 单位1mA	可选
			0x1B7D	ch1_leak_current	int	min:0 max:20000	通道1漏电流 单位1mA	可选
			0x1B7E	ch1_power	int	min:0 max:100000	通道1功率 单位0.1W	可选
			0x1B7F	ch1_power_effect	int	min:0 max:1000	通道1功率因素 单位0.001	可选
			0x1B80	ch1_running_time	int	min:0 max:99999999	通道1运行时长 单位min	可选
			0x1B81	ch1_lighting_time	int	min:0 max:99999999	通道1亮灯时长 单位min	可选
			0x1B82	ch2_consumption	int	min:0 max:99999999	通道2用电量 单位0.01kwh	可选
			0x1B83	ch2_voltage	int	min:0 max:10000	通道2电压 单位0.1V	可选
			0x1B84	ch2_current	int	min:0 max:20000	通道2电流 单位1mA	可选
			0x1B85	ch2_leak_current	int	min:0 max:20000	通道2漏电流 单位1mA	可选
			0x1B86	ch2_power	int	min:0 max:100000	通道2功率 单位0.1W	可选
			0x1B87	ch2_power_effect	int	min:0 max:1000	通道2功率因素 单位0.001	可选
			0x1B88	ch2_running_time	int	min:0 max:99999999	通道2运行时长 单位min	可选
			0x1B89	ch2_lighting_time	int	min:0 max:99999999	通道2亮灯时长 单位min	可选
			0x1B9C	ch3_consumption	int	min:0 max:99999999	通道3用电量 单位0.01kwh	可选
			0x1B9D	ch3_voltage	int	min:0 max:10000	通道3电压 单位0.1V	可选
			0x1B9E	ch3_current	int	min:0 max:20000	通道3电流 单位1mA	可选
			0x1B9F	ch3_leak_current	int	min:0 max:20000	通道3漏电流 单位1mA	可选
			0x1BA0	ch3_power	int	min:0 max:100000	通道3功率 单位0.1W	可选

表3　四灯控制器（续）

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B66	f_realtime_data	四灯实时数据	0x1BA2	ch3_running_time	int	min:0 max:99999999	通道3运行时长 单位min	可选
			0x1BA3	ch3_lighting_time	int	min:0 max:99999999	通道3亮灯时长 单位min	可选
			0x1BA4	ch4_consumption	int	min:0 max:99999999	通道4用电量 单位0.01kwh	可选
			0x1BA5	ch4_voltage	int	min:0 max:10000	通道4电压 单位0.1V	可选
			0x1BA6	ch4_current	int	min:0 max:20000	通道4电流 单位1mA	可选
			0x1BA7	ch4_leak_current	int	min:0 max:20000	通道4漏电流 单位1mA	可选
			0x1BA8	ch4_power	int	min:0 max:100000	通道4功率 单位0.1W	可选
			0x1BA9	ch4_power_effect	int	min:0 max:1000	通道4功率因素 单位0.001	可选
			0x1BAA	ch4_running_time	int	min:0 max:99999999	通道4运行时长 单位min	可选
			0x1BAB	ch4_lighting_time	int	min:0 max:99999999	通道4亮灯时长 单位min	可选
			0x1B64	asix_x	int	min:-1800 max:1800	x轴倾角 单位0.1°	可选
			0x1B65	asix_y	int	min:-1800 max:1800	y轴倾角 单位0.1°	可选
			0x1B66	asix_z	int	min:-1800 max:1800	z轴倾角 单位0.1°	可选
			0x1BBD	water_det	bool	0-没进水 1-进水	水浸检测	可选
			0x1B67	version_hw	string	长度范围[0,64]	硬件版本号	必选
			0x1B68	version_sw	string	长度范围[0,64]	软件版本号	必选
0x1B67	f_alarm_threshold	四灯告警阈值	0x1B69	over_volt_threshold	int	min:0 max:10000	总过压阈值 单位0.1V 过压上报	必选
			0x1B6A	under_volt_threshold	int	min:0 max:10000	总欠压阈值 单位0.1V 欠压上报	必选
			0x1B6B	over_current_threshold	int	min:0 max:20000	总过流阈值 单位1mA 过流上报	必选
			0x1B6C	leak_current_threshold	int	min:0 max:20000	总漏电流阈值 单位1mA 漏电上报	必选
			0x1B6D	under_power_threshold	int	min:0 max:100000	总欠功率阈值 单位0.1W 功率过低上报	必选

表3　四灯控制器（续）

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B67	f_alarm_threshold	四灯告警阈值	0x1B8A	ch1_over_volt_threshold	int	min:0 max:10000	通道1过压阈值 单位0.1V 过压上报	可选
			0x1B8B	ch1_under_volt_threshold	int	min:0 max:10000	通道1欠压阈值 单位0.1V 欠压上报	可选
			0x1B8C	ch1_over_current_threshold	int	min:0 max:20000	通道1过流阈值 单位1mA 过流上报	可选
			0x1B8D	ch1_leak_current_threshold	int	min:0 max:20000	通道1漏电流阈值 单位1mA 漏电上报	可选
			0x1B8E	ch1_under_power_threshold	int	min:0 max:100000	通道1欠功率阈值 单位0.1W 功率过低上报	可选
			0x1B8F	ch2_over_volt_threshold	int	min:0 max:10000	通道2过压阈值 单位0.1V 过压上报	可选
			0x1B90	ch2_under_volt_threshold	int	min:0 max:10000	通道2欠压阈值 单位0.1V 欠压上报	可选
			0x1B91	ch2_over_current_threshold	int	min:0 max:20000	通道2过流阈值 单位1mA 过流上报	可选
			0x1B92	ch2_leak_current_threshold	int	min:0 max:20000	通道2漏电流阈值 单位1mA 漏电上报	可选
			0x1B93	ch2_under_power_threshold	int	min:0 max:100000	通道2欠功率阈值 单位0.1W 功率过低上报	可选
			0x1BAC	ch3_over_volt_threshold	int	min:0 max:10000	通道3过压阈值 单位0.1V 过压上报	可选
			0x1BAD	ch3_under_volt_threshold	int	min:0 max:10000	通道3欠压阈值 单位0.1V 欠压上报	可选
			0x1BAE	ch3_over_current_threshold	int	min:0 max:20000	通道3过流阈值 单位1mA 过流上报	可选
			0x1BAF	ch3_leak_current_threshold	int	min:0 max:20000	通道3漏电流阈值 单位1mA 漏电上报	可选
			0x1BB0	ch3_under_power_threshold	int	min:0 max:100000	通道3欠功率阈值 单位0.1W 功率过低上报	可选
			0x1BB1	ch4_over_volt_threshold	int	min:0 max:10000	通道4过压阈值 单位0.1V 过压上报	可选
			0x1BB2	ch4_under_volt_threshold	int	min:0 max:10000	通道4欠压阈值 单位0.1V 欠压上报	可选

表3　四灯控制器（续）

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B67	f_alarm_threshold	四灯告警阈值	0x1BB3	ch4_over_current_threshold	int	min:0 max:20000	通道4过流阈值 单位1mA 过流上报	可选
			0x1BB4	ch4_leak_current_threshold	int	min:0 max:20000	通道4漏电流阈值 单位1mA 漏电上报	可选
			0x1BB5	ch4_under_power_threshold	int	min:0 max:100000	通道4欠功率阈值 单位0.1W 功率过低上报	可选
			0x1B6E	dip_angle_threshold	int	min:-1800 max:1800	倾角阈值 单位0.1° 倾斜上报	可选

当 PLC 设备为载波电源设备时，其物模型表见表 4。

表4　载波电源

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B69	s_switch	开关	0x1B59	onoff	bool	0-关 1-开	电源开关状态 变化上报	必选
0x1B6A	s_dimming	调光	0x1B5A	brightness	int	min:0 max:100 步长：1	亮度值 变化上报	必选
			0x1B5B	color_temperature	int	min:0 max:100 步长：1	色温值 变化上报	可选
0x1B6B	s_realtime_data	实时数据	0x1B59	onoff	bool	0-关 1-开	电源开关状态	必选
			0x1B5A	brightness	int	min:0 max:100	亮度值	必选
			0x1B5B	color_temperature	int	min:0 max:100	色温值	可选
			0x1B5C	consumption	int	min:0 max:99999999	总用电量 单位0.01kwh	可选
			0x1B5D	voltage	int	min:0 max:10000	输入电压 单位0.1V	可选
			0x1B5E	current	int	min:0 max:20000	输入电流 单位1mA	可选
			0x1B5F	leak_current	int	min:0 max:20000	漏电流 单位1mA	可选
			0x1B60	power	int	min:0 max:100000	功率 单位0.1W	可选
			0x1B61	power_effect	int	min:0 max:1000	功率因素 单位0.001	可选
			0x1BBC	volt_frequency	int	min:0 max:1000	电压频率 单位0.1Hz	可选
			0x1B62	running_time	int	min:0 max:99999999	运行时长 单位min	可选
			0x1B63	lighting_time	int	min:0 max:99999999	亮灯时长 单位min	可选

表4 载波电源（续）

SIID	服务	服务(中文)	CIID	属性	数据类型	取值范围	描述	可选/必选
0x1B6B	s_realtime_data	实时数据	0x1B64	asix_x	int	min:-1800 max:1800	x轴倾角 单位0.1°	可选
			0x1B65	asix_y	int	min:-1800 max:1800	y轴倾角 单位0.1°	可选
			0x1B66	asix_z	int	min:-1800 max:1800	z轴倾角 单位0.1°	可选
			0x1BBD	water_det	bool	0-没进水 1-进水	水浸检测	可选
			0x1B67	version_hw	string	长度范围 [0,64]	硬件版本号	必选
			0x1B68	version_sw	string	长度范围 [0,64]	软件版本号	必选
			0x1BB8	driver_temperature	int	min:-50 max:200	电源温度值	可选
			0x1BB9	driver_outcurrent	int	min:0 max:50000	输出电流 单位1mA	可选
			0x1BBA	driver_outvolt	int	min:0 max:10000	输出电压 单位0.1V	可选
0x1B6C	s_alarm_threshold	告警阈值	0x1B69	over_volt_threshold	int	min:0 max:10000	过压阈值 单位0.1V 过压上报	可选
			0x1B6A	under_volt_threshold	int	min:0 max:10000	欠压阈值 单位0.1V 欠压上报	可选
			0x1B6B	over_current_threshold	int	min:0 max:20000	过流阈值 单位1mA 过流上报	可选
			0x1B6C	leak_current_threshold	int	min:0 max:20000	漏电流阈值 单位1mA 漏电上报	可选
			0x1B6D	under_power_threshold	int	min:0 max:100000	欠功率阈值 单位0.1W 功率过低上报	可选
			0x1B6E	dip_angle_threshold	int	min:-1800 max:1800	倾角阈值 单位0.1° 倾斜上报	可选
			0x1BBB	driver_temperature	int	min:-500 max:2000	电源温度值 单位0.1℃	可选

6 PLC 模组串口接口规范

6.1 协议约定

本章节规定了控制设备MCU与PLC CCO、控制设备MCU与PLC STA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

本文件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 5。

表5 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，格式见表6。

表6 帧格式定义

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

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，不超过 502 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-xmodem(0x1021)，$x^{16}+x^{12}+x^{5}+1$，大端序。

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，定义见表 7。

表7 控制域

D7	D6	D5	D4	D3	D2	D1	D0
Dir	Prm	Rsv					

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）

帧格式中的命令码与相应的命令类别见表8。

表8 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	系统控制数据通信命令	系统控制数据通信命令

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。

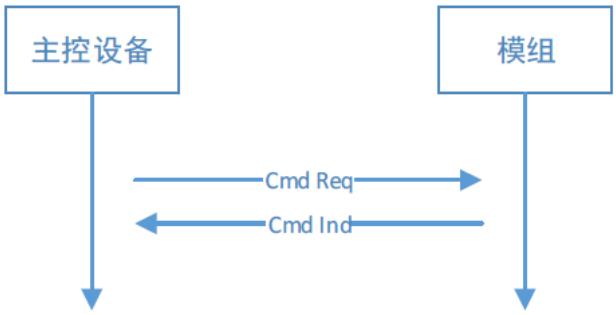


图6 本地命令数据交互流程

6.3.3.1 读取模组版本信息（0001H）

表8命令码中对应的读取模组版本信息指令内容见表9。

表9 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）

表8命令码中对应的读取模组MAC地址指令内容见表10。

表10 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）

表8命令码中对应的读取模组通信地址指令内容见表11。

表11 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）

表8命令码中对应的设置模组通信地址指令内容见表12。

表12 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）
		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）

表8命令码中对应的模组重启指令见表13。

表13　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（1byte）
	Rsv（3bytes）	Rsv（3bytes）

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）

表8命令码中对应的传输文件指令见表14。

表14　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格式见表15 ～ 表17。

6.3.3.6.1　启动文件传输

表8命令码中对应的启动文件传输指令见表15。

表15　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（1byte）	State（1byte）
	Segment Total（2bytes）	Reason（1byte）
	File Length（4bytes）	Rsv（1byte）
	File Crc（4bytes）	
	Trans Timeout（4bytes）	

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

表8命令码中对应的传输文件内容指令见表16。

表16 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	

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)，x16+x12+x5+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

表8命令码中对应的查询处理进度指令见表17。

表17 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 (3bytes)	State (1byte)
		Fail STAs (2bytes)

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

表8命令码中对应的配置升级列表指令见表18。

表18 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 (1byte)	State (1byte)
	Mac List (6 * N Bytes)	Reason (1byte)
		Rsv (1byte)

Mac Cnt：升级列表个数；

Mac List：升级列表，mac地址大端

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”。

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）

表8命令码中对应的读取模块上电时间指令见表19。

表19 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（2bytes）	MAC(6 bytes)
		frame_index(2 bytes)
		on_power_ms_time (4 bytes)

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）

表8命令码中对应的读取白名单中节点数量指令见表20。

表20 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）

表8命令码中对应的读取白名单中节点信息指令见表21。

表21 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)

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）

表8命令码中对应的添加节点到白名单指令见表22。

表22 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)
		Rsv (2bytes)

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）

表8命令码中对应的删除白名单中节点指令见表23。

表23 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)
		Rsv (2bytes)

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）

表8命令码中对应的清空白名单指令见表24。

表24 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)
		Rsv (2bytes)

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）

表8命令码中对应的自组网功能开启指令见表25。

表25　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（1byte）
		reserved（2bytes）

注：本命令只能在CCO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）

表8命令码中对应的设置白名单状态指令见表26。

表26　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（1byte）
	Rsv（3bytes）	Rsv（3bytes）

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）

表8命令码中对应的获取白名单状态指令见表27。

表27　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（1byte）
		Rsv（3bytes）

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）

表8命令码中对应的读取拓扑中节点数量指令见表28。

表28　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）

表8命令码中对应的读取拓扑中节点信息指令见表29。

表29　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)

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。数据格式见表30，每个节点包含11个字节数据内容。

表30　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

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，数据交互流程如图 7。

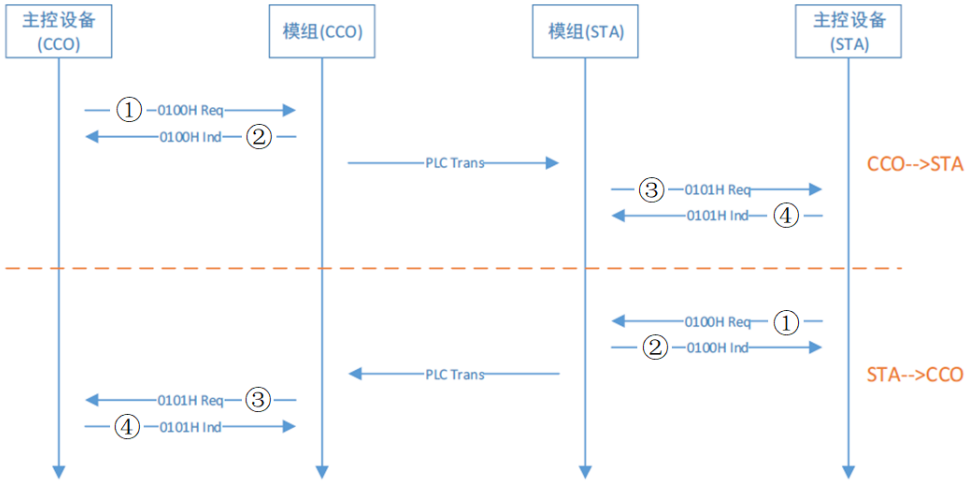


图7　信道转发命令数据交互流程

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 31。

表31　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)

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 32。

表32　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)

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

远程命令是通过中央协调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。

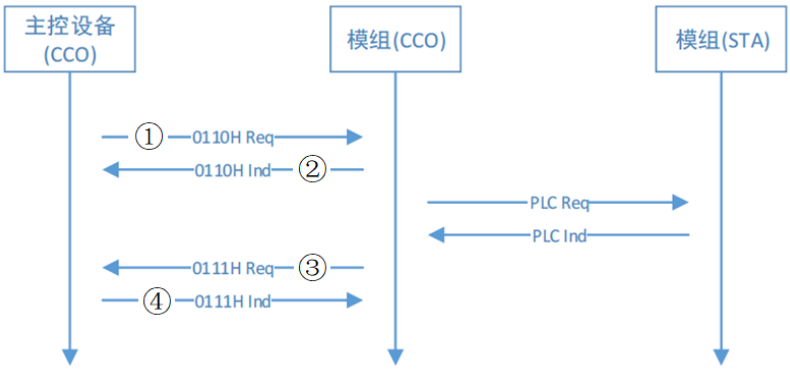


图8 远程调测命令数据交互流程

6.3.5.1 远程发送命令（0110H）

主控设备（CCO）与模组（CCO）交互过程中，远程发送命令见表33。

表33 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)

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）

主控设备（CCO）与模组（CCO）交互过程中，远程接收命令见表34。

表34 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)

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

模组支持本地调试测试接口，调测支持的本地命令见表35。

表35 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。

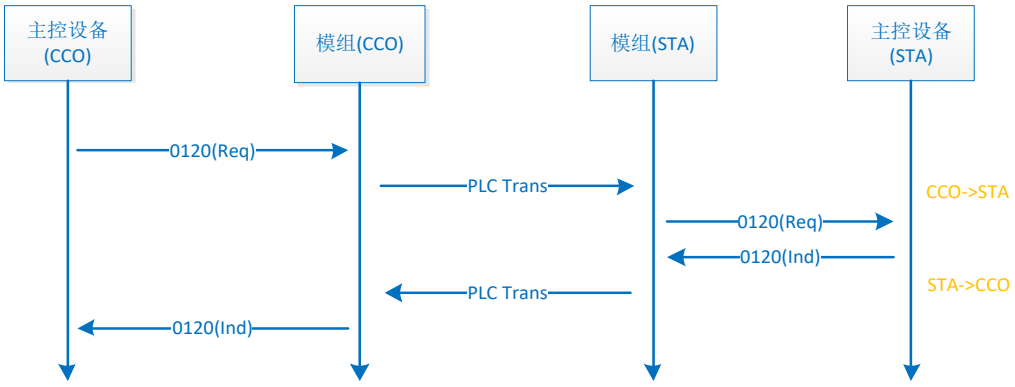


图9 系统控制数据通信命令数据交互流程

主控设备（CCO）与主控设备（STA）交互过程中，通过系统控制数据通信命令进行交互，见表36。

表36 系统控制数据通信命令

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

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

主控设备（CCO）与主控设备（STA）交互过程中通过异常状态代码来表示当前通信过程的状态，状态代码见表37。

表37 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38。

表38 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39。

表39 PLC 应用报文格式

长度（byte）	2	2	L
含义	CRC	L	User Data

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-xmode(0x1021)，$x^{16}+x^{12}+x^5+1$，大端序。CRC源码范例参考附录E。

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 系统控制数据通信命令”来完成，数据交互流程见图9。

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，发送数据格式见表 40。

表40　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，接收数据格式见表41。

表41　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

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。当远端设备为STA站点时，目的设备通信地址指STA的MAC地址。当目的设备为CCO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。当发送数据的设备为CCO时，发送数据设备通信地址指CCO的MAC地址。当发送数据的设备为STA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CCO和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：网关的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44。

DEV Addr：设备应用地址。

Data Body：功能命令数据。

7.4 功能码（Func Code）

总线通信数据中在发送数据和接收数据中采用功能码来定义指令的操作功能，功能码格式见表42，功能码具体定义见表43。

表42 功能码格式

B7	B6	B5	B4	B3	B2	B1	B0
F	x						

注：
“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。

表43 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

在发送数据和接收数据中采用响应状态码来定义指令的应答状态，Status Code 响应状态码定义见表44。

表44 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

接收端按照表44所定义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，目前使用了表44中所定义的Status Code中的Bit0和Bit1。Bit0：表示控制目标设备不回响应报文，“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）

发送数据和接收数据中设备应用地址范围定义见表45。

表45 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 ～ 0xFFFD	保留
0xFFFE	出厂未分配应用地址时的值
0xFFFF	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。

7.5 功能命令详解

7.5.1 查询设备信息（Func Code =0x01）

CCO查询某个STA设备信息，低字节在前，高字节在后。查询设备信息格式见表46。

表46　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。

PLC模组主控设备（STA）查询模组（STA）设备获取信息来响应查询设备信息，低字节在前，高字节在后，查询设备信息响应格式见表47。

表47　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 （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)	0x81
		Status Code (1byte)	0x00 ～ 0x06
		DEV Addr(2bytes)	xx xx
		Data Type (2bytes)	0x03（String）
		Data Len (2bytes)	xx xx
		Dev Infor String (n bytes)	设备信息字符串，格式为：key:value,key:value

表47查询设备信息响中的数据类型表示的控制设备下发到STA设备的控制报文类型，定义见表48。

表48　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47设备信息字符串返回设备信息，由ASC码字符串组成，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

设备信息字符串字段说明见表49。

表49　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	是	075
manu	设备制造商ID，长度为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	是	11
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	否	0010

网关或平台根据设备类型 ID（devType）和设备子型号 ID（subProdId）识别设备物模型。

7.5.2　写入设备应用地址（Func Code =0x02）

PLC网关（CCO）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。格式见表50。

表50　写入设备应用地址

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（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CCO，远程设备(STA)响应写入设备应用地址格式见表51。

表51　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 （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)	0x82
		Status Code (1byte)	0x00 ～ 0x06
		DEV Addr (2bytes)	xx xx

7.5.3　读取设备应用地址（Func Code =0x03）

PLC网关（CCO）读取某个远程设备（STA）应用地址，低字节在前，高字节在后，见表52。

表52　读取设备应用地址

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（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CCO，见表53。

表53　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 （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)	0x83
		Status Code (1byte)	0x00 ～ 0x06
		DEV Addr (2bytes)	xx xx

7.5.4　添加 N 个组地址（Func Code =0x04）

PLC网关（CCO）远程对单个设备（STA）写入N个组地址Group Addr (1个组地址2bytes)，见表54。

表54　添加 N 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)		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)	0x04
		Status Code (1byte)	0x00
		DEV Addr (2 bytes)	xx xx
		Group Number (2bytes)	xx xx
		Group Addr1 (2bytes)	xx xx
		Group Addr2 (2bytes)	xx xx
		……	……
		Group AddrN (2bytes)	xx xx

远程设备（STA）在写入组地址后，给CCO的响应报文，见表55。

表55　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（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(1bytes)	0x84
		Status Code (1byte)	0x00 ～ 0x06
		DEV Addr (2 bytes)	xx xx

7.5.5　读取全部组地址（Func Code =0x05）

PLC网关（CCO）远程读取某个设备（STA）全部组地址Group Addr (2bytes)，见表56。

表56　读取全部组地址

方向	主控设备MCU下发到CCO模组		
Cmd	0x0120H ①		0x0120
Data	Dest MAC Addr (6bytes)		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)	0x05
		Status Code (1byte)	0x00
		DEV Addr (2bytes)	xx xx

远程设备（STA）给CCO的响应报文。参考表57。

表57　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（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)	0x85
		Status Code (1byte)	0x00 ～ 0x06
		DEV Addr (2 bytes)	xx xx
		Group Number (2byte)	xx xx
		Group Addr1 (2bytes)	xx xx
		Group Addr2 (2bytes)	xx xx
		……	……
		Group AddrN (2bytes)	xx xx

7.5.6　删除 N 个组地址（Func Code =0x06）

PLC网关（CCO）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。见表58。

表58　删除 N 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)		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)	0x06
		Status Code (1byte)	0x00
		DEV Addr (2 bytes)	xx xx
		Group Number (2byte)	xx xx 删除的组地址数量，如果填写0000表示删除所有组
		Group Addr1 (2bytes)	xx xx
		Group Addr2 (2bytes)	xx xx
		……	……
		Group AddrN (2bytes)	xx xx

远程设备（STA）给CCO的响应报文。见表59。

表59　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（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)	0x86
		Status Code (1byte)	0x00 ～ 0x06
		DEV Addr (2bytes)	xx xx

7.5.7　写入设备属性（Func Code =0x07）

PLC网关（CCO）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，见表60。

表60　写入设备属性

方向	主控设备MCU下发到CCO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)	xx
		PLC协议次版本号 (1byte)	xx
		Sequence Number (2bytes)	xx xx
		Func Code (1byte)	0x07
		Status Code (1byte)	0x00（返回响应报文，允许上报属性变化） 0x03（不返回响应报文，此时不上报属性变化，组控设备时使用）
		DEV Addr (2bytes)	xx xx（单地址、组地址、广播地址）
		SIID (2bytes)	xx xx
		CIID (2bytes)	xx xx
		Data Type（2byte）	xx xx
		Data Len (2bytes)	xx xx
		Data Value（n byte）	xx …… xx
		……	……
		SIID (2bytes)	xx xx
		CIID (2bytes)	xx xx
		Data Type（2byte）	xx xx
		Data Len (2bytes)	xx xx
		Data Value（n bytes）	xx …… xx

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CCO的响应报文，见表61。

表61　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（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)	0x87
		Status Code (1byte)	0x00 ～ 0x06
		DEV Addr (2bytes)	xx xx

7.5.8　读取设备属性（Func Code =0x08）

PLC 网关（CCO）单播或广播方式读某个（DEV ADDR）设备多个属性参数到 CCO，读取设备属性见表 62。

表62　读取设备属性

方向	主控设备MCU下发到CCO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)		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)	0x08
		Status Code (1byte)	0x00
		DEV Addr(2bytes)	xx xx
		SIID (2bytes)	xx xx
		CIID (2bytes)	xx xx
		……	……
		SIID (2bytes)	xx xx
		CIID (2bytes)	xx xx

注# a：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）向CCO发读取设备属性响应报文，读取设备属性响应格式见表63。

表63　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（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 (1byte)	0x88
		Status Code (1byte)	0x00 ～ 0x06
		DEV Addr(2bytes)	xx xx
		SIID (2bytes)	xx xx
		CIID (2bytes)	xx xx
		Data Type（2byte）	xx xx
		Data Len (2bytes)	xx xx
		Data Value（n byte）	xx …… xx
		……	……
		SIID (2bytes)	xx xx
		CIID (2bytes)	xx xx
		Data Type（2byte）	xx xx
		Data Len (2bytes)	xx xx
		Data Value（n byte）	xx …… xx

7.5.9　上报设备属性（Func Code =0x09）

STA设备（DEV Addr）上报属性数据给CCO，属性格式见表64。

表64　上报设备属性

方向	属性		
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)	xx xx
		CIID (2bytes)	xx xx
		Data Type（2bytes）	xx xx
		Data Len (2bytes)	xx xx
		Data Value（nbytes）	xx …… xx
		……	xx xx
		SIID (2bytes)	xx xx
		CIID (2bytes)	xx xx
		Data Type（2bytes）	xx xx
		Data Len (2bytes)	xx xx
		Data Value（nbytes）	xx …… xx

CCO给远程设备（STA）的响应报文见表65。

表65　上报设备属性

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

7.5.10　上报设备事件（Func Code =0x0A）

STA设备（DEV Addr）上报事件数据给CCO见表66。

表66　上报设备事件

方向	属性		
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)	0x0A
		Status Code (1byte)	0x00
		DEV Addr(2bytes)	xx xx
		SIID (2bytes)	xx xx
		CIID (2bytes)	xx xx
		Data Type（2byte）	xx xx
		Data Len (2bytes)	xx xx
		Data Value（n bytes）	xx …… xx
		……	……
		SIID (2bytes)	xx xx
		CIID (2bytes)	xx xx
		Data Type（2bytes）	xx xx
		Data Len (2bytes)	xx xx
		Data Value（n bytes）	xx …… xx

CCO给远程设备（STA）的响应报文见表67。

表67　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

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

PLC网关（CCO）对远程N个设备（STA）添加或删除1个组地址Group Addr (2bytes)，设备添加与删除地址的数据格式表68。

表68　N 个设备添加/删除 1 个组地址

方向	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的响应报文见表69。

表69　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

7.5.12　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70。

表70　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)	xx xx
		CIID (2bytes)	xx xx
		Data Type（2byte）	xx xx
		Data Len (2bytes)	xx xx
		Data Value（n byte）	xx …… xx
		……	xx xx
		SIID (2bytes)	xx xx
		CIID (2bytes)	xx xx
		Data Type（2byte）	xx xx
		Data Len (2bytes)	xx xx
		Data Value（n byte）	xx …… xx

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71。

表71　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

7.5.13　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，见表72。

表72　查询场景校验值

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)	0x0D
		Status Code (1byte)	0x00
		DEV Addr(2bytes)	xx xx

远程设备（STA）将响应报文发给CCO，查询场景校验值响应见表73。

表73　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（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 (1byte)	0x8D
		Status Code (1byte)	0x00 ～ 0x06
		DEV Addr(2bytes)	xx xx
		CRC 校验码（2bytes）	按场景ID从小到大（升序）排序的所有场景数据CRC校验和，CRC校验生成多项式采用CRC16-CCITT(0x1021)，$x^{16}+x^{12}+x^{5}+1$。

7.5.14 执行场景（Func Code =0x0E）

PLC网关（CCO）控制设备（STA）执行某个场景（场景号），执行场景数据格式见表74。

表74 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(2bytes)	xx xx

远程设备（STA）将执行场景响应的报文发到 CCO，执行场景响应格式见表 75。

表75 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

7.5.15 删除场景（Func Code =0x0F）

PLC网关（CCO）可通过发送命令删除控制设备（STA）若干场景，删除场景的数据格式见表76。

表76 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 (2bytes)	场景ID，如果填写0000则表示删除所有场景

远程设备（STA）将删除场景响应报文发到CCO，见表77。

表77　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

7.5.16　获取心跳（Func Code =0x10）

PLC网关（CCO）可通过报文获取设备（STA）心跳信号，控制心跳的格式见表78。

表78　控制心跳

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)	0x10
		Status Code (1byte)	0x00
		DEV Addr(2bytes)	xx xx
		Mode (2byte)	xx xx

远程设备（STA）将获取心跳响应报文发给CCO，响应数据格式见表79。

表79　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（CCO 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

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，CCO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CCO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。

7.5.17 重启设备（Func Code =0x11）

PLC网关（CCO）可通过报文控制设备（STA）重启，可以单控、组控、广播方式，重启设备数据格式见表80。

表80 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）将重启设备响应报文发给CCO，数据格式见表81。

表81 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（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)	0x91
		Status Code (1byte)	0x00 ～ 0x06
		DEV Addr (2bytes)	xx xx

7.5.18 转发报文（Func Code =0x12）

子设备A（STA）通过CCO转发报文给子设备B（STA）转发报文数据格式见表82。

表82 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）	xx …… xx

不支持返回响应报文。

8 北向接口规范

8.1 集中控制器动态注册授权

设备开机启动的时候先动态获取授权码。
getAuthCode：设备注册获取授权码ProductKey
授权地址如下：https://xxx.xxx.xxx.xxx/getAuthCode

参数数据格式说明：

```
{
    "mqttUser":"ProductKey+Time",     #mqtt账号
    "mqttPwd": "affafaf",     #mqtt密码MD5后的32位值
    "deviceId":"1",    #客户端ID,
    "tenantId": "0002" # 对应的租户ID
}
```

回复API

```
{
    "errMsg":"错误消息",
    "errCode":"错误码", #发送指令时间，时间戳（秒）
    "code":"200", # 200正常
    "data":"对应的授权码32位字符串" #ProductKey
}
```

8.2 验证加密规则说明

Token有效校验时限为Time请求时间120秒内有效；
ProductKey为每个项目专属key。
Seq为每条控制指令专属指令码（唯一性）。
Time为每次指令下发时间。

MQTT指令token的加密规则：MD5(ProductKey+Seq+Time)

API接口Token的加密规则：MD5(ProductKey+Time)

8.3 MQTT 消息中心&数据中心技术规范

MQTT是基于TCP/IP协议栈构建的异步通信消息协议，是一种轻量级的发布、订阅信息传输协议。可在不可靠的网络环境中进行扩展，适用于设备硬件存储空间或网络带宽有限的场景。使用MQTT协议，消息发送者与接收者不受时间和空间的限制。物联网平台支持设备使用MQTT协议接入。

8.4 MQTT 消息中心通信规范说明

8.4.1 Client 角色定义说明

Client角色定义说明见图10。

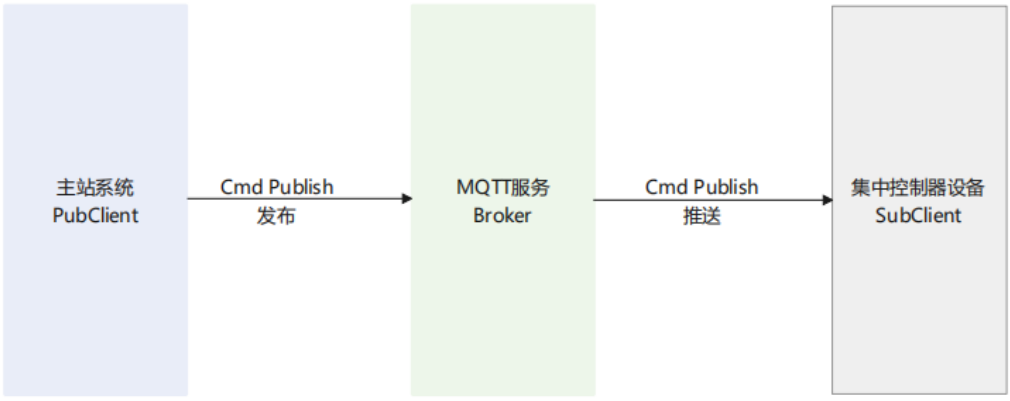


图10 Client 角色定义说明

8.4.2 物模型通信 Topic

物模型通信Topic，见表83。

表83 物模型通信 Topic

服务	Topic类	操作权限	描述
Cmd	/light/cmd/${clientId}	发布	主站指令下发
		订阅	集中控制器指令接收
Ack	/light/ack	发布	集中控制器指令校验反馈
		订阅	主站
Process	/light/process	发布	集中控制器指令执行进度反馈
		订阅	主站
End	/light/end	发布	集中控制器指令执行结果反馈
		订阅	主站
Upgrade	/light/upgrade/${clientId}	发布&订阅	主站发布，集中器订阅
	/light/upgrade/ack	发布&订阅	集中器发布，主站订阅
	/light/upgrade/end	发布&订阅	集中器发布，主站订阅

8.4.2.1 Cmd 物模型 TSL

```
{
"method":"",     #类方法名
"token":"ProductKey+seq+Time",     #ProductKey+seq+Time的MD5加密
"time":"1581667274",       #发送指令时间，时间戳（毫秒）
"mqType":1101,     #参考MQTT Topic物模型说明
"seq":"123445",        #平台唯一32位字符串指令序号，用以回复验证
```

```
"data":{}        #消息数据内容,
}
```

8.4.2.2 Ack 物模型 TSL

```
 {
"token":"seq+Time",     #seq+Time的MD5加密
"mqType" : 1101, #收到什么就返回什么
"time":1581667274,     #客户端接收时间
"clientId":"",  #集中器对应的设备ID
"method":"",    #接口方法
"res":"OK|ERR", # 固定返回OK
"errMsg": "" # 错误消息
"seq":"123445",        #接收的指令序号
}
```

8.4.2.3 End 物模型 TSL

```
 {
"token":"seq+Time",     #seq+Time的MD5加密
"time":1581667274,     #客户端执行时间
"mqType" : 1101, #收到什么就返回什么
"clientId":"",  #集中器对应的设备ID
"method":"",    #接口方法
"res":"OK|ERR", # 固定返回OK
"errMsg": "" # 错误消息
"seq":"123445"        #执行的指令序号
}
```

8.4.2.4 Process 物模型 TSL

```
 {
    "token":"seq+Time",     #seq+Time的MD5加密
    "time":1581667274,     #客户端执行时间
    "mqType" : 1101, #收到什么就返回什么
    "clientId":"",  #集中器对应的设备ID
    "method":"",    #接口方法
    "seq":"123445",        #执行的指令序号
    "res":"1/100",       #进度值1-100
    "message":"message返回码说明"
}
```

8.5 数据中心技术要去

8.5.1 API 接口请求说敏敏

请求头 header 里面必须包含 zcnyToken, zcnyTime, zcnyClientId三个参数
zcnyToken = MD5(授权码 + zcnyTime)
zcnyTime = 接口请求时间（毫秒时间戳）
zcnyClientId = 网关ID

8.5.2 API 接口请求返回格式

```
 {
    "errMsg" :"错误说明",
```

```
    "errCode" : 具体的错误代码,
    "code": 200, #参考code列表，见表84
    "data": {}    #具体的返回值，需支持boolean,字符串，数字，JSON
}
```

表84　Code 列表

code	说明
200	OK正常
401	token 无效
403	没有对应的操作权限
404	找不到对应的接口
500	服务端内部错误
600	参数校验类错误
700	数据不匹配错误，错误操作

8.6　系统控制协议

8.6.1　下行控制 TSL

8.6.1.1　单灯调光

```
{
    "method": "mqLampControl",
    "token": "ProductKey+seq+Time",
    "time": 1581667274,
    "mqType": 1201,
    "seq": "123445",
    "data": {
        "s_dimming": [{
            "lamp_id": "1000011",                  #灯控ID(字符串,长度范围[0,64])
            "brightness": 0,                       #亮度值(整数,取值范围0~100,变化上报)
            "color_temperature": 0                 #色温值(整数,取值范围0~100,变化上报)
        }]
    }
}
```

8.6.1.2　单灯开关

```
{
    "method": "mqLampControl",
    "token": "ProductKey+seq+Time",
    "time": 1581667274,
    "mqType": 1202,
    "seq": "123445",
    "data": {
        "s_switch": [{
            "lamp_id": "1000011",                  #灯控ID(字符串,长度范围[0,64])
            "onoff": 0                             #电源开关状态(枚举,0-关 1-开,变化上
                                                   报)

        }]
    }
```

```
    }
```

8.6.1.3 单灯分组

```
    {
        "method": "mqLampControl",
        "mqType": 1203,
        "seq": "16010241646133844",
        "time": "1601024164669",
        "token": "ProductKey+seq+Time",
        "data": {
            "s_grouping": [{
                "lamp_id": "1000011",              #灯控ID(字符串,长度范围[0,64])
                "group": 1                         #总分组号(整数,取值范围0~99999999)
            }]
        }
    }
```

8.6.1.4 设置单灯告警阈值

```
    {
        "method": "mqLampControl",
        "token": "ProductKey+seq+Time",
        "time": "1581667274",
        "mqType": 1204,
        "seq": "123445",
        "data": {
            "s_alarm_threshold": [{
                "lamp_id": "1000011",              #灯控ID(字符串,长度范围[0,64])
                "over_volt_threshold": 2800,       #过压阈值(整数,取值范围0~10000,单位
                                                   0.1V,过压上报)
                "under_volt_threshold": 1800,      #欠压阈值(整数,取值范围0~10000,单位
                                                   0.1V,欠压上报)
                "over_current_threshold": 30000,   #过流阈值(整数,取值范围0~20000,单位1mA,
                                                   过流上报)
                "leak_current_threshold": 30,      #漏电流阈值(整数,取值范围0~20000,单位
                                                   1mA,漏电上报)
                "under_power_threshold": 22012,    #欠功率阈值(整数,取值范围0~100000,单位
                                                   0.1W,功率过低上报)
                "dip_angle_threshold": 100         #倾角阈值(整数,取值范围-1800~1800,单位
                                                   0.1°,倾斜上报)
            }]
        }
    }
```

8.6.1.5 分组控制

```
    {
        "method": "mqLampControl",
        "token": "ProductKey+seq+Time",
        "time": "1581667274",
        "mqType": 1205,
        "seq": "123445",
```

```
        "data": {
            "group_ctrl": [{
                "ctrl_group": 1,                    #控制组号(整数,取值范围0~99999999)
                "ctrl_onoff": 1,                      #控制开关状态 (枚举,0-关 1-开)
                "ctrl_brightness": 30,                #控制亮度值(整数,取值范围0~100,步
                                                      长：1)
                "ctrl_color_temperature": 30          #控制色温值(整数,取值范围0~100,步
                                                      长：1)
            }]
        }
    }
```

8.7 数据上报 TSL

8.7.1 单灯实时数据

```
    {
        "client_id": "10000772",                    #网关ID(字符串,长度范围[0,64])
        "data": {
            "s_realtime_data": [{
                "lamp_id": "1000011",               #灯控ID(字符串,长度范围[0,64])
                "onoff": 1,                         #电源开关状态(枚举,0-关 1-开)
                "brightness": 1,                    #亮度值(整数,取值范围0~100)
                "color_temperature": 0,             #色温值(整数,取值范围0~100)
                "consumption": 12345,               #总用电量(整数,取值范围0~99999999,单
                                                    位0.01kwh)
                "voltage": 2200,                    #总电压(整数,取值范围0~10000,单位
                                                    0.1V)
                "current": 20,                      #总电流(整数,取值范围0~20000,单位1mA)
                "leak_current": 10,                 #总漏电流(整数,取值范围0~20000,单位
                                                    1mA)
                "power": 10,                        #总功率(整数,取值范围0~100000,单位
                                                    0.1W)
                "power_effect": 950,                #总功率因素(整数,取值范围0~1000,单位
                                                    0.001)
                "running_time": 10,                 #总运行时长(整数,取值范围0~99999999,
                                                    单位min)
                "lighting_time": 10,                #总亮灯时长(整数,取值范围0~99999999,
                                                    单位min)
                "asix_x": 10,                       #x轴倾角(整数,取值范围-1800~1800,单位
                                                    0.1°)
                "asix_y": 10,                       #y轴倾角(整数,取值范围-1800~1800,单位
                                                    0.1°)
                "asix_z": 10,                       #z轴倾角(整数,取值范围-1800~1800,单位
                                                    0.1°)
                "version_hw": "30",                 #硬件版本号(字符串,长度范围[0,64])
                "version_sw": "10",                 #软件版本号(字符串,长度范围[0,64])
                "time": ""                          #时间戳(单位：毫秒)
            }]
        }
    }
```

8.7.2 单灯告警阈值

```
{
    "client_id": "10000772",                    #网关ID(字符串,长度范围[0,64])
    "data": {
        "s_alarm_threshold": [{
            "lamp_id": "1000011",               #灯控ID(字符串,长度范围[0,64])
            "over_volt_threshold": 2800,        #过压阈值(整数,取值范围0~10000,单位
                                                0.1V,过压上报)
           "under_volt_threshold": 1800,        #欠压阈值(整数,取值范围0~10000,单位0.1V,
                                                欠压上报)
            "over_current_threshold": 30000,    #过流阈值(整数,取值范围0~20000,单位1mA,
                                                过流上报)
            "leak_current_threshold": 30,       #漏电流阈值(整数,取值范围0~20000,单位
                                                1mA,漏电上报)
            "under_power_threshold": 22012,     #欠功率阈值(整数,取值范围0~100000,单位
                                                0.1W,功率过低上报)
            "dip_angle_threshold": 100          #倾角阈值(整数,取值范围-1800~1800,单位
                                                0.1°,倾斜上报)
        }]
    }
}
```

8.7.3 报警事件

```
{
    "client_id": "10000772",                    #网关ID(字符串,长度范围[0,64])
    "data": {
        "s_alarm": [{
            "lamp_id": "1000011",               #灯控ID(字符串,长度范围[0,64])
            "alarm_type": 2001,                 #事件类型(字符串,长度范围[0,100])
            "alarm_name": "过压报警",           #事件名称(字符串,长度范围[0,100])
            "alarm_details": "",                #事件详情(字符串,长度范围[0,100])
            "alarm_time": "1581667274",         #事件发生时间（毫秒时间戳）
            "alarm_state": 1                    #事件状态 (枚举,0-解除 1-发生)
        }]
    }
}
```

8.8 类型字典说明

8.8.1 下发指令类型编码

下发指令类型编码见表85。

表85 下发指令类型编码

编码	说明
1201	单灯调光
1202	单灯开关
1203	单灯分组
1204	设置单灯告警阈值
1205	分组控制

8.8.2 事件类型编码

时间类型编码见表86。

表86 时间类型编码

编码	说明
2002	灯具倾斜报警
2003	灯具漏电报警
2010	电流上限报警
2012	电压上限报警
2013	电压下限报警
2014	功率下限报警

附 录 A
（规范性）
物模型表

附录A为CIID与SIID编码表。

a) CIID 编码表应按照 T/SILA 001—2022 表 A.1 以及本文件中表 A.1（道路照明专用集）的要求；

b) SIID 编码表应按照 T/SILA 001—2022 表 A.2 以及本文件中表 A.2（道路照明专用集）的要求。

表A.1 CIID编码表（道路照明专用集）

sid_cid	ciid(HEX:十六进制)	ciid(DEC:十进制)	属性名称	数据类型
_onoff	0x1B59	7001	onoff	bool
_brightness	0x1B5A	7002	brightness	int
_color_temperature	0x1B5B	7003	color_temperature	int
_consumption	0x1B5C	7004	consumption	int
_voltage	0x1B5D	7005	voltage	int
_current	0x1B5E	7006	current	int
_leak_current	0x1B5F	7007	leak_current	int
_power	0x1B60	7008	power	int
_power_effect	0x1B61	7009	power_effect	int
_running_time	0x1B62	7010	running_time	int
_lighting_time	0x1B63	7011	lighting_time	int
_asix_x	0x1B64	7012	asix_x	int
_asix_y	0x1B65	7013	asix_y	int
_asix_z	0x1B66	7014	asix_z	int
_version_hw	0x1B67	7015	version_hw	string
_version_sw	0x1B68	7016	version_sw	string
_over_volt_threshold	0x1B69	7017	over_volt_threshold	int
_under_volt_threshold	0x1B6A	7018	under_volt_threshold	int
_over_current_threshold	0x1B6B	7019	over_current_threshold	int
_leak_current_threshold	0x1B6C	7020	leak_current_threshold	int
_under_power_threshold	0x1B6D	7021	under_power_threshold	int
_dip_angle_thresho	0x1B6E	7022	dip_angle_threshold	int
_group	0x1B6F	7023	group	array
_ctrl_group	0x1B70	7024	ctrl_group	char
_ctrl_onoff	0x1B71	7025	ctrl_onoff	bool
_ctrl_brightness	0x1B72	7026	ctrl_brightness	int
_ctrl_color_temperature	0x1B73	7027	ctrl_color_temperature	int
_ch1_onoff	0x1B74	7028	ch1_onoff	bool
_ch2_onoff	0x1B75	7029	ch2_onoff	bool
_ch1_brightness	0x1B76	7030	ch1_brightness	int
_ch1_color_temperature	0x1B77	7031	ch1_color_temperature	int
_ch2_brightness	0x1B78	7032	ch2_brightness	int
_ch2_color_temperature	0x1B79	7033	ch2_color_temperature	int
_ch1_consumption	0x1B7A	7034	ch1_consumption	int
_ch1_voltage	0x1B7B	7035	ch1_voltage	int
_ch1_current	0x1B7C	7036	ch1_current	int
_ch1_leak_current	0x1B7D	7037	ch1_leak_current	int

表A.1 CIID编码表（道路照明专用集）（续）

sid_cid	ciid(HEX:十六进制)	ciid(DEC:十进制)	属性名称	数据类型
_ch1_power	0x1B7E	7038	ch1_power	int
_ch1_power_effect	0x1B7F	7039	ch1_power_effect	int
_ch1_running_time	0x1B80	7040	ch1_running_time	int
_ch1_lighting_time	0x1B81	7041	ch1_lighting_time	int
_ch2_consumption	0x1B82	7042	ch2_consumption	int
_ch2_voltage	0x1B83	7043	ch2_voltage	int
_ch2_current	0x1B84	7044	ch2_current	int
_ch2_leak_current	0x1B85	7045	ch2_leak_current	int
_ch2_power	0x1B86	7046	ch2_power	int
_ch2_power_effect	0x1B87	7047	ch2_power_effect	int
_ch2_running_time	0x1B88	7048	ch2_running_time	int
_ch2_lighting_time	0x1B89	7049	ch2_lighting_time	int
_ch1_over_volt_threshold	0x1B8A	7050	ch1_over_volt_thresho	int
_ch1_under_volt_threshold	0x1B8B	7051	ch1_under_volt_thresh	int
_ch1_over_current_threshol	0x1B8C	7052	ch1_over_current_thre	int
_ch1_leak_current_threshol	0x1B8D	7053	ch1_leak_current_thre	int
_ch1_under_power_threshold	0x1B8E	7054	ch1_under_power_thres	int
_ch2_over_volt_threshold	0x1B8F	7055	ch2_over_volt_thresho	int
_ch2_under_volt_threshold	0x1B90	7056	ch2_under_volt_thresh	int
_ch2_over_current_threshol	0x1B91	7057	ch2_over_current_thre	int
_ch2_leak_current_threshol	0x1B92	7058	ch2_leak_current_thre	int
_ch2_under_power_threshold	0x1B93	7059	ch2_under_power_thres	int
_ch1_group	0x1B94	7060	ch1_group	int
_ch2_group	0x1B95	7061	ch2_group	int
_ch3_onoff	0x1B96	7062	ch3_onoff	bool
_ch4_onoff	0x1B97	7063	ch4_onoff	bool
_ch3_brightness	0x1B98	7064	ch3_brightness	int
_ch3_color_temperature	0x1B99	7065	ch3_color_temperature	int
_ch4_brightness	0x1B9A	7066	ch4_brightness	int
_ch4_color_temperature	0x1B9B	7067	ch4_color_temperature	int
_ch3_consumption	0x1B9C	7068	ch3_consumption	int
_ch3_voltage	0x1B9D	7069	ch3_voltage	int
_ch3_current	0x1B9E	7070	ch3_current	int
_ch3_leak_current	0x1B9F	7071	ch3_leak_current	int
_ch3_power	0x1BA0	7072	ch3_power	int
_ch3_power_effect	0x1BA1	7073	ch3_power_effect	int
_ch3_running_time	0x1BA2	7074	ch3_running_time	int

表A.1 CIID编码表（道路照明专用集）（续）

sid_cid	ciid(HEX:十六进制)	ciid(DEC:十进制)	属性名称	数据类型
_ch3_lighting_time	0x1BA3	7075	ch3_lighting_time	int
_ch4_consumption	0x1BA4	7076	ch4_consumption	int
_ch4_voltage	0x1BA5	7077	ch4_voltage	int
_ch4_current	0x1BA6	7078	ch4_current	int
_ch4_leak_current	0x1BA7	7079	ch4_leak_current	int
_ch4_power	0x1BA8	7080	ch4_power	int
_ch4_power_effect	0x1BA9	7081	ch4_power_effect	int
_ch4_running_time	0x1BAA	7082	ch4_running_time	int
_ch4_lighting_time	0x1BAB	7083	ch4_lighting_time	int
_ch3_over_volt_threshold	0x1BAC	7084	ch3_over_volt_thresho	int
_ch3_under_volt_threshold	0x1BAD	7085	ch3_under_volt_thresh	int
_ch3_over_current_threshol	0x1BAE	7086	ch3_over_current_thre	int
_ch3_leak_current_threshol	0x1BAF	7087	ch3_leak_current_thre	int
_ch3_under_power_threshold	0x1BB0	7088	ch3_under_power_thres	int
_ch4_over_volt_threshold	0x1BB1	7089	ch4_over_volt_thresho	int
_ch4_under_volt_threshold	0x1BB2	7090	ch4_under_volt_thresh	int
_ch4_over_current_threshol	0x1BB3	7091	ch4_over_current_thre	int
_ch4_leak_current_threshol	0x1BB4	7092	ch4_leak_current_thre	int
_ch4_under_power_threshold	0x1BB5	7093	ch4_under_power_thres	int
_ch3_group	0x1BB6	7094	ch3_group	int
_ch4_group	0x1BB7	7095	ch4_group	int
_driver_temperature	0x1BB8	7096	driver_temperature	int
_driver_outcurrent	0x1BB9	7097	driver_outcurrent	int
_driver_outvolt	0x1BBA	7098	driver_outvolt	int
_driver_temp_threshold	0x1BBB	7099	driver_temp_threshold	int
_volt_frequency	0x1BBC	7100	volt_frequency	int
_water_det	0x1BBD	7101	water_det	bool

表A.2 SIID 编码表（道路照明专用集）

sid	siid(HEX:十六进制)	siid(DEC:十进制)	服务名(中文)
s_switch	0x1B59	7001	单灯开关
s_dimming	0x1B5A	7002	单灯调光
s_realtime_data	0x1B5B	7003	单灯实时数据
s_alarm_threshold	0x1B5C	7004	单灯告警阈值
s_grouping	0x1B5D	7005	单灯分组
group_ctrl	0x1B5E	7006	分组控制
d_switch	0x1B5F	7007	双灯开关
d_dimming	0x1B60	7008	双灯调光
d_realtime_data	0x1B61	7009	双灯实时数据
d_alarm_threshold	0x1B62	7010	双灯告警阈值
d_grouping	0x1B63	7011	双灯分组
f_switch	0x1B64	7012	四灯开关
f_dimming	0x1B65	7013	四灯调光
f_realtime_data	0x1B66	7014	四灯实时数据
f_alarm_threshold	0x1B67	7015	四灯告警阈值
f_grouping	0x1B68	7016	四灯分组
p_switch	0x1B69	7017	电源开关
p_dimming	0x1B6A	7018	电源调光
p_realtime_data	0x1B6B	7019	电源实时数据
p_alarm_threshold	0x1B6C	7020	电源告警阈值

附 录 B
（规范性）
设备类别编码表

设备类别编码表应按照T/SILA 001—2022表B.1以及本文件中表B.1设备类别编码表（道路照明专用集）的要求。

表B.1 设备类别编码表（道路照明专用集）

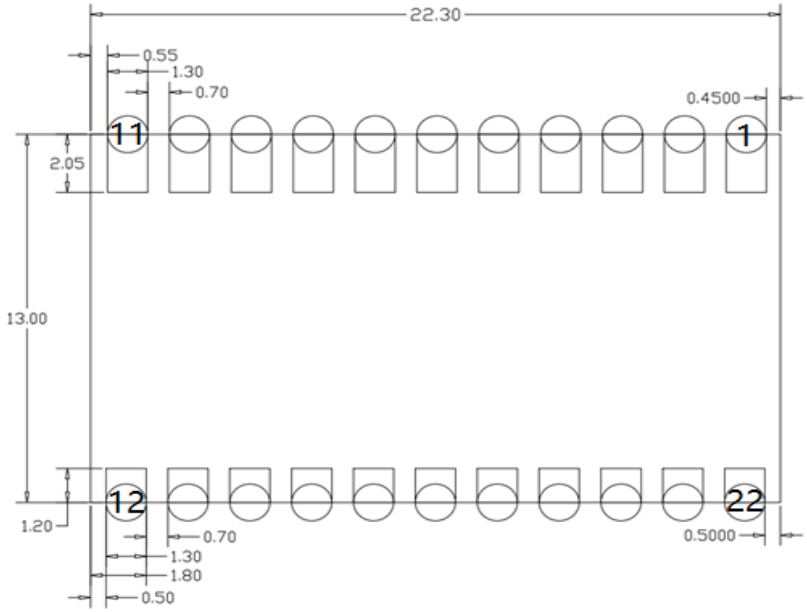
品类	品类描述	品类ID	物模型规范
单灯控制器	控制单个灯头	E50	√
双灯控制器	控制双个灯头	E51	√
四灯控制器	控制四个灯头	E52	√
路灯驱动电源	PLC载波通讯与电源一体化设备	E53	√

附 录 C
（规范性）
模组尺寸及引脚规范

随着PLC技术在各行业中被大量采用，各模组厂家的模组形态五花八门，给终端客户使用上造成不少的困惑与不便。为了能够统一模块引脚定义，尺寸大小，减少因使用不同厂商模组带来的成本增加，特制定PLC模组接口及尺寸定义标准规范。

C.1 A 型模组-邮票孔形态

特点：贴片安装，I/O口多，满足多键面板，传感器等子设备需求。
封装尺寸要求见图C.1。



图C.1 A 型模组尺寸与引脚规范（图中单位为毫米）

A型模组引脚定义以及复用功能说明见表C.1。

表C.1 A 型模组引脚定义及复用说明

PIN序号	PIN定义	备注说明
1	PLC-	PLC- 通信口，需设计滤波网络去其他AC电源隔离；一般要求防护能力：差模/共模：+/-4KV；
2	PLC+	PLC+ 通信口，需设计滤波网络去其他AC电源隔离；一般要求防护能力：差模/共模：+/-4KV
3	GND	系统GND
4	3V3	电源输入
5	UART0_RX	复用信号 0：GPIO_9 输入输出 复用信号1：UART0_RX 业务口,用于和外部MCU通信
6	UART0_TX	复用信号 0：GPIO_10 输入输出 复用信号1：UART0_TX 业务口,用于和外部MCU通信
7	GPIO15	复用信号 0：GPIO_15 输入输出 复用信号 1：SPI1_CK SPI1 从设备时钟 复用信号2：SSP1_CK SPI主设备时钟

表C.1 A型模组引脚定义及复用说明（续）

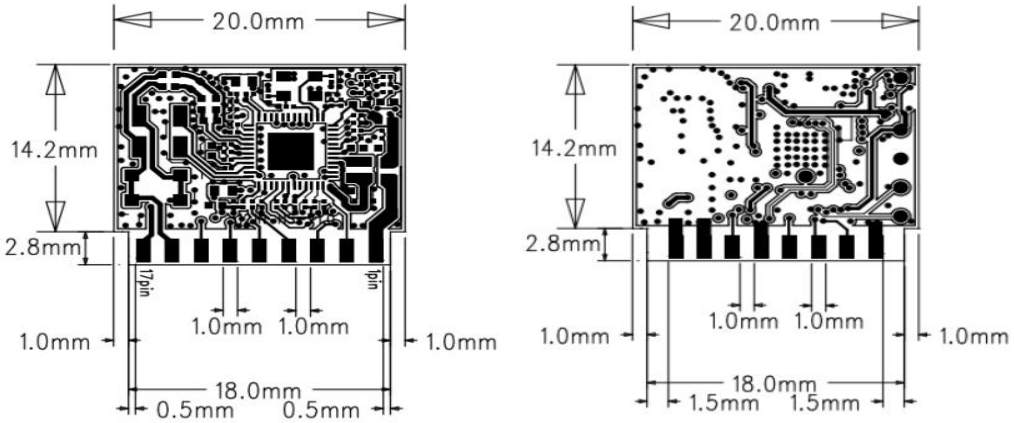
PIN序号	PIN定义	备注说明
8	GPIO3	复用信号 0：GPIO_3 输入输出 复用信号 3：SSP2_DI SPI2 数据输入信号 复用信号4：SSP2_DO SPI2数据输出信号
9	GPIO1	复用信号 0：GPIO_1 输入输出 复用信号 3：SPI2_CK SPI2 从设备时钟输入 复用信号4：SSP2_CK SPI2主设备时钟输出
10	GPIO0	复用信号 0：GPIO_0 输入输出 复用信号 3：PWM_OUT PWM0数据输出
11	GPIO2	复用信号 0：GPIO_2 输入输出 复用信号 3：SPI2_CSN SPI2 从设备片选输入信号 复用信号4：SSP2_CSN SPI2主设备片选输出信号
12	GPIO20	复用信号0：GPIO_20通用输入输出
13	GPIO12	复用信号0：GPIO_12通用输入输出。
14	GPIO4	复用信号 0：GPIO_4 通用输入输出。 复用信号 3：SSP2_DO SPI2 数据输出信号。 复用信号4：SSP2_DI SPI2数据输入信号
15	GPIO16	复用信号 0：GPIO_16 通用输入输出。 复用信号 1：SPI1_CSN SPI1 从设备片选输入信号 复用信号2：SSP1_CSN SPI1主设备片选输出信号
16	GPIO18	复用信号 0：GPIO_18 通用输入输出 复用信号 1：SSP1_DO SPI1 数据输出信号 复用信号2：SSP1_DI SPI1数据输入信号
17	NC/PA Vcc	NC/7V/12V(兼容设计)
18	UART1_TX	复用信号 0：UART1_TXD 默认输出，UART1 数据发送，用于烧录测试 复用信号 1：GPIO_14 通用输入输出 复用信号 3：I2C_SCL I2C 时钟
19	UART1_RX	复用信号 0：UART1_RXD 默认输入，UART1 数据接收，用于烧录测试 复用信号 1：GPIO_13 通用输入输出 复用信号 3：I2C_SDA I2C 数据
20	VIN4	ADC输入
21	GPIO17	复用信号 0：GPIO_17 通用输入输出 复用信号 1：SSP1_DI SPI1 数据输入信号 复用信号2：SSP1_DO SPI1数据输出信号
22	GPIO5	复用信号 1：GPIO_5 通用输入输出。 复用信号3：PWM_OUT_1 PWM1的输出管脚。

表C.1列出的管脚定义中第1，2（PLC-/PLC+），3，4(GND/3.3V)，5，6(RX/TX业务口)，10(PWM0)/22(PWM1)，17(NC/7V/12V)，20(ADC)及为固定功能引脚，其他引脚，各模组厂家可依据芯片功能自定义。

C.2 B 型模组-金手指形态

特点：立式安装，占用空间小，满足LED驱动及开关/场景面板等子设备需求。

封装尺寸要求应与图C.2相符合，PCB厚度为1.2±0.1mm，金手指开槽宽度要大于1.3mm。



a）正面封装尺寸要求　　b）背面封装尺寸要求

图C.2 B 型模组尺寸与引脚规范

B型模组引脚定义以及复用功能说明见表C.2。

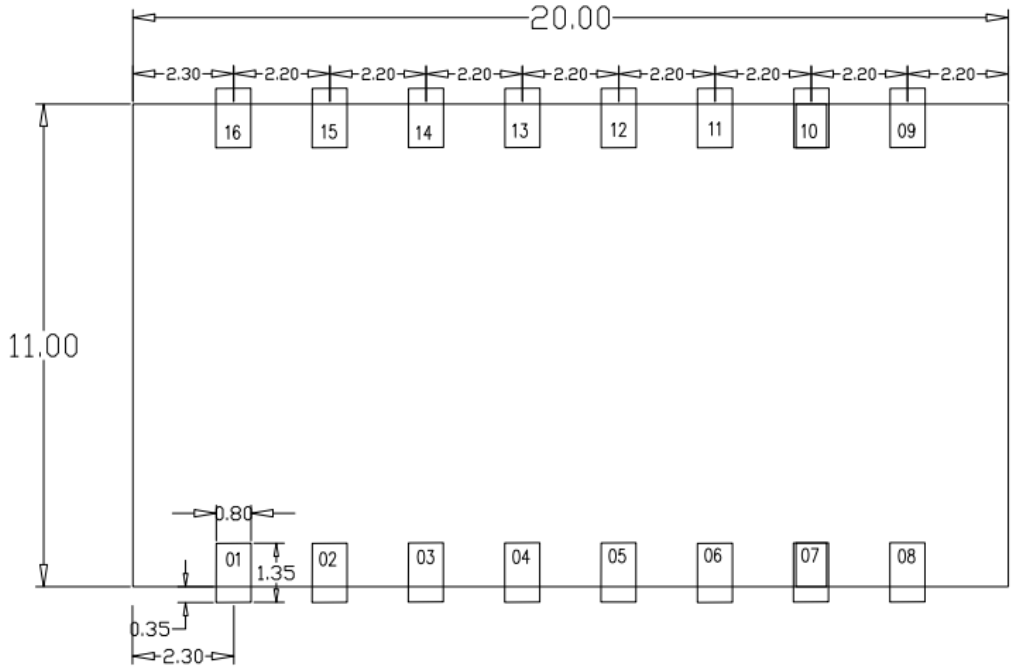
表C.2 B 型模组引脚定义及复用说明

序号	PIN名称	备注说明
1	3.3Vin	模组3.3V 电源输入管脚
2	GND	系统GND
3	GPIO0	复用信号 0：GPIO_9 默认输入，通用输入输出默认 PWM0
4	UART1-RXD	模组默认UART1-RX，业务通信串口接收
5	GPIO3	复用信号 0：GPIO_3 默认输入，通用输入输出
6	UART1-TXD	模组默认UART1-TX，业务通信串口发送
7	GPIO15	复用信号 0：GPIO_15 默认输入，通用输入输出。 复用信号 7：HW_ID_0 硬件版本号
8	GPIO4	复用信号 0：GPIO_4 默认输入，通用输入输出。 复用信号 1：LED3 通用 LED，默认PWM1
9	GPIO16	复用信号 0：GPIO_16 默认输入，通用输入输出。 复用信号 1：LED5 通用 LED
10	NC/PA Vcc	NC/7V/12V供电（兼容设计）
11	VIN4	ADC（Analog to Digital Converter）输入。
12	VIN5	ADC（Analog to Digital Converter）输入。
13	VIN6	ADC（Analog to Digital Converter）输入。
14	GND	系统 GND
15	PLC-	PLC- 通信口，需设计防护和耦合电路隔离 AC 电源；一般要求防护能力：差模/共模：+/-4KV。
16	GND	系统GND
17	PLC+	PLC+ 通信口，需设计防护和耦合电路隔离 AC 电源；一般要求防护能力：差模/共模：+/-4KV;

表C.2所示管脚定义中，第1，2(3.3V/GND)，3.8(PWM0/PWM1)，4，6(RX/TX业务口)，10(NC/7V/12V)，11,12/13(ADC)， 15,17(PLC-/PLC+)为固定功能引脚，其他引脚，各模组厂家可依据芯片功能自定义。

C.3　C 型模组-小尺寸邮票孔

特点：贴片安装，满足轨道灯/磁吸灯等子设备需求。
封装尺寸要求见图C.3。



图C.3 C 型模组尺寸与引脚规范（单位为毫米）

C型模组引脚定义以及复用功能说明见表C.3。

表C.3 C 型模组引脚定义及复用说明

PIN序号	PIN定义	备注说明
1	PLC-	PLC- 通信口，需设计滤波网络去其他AC电源隔离；一般要求防护能力：差模/共模：+/-4KV。
2	PLC+	PLC+ 通信口，需设计滤波网络去其他AC电源隔离；一般要求防护能力：差模/共模：+/-4KV。
3	VIN	ADC 输入
4	UART1_RX	复用信号 0：UART1_RXD 默认输入，UART1 数据接收，用于烧录测试。 复用信号 1：GPIO_13 通用输入输出。 复用信号 3：I2C_SDA I2C 数据。 复用信号 4：AFE_AD_DATA_VLD AFE的数据有效信号。
5	UART1_TX	复用信号 0：UART1_TXD 默认输出，UART1 数据发送，用于烧录测试 复用信号 1：GPIO_14 通用输入输出。 复用信号 2：I2C_SCL I2C 时钟。
6	GPIO0	复用信号 0：GPIO_0 输入输出 复用信号1：PWM0数据输出
7	GND	系统GND
8	3V3	电源输入
9	GPIO4	GPIO_4 输入输出，复用信号0：PWM1数据输出

表C.3　C型模组引脚定义及复用说明（续）

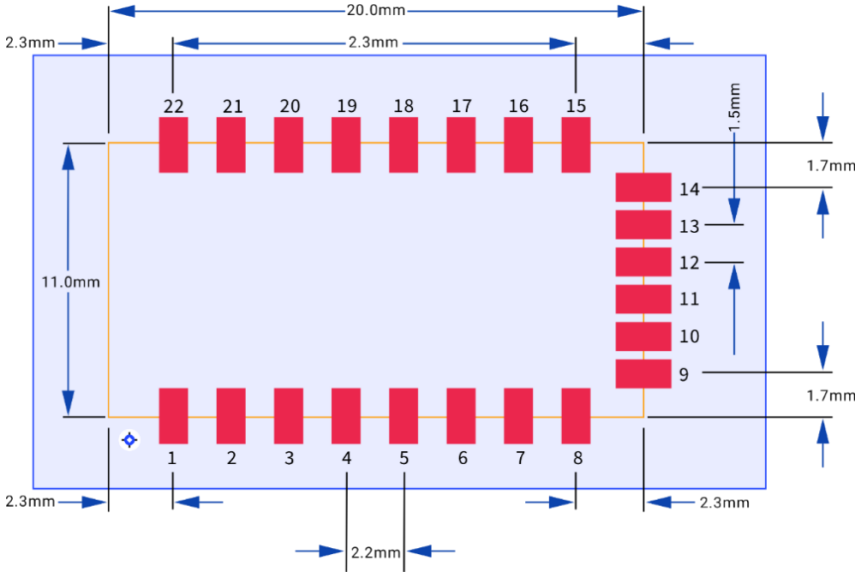
PIN序号	PIN定义	备注说明
10	GPIO3	GPIO输入输出，复用信号1
11	GPIO15	GPIO输入输出
12	GPIO16	GPIO 输入输出，复用信号 1：SPI_CSN SPI片选，低电平有效
13	GPIO17	GPIO输入输出
14	NC/PA Vcc	NC/7V/12V供电（兼容设计）
15	UART0_RX	UART0_RX 业务口，用于和外部 MCU 通信
16	UART0_TX	UART0_TX 业务口，用于和外部MCU通信

表 C.3 所示的管脚定义中，第 1，2(PLC-/PLC+)，3(ADC)，7,8(GND/3.3V)，6,9（PWM0/PWM1）,14(NC/7V/12V)，15,16(RX/TX业务口)为固定功能引脚，其他引脚，各模组厂家可依据芯片功能自定义。

C.4　D 型模组-邮票孔

特点：贴片安装，满足轨道灯/磁吸灯/场景面板等子设备需求。

封装尺寸要求见图C.4。



图C.4 D 型模组尺寸与引脚规范（单位为毫米）

D型模组引脚定义以及复用功能说明见表C.4。

表C.4 D 型模组引脚定义及复用说明

PIN序号	PIN定义	备注说明
1	PLC-	PLC- 通信口，需设计滤波网络去其他AC电源隔离；一般要求防护能力：差模/共模：+/-4KV；
2	PLC+	PLC+ 通信口，需设计滤波网络去其他AC电源隔离；一般要求防护能力：差模/共模：+/-4KV；
3	VIN	ADC 输入
4	UART1_RX	默认UART1_RX　UART1 数据接收
5	UART1_TX	默认UART1_RX　UART1 数据发送

表C.4 D型模组引脚定义及复用说明（续）

PIN序号	PIN定义	备注说明
6	GPIO0	GPIO输入输出 / PWM0数据输出
7	GND	系统GND
8	3V3	电源输入
9	GPIO1	GPIO输入输出
10	GPIO18	GPIO输入输出
11	GPIO19	GPIO输入输出
12	GPIO20	GPIO输入输出
13	GPIO21	GPIO输入输出
14	GPIO11	GPIO输入输出
15	GPIO4	GPIO 输入输出
16	GPIO3	GPIO输入输出
17	GPIO5	GPIO输入输出/ PWM1数据输出
18	GPIO16	GPIO输入输出
19	GPIO17	GPIO输入输出
20	GND	系统地
21	UART0_RX	UART0_RX 业务口
22	UART0_TX	UART0_TX 业务口

附 录 D
（规范性）
PLC 芯片层互联规范

本文件芯片互联规范遵循IEEE Std 1901.1™-2018 IEEE Standard for Medium Frequency (less than 12 MHz) Power Line Communications for Smart Grid Applications，本章节针对修订内容进行补充。

D.1 物理层协议

D.1.1 工作频段

物理层Band1频段作为强制模式支持，Band 0频段可作为可选模式支持。对于支持的频段应支持表D.1 ～ 表D.5中列出的TMI，达到速率和可靠性动态调整的目的。

表D.1 频段说明

频段	频率范围 (MHz)	起始子载波 ID	结束子载波 ID
Band 0	1.953-11.96	80	490
Band 1	2.414-5.615	100	230

D.1.2 TMI模式

为了进一步满足应用物理层速率自适应的目的，对于表D.1中支持的频段应支持表D.2 ～ 表D.5中列出的TMI与eTMI。

TMI与eTMI的定义参考IEEE Std 1901.1™-2018章节8.15.4 Table 140与Table 141。

Band 0 所支持的TMI见表D.2。

表D.2 Band 0 支持的 TMI

TMI/ eTMI	TMI 0	TMI 1	TMI 2	TMI 3	TMI 4	TMI 5	TMI 6	TMI 7	TMI 8	TMI 9	TMI 10	TMI 11	TMI 12
物理块大小	520	520	136	136	136	136	136	520	520	520	520	72	72
1 物理块符号数	51	25	16	73	46	36	23	178	102	88	51	12	24
2 物理块符号数	102	52	34	146	94	74	46	358	204	178	102	24	48
3 物理块符号数	153	77	52	221	142	112	71	538	306	268	153	36	74
4 物理块符号数	204	104	68	294	188	148	94	-	408	358	204	48	98

Band 0 所支持的eTMI见表D.3。

表D.3 Band 0 支持的 eTMI

TMI/ eTMI	eTMI 0	eTMI 1	eTMI 2	eTMI 3	eTMI 4	eTMI 5	eTMI 6	eTMI 7	eTMI 8	eTMI 9	eTMI 10
物理块大小	520	520	520	520	520	520	136	136	136	136	136
1 物理块符号数	3	6	6	13	25	13	7	6	3	3	2
2 物理块符号数	6	14	14	26	52	26	16	14	6	6	4
3 物理块符号数	11	22	22	41	77	41	25	22	11	11	6
4 物理块符号数	14	28	28	54	104	54	34	28	14	14	8

Band 1 所支持的TMI见表D.4。

表D.4 Band 1 支持的 TMI

TMI/ eTMI	TMI 0	TMI 1	TMI 2	TMI 3	TMI 4	TMI 5	TMI 6	TMI 7	TMI 8	TMI 9	TMI 10	TMI 11	TMI 12
物理块大小	520	520	136	136	136	136	136	520	520	520	520	72	72
1 物理块符号数	162	81	52	246	151	123	75	577	324	288	162	38	78
2 物理块符号数	324	162	104	494	302	246	152	-	-	578	324	78	158
3 物理块符号数	486	243	156	X	453	371	227	-	-	-	486	118	238
4 物理块符号数	-	324	208	X	X	494	304	-	-	-	-	158	318

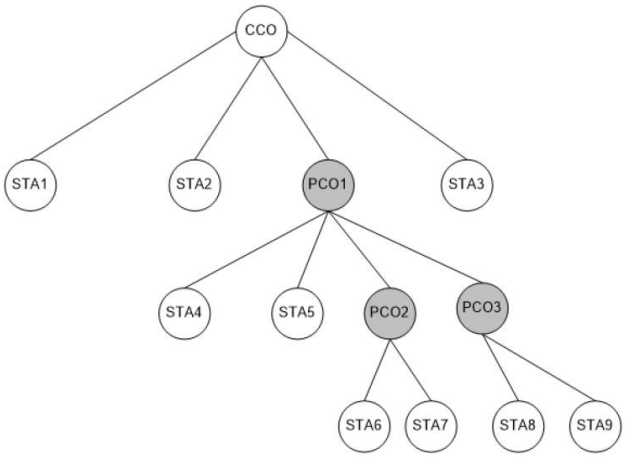
Band 1 所支持的eTMI见表D.5。

表D.5 Band 1 支持的 eTMI

TMI/ eTMI	eTMI 0	eTMI 1	eTMI 2	eTMI 3	eTMI 4	eTMI 5	eTMI 6	eTMI 7	eTMI 8	eTMI 9	eTMI 10
物理块大小	520	520	520	520	520	520	136	136	136	136	136
1 物理块符号数	11	23	18	41	81	38	25	21	11	11	5
2 物理块符号数	22	46	38	82	162	78	52	42	22	22	12
3 物理块符号数	33	71	58	123	243	118	77	63	33	33	17
4 物理块符号数	44	94	78	164	324	158	104	84	44	44	24

D.2 网络拓扑和组网方式

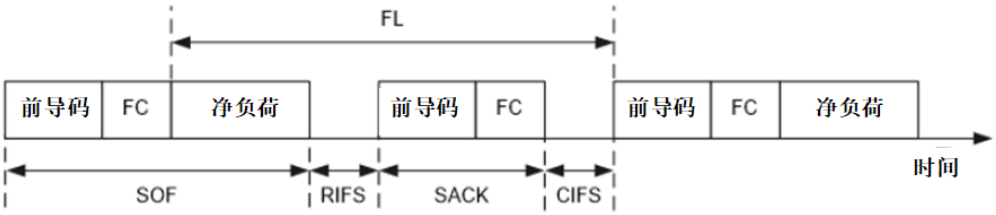
PLC网络中有三种节点，以CCO（中央协调节点）、PCO（代理节点）、STA（终端）为组成的树形结构，见图D.1，组网方式应遵循IEEE Std 1901.1™-2018的规范要求，提高网络覆盖范围和可靠性。



图D.1 树形组网

D.3 报文长度计算规范与间隔

帧间隔是指线路上传输的物理层协议帧之间需要保证的最少时间间隔。本文件中所涉及的报文长度计算FL与帧间隔应遵IEEE Std 1901.1™-2018规范，报文长度计算与帧间隔格式见图D.2。



图D.2 报文长度计算 FL 与帧间隔

D.4 网络管理子层协议

D.4.1 封包类型

网络管理子层应完成基本的组网环节和网络维护环节，通过网络管理报文来实现管理功能，管理包头字格式段见表D.6。

表D.6 管理包头字段

字段	字节号	字段大小(字节)
MMTYPE	0-1	2
保留	2-3	2

表D.6中的MMTYPE表示管理消息类型，其含义见表D.7。

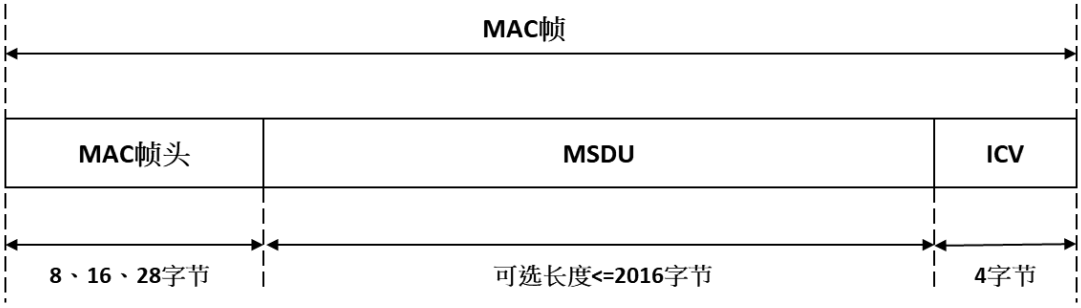
表D.7 MMTYPE

管理消息名称	管理消息类型标识符
关联请求 (MMeAssocReq)	0x0000
关联确认 (MMeAssocCnf)	0x0001
关联汇总指示 (MMeAssocGatherInd)	0x0002
代理变更请求 (MMeChangeProxyReq)	0x0003
代理变更确认 (MMeChangeProxyCnf)	0x0004
代理变更确认位图版(MMeChangeProxyBitMapCnf)	0x0005
离网指示 (MMeLeaveInd)	0x0006
心跳检测 (MMeHeartBeatCheck)	0x0007
发现列表 (MMeDiscoverNodeList)	0x0008
通信成功率上报 (MMeSuccessRateReport)	0x0009
网络冲突上报 (MMeNetworkConflictReport)	0x000A
保留	0x000B-0xFFFF

D.5 MAC 子层协议

D.5.1 MAC帧格式

MAC帧是不同站点的MAC层之间进行数据传送的基本传输单元。一个MAC帧由MAC帧头、MAC业务数据单元MSDU和完整性校验值ICV组成。MAC帧格式应使用IEEE Std 1901.1™-2018定义的帧格式，见图D.3。



图D.3 MAC 帧格式

D.5.2 MAC帧头格式

数据链路层发送MSDU报文时，根据发送原语中的发送类型、MSDU序列号、MSDU类型等，生成MAC帧头，MAC帧头格式表D.8。

表D.8 MAC 帧头格式

字段	字节号	比特位	字段大小(比特)
版本	0	0-3	4
发送类型	0	4-7	4
发送次数限值	1	0-4	5
保留	1	5-7	3
MSDU 序列号	2	0-7	16
	3	0-7	
MSDU 类型	4	0-7	8
MSDU 长度	5	0-7	11
	6	0-2	
重启次数	6	3-6	4
MAC 帧头类型 (default=1)	6	7	1
保留	7	0-7	8
中继可变区域	8-27	0-7	64

表D.8中的MAC帧头类型设置为1时且通常用于数据包中继时，设置中继可变区域，中继可变区域字段定义见表D.9。

表D.9 中继可变区域字段

字段	字节号	比特位	字段大小(比特)
OSTEI	8	0-7	12
	9	0-3	
ODTEI	9	4-7	12
	10	0-7	
路由总跳数	11	0-3	4
路由剩余跳数	11	4-7	4
代理主路径标识	12	0	1
广播方向	12	1-2	2
MAC 地址标识(defaut=0)	12	3	1

表D.9　中继可变区域字段（续）

字段	字节号	比特位	字段大小(比特)
离网最长等待时间	12	4-7	4
组网序列号	13	0-7	8
保留	14-15	0-7	16
MAC地址可变区域	16-27	0-7	96

表D.9中的“MAC 地址标识”为0 表示不使用“MAC 地址可变区域”，1 表示使用“MAC 地址可变区域”，故使用“MAC 地址标识”为 1 时“MAC 帧头格式“总长度为 28 个字节。MAC地址可变区域字段定义见表D.10。

表D.10 MAC 地址可变区域字段

字段	字节号	比特位	字段大小(比特)
原始源MAC地址	16-21	0-7	48
原始目的MAC地址	22-27	0-7	48

离网最长等待时间默认值设为3分钟，可以自定义更改，取值范围为0～15分钟。超时后设备需转换回无组网状态，以利于无头模式(Non-Header-Mode NHM)的转换。

MSDU类型字段用于指示MSDU帧的类型，见表D.11。

表D.11 MSDU 类型

值	定义	MAC帧头类型
0	网络管理消息	0
1-47	数据链路层待扩展	-
48	应用层报文	0
49	IP 报文	0
50	测试报文	0
51	以太网络封包报文	0
52	保留	0
53	无头模式报文	0
其他	保留	-

D.5.3　PLC应用报文补充说明

本章节内容为 “6.4 PLC应用报文”章节中的报文格式的补充说明。

当MAC帧的MSDU类型为“48：应用层报文时”，报文格式见表D.12。

表D.12 通用报文格式

字段	字节号	比特位	域大小(比特)
报文端口号	0	0-7	8
PLC ID	1-2	0-15	16
报文控制字	3	0-7	8
用户数据区域	4-4+L	8*L	8*L

D.5.3.1　报文端口号

报文端口号是8比特的字段，指CCO与STA之间进行交互时，应用层报文传输中的端口号，升级业务取值为0x12。

D.5.3.2 PLC ID

PLC ID是16比特的字段，指CCO与STA之间传输的PLC ID，具体内容和取值见表D.13, 为本文件“6.4.1 PLC ID的补充”。CCO与STA间使用表D.13中的PLC ID传输时，MSDU类型使用48，即使用应用层报文传输。

表D.13 PLC ID

PLC ID	含义	报文端口号
0x0030	开始升级	0x12
0x0031	停止升级	0x12
0x0032	传输文件数据	0x12
0x0033	传输文件数据（单播转本地广播）	0x12
0x0034	查询站点升级状态	0x12
0x0035	执行升级	0x12
0x0036	查询站点信息	0x12

D.5.3.3 报文控制字

报文控制字是8比特的字段，默认设置为0。

D.5.3.4 用户数据区域

用户数据区域的具体格式由PLC ID决定。
当PLC ID为表6.4.1中的数值时，用户数据区域格式见表D.14。

表D.14 通用报文格式

字段	字节号	比特位	域大小(比特)
CRC	0-1	0-15	16
User Data长度	2-3	0-15	16
User Data	4-4+L	L*8	L*8

D.5.3.4.1 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-xmodem（0x1021），$x^{16}+x^{12}+x^{5}+1$，大端序。CRC源码范例参考附录E。

D.5.3.4.2 User Data 长度 L

待发送的报文 User Data长度，小端。

D.5.3.4.3 User Data

待发送的报文。

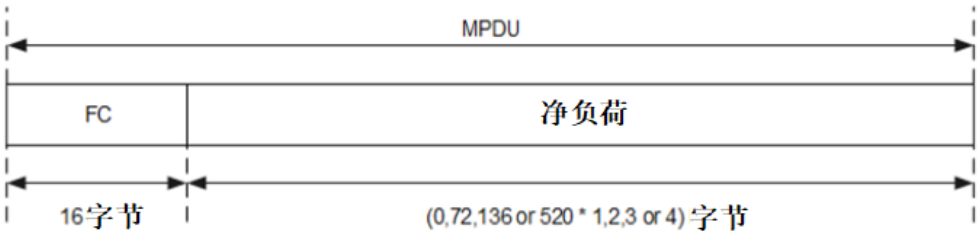
D.5.4 MAC帧尾完整性校验(ICV)

完整性校验是针对MAC帧计算的循环冗余校验值，计算完整性校验值时，不包括MAC帧头。完整性校验应使用32比特的循环冗余校验算法。

D.5.5 MPDU信标模式帧格式

D.5.5.1 MPDU 帧头控制格式

MPDU是MAC层协议数据单元，由MAC子层提供给物理层，在不同站点的物理层之间传送数据的基本传输单元。MPDU帧格式如图D.4所示。



图D.4 MPDU 格式

MPDU的帧控制字段长度为16字节，MPDU帧控制字段的格式表D.15。

表D.15 MPDU 帧控制字段

字段	字节号	比特位	字段大小(比特)
定界符类型	0	0-2	3
网络类型		3-7	5
网路标识	1	0-7	24
	2	0-7	
	3	0-7	
可变区域	4-11	0-7	68
	12	0-3	
标准版本号	12	4-7	4
帧控制校验序列	13-15	0-7	24

定界符类型长度为3比特，用来指示MPDU的帧类型。MPDU帧类型的不同，可变区域也不同。定界符类型的取值见表D.16。

表D.16 定界符类型

定界符值	描述
0x0	信标帧
0x1	SOF 帧
0x2	选择确认帧
0x3	网间协调帧
0x4-0x7	保留

信标帧用于CCO进行网络管理。信标帧的可变区域的格式见表D.17。

表D.17 信标帧可变区域

字段	字节号	比特位	字段大小(比特)
信标时间戳	4	0-7	32
	5	0-7	
	6	0-7	
	7	0-7	
源TEI	8	0-7	12
	9	0-3	
分集拷贝基本模式		4-7	4
相线	10	0-1	2
追随符号数PSS		2-5	4
保留		6-7	2
	11	0-7	8
	12	0-3	4

SOF帧主要用于设备之间传输数据。SOF帧的可变区域内容见表D.18。

表D.18 SOF 帧可变区域

字段	字节号	比特位	字段大小(比特)
源TEI	4	0-7	12
	5	0-3	
目的TEI		4-7	12
	6	0-7	
链路标识符	7	0-7	8
帧长	8	0-7	12
	9	0-3	
物理块个数		4-7	4
广播标志位	10	0	1
重传标志位		1	1
加密模式选择		2-3	2
分级拷贝基本模式		4-7	4
分级拷贝扩展模式	11	0	1
追随符号数PSS		1-4	4
保留		5-7	3
	12	0-3	4

导频符号数用于表示导频符号插入方式，按照每m个数据载荷符号插入n个导频符号，导频符号数见表D.19。

表D.19 导频符号数

值	描述
0x0	不使用导频符号
0x1	m=2，n=1
0x2	m=4，n=1
0x3	m=8，n=1
0x4	m=16，n=1
0x5	m=4，n=2
0x6	m=8，n=2
0x7	m=16，n=2
0x8	m=8，n=4
0x9	m=16，n=4
0xA-0xF	保留

选择确认帧是接收设备用来向发送设备反馈SOF帧的接收情况。选择确认帧的可变区域内容见表D.20。

表D.20 选择确认帧可变区域

字段	字节号	比特位	字段大小(比特)
接收结果	4	0-3	4
源TEI	4	4-7	12
	5	0-7	
目的TEI	6	0-7	12
	7	0-3	
接收物理块个数		4-6	3
保留		7	1
信道质量	8	0-7	8
站点负载	9	0-7	8
保留	10-11	0-7	16
扩展帧类型	12	0-3	4

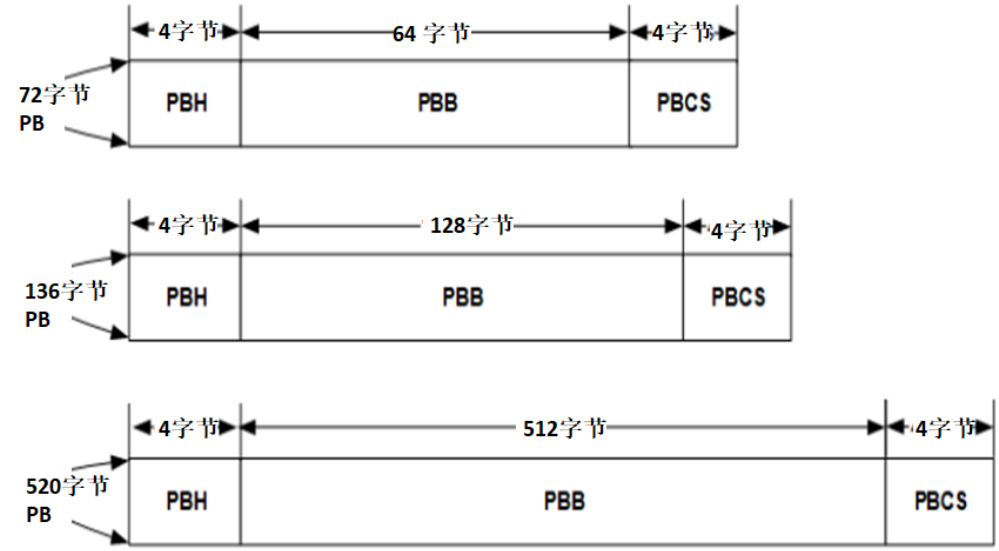
网间协调帧用于CCO进行网间时隙的竞争协调，网间协调帧的可变区域内容见表D.21。

表D.21 网间协调帧可变区域

字段	字节号	比特位	字段大小(比特)
持续时间（1 ms）	4	0-7	16
	5	0-7	
带宽开始偏移	6	0-7	16
	7	0-7	
接收到的邻居网络号	8	0-7	24
	9	0-7	
	10	0-7	
保留	11	0-7	12
	12	0-3	

D.5.5.2 MPDU 帧载荷数据格式

SOF 帧的 PB 块携带由 MSDU 所组成的 MAC 帧的分段，每个 PB 块包含一个物理块头 PBH、物理块体 PBB 和物理块检查序列 PBCS，PB 块格式如图 D.5 所示。



图D.5 MPDU 的 PB 格式

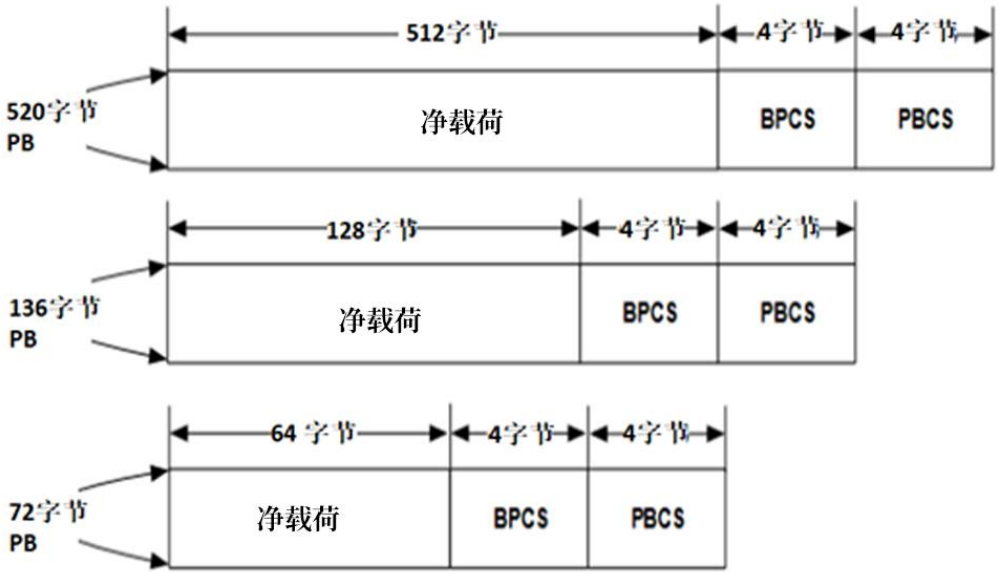
物理块头包含物理块体的属性信息，物理块头的格式见表D.22。

表D.22 物理块头格式

字段	字节号	比特位	字段大小(比特)
序列号	0	0-5	6
帧起始标志	0	6	1
帧结束标志	0	7	1
保留	3	0-7	24

帧载荷校验序列(PBCS)为使用的32比特的循环冗余校验算法，物理块检查序列是一个32比特的字段。校验时，以帧载为目标，使用32比特的循环冗余校验算法，进行校验，校验值填充在物理块检查序列的位置。

信标帧的PB块包含数据净载荷、帧载荷校验序列BPCS，物理块PB检查序列PBCS，格式见图D.6。



图D.6 信标 MPDU 的 PB 格式

帧载荷校验序列(PBCS)是信标帧载荷内容的校验值，校验的范围是信标物理块中帧载荷(BPCS)部份的内容。帧载荷校验序列使用的32比特的循环冗余校验算法。

物理块检查序列是一个32比特的字段。校验时，以帧载荷和帧载荷序列两部份为目标，使用32比特的循环冗余校验算法，进行校验，校验值填充在物理块检查序列的位置。

CRC-32 应使用下列标准生成32次多项式计算：

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

式中：

x —— 计算校验取值位。

G(x)——所有字段经循环冗余校验算法加总值。

D.5.6 MPDU无头模式（NHM）帧格式

全屋互联规范中无头模式可作为必选模式支持，在道路照明规范中无头模式可作为可选模式支持。无头模式的MPDU帧头格式见表D.23。

表D.23 无头模式 MPDU 帧头

字段	字节号	比特位	字段大小(比特)	无头模式值
定界符类型	0	0-2	3	0x1
网络类型		3-7	5	0x00
网路标识	1	0-7	24	0x000000
	2	0-7		
	3	0-7		
可变区域	4-11	0-7	68	-
	12	0-3		
标准版本号	12	4-7	4	0x0
帧控制校验序列	13-15	0-7	24	-

无头模式的SOF帧主要用于网络处于无头模式时设备之间传输数据。无头模式MPDU SOF帧的可变区域内容见表D.24。

表D.24 无头模式 MPDU SOF 可变区域

字段	字节号	比特位	字段大小(比特)	无头模式值
源TEI	4	0-7	12	0x000
	5	0-3		
目的TEI		4-7	12	0xFFF
	6	0-7		
链路标识符(LID)	7	0-7	8	0 ～ 254
帧长(FL)	8	0-7	12	1 ～ 4095
	9	0-3		
物理块个数(PB Count)		4-7	4	1 ～ 4
广播标志位	10	0	1	1
重传标志位		1	1	0 ～ 1
加密模式选择		2-3	2	3
分集拷贝基本模式		4-7	4	0 ～ 15
分集拷贝扩展模式	11	0	1	0 ～ 1
追随符号数(PSS)		1-4	4	0 ～ 9
保留		5-7	3	-
	12	0-3	4	

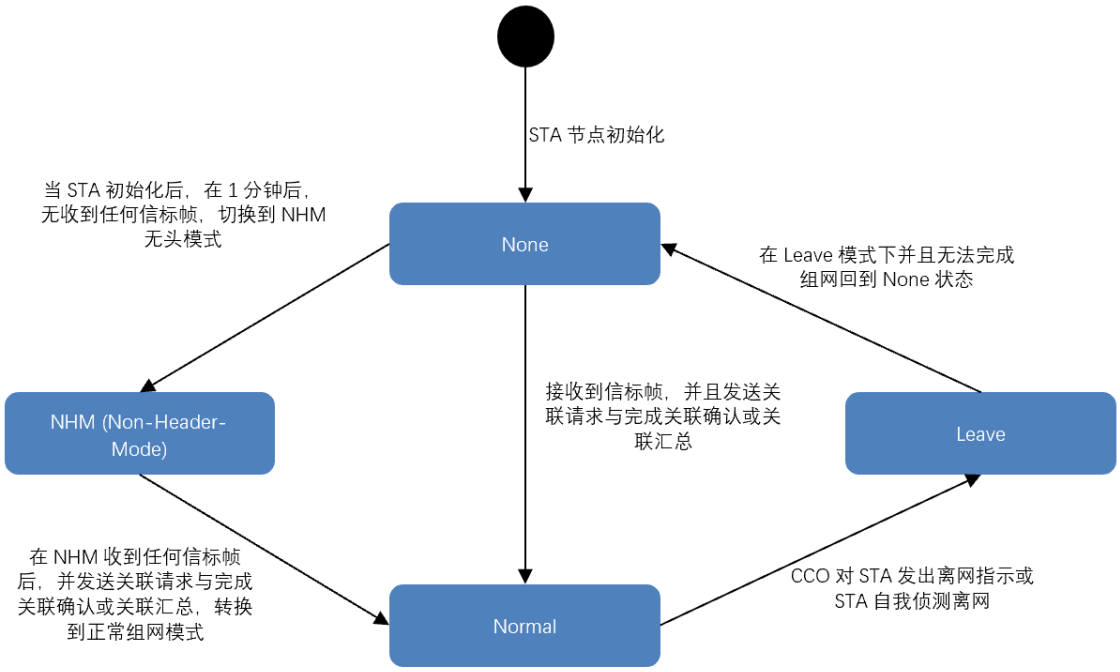
网络处于组网模式与网络处于无头模式，网络MAC帧头与地址不同，针对无头模式的新增字段见表D.25。

表D.25 无头模式新增字段

MAC 帧头	无头模式新增字段			MSDU	ICV
	NHM帧头	NHM MAC 地址	NHM帧尾		
16 bytes	1 bytes = 0x22	6 bytes	1 bytes = 0x03	…	4 bytes

表D.25中的ICV的计算是针对“无头模式新增字段”与MSDU的校验数据。

在CCO失效后进入无头模式，考虑全部离网的情况下，当STA切换到NHM模式时，应采用MAC帧头填入STEI = 0x000, DTEI = 0xFFF，以广播的方式、并采用与CSMA/CA避免碰撞的机制发送，以保证每个节点都可以收到控制设备的报文。为了避免方法产生广播风暴，设备必需在切换到NHM模式时，每个原发送节点发送每个封包时都需要增加序列号，且转发节点针对原发节点的NHM MAC 地址与MSDU 序列号皆不做修改，并且MSDU净负荷前面应增加NHM的帧头。其中无头模式的帧头包含NHM帧头与帧尾的标签与MAC地址，在每个节点需要记录转传的MAC地址、MSDU序列号与MAC ResetCnt来过滤此封包，已经转传则不再转发，当在网站点收到无头模式报文时不做转发，用此方法来避免广播风暴的产生。MAC Header SendType = 1 (Global Broadcast), MAC Header Hop Count = 15。设备从Leave状态需依照“最长离网等待时间”等待超时后转换到None状态。“最长离网等待时间”默认设为3分钟，取值范围为0 ～ 15分钟。状态转换见图D.7。



图D.7 无头模式状态转换图

D.6 远程升级协议

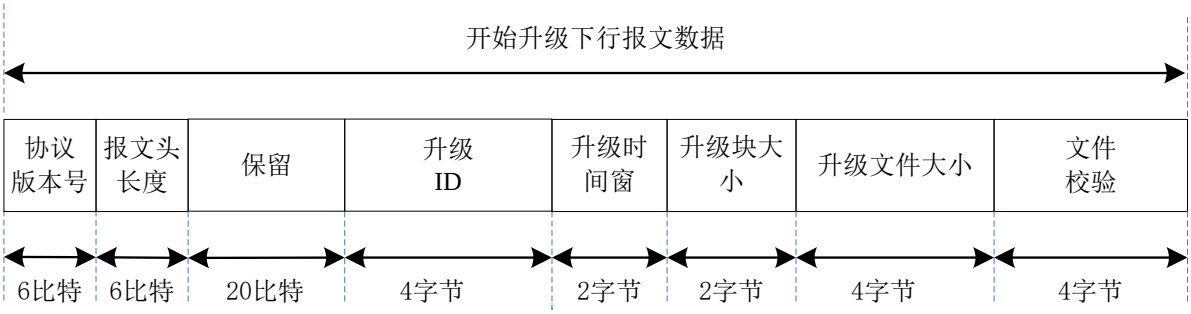
D.6.1 升级报文

D.6.1.1 下行报文格式

D.6.1.1.1 开始升级

D.6.1.1.1.1 开始升级下行报文格式

CCO向STA发送的开始升级下行报文数据格式见图D.8。



图D.8 开始升级下行报文数据格式

开始升级下行报文数据字段见表D.26。

表D.26 开始升级下行报文数据字段说明

字段	字节号	比特位	域大小(比特)
协议版本号	0	0-5	6
报文头长度		6-7	6
	1	0-3	
保留		4-7	4
	2-3	0-15	16
升级ID	4-7	0-31	32
升级时间窗	8-9	0-15	16
升级块大小	10-11	0-15	16
升级文件大小	12-15	0-31	32
文件CRC校验	16-19	0-31	32

D.6.1.1.1.2 协议版本号

协议版本号是6比特的字段，指从CCO发送给STA的应用层数据的协议版本。考虑兼容性，本版本取值固定为1。

D.6.1.1.1.3 报文头长度

报文头长度是6比特的字段，由发送方给定，描述报文头（除数据域长度外）的长度，用于接收方从报文头偏移报文头长度找到数据域的位置。

D.6.1.1.1.4 升级 ID

升级ID是32比特的字段，在开始升级时产生该值，每次升级不应重复，且不能为0。下发停止升级命令时，如果不知道该次升级的升级ID，可以使用0作为通用升级ID终止本次升级操作。

升级ID用于区分每次升级，即每次升级都应该有变化（可以递增，也可以随机变化）。STA端在收到开始升级报文时，需要保存此升级ID，在应答CCO时使用自身存储的升级ID，以此向CCO表明STA当前正工作在哪次升级流程中（忽略CCO 发送的升级ID）；CCO在查询STA时，根据STA应答的文件ID判断STA端是否正处于当前升级流程，并以此决定继续流程或者忽略此STA，如果当前 STA 不在升级状态，即空闲态，则回复 0，如果在升级状态，回复真实升级 ID。

D.6.1.1.1.5 升级时间窗

升级时间窗是16比特的字段，表示升级过程的最长时间，超过该时间文件没有收全，本次传输STA自动放弃。单位：分钟。

文件传输完毕后，CCO会通知站点重启，使新程序生效；如果STA识别到自身需要升级软件，且升级文件实际已全部收全，但在时间窗内没有收到过重启命令，则时间窗到期时自行重启。

D.6.1.1.1.6 升级块大小

升级块大小是16比特的字段，表示升级包载荷中包含的数据块的大小，每个数据帧只传输一个数据块，除最后1个数据块外，每个数据块的大小应该相等。允许的取值为：100、200、300、400字节。

D.6.1.1.1.7 升级文件大小

升级文件大小是32比特的字段，表示升级文件包含的字节数。

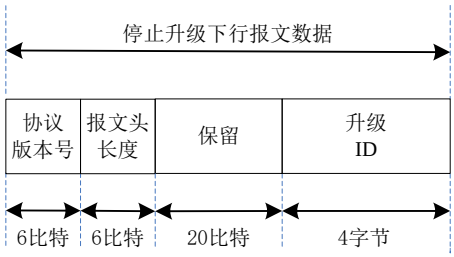
D.6.1.1.1.8 文件校验

文件校验是32比特的字段，表示文件所有内容的CRC-32校验。

D.6.1.1.2 停止升级

D.6.1.1.2.1 停止升级下行报文格式

CCO向STA发送的停止升级下行报文数据格式应与图D.9相符合。



图D.9 停止升级下行报文数据格式

停止升级下行报文数据字段见表D.27。

表D.27 停止升级下行报文数据字段说明

字段	字节号	比特位	域大小(比特)
协议版本号	0	0-5	6
报文头长度	0	6-7	6
保留	1	0-3	4
		4-7	
	2-3	0-15	16
升级ID	4-7	0-31	32

D.6.1.1.2.2 协议版本号

协议版本号是6比特的字段，指从CCO发送给STA的应用层数据的协议版本。考虑兼容性，本版本取值固定为1。

D.6.1.1.2.3 报文头长度

报文头长度是6比特的字段，由发送方给定，描述报文头（除数据域长度外）的长度，用于接收方从报文头偏移报文头长度找到数据域的位置。

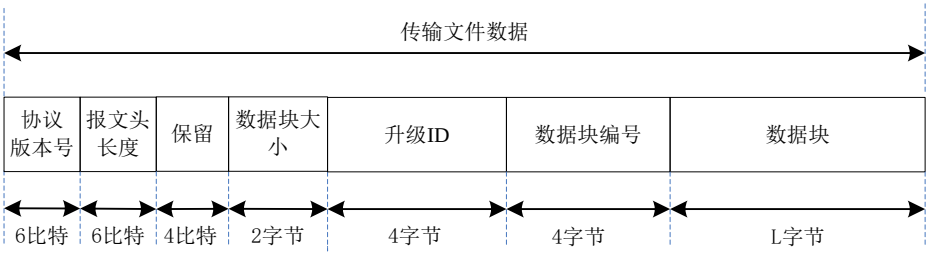
D.6.1.1.2.4 升级 ID

升级ID是32位的字段，含义同D.6.1.1.1.4。

D.6.1.1.3 传输文件数据

D.6.1.1.3.1 传输文件数据下行报文格式

CCO向STA发送的传输文件数据数据格式见图D.10。



图D.10 传输文件数据下行报文数据格式

传输文件数据字段见表D.28。

表D.28 传输文件数据下行报文字段说明

字段	字节号	比特位	域大小(比特)
协议版本号	0	0-5	6
报文头长度		6-7	6
	1	0-3	
保留		4-7	4
数据块大小	2-3	0-15	16
升级ID	4-7	0-31	32
数据块编号	8-11	0-31	32

D.6.1.1.3.2 协议版本号

协议版本号是6比特的字段，指从CCO发送给STA的应用层数据的协议版本。考虑兼容性，本版本取值固定为1。

D.6.1.1.3.3 报文头长度

报文头长度是6比特的字段，由发送方给定，描述报文头（除数据域长度外）的长度，用于接收方从报文头偏移报文头长度找到数据域的位置。

D.6.1.1.3.4 数据块大小

数据块大小是16位的字段，表示数据块包含数据的字节数。

D.6.1.1.3.5 升级 ID

升级ID是32位的字段，含义同D.6.1.1.1.4。

D.6.1.1.3.6 数据块编号

起始数据块编号是32位的字段，每帧报文传输1个数据块。

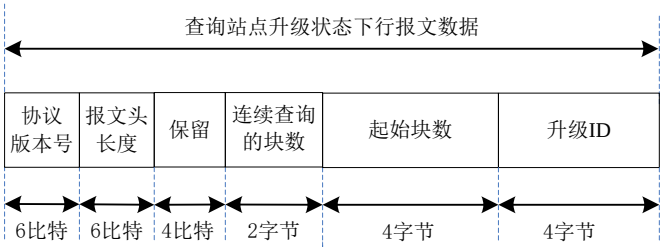
D.6.1.1.3.7 数据块

升级数据块，长度等于数据块大小。

D.6.1.1.4 查询站点升级状态

D.6.1.1.4.1 查询站点升级状态下行报文格式

CCO向STA发送的查询站点升级状态下行报文数据格式应见图D.11。



图D.11 查询站点升级状态下行报文数据格式

查询站点升级状态下行报文数据字段见表D.29。

表D.29 查询站点升级状态下行报文数据字段说明

字段	字节号	比特位	域大小(比特)
协议版本号	0	0-5	6
报文头长度		6-7	6
	1	0-3	
保留		4-7	4
连续查询的块数	2-3	0-15	16
起始块号	4-7	0-31	32
升级 ID	8-11	0-31	32

D.6.1.1.4.2 协议版本号

协议版本号是6比特的字段，指从CCO发送给STA的应用层数据的协议版本。考虑兼容性，本版本取值固定为1。

D.6.1.1.4.3 报文头长度

报文头长度是6比特的字段，由发送方给定，描述报文头（除数据域长度外）的长度，用于接收方从报文头偏移报文头长度找到数据域的位置。

D.6.1.1.4.4 连续查询的块数

连续查询的块个数，0xFFFF表示查询所有的块状态。

D.6.1.1.4.5 起始块号

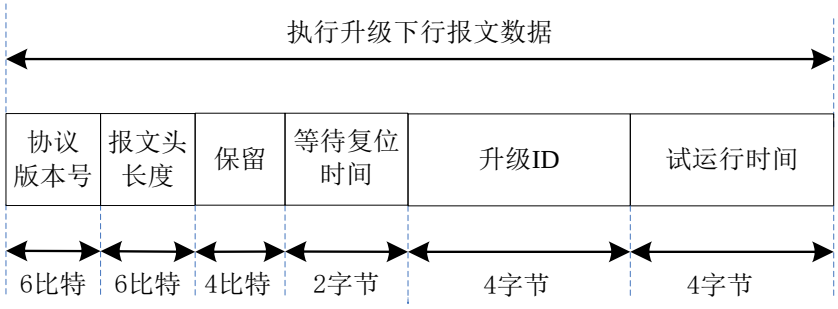
查询的起始块号。

D.6.1.1.4.6 升级 ID

升级ID是32位的字段，含义同D.6.1.1.1.4。

D.6.1.1.5 执行升级执行升级下行报文格式

CCO向STA发送的执行升级下行报文数据格式见图D.12。



图D.12 执行升级下行报文数据格式

执行升级下行报文数据字段见表D.30。

表D.30 执行升级下行报文数据字段说明

字段	字节号	比特位	域大小(比特)
协议版本号	0	0-5	6
报文头长度		6-7	6
	1	0-3	
保留		4-7	4
等待复位时间	2-3	0-15	16
升级 ID	4-7	0-31	32
试运行时间	8-12	0-31	32

D.6.1.1.5.2 协议版本号

协议版本号是6比特的字段，指从CCO发送给STA的应用层数据的协议版本。考虑兼容性，本版本取值固定为1。

D.6.1.1.5.3 报文头长度

报文头长度是6比特的字段，由发送方给定，描述报文头（除数据域长度外）的长度，用于接收方从报文头偏移报文头长度找到数据域的位置。

D.6.1.1.5.4 等待复位时间

等待复位时间是16位的字段，站点收到此报文后等待该时间后重启，单位：秒。

D.6.1.1.5.5 升级 ID

升级ID是32位的字段，含义同D.6.1.1.1.4 。

D.6.1.1.5.6 试运行时间

试运行时间是32位的字段，表示站点可以试运行新版程序多长时间，从重启的那一刻开始计时，若为0表示不需要试运行，单位：秒。

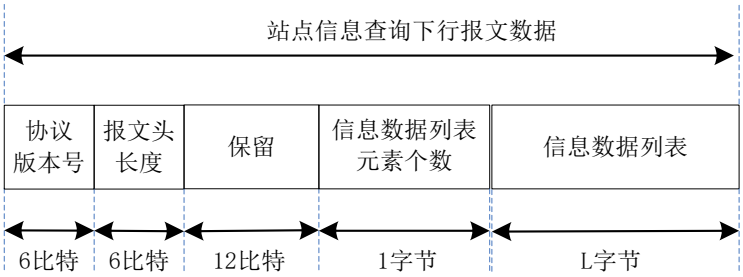
D.6.1.1.6 传输文件数据（单播转本地广播）

报文数据格式同“D.6.1.1.3 传输文件数据（单播）”。站点收到此报文后，把报文ID修改为“传输文件数据（单播）”的报文ID（0x033），在本地广播修改后的报文。

D.6.1.1.7 查询站点信息

D.6.1.1.7.1 查询站点信息下行报文格式

CCO向STA发送的查询站点信息下行报文数据格式见图D.13。



图D.13 查询站点信息下行报文数据格式

查询站点信息下行报文数据字段见表D.31。

表D.31 查询站点信息下行报文数据字段说明

字段	字节号	比特位	域大小(比特)
协议版本号	0	0-5	6
报文头长度		6-7	6
	1-2	0-3	
保留	3	4-15	12
信息列表元素个数	3	0-7	8

D.6.1.1.7.2 协议版本号

协议版本号是6比特的字段，指从CCO发送给STA的应用层数据的协议版本。考虑兼容性，本版本取值固定为1。

D.6.1.1.7.3 报文头长度

报文头长度是6比特的字段，由发送方给定，描述报文头（除数据域长度外）的长度，用于接收方从报文头偏移报文头长度找到数据域的位置。

D.6.1.1.7.4 信息列表元素个数

信息列表中，元素的个数。

D.6.1.1.7.5 信息列表

信息列表中可包括1个或多个信息元素，每个元素ID为1字节，允许同时查询多个元素ID。信息列表元素ID见表D.32。

表D.32 信息列表数据字段说明

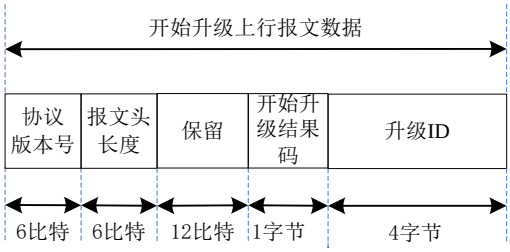
元素ID取值	说明
0	厂商编号，2字节ASCII
1	版本信息，2字节BCD码
其他	保留

D.6.1.2 上行报文格式

D.6.1.2.1 开始升级

D.6.1.2.1.1 开始升级上行报文格式

STA向CCO发送的开始升级上行报文数据格式见图D.14。



图D.14 开始升级上行报文数据格式

开始升级下行报文数据字段见表D.33。

表D.33 开始升级上行报文数据字段说明

字段	字节号	比特位	域大小(比特)
协议版本号	0	0-5	6
报文头长度	0	6-7	6
	1	0-3	
保留		4-7	4
	2	0-7	8
开始升级结果码	3	0-7	8
升级 ID	4-7	0-31	32

D.6.1.2.1.2 协议版本号

协议版本号是6比特的字段，指从STA发送给CCO的应用层数据的协议版本。考虑兼容性，当前版本取值固定为1。

D.6.1.2.1.3 报文头长度

报文头长度是6比特的字段，由发送方给定，描述报文头（除数据域长度外）的长度，用于接收方从报文头偏移报文头长度找到数据域的位置。

D.6.1.2.1.4 开始升级结果码

开始升级结果码是8位的字段，表示STA收到开始升级报文之后的处理结果错误码，0表示成功，其他值表示失败。

D.6.1.2.1.5 升级 ID

升级ID是32位的字段，含义同D.6.1.1.1.4。

D.6.1.2.2 停止升级

上行无应答。

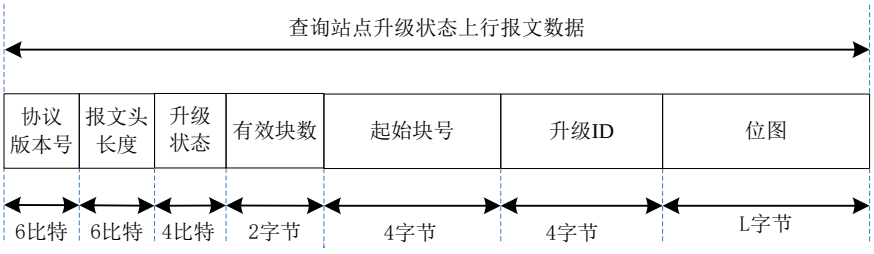
D.6.1.2.3 传输文件数据（单播）

上行无应答。

D.6.1.2.4 查询站点升级状态

D.6.1.2.4.1 查询站点升级状态上行报文格式

STA向CCO发送的查询站点升级状态上行报文数据格式见图D.15。



图D.15 查询站点升级状态上行报文数据格式

查询站点升级状态上行报文数据字段见表D.34。

表D.34 开始升级上行报文数据字段说明

字段	字节号	比特位	域大小(比特)
协议版本号	0	0-5	6
报文头长度		6-7	6
报文头长度	1	0-3	
升级状态		4-7	4
有效块数	2-3	0-15	16
起始块号	4-7	0-31	32
升级ID	8-11	0-31	32

D.6.1.2.4.2 协议版本号

协议版本号是6比特的字段，指从STA发送给CCO的应用层数据的协议版本。考虑兼容性，本版本取值固定为1。

D.6.1.2.4.3 报文头长度

报文头长度是6比特的字段，由发送方给定，描述报文头（除数据域长度外）的长度，用于接收方从报文头偏移报文头长度找到数据域的位置。

D.6.1.2.4.4 升级状态

升级的进展情况， 0-空闲态、1-接收进行态、2-接收完成态、3-升级进行态、4-试运行态。

D.6.1.2.4.5 有效块数

在位图中，有效的块数，从位图的第0个比特开始计算，当传输文件的块数不是8的整数倍时，最后有几个比特会无效。

D.6.1.2.4.6 起始块号

查询的起始块号。

D.6.1.2.4.7 升级 ID

升级ID是32位的字段，含义同D.6.1.1.1.4。

D.6.1.2.4.8 位图

描述传输中接收到的文件块位图，0表示该块数据未收到，1表示该块数据已接收到。

D.6.1.2.5 执行升级

上行无应答。

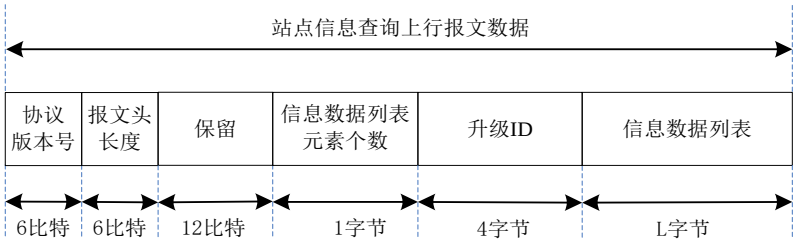
D.6.1.2.6 传输文件数据（单播转本地广播）

上行无应答。

D.6.1.2.7 查询站点信息

D.6.1.2.7.1 查询站点信息上行报文格式

STA应答CCO发送的查询站点信息上行报文数据格式见图D.16。



图D.16 查询站点信息上行报文数据格式

查询站点信息上行报文数据字段见表D.35。

表D.35 查询站点信息上行报文数据字段说明

字段	字节号	比特位	域大小(比特)
协议版本号	0	0-5	6
报文头长度		6-7	6
保留	1	0-3	
		4-7	4
	2	0-7	8
信息数据列表元素个数	3	0-7	8
升级ID	4-7	0-31	32

D.6.1.2.7.2 协议版本号

协议版本号是6比特的字段，指从STA发送给CCO的应用层数据的协议版本。考虑兼容性，本版本取值固定为1。

D.6.1.2.7.3 报文头长度

报文头长度是6比特的字段，由发送方给定，描述报文头（除数据域长度外）的长度，用于接收方从报文头偏移报文头长度找到数据域的位置。

D.6.1.2.7.4 信息数据列表元素个数

信息数据列表中元素的个数。

D.6.1.2.7.5 升级 ID

升级ID是32位的字段，含义同D.6.1.1.1.4。

D.6.1.2.7.6 信息列表

信息数据列表中，包括多个信息元素数据，每个信息元素数据的结构字段见表D.36。

表D.36 查询站点信息上行报文数据字段说明

字段	字节号	比特位	域大小(比特)
元素ID	0	0-7	8
元素数据长度	1	0-7	8
元素数据	2-N	/	/

元素ID取值以及元素长度内容定义见表D.32。

D.6.2 升级业务传输流程

站点的升级过程分为五种状态：空闲态、接收进行态、接收完成态、升级进行态、试运行态。

STA没有进行在线升级时，处于空闲状态。STA进行在线升级时，若正传输文件数据，且文件数据尚未传输完成，则处于接收进行态。STA进行在线升级时，若已完成文件数据传输，且文件数据CRC校验正确，则处于接收完成态。STA进行在线升级时，若文件数据CRC校验正确，且收到执行升级命令，还未进行重启，则处于升级进行态。STA进行在线升级时，若已经重启，且未到试运行结束时刻，则处于试运行态。

站点各状态间的转移触发条件见表D.37。

表D.37 在线升级状态转移表

当前状态	触发条件	输出	下一状态
空闲态	收到开始升级报文	开始升级应答报文	接收进行态
	收到停止升级报文	忽略	空闲态
	收到传输文件数据（单播）报文	忽略	空闲态
	收到传输文件数据（单播转本地广播）报文	忽略	空闲态
	收到查询站点升级状态报文	查询站点升级状态应答报文	空闲态
	收到执行升级报文	忽略	空闲态
	收到查询站点信息报文	查询站点信息应答报文	空闲态
接收进行态	收到开始升级报文	忽略	接收进行态
	收到停止升级报文	/	空闲
	收到传输文件数据（单播）报文	处理接收到文件数据	接收进行态
	收到传输文件数据（单播转本地广播）报文	处理接收到文件数据	接收进行态
	收到查询站点升级状态报文	查询站点升级状态应答报文	接收进行态
	收到执行升级报文	忽略	接收进行态
	收到查询站点信息报文	查询站点信息应答报文	接收进行态
	完成文件数据接收且CRC正确	/	接收完成态
接收完成态	收到开始升级报文	忽略	接收完成态
	收到停止升级报文	/	空闲态
接收完成态	收到传输文件数据（单播）报文	忽略	接收完成态
	收到传输文件数据（单播转本地广播）报文	忽略	接收完成态
	收到查询站点升级状态报文	查询站点升级状态应答报文	接收完成态
	收到执行升级报文	/	升级进行态
	收到查询站点信息报文	查询站点信息应答报文	接收完成态
升级进行态	收到开始升级报文	忽略	升级进行态
	收到停止升级报文	/	空闲态
	收到传输文件数据（单播）报文	忽略	升级进行态
	收到传输文件数据（单播转本地广播）报文	忽略	升级进行态
	收到查询站点升级状态报文	查询站点升级状态应答报文	升级进行态
	收到执行升级报文	忽略	升级进行态
	收到查询站点信息报文	查询站点信息报文应答报文	升级进行态
试运行态	收到开始升级报文	忽略	试运行态
	收到停止升级报文	/	空闲态
	收到传输文件数据（单播）报文	忽略	试运行态
	收到传输文件数据（单播转本地广播）报文	忽略	试运行态
	收到查询站点升级状态报文	查询站点升级状态应答报文	试运行态
	收到执行升级报文	忽略	试运行态
	收到查询站点信息报文	查询站点信息报文应答报文	试运行态
	试运行时间结束	/	空闲态

升级业务传输流程见图D.17。

CCO向STA发送开始升级命令，STA收到后，进入升级状态；

CCO向STA发送数据块，STA收到数据块后保持下来，并更新本地位图；

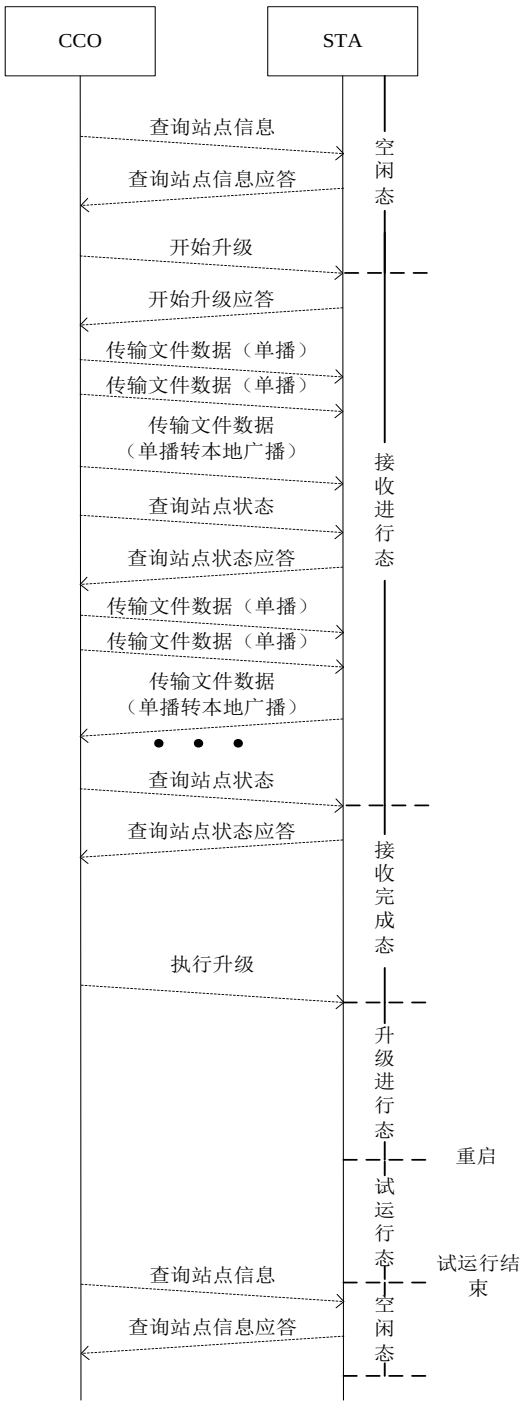
CCO查询STA状态， STA接收到后，返回状态及接收到数据块位图情况；

针对STA站点缺少的数据块，CCO向STA站点补包；

重复第出c），d）步，直到STA收齐数据为止；

CCO向STA发送执行升级，STA接收到后，验证升级包的完整性，并试运行成功后，本地保存接收到升级包的长度、CRC备查；如果失败，将长度和CRC置为0x00；

CCO查询站点信息，如果STA返回的长度和CRC值与CCO下发的相同，则认为站点升级成功，否则判断升级失败。



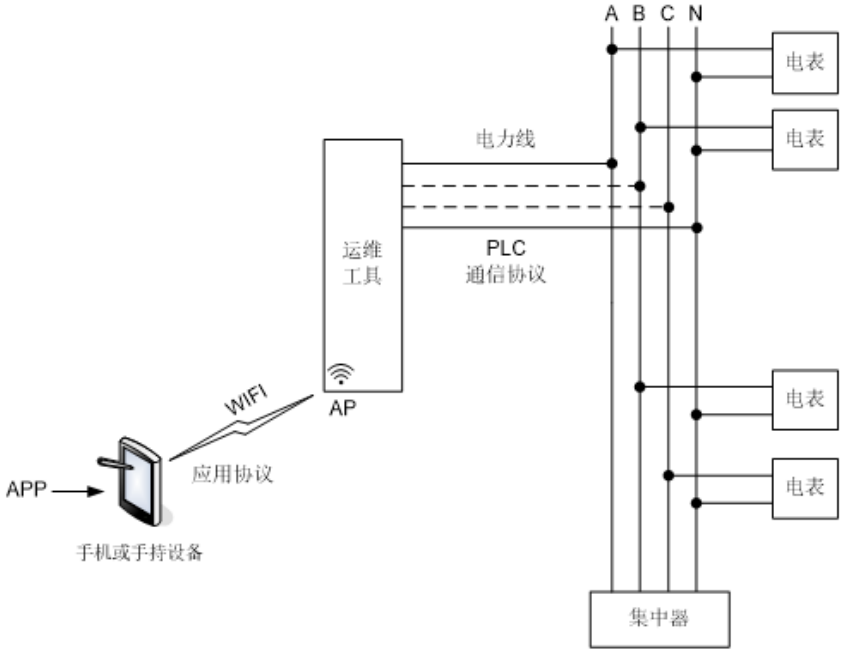
图D.17 升级传输流程

D.7 运维协议

本规范定义的运维协议是指运维工具在网络系统运维或者调试时接入CCO或者STA的通信报文协议。

D.7.1 现场使用场景描述

PLC控制系统的运维典型场景如图D.18所示，通常可通过手持设备通过与运维工具连接后，采用基于本章节所定义的协议与网络中的目标设备完成运维交互流程。



图D.18 运维工具应用场景图

每个PLC网络诊断或者维护时允许接入通过电力线单相接入运维工具，运维工具功能描述见表D.38。

表D.38 运维工具功能描述

编号	使用场景	功能要求
1	连接 CCO	1、 连接 CCO，不影响现网络全网连接（配备“取消连接”命令）。 2、 支持传输 PLC 模组串口命令。 3、 支持传输 APP 数据。
2	连接入网或不入网 STA	1、 连接从节点（不论是否在网），不改变在网和离网节点的状态。 2、 支持传输 PLC 模组串口命令。 3、 支持传输 APP 数据。

D.7.2 运维报文协议与交互流程

运维报文基于选择确认帧进行报文类型扩展，根据报文类型进行不同版本的运维协议选择。
运维协议版本约定见表D.39。

表D.39 运维协议版本

扩展帧类型	协议版本
1 和 2	1
8 和 9	0

D.7.2.1 版本 1 协议定义

D.7.2.1.1 运维报文协议

运维协议报文通信模式使用导频模式和无导频模式报文。

D.7.2.1.2 MAC 子层协议 MPDU 帧头协议扩展

以下扩展协议均基于MPDU的“选择确认帧(SACK) ”格式进行协议定义。
针对扩展帧类型的进行帧类型的扩展，增加两类报文类型，报文类型见表D.40。

表D.40 SACK 扩展帧类型描述

扩展帧类型编号	帧类型
扩展帧类型 1	网络搜索帧
扩展帧类型 2	同步帧

网络搜索帧是用于进行运维设备搜索目标设备的数据传输报文，定义如表D.41。

表D.41 网络搜索帧

字段	字节号	比特位	字段大小(比特)
目标站点地址	4	0-7	48
	5	0-7	
	6	0-3	
	7	0-7	
	8	0-7	
	9	0-7	
STEI	10	0-7	8
	11	0-3	—
保留	11	4-7	4
扩展帧类型	12	0-3	4

D.7.2.1.2.1 目的站点地址

CCO或STA的MAC地址。

D.7.2.1.2.2 STEI

运维工具的TEI地址。
同步帧是目标设备地址针对运维设备的应答帧，同时也用于维护网络心跳，帧格式定义如表D.42。

表D.42 同步帧

字段	字节号	比特位	字段大小(比特)
时间戳	4	0-7	32
	5	0-7	
	6	0-7	
	7	0-7	
STEI	8	0-7	12
	9	0-3	
保留	9	4-7	4
保留	10	0-7	8
保留	11	0-7	8
扩展帧类型	12	0-3	4

D.7.2.1.2.3 时间戳

CCO和入网的节点，发送网络时钟，未入网的STA为本地时钟值。

D.7.2.1.2.4 STEI

待连接模块的TEI地址，连接未入网STA的模块STEI为0。

CCO和已入网的模块，发送同步帧时，网络号为本网络的网络号，未入网的模块网络号为0。

说明：

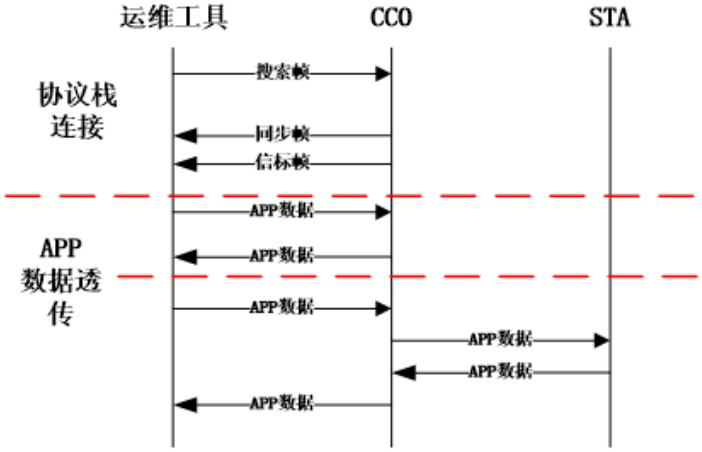
运维工具TEI固定为0xFFD，运维工具与未入网的STA模块同步后，未入网模块锁定当前频段，并停止组网，与运维工具保持在同一个频段上。故障模块未收到运维工具命令（应用帧）3分钟后（建议值）恢复到正常工作状态。

D.7.2.2 运维协议版本 1 交互流程

D.7.2.2.1 运维工具与 CCO 交互流程

运维工具与CCO的交互流程见图D.19。

a) 运维工具在各个载波频段上发送“搜索帧”，搜索帧携带目标站点的 MAC 地址，搜索目标站点；
b) 目标站点接收到“搜索帧”后，回复“同步帧”，CCO 回复同步帧中携带的网络号为本网络的网络号；
c) 运维工具收到同步帧后，配置与同步帧相同的网络号；
d) 目标站点周期性发送“同步帧”，用于同步运维工具模块；（如果入网节点，遵循信标帧发送原则）
e) 运维工具接收到目标站点回应的报文后，进入连接状态，当运维工具进入同步状态后，通知上位机与目标节点配对成功。



图D.19 运维工具连接 CCO 交互示意图

说明：

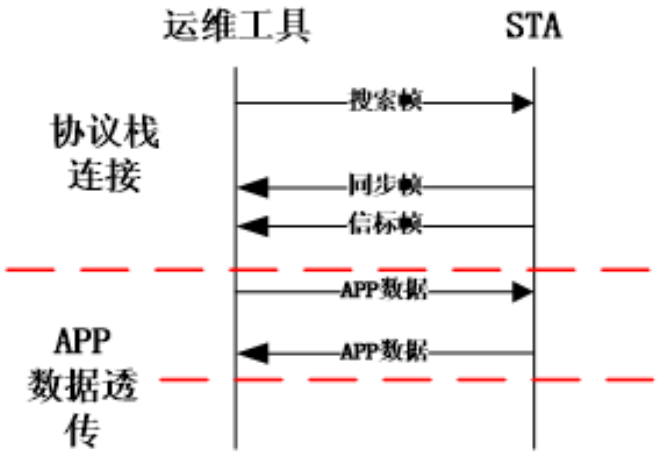
1) 连接过程中：同步帧以 100ms 为间隔发送 5 帧。
2) 连接成功后：被连接节点收到运维工具发送诊断命令，间隔 T 时间发送同步帧（建议间隔周期 T=30 秒）。

D.7.2.2.2 运维工具与 STA 交互流程

运维工具与STA交互流程见图D.20。

a) 运维工具在各个载波频段上发送“搜索帧”，搜索目标站点；（搜索帧携带目标站点的 MAC 地址）
b) 目标站点接收到“搜索帧”后，回复“同步帧”，针对已入网的 STA 回复同步帧时，所携带的网络号为本网络的网络号，针对未入网的 STA 同步帧中的，所携带的网络号为 0；

c) 运维工具收到同步帧后，配置与同步帧相同的网络号；
d) 目标站点周期性发送“同步帧”，用于同步运维工具模块；（如果入网节点，遵循信标帧发送原则）
e) 运维工具接收到回应帧后，进入链接状态，当运维工具进入同步状态后，通知上位机与目标节点配对成功。



图D.20 运维工具连接 STA 交互示意图

说明：
1) 连接过程中：同步帧以 100ms 为间隔发送 5 帧。
2) 连接成功后：被连接节点收到运维工具发送诊断命令，间隔 T 发送同步帧（建议间隔周期 T=30 秒）。

D.7.2.3 版本 0 协议定义

D.7.2.3.1 运维报文协议

运维协议报文通信模式使用导频模式。

D.7.2.3.2 MAC 子层协议 MPDU 帧头协议扩展

运维工具TEI使用4079。

以下扩展协议均基于MPDU的“选择确认帧(SACK) ”格式进行协议定义。针对扩展帧类型进行扩展，增加两类报文类型，见表D.43。

表D.43 SACK 扩展帧类型描述

扩展帧类型编号	帧类型
9	连接请求帧
10	连接应答帧

连接请求帧是发起连接请求的节点向被连接节点发的请求帧，用于建立连接，帧格式见表D.44。

表D.44 连接请求帧

字段	字节号	比特位	字段大小(比特)
定界符类型	0	0-2	3
网络类型		3-7	5
网络标识	1	0-7	24
	2	0-7	
	3	0-7	
目标站点地址	4	0-7	48
	5	0-7	
	6	0-3	
	7	0-7	
	8	0-7	
	9	0-7	
连接模式	10	0-2	3
是否需要应答	10	3	1
保留	10	4-7	12
	11	0-7	
扩展帧类型	12	0-3	4
标准版本号	12	4-7	4
帧控制校验序列	13	0-7	24
	14	0-7	
	15	0-7	

D.7.2.3.2.1 目标站点地址

连接STA的MAC地址。

D.7.2.3.2.2 连接模式

0：正常模式。
其他：保留。

D.7.2.3.2.3 是否需要应答

0：需要应答。
1：不需要应答。
连接应答帧是用于被连接节点向发起请求节点的应答，帧格式见表D.45。

表D.45 连接应答帧

字段	字节号	比特位	字段大小(比特)
定界符类型	0	0-2	3
网络类型		3-7	5
网络标识	1	0-7	24
	2	0-7	
	3	0-7	
连接站点地址	4	0-7	48
	5	0-7	
	6	0-3	
	7	0-7	
	8	0-7	
	9	0-7	
应答结果	10	0-3	4
STEI	10	4-7	12
	11	0-7	
扩展帧类型	12	0-3	4
标准版本号	12	4-7	4
帧控制校验序列	13	0-7	24
	14	0-7	
	15	0-7	

D.7.2.3.2.4 连接站点站点地址

连接站点的MAC地址。

D.7.2.3.2.5 应答结果

0：连接成功。
1：拒绝连接。

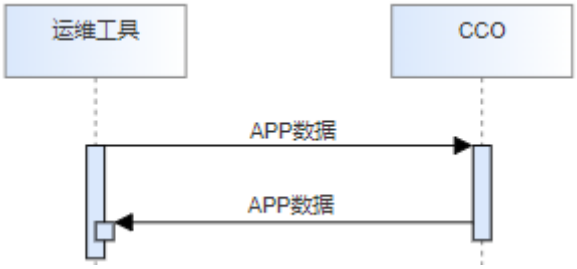
D.7.2.3.2.6 STEI

连接站点的TEI。

D.7.2.4 运维协议版本0交互流程

D.7.2.4.1 运维工具与CCO交互流程

运维工具与CCO交互流程见图D.21。

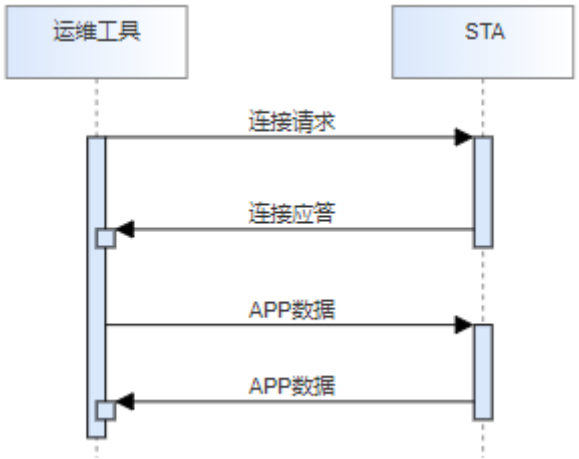


图D.21 运维工具连接 CCO 交互示意图

a) 运维工具发送 APP 数据给 CCO。
b) CCO 回复 APP 数据。

D.7.2.4.2 运维工具与 STA 交互流程

运维工具与STA交互流程见图D.22。



图D.22 运维工具连接 STA 交互示意图

a) 运维工具在发送 APP 数据包前先在各个载波频段上发送“连接请求”帧，连接 STA；（连接请求帧携带 STA 的 MAC 地址）。
b) STA 接收到“连接请求”帧后，回复“连接应答帧”。入网 STA 不改变 STA 的入网状态，离网 STA 不关闭盲检，不禁止接入网络。
c) 运维工具收到连接应答帧时触发 APP 数据包发送。
d) STA 收到 APP 数据后回复。

附 录 E
（规范性）
CRC-16 范例程序

```
const unsigned short crc16_xmodem_table[256]={0x0000, 0x1021, 0x2042, 0x3063, 0x4084,
0x50a5, 0x60c6, 0x70e7,0x8108, 0x9129, 0xa14a, 0xb16b, 0xc18c, 0xd1ad, 0xe1ce,
0xf1ef,0x1231, 0x0210, 0x3273, 0x2252, 0x52b5, 0x4294, 0x72f7, 0x62d6,0x9339, 0x8318,
0xb37b, 0xa35a, 0xd3bd, 0xc39c, 0xf3ff, 0xe3de,0x2462, 0x3443, 0x0420, 0x1401, 0x64e6,
0x74c7, 0x44a4, 0x5485,0xa56a, 0xb54b, 0x8528, 0x9509, 0xe5ee, 0xf5cf, 0xc5ac,
0xd58d,0x3653, 0x2672, 0x1611, 0x0630, 0x76d7, 0x66f6, 0x5695, 0x46b4,0xb75b, 0xa77a,
0x9719, 0x8738, 0xf7df, 0xe7fe, 0xd79d, 0xc7bc,0x48c4, 0x58e5, 0x6886, 0x78a7, 0x0840,
0x1861, 0x2802, 0x3823,0xc9cc, 0xd9ed, 0xe98e, 0xf9af, 0x8948, 0x9969, 0xa90a,
0xb92b,0x5af5, 0x4ad4, 0x7ab7, 0x6a96, 0x1a71, 0x0a50, 0x3a33, 0x2a12,0xdbfd, 0xcbdc,
0xfbbf, 0xeb9e, 0x9b79, 0x8b58, 0xbb3b, 0xab1a,0x6ca6, 0x7c87, 0x4ce4, 0x5cc5, 0x2c22,
0x3c03, 0x0c60, 0x1c41,0xedae, 0xfd8f, 0xcdec, 0xddcd, 0xad2a, 0xbd0b, 0x8d68,
0x9d49,0x7e97, 0x6eb6, 0x5ed5, 0x4ef4, 0x3e13, 0x2e32, 0x1e51, 0x0e70,0xff9f, 0xefbe,
0xdfdd, 0xcffc, 0xbf1b, 0xaf3a, 0x9f59, 0x8f78,0x9188, 0x81a9, 0xb1ca, 0xa1eb, 0xd10c,
0xc12d, 0xf14e, 0xe16f,0x1080, 0x00a1, 0x30c2, 0x20e3, 0x5004, 0x4025, 0x7046,
0x6067,0x83b9, 0x9398, 0xa3fb, 0xb3da, 0xc33d, 0xd31c, 0xe37f, 0xf35e,0x02b1, 0x1290,
0x22f3, 0x32d2, 0x4235, 0x5214, 0x6277, 0x7256,0xb5ea, 0xa5cb, 0x95a8, 0x8589, 0xf56e,
0xe54f, 0xd52c, 0xc50d,0x34e2, 0x24c3, 0x14a0, 0x0481, 0x7466, 0x6447, 0x5424,
0x4405,0xa7db, 0xb7fa, 0x8799, 0x97b8, 0xe75f, 0xf77e, 0xc71d, 0xd73c,0x26d3, 0x36f2,
0x0691, 0x16b0, 0x6657, 0x7676, 0x4615, 0x5634,0xd94c, 0xc96d, 0xf90e, 0xe92f, 0x99c8,
0x89e9, 0xb98a, 0xa9ab,0x5844, 0x4865, 0x7806, 0x6827, 0x18c0, 0x08e1, 0x3882,
0x28a3,0xcb7d, 0xdb5c, 0xeb3f, 0xfb1e, 0x8bf9, 0x9bd8, 0xabbb, 0xbb9a,0x4a75, 0x5a54,
0x6a37, 0x7a16, 0x0af1, 0x1ad0, 0x2ab3, 0x3a92,0xfd2e, 0xed0f, 0xdd6c, 0xcd4d, 0xbdaa,
0xad8b, 0x9de8, 0x8dc9,0x7c26, 0x6c07, 0x5c64, 0x4c45, 0x3ca2, 0x2c83, 0x1ce0,
0x0cc1,0xef1f, 0xff3e, 0xcf5d, 0xdf7c, 0xaf9b, 0xbfba, 0x8fd9, 0x9ff8,0x6e17, 0x7e36,
0x4e55, 0x5e74, 0x2e93, 0x3eb2, 0x0ed1, 0x1ef0};
unsigned short crc16_xmodem(unsigned char *frm, unsigned int len)
{
    unsigned short ans = 0;
    while (len--)
    {
        ans = (ans<<8) ^ crc16_xmodem_table[(ans>>8) ^ *frm++];
    }
    return ans;
}
```