欧姆龙 CP 系列 PLC 以太网 modbusTCP 通讯

BCNet-CP 模块内部集成 ModbusTCP 通讯服务器，因此 ModbusTCP 客户机，如支持 ModbusTCP 的组态软件、OPC 服务器、PLC 以及实现 ModbusTCP 客户机的高级语言开发的软件等，可以直接访问欧姆龙 CP 系列 PLC 的内部数据区，Modbus 协议地址在 BCNet 内部已经被默认映射到 CP 系列 PLC 的地址区，实现的功能号包括：FC1、FC2、FC3、FC5、FC6、FC15 和 FC16。

ModbusTCP 协议帧格式：

事务处理标识符	事务处理标识符	协议标识符	协议标识符	长度字段（高字节）	长度字段（低字节）	从站地址	功能号	数据地址（高字节）	数据地址（低字节）	指令数（高字节）	指令数（低字节）
0x0	0x0	0x0	0x0	0x0	后面的字节数						

1、地址映射表

说明：

Modbus 从站地址	CP 系列 PLC 内部软元件	数据类型	计算公式	功能号	最大指令数
000001～	CIO 区：CIO0.0～	位	CIOm.n = 000001+m*16+n ①	FC1(读线圈) FC5(写单个线圈) FC15(写多个线圈)	FC1:512 FC5:1
025001～	工作区：WR0.0～		WRm.n = 025001+m*16+n ①		
033201～	保持区：HR0.0～		HRm.n = 033201+m*16+n ①		
041401～	辅助区：AR0.0～		ARm.n = 041401+m*16+n ①		
056901～	定时器完成标志：TCF0～		TCFm= 056901+m		
061001～	计数器完成标志：CCF0～		CCFm = 061001+m		
065101～	任务标志：TK0～		TKm = 065101+m		
400001～	CIO 区：CIO0～	字	CIOm = 400001+m	FC3(读寄存器) FC6(写单个寄存器) FC16(写多个寄存器)	FC3:125 FC16:125 FC6:1
406151～	工作区：WR0～		WRm = 406151+m		
406671～	保持区：HR0～		HRm = 406671+m		
407191～	辅助区：AR0～		ARm = 407191+m		
408191～	定时器：TIM0～		TIMm= 408191+m		
412291～	计数器：CNT0～		CNTm= 412291+m		
417001～	数据内存：DM0～		DMm = 417001+m		
450001～	外部内存：EM0～		EMm = 450001+m		

*①、该项为对应存储区的位操作，例如 CIO100.3，则 m=100，n=3，计算公式为：000001+100*16+3=001604。在 Modbus 的对应地址为 0 区的 01604 地址。*

2、用 ModScan32 测试

解压产品光盘\使用手册\通讯测试软件下的 modscan2_cr.rar。

1. 运行 ModScan32 软件。

2. 选择菜单 Connection/Connect，选择 Remote TCP/IP Server，输入 BCNet-CP 的 IP 地址，Service 端口为 502；点击[OK]按钮，如图 1 所示。

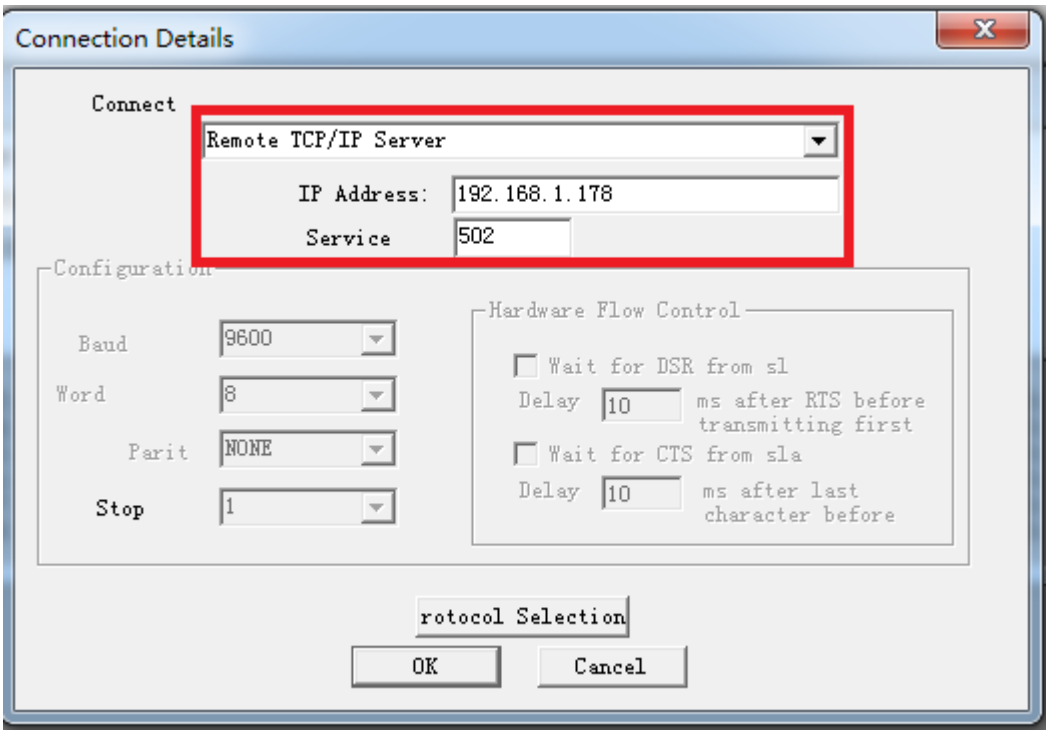

图 1

3. 在子窗口“ModSca1”中设置 Device ID 为 PLC 的站地址（如 1），功能号选择 03:HOLDING REGISTER，Address = 0001，Length = 100。

4. 子窗口数据区显示 400001～400100 的 16 进制数据，其对应于欧姆龙 CP 系列 PLC 的寄存器 CIO0 到 CIO100 的数值，如图 2 所示。

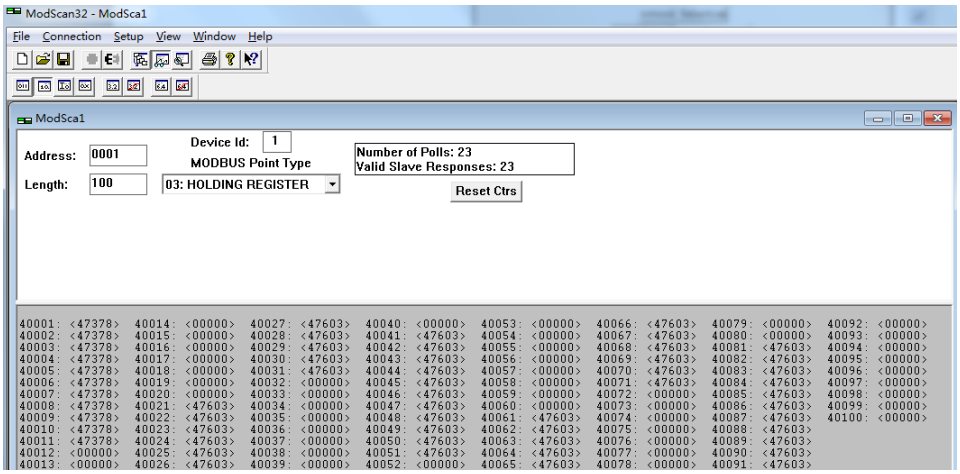

图 2

双击子窗口数据区的数据可以修改数值。