

第 5 章

CHAPTER 5

功能码详解

在以下章节的功能码中,请求报文是由主站向从站发起的,而响应报文是由接收到主站请求的从站发起的,响应报文又分为正常响应和异常响应,下述响应报文均为正常响应的示例,异常响应的介绍将在 5.10 节展开。

请求报文和响应报文均有一个共同点,那就是报文中都包含以下 3 个元素:从站地址、功能码、CRC-16 校验码,基于这个特点在下述报文构成中不再赘述以上 3 个元素,只介绍各个功能码报文构成的其他组成元素。

5.1 寄存器功能异同点介绍



寄存器功能包含线圈功能、离散输入功能、保持寄存器功能和输入寄存器功能。线圈功能与离散输入功能类似,作为一组介绍。保持寄存器与输入寄存器功能类似,作为一组介绍。

20min

线圈与离散输入的异同点如下。

(1) 相同点:由于线圈与离散输入均是以位(bit)为单位的,因此其状态值只有 1 和 0 两种,同时,两者均支持被读取单个或连续多种状态值,并且状态值组合成字节数据的方式是一致的。

(2) 不同点:线圈支持被读和被写,而离散输入只支持被读。

保持寄存器与输入寄存器的异同点如下。

(1) 相同点:保持寄存器与输入寄存器的值均是 16 位的数据类型,换句话说,一个寄存器存放两字节的数据。保持寄存器与输入寄存器支持被读单个或连续多个寄存器的值,如果是读取多个寄存器的值,则可能要考虑字节序的问题。

(2) 不同点:保持寄存器支持被读和被写,而输入寄存器支持被读,此外,如果是写多个保持寄存器的值,则可能要考虑字节序的问题。

5.2 01(0x01)读取线圈/离散输出状态



01 功能码用于读取从站设备的一种或多种线圈状态,有关该功能码的请求报文和响应报文的构成细节将在下述展开。

30min

1. 功能说明

读取从站线圈或离散输出(DO)的开或关的状态。

2. 请求报文

请求报文的信息要指定需读取的线圈的起始地址和数量,其中地址和数量各占用两字节,并且都是先传输高位字节数据,再传输低位字节数据。

在请求报文的信息里,访问的从站地址是4,访问的线圈地址范围是10~22,共计13个值,见表5-1。

表 5-1 功能码 01 请求报文示例

字 段	从站地址	功能码	起始地址 (高位)	起始地址 (低位)	线圈数量 (高位)	线圈数量 (低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x04	0x01	0x00	0x0A	0x00	0x0D	CRC(2 字节)	8

3. 响应报文

在响应报文的数据字段中,每个线圈占用一个位,1 用于标识开,0 用于标识关。第 1 个数据字节的 LSB 用于标识请求报文中访问的第 1 个线圈地址的值,其他线圈紧随该 LSB 的高位端,一直到这字节的 MSB 为止,并在后续字节中按照同样的方式(由低到高)排列。如果访问的线圈数量不是 8 的倍数,则最后一个数据字节中的其余位将用 0 填充(朝向字节的高位端)。

字节数字段标识完整数据字节的数量。

读取到的线圈状态见表 5-2,线圈 10~17 的数据则表现为 0x0A,其中 LSB 对应于线圈 10;线圈 18~22 显然不足 8 位数据,其余位用 0 填充,因此线圈 18~22 的数据则表现为 0x11,其中 LSB 对应于线圈 18。读取的线圈数量虽不足 16 个,但仍需按 2 字节存储上述的线圈状态值。

表 5-2 读取到的线圈状态

线圈地址	17	16	15	14	13	12	11	10	-	-	-	22	21	20	19	18
二进制值	0	0	0	0	1	0	1	0	0	0	0	1	0	0	0	1

响应报文见表 5-3。

表 5-3 功能码 01 响应报文示例

字 段	从站地址	功能码	字节数	数据 1	数据 2	CRC-16 校验	合计字节数
RTU 模式 8 位(Hex)	0x04	0x01	0x02	0x0A	0x11	CRC(2 字节)	7

5.3 02(0x02)读取离散输入状态

02 功能码用于读取从站设备的一种或多种离散输入状态,有关该功能码的请求报文和响应报文的构成细节将在下述展开。

1. 功能说明

读取从站中离散输入(DI)的开或关的状态。

2. 请求报文

请求报文的信息要指定需读取的离散输入的起始地址和数量。

在请求报文的信息里,访问的从站地址是 3,访问的离散输入地址范围是 5~9,共计 5 个值,见表 5-4。

表 5-4 功能码 02 请求报文示例

字 段	从站地址	功能码	起始地址 (高位)	起始地址 (低位)	离散输入数 量(高位)	离散输入数 量(低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x03	0x02	0x00	0x05	0x00	0x05	CRC (2 字节)	8

3. 响应报文

响应报文的各项字段与前一节的功能码(01)相同,见表 5-5。

表 5-5 功能码 02 响应报文示例

字 段	从站地址	功能码	字节数	数据	CRC-16 校验	合计字节数
RTU 模式 8 位(Hex)	0x03	0x02	0x01	0x17	CRC(2 字节)	6

5.4 03(0x03)读取保持寄存器的值



19min

03 功能码用于读取从站设备的一个或多个保持寄存器的值,有关该功能码的请求报文和响应报文的构成细节将在下述展开。

1. 功能说明

读取从站中保持寄存器的数据。保持寄存器的各个地址和数据意义由设备开发者自行规定。

2. 请求报文

请求报文的信息要指定需读取的保持寄存器的起始地址和数量。

在请求报文的信息里,访问的从站地址是 1,访问的保持寄存器地址范围是 0~1,共计读取两个寄存器,见表 5-6。

表 5-6 功能码 03 请求报文示例

字 段	从站地址	功能码	起始地址 (高位)	起始地址 (低位)	寄存器数 量(高位)	寄存器数 量(低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x01	0x03	0x00	0x00	0x00	0x02	CRC (2 字节)	8

3. 响应报文

有一点需要特别注意,Modbus 的保持寄存器和输入寄存器是以字(Word)为基本单位的(1Word=16 位),所以,当读取一个寄存器数据时,响应报文将返回两字节的数据。此外,如果读取的是两个寄存器数据(32 位数据),并且这种数据类型是浮点数或 32 位整数,则必须连续读取两个寄存器的数据,同时,这两个寄存器的地址必须相邻,例如当前需要连续读取两个 32 位的浮点数数据,读取的寄存器的起始地址是 1,那么,需要先把读到的地址 1 和地址 2 的数据组合成 32 位浮点数,随后再把读到的地址 3 和地址 4 的数据组合成另一个 32 位浮点数,至于两个寄存器的数据如何组合起来这里就涉及字节序和大小端问题,这一点需要根据从站设备的文档指示进行配置。

假设两个寄存器的数据是独立的数据,并非组合成一个 32 位数据,而一个寄存器的数据由两字节数据组成,则第 1 字节数据是传输寄存器数据的高 8 位,第 2 字节数据是传输寄存器数据的低 8 位,由于主站读取的是两个寄存器数据,因此返回 4 字节数据,见表 5-7。

表 5-7 功能码 03 响应报文示例

字 段	从站地址	功能码	字节数	数据 1 (高位)	数据 1 (低位)	数据 2 (高位)	数据 2 (低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x01	0x03	0x04	0x00	0xFF	0x00	0x06	CRC (2 字节)	9

5.5 04(0x04)读取输入寄存器的值

04 功能码用于读取从站设备的一个或多个输入寄存器的值,有关该功能码的请求报文和响应报文的构成细节将在下述展开。

1. 功能说明

读取从站中输入寄存器的数据。输入寄存器的各个地址和数据意义由设备开发者自行规定。

2. 请求报文

请求报文的信息要指定需读取的输入寄存器的起始地址和数量。

在请求报文的信息里,访问的从站地址是 1,访问的输入寄存器的地址是 1,共计读取一个寄存器,见表 5-8。

表 5-8 功能码 04 请求报文示例

字 段	从站地址	功能码	起始地址 (高位)	起始地址 (低位)	寄存器数 量(高位)	寄存器数 量(低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x01	0x04	0x00	0x01	0x00	0x01	CRC (2 字节)	8

3. 响应报文

响应报文的各项字段与前一节的功能码(03)相同,见表 5-9。

表 5-9 功能码 04 响应报文示例

字 段	从站地址	功能码	字节数	数据(高位)	数据(低位)	CRC-16 校验	合计字节数
RTU 模式 8 位(Hex)	0x01	0x04	0x02	0x12	0x64	CRC(2 字节)	7

5.6 05(0x05)写单个线圈/离散输出状态

05 功能码用于写从站设备的单个线圈状态,可写状态为开或关,有关该功能码的请求报文和响应报文的构成细节将在下述展开。

1. 功能说明

将从站中单个线圈/离散输出(DO)设置为开或关的状态。此功能码支持广播模式,在广播模式下,所有从站设备的同一地址的值将被统一修改,但均不对主站发起响应。

2. 请求报文

请求报文的信息要指定需写入的线圈地址和线圈的状态数据,其中,地址和数据各占用两字节。在请求报文的数据字段中,线圈的开或关状态分别由两个常数指定,0xFF00 用于标识开状态,0x0000 用于标识关状态。除此之外,写入其他值均为非法值,对线圈不起作用的同时,还会返回异常响应。

在请求报文的信息里,访问的从站地址是 17,将线圈的地址为 173 的值设置为开状态,见表 5-10。

表 5-10 功能码 05 请求报文示例

字 段	从站地址	功能码	线圈地址 (高位)	线圈地址 (低位)	线圈状态 (高位)	线圈状态 (低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x11	0x05	0x00	0xAD	0xFF	0x00	CRC (2 字节)	8

3. 响应报文

当从站正确地执行了主站的请求后,从站将返回与请求报文一致的响应报文,如表 5-11 所示,如果从站执行失败,则返回异常响应。

表 5-11 功能码 05 响应报文示例

字 段	从站地址	功能码	线圈地址 (高位)	线圈地址 (低位)	线圈状态 (高位)	线圈状态 (低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x11	0x05	0x00	0xAD	0xFF	0x00	CRC (2 字节)	8

5.7 06(0x06)写单个保持寄存器

06 功能码用于写从站设备的单个保持寄存器的值,有关该功能码的请求报文和响应报文的构成细节将在下述展开。

1. 功能说明

设置从站中单个保持寄存器的值。此功能码支持广播模式,在广播模式下,所有从站设备的同一地址的值将被统一修改,但均不对主站发起响应。

2. 请求报文

请求报文的信息要指定需写入的保持寄存器的地址和数据,其中,地址和数据各占用两字节。

在请求报文的信息里,访问的从站地址是 17,将寄存器地址为 2 的值设置为 3,见表 5-12。

表 5-12 功能码 06 请求报文示例

字 段	从站地址	功能码	寄存器地址 (高位)	寄存器地址 (低位)	设定数据 (高位)	设定数据 (低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x11	0x06	0x00	0x02	0x00	0x03	CRC (2 字节)	8

3. 响应报文

当从站正确地执行了主站的请求后,从站将返回与请求报文一致的响应报文,如表 5-13 所示,如果从站执行失败,则返回异常响应。

表 5-13 功能码 06 响应报文示例

字 段	从站地址	功能码	寄存器地址 (高位)	寄存器地址 (低位)	设定数据 (高位)	设定数据 (低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x11	0x06	0x00	0x02	0x00	0x03	CRC (2 字节)	8

5.8 15(0x0F)写多个线圈/离散输出状态

15 功能码用于写从站设备的连续多个线圈的状态值,可写状态为开或关,有关该功能码的请求报文和响应报文的构成细节将在下述展开。

1. 功能说明

将从站中连续的多个线圈/离散输出(DO)设置为开状态或关状态。此功能码支持广播模式,在广播模式下,所有从站设备的同一地址的值将被统一修改,但均不对主站发起响应。

2. 请求报文

请求报文的信息要指定需写入的线圈或离散输出的起始地址、数量、字节数和设定数据,其中,起始地址和数量各占用两字节,字节数占用一字节,设定数据所占用的字节长度依据线圈数量决定,将数据中逻辑 1 的位设定为线圈的开状态,将数据中逻辑 0 的位设定为线圈的关状态。每个线圈的开或关状态与设定数据字段的对应关系可参考 5.2 节“01(0x01)读取线圈/离散输出状态”中的内容。

在请求报文的信息里,访问的从站地址是 17,将线圈的地址范围设置为 10~19,共计 10 个值,因此设定的数据需要占用两字节,在请求报文中将数据 1 字段设定为对应于 17~10 的线圈值,其中,LSB 对应于线圈 10;将数据 2 字段设定为对应于 19~18 的线圈值,其中,LSB 对应于线圈 18,其余未使用的位用 0 填充,见表 5-14。将数据分别设定为 0xCD 和 0x01,设定数据与线圈的关系,见表 5-15。

表 5-14 线圈状态

线圈地址	17	16	15	14	13	12	11	10	-	-	-	-	-	-	19	18
二进制值	1	1	0	0	1	1	0	1	0	0	0	0	0	0	0	1

表 5-15 功能码 0F 请求报文示例

字段	从站地址	功能码	起始地址 (高位)	起始地址 (低位)	线圈数量 (高位)	线圈数量 (低位)	字节数	设定数 据 1	设定数 据 2	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x11	0x0F	0x00	0x0A	0x00	0x0A	0x02	0xCD	0x01	CRC (2 字节)	11

3. 响应报文

当从站正确地执行了主站的请求后,从站将返回这组线圈的起始地址及数量,见表 5-16。

表 5-16 功能码 0F 响应报文示例

字 段	从站地址	功能码	线圈起始地 址(高位)	线圈起始地 址(低位)	线圈数量 (高位)	线圈数量 (低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x11	0x0F	0x00	0x0A	0x00	0x0A	CRC (2 字节)	8

5.9 16(0x10)写多个保持寄存器

16 功能码用于写从站设备的连续多个保持寄存器的值,有关该功能码的请求报文和响应报文的构成细节将在下述展开。

1. 功能说明

设置从站中连续的多个保持寄存器的值。此功能码支持广播模式,在广播模式下,所有

从站设备的同一地址的值将被统一修改,但均不对主站发起响应。

2. 请求报文

请求报文的信息要指定需写入的保持寄存器的地址、数量、字节数和设定数据,其中,地址和数据各占用两字节,字节数占用一字节,设定数据所占用的字节长度依据寄存器的数量决定,各设定数据按每个寄存器两字节存放。

将从站保持寄存器地址为 1~2 的值设置为 0x000A 和 0x0152,见表 5-17。

表 5-17 保持寄存器的设置

保持寄存器地址	设定值
1	0x000A
2	0x0152

在请求报文的信息里,访问的从站地址是 17,将地址 1 的保持寄存器的值设置为 0x000A,将地址 2 的保持寄存器的值设置为 0x0152,共计两个寄存器,因此字节数为 4,见表 5-18。

表 5-18 功能码 10 请求报文示例

字段	从站地址	功能码	起始地址 (高位)	起始地址 (低位)	寄存器数量 (高位)	寄存器数量 (低位)	字节数	设定数据 1 (高位)	设定数据 1 (低位)	设定数据 2 (高位)	设定数据 2 (低位)	CRC-16 校验	合计字节数
RTU 模式 8 位(Hex)	0x11	0x10	0x00	0x01	0x00	0x02	0x04	0x00	0x0A	0x01	0x52	CRC (2 字节)	13

3. 响应报文

当从站正确地执行了主站的请求后,从站将返回这组保持寄存器的起始地址及数量,见表 5-19。

表 5-19 功能码 10 响应报文示例

字 段	从站地址	功能码	寄存器起始 地址(高位)	寄存器起始 地址(低位)	寄存器数量 (高位)	寄存器数量 (低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x11	0x10	0x00	0x01	0x00	0x02	CRC (2 字节)	8

关于多个寄存器的读或写操作在实际开发中多用于操作多字节类型的数据,例如,如果需要对保持寄存器写入一个 32 位的数据,则该数据将占用两个保持寄存器;如果需要对保持寄存器写入一个 64 位的数据,则该数据将占用 4 个保持寄存器。

假如设定数据是 32 位的无符号整型数,占用的保持寄存器的地址为 1 和 2,设定值是 0x11223344,字节序为 ABCD(参考 4.2.4 节“大小端模式和字节序”),从站地址是 1,那么实际上的请求报文和响应报文如下。

请求报文(Hex): 01 10 00 01 00 02 04 11 22 33 44 83 96

响应报文(Hex): 01 10 00 01 00 02 10 08

注意：主站设备和从站设备对数据的字节序规则处理必须保持一致，否则可能存在数据处理错误。

5.10 Modbus 异常响应



22min

当从站未能正确地执行主站的请求时，从站会返回一个异常响应报文，以此通知主站本次通信异常。

5.10.1 触发机制

以上章节介绍了常用的功能码的报文构成，除广播模式的请求报文外，主站都希望获得一个正常的响应报文，但在某些特殊的情况下，从站会返回一个异常的响应报文。

对于请求报文，存在以下 4 种处理反馈：

- (1) 被访问的从站正常接收并正常处理，随后返回正常的响应报文。
- (2) 因为通信错误等原因，造成被访问的从站没有收到主站的请求报文，主站将按超时处理。
- (3) 被访问的从站设备接收的请求报文存在通信错误（例如 CRC 错误），此时从站将丢弃报文不响应，主站将按超时处理。
- (4) 被访问的从站接收到正确的请求报文，但由于超过其处理范围（例如不存在的功能码或不存在的寄存器地址等），此时从站将返回包含异常码(Exception Code)的响应报文。

5.10.2 响应报文构成

异常响应报文包含异常功能码和异常码。

异常功能码其实就是功能码的最高位(MSB)被置 1，并以此来提示主站本次通信异常，因此异常功能码=0x80+正常功能码。

当前主站访问的从站设备地址码为 2，主站需要读取一个地址为 9 的输入寄存器的值，见表 5-20，但从站设备不存在地址为 2 的输入寄存器，因此在从站收到主站的请求报文后，从站会返回一个异常响应报文，见表 5-21。

表 5-20 读取输入寄存器的请求报文

字 段	从站地址	功能码	起始地址 (高位)	起始地址 (低位)	寄存器数量 (高位)	寄存器数量 (低位)	CRC-16 校验	合计字 节数
RTU 模式 8 位(Hex)	0x02	0x04	0x00	0x09	0x00	0x01	CRC (2 字节)	8

表 5-21 异常响应报文

字 段	从站地址	异常功能码	异常码	CRC-16 校验	合计字节数
RTU 模式 8 位(Hex)	0x02	0x84	0x02	CRC(2 字节)	5

常见的异常码见表 5-22。

表 5-22 常见异常码及说明

异常码(Hex)	名 称	说 明
01	非法功能码	从站设备不支持此功能码
02	非法数据地址	指定的数据地址在从站设备中不存在
03	非法数据值	指定的数据超过范围或者不允许使用
04	从站设备故障	从站设备在处理响应的过程中出现未知错误等