IOT设备通讯协议

文档历史

|  |  |  |
| --- | --- | --- |
| 日期 | 作者 | 说明 |
| 20200215 | 熊毅 | 创建文档 |
|  |  |  |

# 概述

IOT设备通讯协议是一个通用的通讯协议，旨在对物联网设备进行控制。

# 基本协议

设备与服务器之间可以通过TCP、UDP或者是更上层的MQTT来进行通讯。

## 控制字

在通讯协议中，将使用到以下的控制字，控制字需要转义：

|  |  |  |
| --- | --- | --- |
| 控制字 | 值 | 意义 |
| STX | 0x02 | 报文开始 |
| ETX | 0x03 | 报文结束 |
| DLE | 0x10 | 转义字符 |
| NAK | 0x15 | 检测连接状态时使用 |
| ACK | 0x06 | ACK |

## 通讯帧格式

|  |  |  |  |
| --- | --- | --- | --- |
| STX | 数据 | ETX | BCC |

BCC（块校验值）：用于校验数据是否正确，其值为数据字节的异或值（不包含转义DLE）。

为了防止在数据接收时出现二义性，在所有编码前的数据中，凡是出现通讯控制字的字节前加入DLE转义控制字。例如有以下的数据片段：

0x1B 0x2A 0x02 0x03 0x3C

编码后的数据如下：

0x1B 0x2A 0x10 0x02 0x10 0x03 0x3C

## 通讯数据格式

如无特殊说明，本协议中的多字节数据均为小端模式。

|  |  |  |  |
| --- | --- | --- | --- |
| 设备类型  (2字节) | 命令字  （1字节） | 数据长度  （2字节） | 命令数据  （N字节，如果没有则为空） |

数据长度只表示命令数据的长度，如果没有命令数据，则数据长度为0。

1. 设备类型表

|  |  |  |
| --- | --- | --- |
| 类型码 (2字节) | 设备类型 | 说明 |
| 0x0001 | 污水控制器 | 污水控制器 |
|  |  |  |

1. 设备命令表

|  |  |  |  |
| --- | --- | --- | --- |
| 命令码 | 命令方向 | 命令发起者 | 说明 |
| 0x01 | 设备->服务器 | 设备 | 设备注册 |
| 0x81 | 服务器->设备 | 设备 | 设备注册应答 |
| 0x02 | 设备->服务器 | 设备 | 设备心跳 |
| 0x82 | 服务器->设备 | 设备 | 设备心跳应答 |
| 0x13 | 服务器->设备 | 服务器 | 重启设备 |
| 0x93 | 设备->服务器 | 服务器 | 重启设备应答 |
| 0x14 | 服务器->设备 | 服务器 | 读取设备数据 |
| 0x94 | 设备->服务器 | 服务器 | 读取设备数据应答 |
| 0x15 | 服务器->设备 | 服务器 | 写入设备数据 |
| 0x95 | 设备->服务器 | 服务器 | 写入设备数据应答 |
| 0x06 | 设备->服务器 | 设备 | 请求数据 |
| 0x86 | 服务器->设备 | 设备 | 请求数据应答 |
| 0x8F | 服务器->设备 | 服务器 | 获取设备命令（全双工通讯无需实现此命令） |
| 0x0F | 设备->服务器 | 服务器 | 无命令应答（全双工通讯无需实现此命令） |

# 设备注册

## 设备注册命令

当设备上电或重启后，向预先配置的服务器地址发送注册命令。注册成功后设备开始正常工作，并根据注册命令应答发送心跳包。如果没有收到注册命令应答，则尝试重新注册。

方向：设备->服务器

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x01 |
| Byte 3-4 | 数据长度 | 固定为 25 |
| Byte 5 | 连接方式 | 如果设备支持多种连接方式可以将各方式或在一起。例如0x14表示设备同时通过4G和网线连接。  0x01：2G  0x02：WIFI  0x04：4G  0x08：5G  0x10：有线 |
| Byte6-13 | 设备ID | 设备唯一ID号 |
| Byte14-17 | 设备硬件版本 | 硬件版本 |
| Byte18-21 | 设备固件版本 | 固件版本 |
| Byte22-25 | 心跳数据地址 | 设备心跳上报数据地址 |
| Byte26-29 | 心跳数据长度 | 设备必跳上报数据长度 |

## 设备注册应答

服务器收到注册报文后进行解析，解析成功后发送注册应答报文。并在应答报文中

方向：服务器->设备

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x81 |
| Byte 3-4 | 数据长度 | 固定为 25 |
| Byte 5 | 连接方式 | 服务器支持的连接方式 |
| Byte6-13 | 设备ID | 设备唯一ID号，设备根据此判断命令是否是发给自己的 |
| Byte14-17 | 设备硬件版本 | 服务器支持的硬件版本，如果此项与设备不同，表示服务器不支持此硬件设备 |
| Byte18-21 | 设备固件版本 | 服务器上最新的固件版本，如果服务器上的版本比设备更新，设备可以相机更新固件 |
| Byte22-25 | 心跳数据地址 | 设备心跳上报数据地址 |
| Byte26-29 | 心跳数据长度 | 设备心跳上报数据长度 |

# 设备心跳

## 设备心跳命令

当设备上电或重启后，向预先配置的服务器地址发送注册命令。

方向：设备->服务器

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x02 |
| Byte 3-4 | 数据长度 | N-5 |
| Byte5-13 | 设备ID | 设备唯一ID号，设备根据此判断命令是否是发给自己的 |
| Byte14-17 | 心跳序列号 | 收到注册应答后，从0开始计数 |
| Byte18-21 | 心跳数据地址 | 由注册应答命令指定的心跳数据地址 |
| Byte22-N | 心跳数据 | 心跳数据，长度由注册应答命令指定 |

## 设备心跳应答

方向：服务器->设备

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x82 |
| Byte 3-4 | 数据长度 | 12 |
| Byte5-13 | 设备ID | 设备唯一ID号，设备根据此判断命令是否是发给自己的 |
| Byte14-17 | 心跳序列号 | 心跳命令序列号 |

设备根据心跳序列号判断是否有心跳丢失的情况。

# 服务器重启设备

## 重启命令

方向：服务器->设备

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x13 |
| Byte 3-4 | 数据长度 | 12 |
| Byte5-13 | 设备ID | 设备唯一ID号，设备根据此判断命令是否是发给自己的 |
| Byte14-17 | 时间戳 | 服务器UTC时间戳 |

## 重启应答

方向：设备->服务器

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x93 |
| Byte 3-4 | 数据长度 | 12 |
| Byte5-13 | 设备ID | 设备唯一ID号，服务器根据此确认设备 |
| Byte14-17 | 时间戳 | 与重启命令相同 |

设备收到重启命令后，先发送重启应答再重启。如果网络不畅，服务器有可能收不到重启应答，但是设备重启成功后会再次注册，服务器收到再次注册的命令也可以认为设备重启成功。

# 服务器读取设备数据

## 读数据命令

方向：服务器->设备

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x14 |
| Byte 3-4 | 数据长度 | 21 |
| Byte5-13 | 设备ID | 设备唯一ID号，设备根据此判断命令是否是发给自己的 |
| Byte14-17 | 时间戳 | 服务器UTC时间戳 |
| Byte18-21 | 读取数据地址 | 设备数据地址 |
| Byte22-25 | 读取数据长度 | 设备数据长度 |

## 读数据应答

方向：设备->服务器

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x94 |
| Byte 3-4 | 数据长度 | N-5 |
| Byte5-13 | 设备ID | 设备唯一ID号，服务器根据此确认设备 |
| Byte14-17 | 时间戳 | 与读数据命令相同 |
| Byte18-21 | 读取数据地址 | 与读数据命令相同。如果数据内容长度为零，此项包含错误详细信息。 |
| Byte22-N | 读取数据内容 | 设备数据，如果读取错误，此项内容长度为0 |

# 服务器写入设备数据

## 写数据命令

方向：服务器->设备

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x15 |
| Byte 3-4 | 数据长度 | N-5 |
| Byte5-13 | 设备ID | 设备唯一ID号，设备根据此判断命令是否是发给自己的 |
| Byte14-17 | 时间戳 | 服务器UTC时间戳 |
| Byte18-21 | 数据地址 | 设备数据地址 |
| Byte22-25 | 数据长度 | 设备数据长度 |
| Byte26-N | 数据内容 |  |

## 写数据应答

方向：设备->服务器

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x95 |
| Byte 3-4 | 数据长度 | 21 |
| Byte5-13 | 设备ID | 设备唯一ID号，服务器根据此确认设备 |
| Byte14-17 | 时间戳 | 与写数据命令相同 |
| Byte18-21 | 写入数据地址 | 与写数据命令相同，如果应答长度为零，这里包含错误详细信息。 |
| Byte22-25 | 定入数据长度 | 写入设备数据的长度，返回0表示错误 |

# 设备请求数据

## 请求数据命令

方向：设备->服务器

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x06 |
| Byte 3-4 | 数据长度 | 21 |
| Byte5-13 | 设备ID | 设备唯一ID号，设备根据此判断命令是否是发给自己的 |
| Byte14-17 | 时间戳 | 设备UTC时间戳 |
| Byte18-21 | 数据地址 | 设备请求数据地址 |
| Byte22-25 | 数据长度 | 设备请求数据长度 |

## 请求数据应答

方向：服务器->设备

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x86 |
| Byte 3-4 | 数据长度 | N-5 |
| Byte5-13 | 设备ID | 设备唯一ID号，服务器根据此确认设备 |
| Byte14-17 | 时间戳 | 与请求数据命令相同 |
| Byte18-21 | 数据地址 | 与请求数据命令相同，如果出错，此项包含详细错误信息 |
| Byte22-25 | 数据位长度 | 设备请求数据的位长度，如果出错此项内容为0。 |
| Byte26-N | 数据内容 | 设备请求数据内容 |

# 获取设备命令

半双工设备需要实现此命令。当工作在半双工通讯环境时，设备不能主动上报数据，需要等到服务器请求数据时才能上报。

## 获取设备命令

方向：服务器->设备

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x8F |
| Byte 3-4 | 数据长度 | 12 |
| Byte5-13 | 设备ID | 设备唯一ID号，设备根据此判断命令是否是发给自己的 |
| Byte14-17 | 时间戳 | 设备UTC时间戳 |

当设备收到此命令后，如果没有需要发给主机的命令，则回应无命令应答。

如果有数据发给主机，则发送相应的命令。如果有多个命令需要发送，可以将多个命令在同一个获取设备命令中进行返回，主机收到后分别解析处理。

## 设备无命令应答

方向：设备->服务器

|  |  |  |
| --- | --- | --- |
|  | 名称 | 说明 |
| Byte 0-1 | 设备类型 | 见表1 设备类型表 |
| Byte 2 | 命令字 | 0x0F |
| Byte 3-4 | 数据长度 | 12 |
| Byte5-13 | 设备ID | 设备唯一ID号，设备根据此判断命令是否是发给自己的 |
| Byte14-17 | 时间戳 | 设备UTC时间戳 |

当设备收到获取设备命令，没有数据需要发给主机时，回应此命令。