标准ModBus

ModBus网络只有一个主机，所有通信都由他发出。网络可支持247个之多的远程从属控制器，但实际所支持的从机数要由所用通信设备决定。表1是ModBus各功能码对应的数据类型（部分）。 不同数据通信通过功能码确定。

表1 ModBus功能码与数据类型对应表

|  |  |  |
| --- | --- | --- |
| 代码 | 功能 | 数据类型 |
| 03 | 读 | 整型、字符型、状态字、浮点型 |
| 16 | 写 | 把具体的二进制值装入一串连续的保持寄存器 |

ModBus的传输方式及协议格式——RTU（远程终端设备）

表2给出了以RTU方式读取整数据的例子

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 主机请求 | | | | | | | |
| 地址 | 功能码 | 第一个寄存器的高位地址 | 第一个寄存器的低位地址 | 寄存器的数量的高位 | 寄存器的数量的底位 | CRC错误校验 | |
| 01 | 03 | 00 | 08 | 00 | 01 | 04 | 7F |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 从机应答 | | | | | |
| 地址 | 功能码 | 字节数 | 数据高字节 | 数据低字节 | CRC错误校验 |
| 01 | 03 | 02 | 41 | 24 | XX |
| 十六进制数4124表示的十进制整数为16676，错误校验值要根据传输方式而定。 | | | | | |

功能码03的作用是读取保持寄存器的值。保持寄存器，就是其值不被外部输入信号改变的寄存器。例如，保存模拟量输出接点(Analog Output，AO)的数字量(即D/A转换的数字量)的寄存器，就是保持寄存器。功能码03也可以被扩展为读取控制器内部多种16位寄存器的值。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 主机请求 | | | | | | | | | |
| 地址 | 功能码 | 第一个寄存器的高位地址 | 第一个寄存器的低位地址 | 寄存器个数的高位 | 寄存器个数的低位 | 数据字节个数 | 数据 | 错误校验 | |
| 01 | 0x10 | 00 | 38 | 00 | 02 | 04 | …… | XX | |
| 从机应答 | | | | | | | | | |
| 地址 | 功能码 | 第一个寄存器的高位地址 | 第一个寄存器的低位地址 | 寄存器个数的高位 | 寄存器个数的低位 | 错误校验 | | |
| 01 | 0x10 | 00 | 38 | 00 | 02 | XX | | |

功能码0x10的作用是写入多个保持寄存器的值。例如：模拟量输出接点(Analog Output，AO)的数字量(即D/A转换的数字量)的寄存器。

### Modbus返回异常码方式

Modbus协议中，异常响应包含一个异常码，这个码表示了出现问题的原因。当Modbus从机设备执行一个功能后，如果出现异常（例如，无法读取寄存器、无法写入寄存器、无法执行算数运算等），它会返回一个异常响应而不是正常的数据响应。

Modbus异常响应的格式如下：

* 从机地址，功能码（异常响应中为80h + 原始功能码），异常码，校验码