Modbus 通讯协议简化

V1.0　　2004-5-21

1　Modbus 协议概述

Modbus 协议是主从站通讯协议，用异步串行口完成通讯，物理层采用 RS485 或 RS232。传输速率可以达到 115kbps，理论上可接（寻址）一台主站和至多 247 台从站。受线路和设备的限制，最多可接一台主站和 32 台从站。

Modbus 协议的某些特性是固定的，如帧格式、帧顺序、通讯错误和异常情况的处理，以及所执行的功能等，都不能随便改动。其他特性属于用户可选的，如传输介质、波特率、字符奇偶校验、停止位的个数等等，传输模式为 RTU。用户所选择的参数对于各个站必须一致，在系统运行时不能改变。

1.1 Modbus 协议传输模式

Modbus 的传输模式：RTU 方式。

表 1-1 RTU 传输模式的特性

特性		RTU
编码系统		十六进制
每个字符的位数	起始位	1 位
	数据位	8 位
	奇偶校验位	0 或 1 位
	停止位	1 或 2 位
校验和		CRC（循环冗余校验）

1.2 帧

Modbus 协议的帧（报文）格式：RTU 帧。

下表是 RTU 传输模式的一般格式命令帧。

从站地址	功能码	数据	校验和
8 位	8 位	N*8 位	16 位

2　Modbus 协议

2.1　通讯方式

Modbus 有两种通讯方式：应答方式和广播方式。

应答方式是主站向某个从站（地址 1~247）发出命令，然后等待从站的应答；从站接到主站命令后，执行命令，并将执行结果返回给主站作为应答，然后等待下一个命令。

广播方式是主站向所有从站发送命令（从站地址为 0），不需要等待从站应答；从站接到广播命令后，执行命令，也不向主站应答。

除了会送诊断校验外，只有 05、06、15、16 这四项功能（见 2.3）对广播方式有效。

2.2 Modbus 帧

Modbus 的帧按应答方式分为命令帧（询问帧）和应答帧。命令帧为一般格式命令帧，应答帧有显长度帧和隐长度帧之分，图 2-1、2-3、2-4 给出了典型的帧格式。

从站地址	功能码	数据				校验和
		数据起始寄存器高位	数据起始寄存器地位	数据寄存器高位	数据寄存器地位	

图 2-1 一般格式命令帧

起始地址偏置(+XXX)

从站地址	功能码	数据长度	数据	校验和

图 2-3 显长度应答帧

从站地址	功能码	数据	校验和

图 2-4 隐长度应答帧

2.2.1 从站地址字段

帧中的从站地址字段表示接收主站报文的从站地址。当从站地址字段为 0 时，表示所有从站，此时的报文是广播报文。

用户必须设定每台从站的专用地址。只有被编址的设备才能对主机的命令（询问）做出应答。从站发送应答报文时，报文中地址的作用是向主站报告正在通讯的是哪台从站。

2.2.2 功能码字段

功能码字段同志从站应执行何种功能。表 2-1 列出了功能码的意义和作用。2.3 节给出了各个功能码对应报文的详细格式和功能。

表 2-1 Modbus 功能码

功能码	名称	作用（对主站而言）
01	读取开出状态	取得一组开关量输出的当前状态
02	读取开入状态	取得一组开关量输入的当前状态
03	读取模出状态	取得一组模拟量输出的当前状态
04	读取模入状态	取得一组模拟量输入的当前状态
05	强制单路开出	强制设定某个开关量输出的值
06	强制单路模出	强制设定某个模拟量输出的值
07	读取异常状态	取得从站的一些状态（8 位）
08	回送诊断校验	把诊断校验报文送从站，以对通讯处理进行评鉴
09	编程	主机模拟编程器的作用，修改从站逻辑
10	探询	定期探询从站是否已完成某长程序任务
11	读取事件计数	取得通讯状态和通讯事件的次数
12	读取通讯事件记录	取得通讯状态、事件次数、报文数量和至多 64 个事件

13	编程	主机模拟编程器的作用，修改从站逻辑
14	探询	定期探询从站是否已完成某长程序任务
15	强制多路开出	强制设定从站几个开关量输出的值
16	强制多路模出	强制设定从站几个模拟量输出的值
17	报告从站标识	取得从站类型和运行指示灯的状态
18	编程	主机模拟编程器的作用，修改从站逻辑
19	重置通讯链路	使从站复位于已知状态
20-72	保留	留作扩展功能备用
73-119	非法功能	
120-127	保留	留作内部使用
128-255	保留	用作异常应答

2.2.2　数据长度字段

数据长度字段记录的是随后的数据字段的长度，单位为字符（字节）。数据字段的长度总是被规定为 RTU 模式下数据字符的总数，数据字符的数量总是按 RTU 模式下的数据字符计算。

2.2.4　数据字段

数据字段内含有从站执行某项具体功能的信息，或者含有从站应答询问的信息。这些信息可以是数值、地址参数或范围，例如，从哪路开关量或寄存器开始，处理几个开关位或寄存器、开关量或寄存器的值等等。

2.2.5　校验和字段

校验和字段用于检查通讯报文在通讯线路中是否出错。

RTU 模式传送时，用 CRC-16,参见附录 A。

2.3 功能码

2.3.1 读取开出状态（功能码 01）

本功能可使主站获得被编址从站的开关量输出的通断状态。起始地址是指从哪一路开关量开始（编号从 0 开始），数据线圈数是指读取几路。应答帧中的数据是按上述要求读取的开关量数据（每路一位，每 8 位组成一个字节，最后一个字节的不足部分补 0）。本功能不支持广播方式。

以下例子是读取 17 号从站开关量输出 020-056 的状态，读出的 37 位组成 5 个字节，最后一个字节的高三位补 0。

询问 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	数据线圈数高位	数据线圈数低位	校验和 CRC
11H	01H	00H	13H	00H	25H	0EH　84H

应答 RTU 帧：

从站地址	功能码	字节计数	数据	校验和 CRC
11H	01H	05H	CDH 6BH B2H 0EH 1BH	45H　E6H

2.2.3　读取开入状态（功能码 02）

本功能可使主站获得被编址从站的开关量输入的通断状态。起始地址是指从哪一路开关量开始（编号从 0 开始），数据线圈数是指读取几路。应答帧中的数据是按上述要求读取的开关量数据（每路一位，每 8 位组成一个字节，最后一个字节的不足部分补 0）。本功能不支持广播方式。

以下例子是读取 17 号从站开关量输入 0197-0218 的状态，读出的 22 位组成 3 个字节，最后一个字节的高 2 位补 0。

询问 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	数据线圈数高位	数据线圈数低位	校验和 CRC
11H	02H	00H	C4H	00H	16H	BAH A9H

应答 RTU 帧：

从站地址	功能码	字节计数	数据	校验和 CRC
11H	02H	03H	ACH DBH 35H	20H 18H

2.2.4　读取模出状态（功能码 03）

本功能可使主站获得被编址从站的模拟量输出的通断状态。起始地址是指从哪一路模拟量开始（编号从 0 开始），寄存器数是指读取几路模拟量（每路模拟量 2 个字节，高位在前，低位在后）。应答帧中的数据是按上述要求读取的模拟量数据。本功能不支持广播方式。

以下例子是读取 17 号从站模出点 0108-0110 的状态。应答数据高字节在前。108 是 555，109 是 0，110 是 100。

询问 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	寄存器数高位	寄存器数低位	校验和 CRC
11H	03H	00H	6BH	00H	03H	76H 87H

应答 RTU 帧：

从站地址	功能码	字节计数	数据	校验和 CRC
11H	03H	06H	02H 2BH 00H 00H 00H 64H	CBH BAH

11 03 80

2.2.5　读取模入状态（功能码 04）　低地址数据在前,

本功能可使主站获得被编址从站的模拟量输入值。起始地址是指从哪一路模拟量开

始（编号从 0 开始），寄存器数是指读取几路模拟量（每路模拟量 2 个字节，高位在前，低位在后）。应答帧中的数据是按上述要求读取的模拟量数据。本功能不支持广播方式。

以下例子是读取 17 号节点的模入点 0108-0110 的状态。应答数据高字节在前。108 是 555，109 是 0，110 是 100。

询问 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	寄存器数高位	寄存器数低位	校验和 CRC
11H	04H	00H	6BH	00H	03H	C3H 47H

应答 RTU 帧：

从站地址	功能码	字节计数	数据	校验和 CRC
11H	04H	06H	02H 2BH 00H 00H 00H 64H	5C 89H

2.2.6 强制单路开出（功能码 05）

本功能可使主站强行设定被编址从站某路开关量输出的通断状态。从站内部的任何一路开关量均能被强制。起始地址是指设定开关量的哪一路（编号从 0 开始），数据用于设定开或关：FF 为开，0 为关，其他值为非法值。正常应答是将报文原文发回。从站地址为 0 时，为广播方式。

以下例子是强制 17 号从站开出点 173 为 ON。

询问 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	数据	开关原状态	校验和 CRC
11H	05H	00H	ACH	FFH	00H	4EH 8BH

应答 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	数据	开关原状态	校验和 CRC
11H	05H	00H	ACH	FFH	00H	4EH 8BH

2.2.7 强制单路模出（功能码 06）

本功能可使主站强行设定被编址从站某路模拟量输出的值。从站内部的任何一路模拟量均能被强制。起始地址是指设定哪一路模拟量（编号从 0 开始），数据用于设定该模拟量的值（高位在前，低位在后）。正常应答是将报文原文发回。从站地址为 0 时，为广播方式。

以下例子是强制 17 号从站模出点 136 为 039EH。

询问 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	数据高位	数据低位	校验和 CRC
11H	06H	00H	87H	03H	9EH	BAH 2BH

应答 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	数据高位	数据低位	校验和 CRC
11H	06H	00H	87H	03H	9EH	BAH 2BH

2.2.8 强制多路开出（功能码 15）

本功能可使主站强行设定被编址从站一组连续开关量输出的通断状态。从站内部的任何开出量均能被强制。起始地址是从哪一路开关量开始（编号从 0 开始），寄存器数是指设定几路。字节计数是指随后的线圈状态（开关量设定值）的字节数。线圈状态是设定的开出值，每一路开出占用一位（1 为开，0 为关），每八位组成一个字节，最后一个字节的不足部分补 0。正常应答内容是回送从站地址、功能码、起始地址和强置的开关量数。从站地址为 0 时，为广播模式。

以下例子是强置 17 号从站开关量输出 0020-0029 的状态，设定值 CD（11001101）和 00（00000000）表示开关量输出的第 27、26、23、22 和 20 将被强置为开状态。

询问 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	寄存器数高位	寄存器数低位	字节计数	数据	校验和 CRC
11H	0FH	00H	13H	00H	0AH	02H	CDH 00H	7EH CBH

应答 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	寄存器数高位	寄存器数低位	校验和 CRC
11H	0FH	00H	13H	00H	0AH	26H 99H

2.2.9 强制多路模出（功能码 16）

本功能可使主站强行设定被编址从站一组连续模拟量输出的值。从站内部的任何模出量均能被强制。起始地址是从哪一路模拟量开始（编号从 0 开始），寄存器数是指设定几路。字节计数是指随后的数据（模拟量设定值）的字节数。数据是设定的模出值，每一路模出两个字节（高位在前，低位在后）。正常应答内容是回送从站地址、功能码、

起始地址和强置的模拟量数。从站地址为 0 时，为广播模式。

以下例子是强置 17 号从站模拟量输出 0136-0137 的状态，设定值 0136 为 000A，设定 0137 为 0102。

询问 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	寄存器数高位	寄存器数低位	字节计数	数据	校验和 CRC
11H	10H	00H	87H	00H	02H	04H	00H 0AH 01H 02H	4EH BAH

应答 RTU 帧：

从站地址	功能码	起始地址高位	起始地址低位	寄存器数高位	寄存器数低位	校验和 CRC
11H	10H	00H	87H	00H	02H	F3H 71H

附录 A 循环冗余校验 （CRC）码算法

生成 CRC-16 校验字节的步骤如下：

1. 装入一个 16 位寄存器，所有数位均为 1。
2. 装 16 位寄存器的低位字节与开始 8 位字节进行“异或”运算。运算结果放入这个 16 位寄存器。
3. 把这个 16 位寄存器向右移 1 位。
4. 若向右（标记位）移出的数位是 1，则生成多项式 1010000000000001 和这个寄存器进行异或运算。若向右移出的数位是 0，则返回（3）。
5. 重复（3）和（4），直到移出 8 位。
6. 另外 8 位与该 16 位寄存器进行“异或”运算。
7. 重复（3）-（6），直至该报文所有字节均与 16 位寄存器进行“异或”运算，并移位 8 次。
8. 这个 16 位寄存器的内容即是 2 字节 CRC 校验值。

附录 B. 数据通道表

不同的数据通道表应由数据传送方提供，表格式如下表（数据名称、数据地址、取值范围应根据实际而定）

序号	数据名称	数据类型	功能码	数据地址	传输方向	缩放倍数	取值范围
1	模拟量 1	16 位二进制, 有符号整数	0x03	40001	主站 < 子站	1	2000-2100
2	模拟量 2		0x03	40002	主站 < 子站	0.5	1-100
3	模拟量 3		0x03	40003	主站 < 子站	0.5	0-50
4	模拟量 4		0x03	40004	主站 < 子站	1	0-23
5	模拟量 5		0x03	40005	主站 < 子站	0.01	0-9999
6	模拟量 6		0x03	40006	主站 < 子站	0.01	0-999
7	模拟量 7		0x03	40007	主站 < 子站	0.1	200-210
8	模拟量 8		0x03	40008	主站 < 子站	1	1-12

序号	数据名称	功能码	数据地址	传输方向	取值范围
1	开关量 1	0X02	10001	主站< 子站	0/1
2	开关量 2	0X02	10002	主站 < 子站	0/1
3	开关量 3	0X02	10003	主站 < 子站	0/1
4	开关量 4	0X02	10004	主站 < 子站	0/1
5	开关量 5	0X02	10005	主站 < 子站	0/1
6	开关量 1	0x02	10001	主站 < 子站	0/1
	….				

序号	数据名称	数据类型	功能码	数据地址	传输方向	缩放倍数	取值范围
1	模拟量 1	16 位二进制, 有符号整数	0x10	40101	主站 >子站	1	2000-2100
2	模拟量 2		0x10	40102	主站 >子站	0.5	1-100
3	模拟量 3		0x10	40103	主站 >子站	0.5	0-50
4	模拟量 4		0x10	40104	主站 >子站	1	0-23
5	模拟量 5		0x10	40105	主站 >子站	0.01	0-9999
6	模拟量 6		0x10	40106	主站 > 子站	0.01	0-999
7	模拟量 7		0x10	40107	主站 >子站	0.1	200-210
8	模拟量 8		0x10	40108	主站 >子站	1	1-12

序号	数据名称	功能码	数据地址	传输方向	取值范围
1	开关量 1	0X0A	00001	主站 > 子站	0/1
2	开关量 2	0X0A	00002	主站 > 子站	0/1
3	开关量 3	0X0A	00003	主站 > 子站	0/1
4	开关量 4	0X0A	00004	主站 > 子站	0/1
5	开关量 5	0X0A	00005	主站 > 子站	0/1
6	开关量 1	0x02	10001	主站 < 子站	0/1
	….				