**zigbee3.0设备对接YH协议**

|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 时间 | 修改内容 | 修改者 |
| V0001 | 2021-07-11 | 初始发布版本 |  |
| V0002 | 2021-07-15 | 增加识别安防类设备信息。 |  |
| V0003 | 2021-07-20 | 修改协议头 |  |
| V0004 | 2021-07-22- | 新增窗帘操作指令 |  |
| V0005 | 20210804 | 增加ZDO和读版本  命令 |  |
| V0006 | 20210920 | 新增设备 |  |
| V0006 | 20211018 | 新增门锁指令 |  |

目录

[一，操作3.0网络 2](#_Toc85410418)

[1，创建3.0网络 2](#_Toc85410419)

[2，打开允许3.0设备加入操作； 2](#_Toc85410420)

[3，关闭3.0设备加入操作； 3](#_Toc85410421)

[4，复位 3](#_Toc85410422)

[5，退网 3](#_Toc85410423)

[6，读是否存在3.0网络的必要参数 3](#_Toc85410424)

[7，读取GW软件版本号 3](#_Toc85410425)

[二，ZDO层消息 4](#_Toc85410426)

[1，设备入网信息： 4](#_Toc85410427)

[2，获取简单设备类型： 4](#_Toc85410428)

[3，通过短地址获取长地址： 5](#_Toc85410429)

[三，网络层消息： 5](#_Toc85410430)

[1，设备离网消息（上行）： 5](#_Toc85410431)

[2，请求设备离网（下行）； 5](#_Toc85410432)

[四，应用层层消息 6](#_Toc85410433)

[1，上行： 6](#_Toc85410434)

[2，举例： 7](#_Toc85410435)

[1，电压上报数据：（每一个小时上报一次，可作为心跳包，容忍丢两包） 7](#_Toc85410436)

[2，电量百分比上报：（每一个小时上报一次，可作为心跳包，容忍丢两包） 8](#_Toc85410437)

[3，检测水 8](#_Toc85410438)

[4，窗帘： 10](#_Toc85410439)

[5，门锁 12](#_Toc85410440)

[五，远程控制失败错误码 12](#_Toc85410441)

# 一，操作3.0网络

帧格式：A5 AA 5A cmd

## 1，创建3.0网络

A5 AA 5A A1

返回 A5 AA 5A A1 00（成功）

返回 A5 AA 5A A1 01（失败）

## 2，打开允许3.0设备加入操作；

A5 AA 5A A2

返回 A5 AA 5A A2 00（成功）

返回 A5 AA 5A A2 01（失败）

## 3，关闭3.0设备加入操作；

A5 AA 5A A3

返回 A5 AA 5A A3 00（成功）

返回 A5 AA 5A A3 01（失败）

## 4，复位

A5 AA 5A 11

## 5，退网

A5 AA 5A A4

返回 A5 AA 5A A4 00（成功）

返回 A5 AA 5A A4 01（失败）

## 6，读是否存在3.0网络的必要参数

A5 AA 5A A5

返回 A5 AA 5A A5 FF FF FF FF FF为不存在3.0网络的必要参数，否则已存在3.0网络的必要参数；

## 7，读取GW软件版本号

发送 A5 AA 5A A6

返回：A5 AA 5A A6 xx

其中xx为一个字节的版本号。

# 二，ZDO层消息

：

## 1，设备入网信息：

设备ZDO入网消息协议：30端点号 cluster消息类型 数据域长度 数据域 03

30 ：帧头；

端点号：0为ZDO层消息，即入网消息；

cluster消息类型 ：如，该值为0x0013为设备入网消息类型；

数据域长度：该长度仅为数据域长度（一般为固定12字节长度）；

数据域：消息的SEQ（1B） nodeID(2B) longID(8B) 设备能力(1B)

消息的SEQ（1B）:消息的帧计数器，可忽略；

nodeID(2B):网络短地址，注意，低字节在前面；

longID(8B):网络长地址，注意，低字节在前面；

设备能力(1B)：只关注第1位的值（从零开始数），其他位的值可以忽略，“0“代表为低功耗设备，”1“代表为非低功耗设备；

03：帧结束符号；

## 2，获取简单设备类型：

帧格式：31 nodeID端点号 cluster消息类型 数据域长度 数据域 13

31:帧头；

nodeID：短ID；

端点号：就是哪个端点发来的，0端点代表的是ZDO层消息；

Cluster消息类型：低字节在前，0x8004代表的是简单描述符消息，主要获取设备类型；

数据域：从零开始数（指数据域字段），第8，9个字节即为设备类型的ID（2字节，低字节在前）（如，窗帘的设备ID为0x0202,安防类的设备ID为0x0402,其中，水浸也是属性安防类的一种，所以，安防类的话，还要获取其他属性区分是什么安防设备。），其他数据可以暂时忽略；

13 ：结束符。

设备列表，参考上述：

|  |  |  |
| --- | --- | --- |
| 设备ID | 设备名称 | 备注 |
| 0x0402 | 安防类设备 |  |
| 0x0202 | 窗帘 |  |
| 0x000a | 门锁 |  |
| 0x0162 | 红外转发设备 |  |

## 3，通过短地址获取长地址：

下行帧格式：

31 nodeID 13

31 9f a6 13

上行帧格式：31 nodeID端点号 cluster消息类型 数据域长度 数据域 13

如：31 9F A6 00 01 80 0C 83 00 1D 2B 39 FE FF EC 86 CC 9F A6 13

31:帧头；

nodeID：短ID；

端点号：就是哪个端点发来的，0端点代表的是ZDO层消息；

Cluster消息类型：低字节在前，0x8001代表的是获取长地址相应消息；

数据域：83 00 1D 2B 39 FE FF EC 86 CC 9F A6

83：为seq，可忽略；

00：代表获取成功；

1D 2B 39 FE FF EC 86 CC：为长地址，小端；

9F A6：短地址；

# 三，网络层消息：

## 1，设备离网消息（上行）：

帧格式： 41 nodeID longID 14

41：帧头；

NodeID：网络地址，两个字节，低字节在前；

LongID：长地址（MACID），8个字节，低字节在前；

14：帧结束符；

## 2，请求设备离网（下行）；

帧格式： 41 nodeID 14

nodeID：短ID，低字节在前；

# 四，应用层层消息

## 1，上行：

帧格式: 51 nodeID 端点号 clusterID LEN yh数据域 15

51：帧头；

nodeID ：2字节，短ID；

端点号: 1字节，端点号为非零值，一般为1。

clusterID：2字节 设备的某个通讯通道；

LEN：1字节 ，ZCL数据域长度；

yh数据域：yh头+ seq+cmd + ZCLpayload；

其中，

yh头：只关注第零位，第零位为1，这个cmd代表CMD1，为0则代表CMD0；

Seq：帧计数器，可以忽略；

CMD0/CMD1:

其中CMD0命令如下：（CMD1具体设备具体分析，不同设备可能不一样的）

|  |  |
| --- | --- |
| 0x00 | Read Attributes |
| 0x01 | Read Attributes Response |
| 0x02 | Write Attributes |
| 0x03 | Write Attributes Undivided |
| 0x04 | Write Attributes Response |
| 0x05 | Write Attributes No Response |
| 0x06 | Configure Reporting |
| 0x07 | Configure Reporting Response |
| 0x08 | Read Reporting Configuration |
| 0x09 | Read Reporting Configuration Response |
| 0x0a | Report attributes |
| 0x0b | Default Response |
| 0x0c | Discover Attributes |
| 0x0d | Discover Attributes Response |
| 0x0e | Read Attributes Structured |
| 0x0f | Write Attributes Structured |
| 0x10 | Write Attributes Structured response |
| 0x11 | Discover Commands Received |
| 0x12 | Discover Commands Received Response |
| 0x13 | Discover Commands Generated |
| 0x14 | Discover Commands Generated Response |
| 0x15 | Discover Attributes Extended |
| 0x16 | Discover Attributes Extended Response |

15：帧结束符；

## 2，举例：

水浸（一般低功耗设备不可控制，要让其离开网络时，要做在收到其信息后立即）：

这个信息是解析安防类具体是什么设备：

51 F0 7B 01 00 05 14 18 02 01 00 00 00 30 00 01 00 00 31 2A 00 02 00 00 19 00 00 15

51：帧头；

F0 7B：短ID；

01：端点；

00 05：表示clusterID为0x0500;

14：yh数据域长度位20；

只关注yh数据域中的第12，13个字节（从零开始数），如上信息位2A 00：即0x002A就是代表是水浸。

|  |  |  |  |
| --- | --- | --- | --- |
| 安防类设备类型ID | 设备名称 | 心跳 | 备注 |
| 0x002A | 水浸 | 一个小时上报电压 | 低功耗安防设备 |
| 0x000D | 人体感应 | 十五分钟上报电压 | 低功耗安防设备 |
| 0x0015 | 门磁 |  | 低功耗安防设备 |
| 0x0028 | 烟感 |  | 低功耗设备 |

人体感应：

51 E0 F1 01 00 05 14 18 05 01 00 00 00 30 00 01 00 00 31 0D 00 02 00 00 19 00 00 15

同上，0D 00即0x000D,代表这个设备是人体红外的设备。注意，人体红外十五分钟上报一次心跳，心跳内容如下的电压及百分比的上报。

### 1，电压上报数据：（每一个小时上报一次，可作为心跳包，容忍丢两包）

51 2C 60 01 01 00 07 18 71 0A 20 00 20 1F 15

51：帧头；

2C 60 :表示nodeID为0x602c;

01：端点为1；

01 00：表示clusterID为0x0001;

07:yh数据域长度；

18：第零位为零，则cmd为cmd0；

71：seq，可忽略；

0A:表示ZCLCMD，即Report attributes,即为设备上报信息;

20 00 ：表示属性ID为0X0020（电压属性）;

20：表示值为U8的数据类型；

1F：表示为31mv；

51为结束符；

### 2，电量百分比上报：（每一个小时上报一次，可作为心跳包，容忍丢两包）

51 2C 60 01 01 00 07 18 72 0A 21 00 20 C6 15

51：帧头；

2C 60 :表示nodeID为0x602c;

01：端点为1；

01 00：表示clusterID为0x0001;

07:yh数据域长度；

18：第零位为零，则cmd为cmd0；

72：seq，可忽略；

0A:表示CMD0，即Report attributes,即为设备上报信息;

21 00 ：表示属性ID为0X0021（电量百分比属性）;

20：表示值为U8的数据类型；

C6：表示98%，注意，C6十进制为198，这个有可能是设备端算法错误，直接减去100即可；

15为结束符；

### 3，检测水

#### 1）水浸检测到水报警信息

51 2C 60 01 00 05 09 09 74 00 01 00 00 00 00 00 15

51：帧头；

2C 60 :表示nodeID为0x602c;

01：端点为1；

00 05：表示clusterID为0x0500;

09：表示cmd为cmd1；

74：seq，可忽略；

00：设备检测状态变化命令；

01 00 ：表示设备检测状态值为0x0001，即为检测到水的存在从而上报报警；

00 00 00 00：目前用不到，可忽略；

15：结束符。

#### 2）设备消除水报警信息

51 2C 60 01 00 05 09 76 00 00 00 00 00 00 00 15

51：帧头；

2C 60 :表示nodeID为0x602c;

01：端点为1；

00 05：表示clusterID为0x0500;

09：yh数据域长度；

09：表示cmd为cmd1；

76：seq，可忽略；

00：设备检测状态变化命令；

00 00 ：表示设备检测状态值为0x0000，即为检测到没有水的存在从而上报报警；

00 00 00 00：目前用不到，可忽略；

15：结束符。

#### 3）上报设备的检测状态

51 2C 60 01 00 05 08 18 75 0A 02 00 19 01 00 15

51：帧头；

2C 60 :表示nodeID为0x602c;

01：端点为1；

01 00：表示clusterID为0x0001;

08：yh数据域长度；

18：第零位为零，则cmd为cmd0；

75：seq，可忽略；

0A：表示CMD0，即Report attributes,即为设备上报信息;

02 00：表示设备的属性ID为0x0002；

19：值为表示16位数据类型；

01 00：表示值为0x0001,即为检测到水的状态；

15：结束符。

其他安防设备触发值，在这里要重点关注状态值。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安防类设备类型ID | 设备名称 | 功能 | 状态值 | 备注 |
| 0x002A | 水浸 | 检测到水/未检测到水 | 0x0001/0x0000 | 注意，是第一位置为则为报警 |
| 0x000D | 人体感应 | 检测到人/未检测到人 | 0x0001/0x0000 | 注意，是第一位置为则为报警 |
| 0x0015 | 门磁 | 门磁开/关 | 0x0001/0x0000 | 注意，是第一位置为则为报警 |

### 4，窗帘：

#### 上行：

##### 1，心跳包（每五分钟报一次，容忍丢两三次包）

51 27 D8 01 02 01 07 18 6F 0A 07 00 18 03 15

51：帧头；

27 D8：nodeID为0xd827;

1. ：端点为01；

0201：表示通讯clusterID为0x0102;

07：yh数据域长度；

18：第零位为零，便是cmd为cmd0；

6f：seq，可忽略；

0A：表示CMD0，即Report attributes,即为设备上报信息;

07 00：表示属性ID为0x0007;

18:表示U8数据类型；

03：表示值为0x03，目前可理解为心态包；

15：结束符。

##### 2，发送指令回应包

51 27 D8 01 02 01 05 08 00 0B 01 81 15

51：帧头；

27 D8：nodeID为0xd827;

1. ：端点为01；

0201：表示通讯clusterID为0x0102;

05：yh数据域长度；

08：表示cmd为cmd1；

00：表示seq，可忽略；

0B：表示默认回应命令；

01 ：表示01命令的回应包；

81：暂时忽略；

15：结束符。

##### 3，百分比上报

如，下发百分比控制命令：

51a691010201052015

百分比值20：代表为0x20即为32%

回应：

51 A6 91 01 02 01 07 18 08 0A 08 00 20 20 15

51：帧头；

A6 91：nodeID为0x91A6;

1. ：端点为01；

0201：表示通讯clusterID为0x0102;

07：yh数据域长度；

18：第零位为零，便是cmd为cmd0；

6f：seq，可忽略；

0A：表示CMD0，即Report attributes,即为设备上报信息;

08 00：代表百分比的属性ID为0x0008;

20:U8数据类型；

20：代表百分比为0x20，即为32%；

15：结束；

#### 下行：

窗帘控制(clusterID: 0x0102)：

1)开，关，停止操作协议格式：

帧格式: 51 nodeID 端点 clusterID cmd 15

51：帧头；

NodeID：短ID，低字节在前；

端点：非零值，一般为1；

ClusterID：通讯通道，低字节在前；

Cmd：操作命令；

Cmd:（目前仅支持这三种命令）

|  |  |  |
| --- | --- | --- |
| 0x00 | Up / Open | M |
| 0x01 | Down / Close | M |
| 0x02 | Stop | M |

2）百分比操作协议格式：

帧格式: 51 nodeID 端点 clusterID cmd percentageData(1B) 15

51：帧头；

NodeID：短ID，低字节在前；

端点：非零值，一般为1；

ClusterID：通讯通道，低字节在前；

Cmd：操作命令；

|  |  |  |
| --- | --- | --- |
| 0x05 | Go to Lift Percentage | O |

percentageData:一个字节代表百分比值（要十六进制格式）；

15：结束符；

### 5，门锁

#### 上行

1. 入网，参考第二章第二小节，入网的设备ID不一样；
2. 电量上报，请参考2.2章节；
3. 发送固定直接上报信息；（具体解析可以参考门锁协议文档）；
4. 其他控制或者本地控制信息，暂时用不到，可以忽略；

#### 下行

格式：帧格式: 51 nodeID 端点 clusterID cmd 15

51：帧头；

NodeID：短ID，低字节在前；

端点：非零值，一般为1；

ClusterID：通讯通道，低字节在前；

Cmd：操作命令；

CMD:固定为：0xf0

1. 红外转发设备：
2. 下行

格式：帧格式: 51 nodeID 端点 clusterID cmd 属性ID 属性类型 属性数的域长度 属性数据域 15

列如：

516a16010000020c41421bAAAA0017DC00110164373430376636646162646434666465DF5555 15

cmd ：02为写属性；

属性ID：0c41 即0x410c;

属性类型:42,此属性目前仅支持42类型；

1b:属性属于域长度；

AAAA0017DC00110164373430376636646162646434666465DF5555：数据域；

1. 上行（主要为透传数据）

格式：帧格式: 51 nodeID 端点 clusterID ZCL帧长度 ZCL帧 15

列如：

51 6a16 01 0000 11 18 2e 0a 0c41 42 0a aaaa0006dc0000da5555 15

6a16 ： 短地址0x166a；

01：端点1；

0000：clusterID；

11：ZCL帧长度；

18 2e 0a 0c41 42 0a aaaa0006dc0000da5555 ：ZCL帧；

其中：

18为ZCL帧头；

2e:zcl 包计数器；

0a：zcl报告命令；

0c41：zcl的属性ID为0x410c；

42：字符串类型；

0a:数据的长度；

aaaa0006dc0000da5555：这里就是红外真正透传的数据；

# 五，远程控制失败错误码

61 xxxx xx xx xxxx 16 长度为固定的8

61:帧头；

Xxxx:发送目标的短ID

Xx:端点号；

Xx:错误码，一般为0x66时为发送失败；

Xxxx