Modbus 协议主要构成是地址码/标识码，功能码，寄存器地址，数据报文等内容。由于 modbus 协议是请求/应答通信协议，其其中功能码主要用于表述该数据报文执行的功能，当服务器对客户机进行响应时，它使用功能码域来指示正常响应（无差错）或者异常响应（即出现某种差错），其中的 modbus 协议的功能码众多，在此我们一一列出与大家分享。

功能码表

	数据类型	功能描述	功能码	功能码（十六进制）	异常功能码
比特访问	物理离散量输入	读输入离散量	02	0x02	0x82
	内部比特或者物理线圈	读线圈	01	0x01	0x81
		写单个线圈	05	0x05	0x85
		写多个线圈	15	0x0F	0x8F
16比特访问	输入存储器	读输入寄存器	04	0x04	0x84
	内部存储器或物理输出存储器（保持寄存器）	读多个寄存器	03	0x03	0x83
		写单个寄存器	06	0x06	0x86
		写多个寄存器	16	0x10	0x90
		读/写多个寄存器	23	0x17	0x97
		屏蔽写寄存器	22	0x16	0x96
文件记录访问		读文件记录	20	0x14	
		写文件记录	21	0x15	

其中物理离散量输入和输入寄存器只能有 I/O 系统提供的数据类型，即只能是由 I/O 系统改变离散量输入和输入寄存器的数值，而上位机程序不能改变的数据类型，在数据读写上表现为只读，而内部比特或者物理线圈和内部寄存器或物理输出寄存器（保持寄存器）则是上位机应用程序可以改变的数据类型，在数据读写上表现为可读可写。

错误代码表

代码	名称	含义
01	非法功能	对于服务器（或从站）来说，询问中接收到的功能码是不可允许的操作，可能是因为功能码仅适用于新设备而被选单元中不可实现同时，还指出服务器（或从站）在错误状态中处理这种请求，例如：它是未配置的，且要求返回寄存器值。
02	非法数据地址	对于服务器（或从站）来说，询问中接收的数据地址是不可允许的地址，特别是参考号和传输长度的

		组合是无效的。对于带有 100 个寄存器的控制器来说，偏移量 96 和长度 4 的请求会成功，而偏移量 96 和长度 5 的请求将产生异常码 02。
03	非法数据值	对于服务器（或从站）来说，询问中包括的值是不可允许的值。该值指示了组合请求剩余结构中的故障。例如：隐含长度是不正确的。modbus 协议不知道任何特殊寄存器的任何特殊值的重要意义，寄存器中被提交存储的数据项有一个应用程序期望之外的值。
04	从站设备故障	当服务器（或从站）正在设法执行请求的操作时，产生不可重新获得的差错。
05	确认	与编程命令一起使用，服务器（或从站）已经接受请求，并且正在处理这个请求，但是需要长持续时间进行这些操作，返回这个响应防止在客户机（或主站）中发生超时错误，客户机（或主机）可以继续发送轮询程序完成报文来确认是否完成处理。
07	从属设备忙	与编程命令一起使用，服务器（或从站）正在处理长持续时间的程序命令，当服务器（或从站）空闲时，客户机（或主站）应该稍后重新传输报文。
08	存储奇偶性差错	与功能码 20 和 21 以及参考类型 6 一起使用，指示扩展文件区不能通过一致性校验。服务器（或从站）设备读取记录文件，但在存储器中发现一个奇偶校验错误。客户机（或主机）可重新发送请求，但可以在服务器（或从站）设备上要求服务。
0A	不可用网关路径	与网关一起使用，指示网关不能为处理请求分配输入端口值输出端口的内部通信路径，通常意味着网关是错误配置的或过载的。
0B	网关目标设备响应失败	与网关一起使用，指示没有从目标设备中获得响应，通常意味着设备未在网络中。

我们以 Modbus RTU 协议为例，地址码为 0x01，写操作 0x10,寄存器地址为 0x018E,CRC 校验。如寄存器可读写的话，返回正常，如寄存器只读，返回异常。

下发指令：01 10 01 8E 00 01 02 00 00 69 BE（向寄存器 0x018E 写入一个数值为 0 的数据）

正确回应指令：01 10 01 8E 00 01 60 1E(向寄存器地址 0x018E 写操作一个寄存器）

错误回应指令：01 90 01 8D C0（写操作非法功能，可能是向输入寄存器写数据）