1. 帧解析
2. 帧格式

固定帧格式：

|  |  |  |
| --- | --- | --- |
| 10 H | ----------- | 启动字符（1byte） |
| CTRL | ----------- | 控制域 （1 byte） |
| ADDR | ----------- | 地址域（2 byte） |
| C S | ----------- | 校验和（1 byte） |
| 16 H | ----------- | 结束字符（1 byte） |

可变帧格式：

|  |  |  |
| --- | --- | --- |
| 68 H | ———— | 启动字符1（1byte） |
| Length | ———— | 长度（1byte） |
| Length | ———— | 长度（重复）（1byte） |
| 68 H | ———— | 启动字符2（重复）（1byte） |
| CTRL | ———— | 控制域（1byte） |
| ADDR | ———— | 地址域（2byte） |
| ASDU | ———— | 链路用户数据[（length-2-1）byte] |
| C S | ———— | 校验和（1byte） |
| 16 H | ———— | 结束字符（1byte） |

1. 判断方法

判断方法：判断第1个字节是否为10H还是68H

1. 解析CTRL字节

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | D7 | D6 | D5 | D4 | D3 | D2 | D1 | D0 |
| 主导从 | DIR(0) | PRM(1) | FCB | FCV | 功能码 |  |  |  |
| 从到主 | DIR(1) | PRM(0) | ACD | DFC | 功能码 |  |  |  |

判断帧方向方法：判断CTRL中的DIR和PRM为0、1还是为1、0

功能码（主到从）：

|  |  |  |  |
| --- | --- | --- | --- |
| 功能码 | 帧类型 | 功能描述 | FCV状态 |
| 0 | 发送/确认帧 | 复位通信单元 | 0 |
| 3 | 发送/确认帧 | 传送数据 | 1 |
| 4 | 发送/无回答帧 | 传送数据 | 0 |
| 6 | 协商定义 | 协商定义 | 1 |
| 7 | 复位帧计数位 | 传送数据 | 0 |
| 9 | 请求/响应帧 | 召唤链路状态 | 0 |
| a | 请求/响应帧 | 召唤1级数据 | 1 |
| b | 请求/响应帧 | 召唤2级数据 | 1 |

功能码（从到主）：

|  |  |  |
| --- | --- | --- |
| 功能码 | 帧类型 | 功　　　能 |
| 0 | 确认帧 | 确认 |
| 1 | 确认帧 | 链路忙，未收到报文 |
| 6 | 协商定义帧 | 协商功能定义 |
| 8 | 响应帧 | 以数据包响应请求帧 |
| 9 | 响应帧 | 从站没有所召唤的数据 |
| 11 | 响应帧 | 从站以链路状态响应主站请求 |

FCB位的作用：主站为每个从站保存一个FCB的拷贝，且主站每向从站发送1个FCV位为1的帧后，若收到了从站的确认帧或响应帧则FCB取反一次，否则主站重发此帧且FCB保持不变，主站在发送帧的时候要先判断FCV位的值，从而判断是否改变FCB。

ADC位的作用：ACD = 1，通知主站，从站有I级数据请求传送。

DFC位的作用：DFC = 0表示从站可以接受数据，DFC ＝1表示从站缓冲区已满，无法接受新数据。

1. 解析ADDR字节

ADDR1：站号低字节；ADDR2：站号高字节

1. 解析CS字节

固定帧：CS = (CTRL + SUM(ADDR)) % 0XFF

可变帧：CS = (CTRL + SUM(ADDR) + SUM(ASDU)) % 0XFF

1. ASDU格式

|  |  |  |
| --- | --- | --- |
| TYPE | ------------ | ASDU类型标识(1 byte) |
| VSQ | ------------ | 可变结构限定词(1 byte) |
| COT | ------------ | 传送原因(1 byte) |
| ASDU\_ADDR | ------------ | 应用服务数据单元公共地址  (2 byte) |
| FUN | ------------ | 功能类型(1 byte) |
| INF | ------------ | 信息序号(1 byte) |
| 信息元 |  |  |
| …… |  |  |

总召命令帧：

0x68, 0x0b, 0x0b, 0x68, 0x53, 0xff, 0xff, 0x64, 0x01, 0x06, 0xff, 0xff, 0x00, 0x00, 0x14, 0xce, 0x16

680b0b6853ffff640106ffff000014ce16

0xCE(校验和) = 0x53 + 0xff + 0xff + 0x64 + 0x01 + 0x06 + 0xff + 0xff + 0x00 + 0x00 + 0x14

确认帧：

0x68, 0x0b, 0x0b, 0x68, 0x80, 0xff, 0xff, 0x64, 0x01, 0x07, 0xff, 0xff, 0x00, 0x00, 0x14, 0xFC, 0x16

680b0b6880ffff640107ffff000014FC16

0xFC(校验和) = 0x80 + 0xff + 0xff + 0x64 + 0x01 + 0x07 + 0xff + 0xff + 0x00 + 0x00 + 0x14

遥测数据帧：

结束帧：

0x68, 0x0b, 0x0b, 0x68, 0x88, 0xff, 0xff, 0x64, 0x01, 0x0a, 0xff, 0xff, 0x00, 0x00, 0x14, 0x07, 0x16

680b0b6888ffff64010affff0000140716

0x07(校验和) = 0x88 + 0xff + 0xff + 0x64 + 0x01 + 0x0a + 0xff + 0xff + 0x00 + 0x00 + 0x14

功能模块：

组

装

解

析

TCP

接

收

TCP

发

送

分析

Http服务器

http发送

服务器

组

装

解

析

TCP

接

收

TCP

发

送

分析

客户端

http组装