MODBUS 协议整理

整理 徐凯

江南大学 机械工程学院

Email xukai19871105@126.com

MODBUS 部分功能代码

下表列出 MODBUS 支持的部分功能代码：以十进制表示。

代码	中文名称	寄存器信息地址	位操作/字操作	操作数量
01	读线圈状态	00001-09999	位操作	单个或多个
02	读(开关)输入状态	10001-19999	位操作	单个或多个
03	读保持寄存器	40001-49999	字操作	单个或多个
04	读输入寄存器	30001-39999	字操作	单个或多个
05	写单个线圈	00001-09999	位操作	单个
06	写单个保持寄存器	40001-49999	字操作	单个
15	写多个线圈	00001-09999	位操作	多个
16	写多个保持寄存器	40001-49999	字操作	多个

表 MODBUS 部分功能码

功能码说明

功能码可以分为位操作和字操作两类

位操作包指令包括，读线圈状态 01，读(开关)输入状态 02，写单个线圈 06 和写多个线圈 15。

字操作(2 个字节)指令包括：读保持寄存器 03，写单个寄存器 06，写多个保持寄存器 16。

Modbus 寄存器地址分配

寄存器信息地址 (PLC 地址)	适用功能码 (10 进制)	寄存器种类	读写状态
00001-09999	01 05 15	线圈状态	可读可写
10001-19999	02	(开关)输入状态	可读
30001-39999	04	输入寄存器	可读
40001-49999	03 06 16	保持寄存器	可读可写

寄存器种类说明

寄存器种类	说明	PLC 类比	举例说明
线圈状态	输出端口，按位操作，可设定端口的输出状态，也可以读取该位的输出状态。	DO	电磁阀输出，MOSFET 输出，LED 显示等。
开关输入状态	输入端口，按位操作，通过外部设定改变输入状态，可读不可写。	DI	拨码开关，接近开关，机械开关等
保持寄存器	输出参数或是保持参数，控制器运行时被设定的某些参数。可读可写。	AO	模拟量输出设定值，PID 运行参数，AD 转换采样频率等参数。
输入寄存器	输入参数。控制器运行时从外部设备获得的参数	AI	模拟量输入

特别说明

寄存器信息地址（**PLC 地址**）

寄存器信息地址指的是存放于控制器中的地址，这些控制器可以是 PLC，也可以使触摸屏，或是文本显示器。例如 40001、30002 等，这些地址一般使用 10 进制描述。

寄存器寻址地址（**协议地址**）

寄存器寻址地址指的是通信时使用的寄存器地址，例如信息地址 40001 对应寻址地址 0x0000，40002 对应寻址地址 0x0001，寄存器寻址地址一般使用 16 进制描述。再如，信息寄存器 40003 对应寻址地址 0002，信息寄存器 30003 对应寻址地址 0002，虽然两个信息寄存器通信时使用相同的地址，但是需要使用不同的命令才可以访问，所以访问时不存在冲突。

01 读线圈状态

描述

读从机离散量输出口的 ON/OFF 状态。离散量输出口可以为继电器输出口，也可以为 MOSFET 输出接口，这些接口本质上都是位操作。

查询

查询信息规定被访问的线圈起始地址和线圈数量。

例：请求从机设备 17 读 00020-00056 线圈。其中 00020-00056 为线圈的寄存器信息地址，这些线圈的寄存器寻址地址为 0019 – 0055，共访问 37 个线圈。

	Hex
从机地址	11
功能码	01
寄存器起始地址高位	00
寄存器起始地址低位	13
寄存器数量高位	00
寄存器数量低位	25
CRC 校验高位	
CRC 校验低位	

表 读线圈状态－查询

响应

响应信息中的各线圈的状态与数据区的每一位的值相对应，1 代表 ON；0 代表 OFF。若返回的线圈数不是 8 的倍数，则在最后的数据字节未使用的位中全部填充 0，字节数区说明全部数据的字节数。

	Hex
从机地址	11
功能码	01
返回字节数	05
数据 1(线圈 00027-线圈 00020)	CD
数据 2(线圈 00035-线圈 00028)	6B
数据 3(线圈 00043-线圈 00036)	B2
数据 4(线圈 00051-线圈 00044)	0E
数据 5(线圈 00056-线圈 00052)	1B
CRC 校验高位	
CRC 校验低位	

表: 读线圈状态－响应

线圈 27-20 的状态用 CDH 表示，二进制值为 11001101，该字节的最高位为线圈 27，最低位为线圈 20。线圈从左(27)向右(20)状态分别为 ON-ON-OFF-OFF-ON-ON-OFF-ON。下一个字节的线圈应为 35 至 28。

地址	00027	00026	00025	00024	00023	00022	00021	00020
状态	ON	ON	OFF	OFF	ON	ON	OFF	ON

表 线圈 00027 到 00020 状态

最后一个数据字节中，56-52 线圈的状态为 1BH(或二进制 00011011)，线圈 56 是左数第 4 位，线圈 52 是该字节的最低位，所线圈 56 至 52 的状态分别为 ON-ON-OFF-ON-ON，3 个剩余位全部填 0。

地址	00059	00058	00057	00056	00055	00054	00053	00052
状态	填充	填充	填充	ON	ON	OFF	ON	ON

表 线圈 00056 到 00052 状态

02 读输入位状态

说明

读从机离散量输入信号的 ON/OFF 状态。

查询

查询信息规定了要读的输入起始地址，以及输入信号的数量。

例：请求读从机设备 17 的 10197-10218 的输入位状态。

	Hex
从机地址	11
功能码	02
寄存器地址高位	00
寄存器地址低位	C4
寄存器数量高位	00
寄存器数量低位	16
CRC 校验高位	
CRC 校验低位	

表 读输入位状态－查询

响应

响应信息中的各输入口的状态，分别对应于数据区中的每一位值，1 代表 ON；0 代表 OFF。第一个数据字节的 LSB(最低位)为查询的寻址地址，其他输入口按顺序在该字节中由低位向高位排列，直至 8 位为止。下一个字节中的 8 个输入位也是从低位到高位排列。

若返回的输入位数不是 8 的倍数，则在最后的数据字节中的剩余位直至字节的最高位全部填零。字节数区，说明了全部数据的字节数。

	Hex
从机地址	11
功能码	02
返回字节数	03
数据 1(开关 10204-开关 10197)	AC
数据 2(开关 10212-开关 10205)	DB
数据 3(开关 10218-开关 10213)	35
CRC 校验高位	
CRC 校验低位	1B

表 读输入位状态－响应

输入位 10204-10197 的状态用 35H (或二进制 00110101) 表示。输入位 10218 为左数第 3 位，10213 输入位为 LSB，输入位 10218-10213 的状态分别为 ON-ON-OFF-ON-OFF-ON，最后 2 个剩余位填零。

地址	10204	10023	10022	10021	10020	10019	10018	10017
状态	0	0	1	1	0	1	0	1
地址	10212	10211	20210	10209	10208	10207	10206	10205
状态	1	1	1	0	1	0	1	1
地址	10220	10219	10218	10217	10216	10215	10214	10213
状态	填充	填充	1	1	0	1	0	1

表 开关输入位 10204 到 10017 状态

03 读保持寄存器

说明

读从机保持寄存器的二进制数据。

查询

查询信息规定了寄存器起始地址及寄存器的数量。

	Hex
从机地址	11
功能码	03
寄存器地址高位	00
寄存器地址低位	6B
寄存器数量高位	00
寄存器数量低位	03
CRC 高位	
CRC 低位	

表 读保持寄存器-查询

响应

响应信息中的寄存器数据为二进制数据，每个寄存器分别对应 2 个字节，第一个字节为高位数据，第二个字节为低位数据。

例按查询要求返回响应。

	Hex
从机地址	11
功能码	03
字节数	
数据 1 高位(寄存器 40108)	00
数据 1 低位(寄存器 40108)	6B
数据 2 高位(寄存器 40109)	00
数据 2 低位(寄存器 40109)	03
数据 3 高位寄存器 40110)	00
数据 3 低位寄存器 40110)	00
CRC 高位	
CRC 低位	

表 读寄存器-响应

寄存器 40108 的数据用 022BH 2 个字节(或用十进制 555)表示，寄存器 40109-40110 中的数据为 0000 和 0064H，(十进制时为 0 和 100)

地址	40108 高字节	40108 低字节	40109 高字节	40109 低字节	40110 高字节	40110 低字节
状态	00	6B	00	13	00	00

表 保持寄存器 40108 到 40110 数值

04 读输入寄存器

说明

读从机输入寄存器(3XXXX 类型)中的二进制数据。

查询

查询信息规定了要读的寄存器的起始地址及寄存器的数量，寄存器 30001-30016 所对应的地址分别为 0-15。

例：请求读从机设备 17 中的 30009 寄存器。

	Hex 格式
从机地址	11
功能码	04
寄存器起始地址高位	00
寄存器起始地址低位	08
寄存器个数高位	00
寄存器个数低位	01
CRC 高位	
CRC 低位	

表 读输入寄存器-查询

响应

响应信息中的寄存器数据为每个寄存器分别对应 2 个字节，第一个字节为高位数据，第二个字节为低位数据。

例按查询要求返回响应

	Hex 格式
从机地址	11
功能码	04
字节数	02
数据高位(地址 30009)	00
数据低位(地址 30009)	0A
CRC 高位	
CRC 低位	

表 读寄存器-响应

寄存器 30009 中的数据用 000AH 2 个字节(或用十进制 10)表示。

05 强制单个线圈

说明

强制单个线圈(0XXXX 类型)为 ON 或 OFF 状态。

查询

查询信息规定了需要强制线圈的类型。

由查询数据区中的一个常量。规定被请求线圈的 ON/OFF 状态， **FF00H 值请求线圈处于 ON 状态，0000H 值请求线圈处于 OFF 状态**。05 指令设置单个线圈的状态，15 指令可以设置多个线圈的状态，虽然都是设定线圈的 ON/OFF 状态，但是 ON/OFF 的表达方式却不同。

例：强制从机设备 17 中的 00173 线圈为 ON 状态

	Hex
从机地址	11
功能码	05
寄存器地址高位	00
寄存器地址低位	AC
寄存器数量高位	FF
寄存器数量低位	00
CRC 校验高位	
CRC 校验低位	

表 强制单个线圈-查询

响应

线圈为强制状态后即返回正常响应

例：按查询要求返回响应

	Hex
从机地址	11
功能码	05
寄存器地址高位	00
寄存器地址低位	AC
寄存器数量高位	FF
寄存器数量低位	00
CRC 校验高位	
CRC 校验低位	

表 强制单个线圈

06 预置单个保持寄存器

说明

把一个值预置到一个 4XXXX 类型保持寄存器中。请注意，06 指令只能操作单个保持寄存器，16 指令可以设置单个或多个保持寄存器。

查询

例：请求把从机设备 17 中的 40002 寄存器预置为 0003H 值。

	Hex
从机地址	11
功能码	06
寄存器起始地址高位	00
寄存器起始地址低位	01
数据高位	00
数据低位	00
CRC 校验高位	
CRC 校验低位	

表 预置单个寄存器-查询

响应

寄存器内容被预置后返回正常响应。

例：按查询要求返回响应

	Hex
从机地址	11
功能码	06
寄存器起始地址高位	00
寄存器起始地址低位	01
寄存器数量高位	00
寄存器数量低位	00
CRC 校验高位	
CRC 校验低位	

表 预置单个寄存器-响应

15 (0F H) 强制多个线圈

说明

按线圈的顺序把各线圈 (0XXXXX 类型) 强制成 ON 或 OFF。

查询

查询信息规定了被强制线圈的类型。

查询数据区规定了被请求线圈的 ON/OFF 状态，如数据区的某位值为“1”表示请求的相应线圈状态为 ON，位值为“0”，则为 OFF 状态。

下述例子为请求从机设备 17 中一组 10 个线圈为强制状态，起始线圈信息地址为 20 ，则寻址地址为 19(13H)，查询的数据为 2 个字节，即 CD01H (二进制 11001101 0000 0001) 相应线圈的二进制位排列如下表所示。

位	27	26	25	24	23	22	24	20	35	34	33	32	31	30	29	28
值	1	1	0	0	1	1	0	1	0	0	0	0	0	0	0	1

传送的第一个字节 CDH 对应线圈为 27-20，LSB（最低位） 对应线圈 20，传送的第二个字节为 01H，对应的线圈为 29-28， LSB 对应继圈 28，其余未使用的位均填“0”。

	Hex
从机地址	11
功能码	0F
寄存器地址高位	00
寄存器地址低位	13
寄存器数量高位	00
寄存器数量低位	0A
字节数	02
数据 1 (线圈 27-线圈 20)	CD
数据 2(线圈 29-线圈 28)	01
CRC 校验高位	
CRC 校验低位	

表 强制多个线圈-查询

响应

正常响应返回从机地址，功能代码，起始地址以及强制线圈数

例：对上述查询返回的响应

	Hex
从机地址	11
功能码	0F
寄存器地址高位	00
寄存器地址低位	13
寄存器数量高位	00
寄存器数量低位	0A
字节数	02
CRC 校验高位	
CRC 校验低位	

表 强制个多个圈—响应

16(10 Hex)预置多个保持寄存器

说明

把数据按顺序预置到各 (4XXXX 类型) 寄存器中。

查询

例：请求在从机设备 17 中的 2 个寄存器中放入预置值，起始寄存器信息地址为 40002，寻址地址位 0001，预置值为 000AH 和 0102H。

	Hex
从机地址	11
功能码	10
寄存器起始地址高位	00
寄存器起始地址低位	01
寄存器数量高位	00
寄存器数量低位	02
字节数	04
数据 1 高位	00
数据 1 低位	0A
数据 2 高位	01
数据 2 低位	02
CRC 校验高位	
CRC 校验低位	

表 预置多个寄存器

地址	40002 高字节	40002 低字节	40003 高字节	40003 低字节
状态	00	0A	01	12

表 寄存器 40002 到 40003 数值

响应

正常响应返回从机地址，功能代码和起始地址和预置寄存器数。

例：按查询要求返回响应

	Hex
从机地址	11
功能码	10
寄存器起始地址高位	00
寄存器起始地址低位	01
寄存器数量高位	00
寄存器数量低位	02
CRC 校验高位	
CRC 校验低位	

表 预置多个寄存器—响应