### S7-200 SMART Modbus TCP 客户端指令

STEP7-Micro/WIN SMART 从V2.4 版本开始，软件中直接集成 Modbus TCP 库指令，无需单独安装或者购买。安装软件后，Modbus TCP 指令位于 STEP7-Micro/WIN SMART 项目树中“指令”文件夹的“库”文件夹中。如图1.Modbus TCP库指令所示。

指令分为客户端和服务器两种，目前指令版本为 V1.0。客户端指令会占用开放式用户通信资源主动连接，最多8个；服务器指令会占用开放式用户通信资源的被动连接资源，最多也是8个。



图1.Modbus TCP库指令

#### 实验环境及通信任务

下面以两台S7-200 SMART 之间进行Modbus TCP 通信为例，详细阐述客户端与服务器侧如何编程及通信的过程。具体的实验环境见表1.；通信任务见表2：

表1.实验环境

|  |  |
| --- | --- |
| **操作系统** | **WIN7 SP1 专业版 64位** |
| **编程软件** | STEP7-Micro/WIN SMART V2.4版本 |
| **硬件** | SR60:6ES7288-1SR60-0AA0 固件：V2.4 版本ST20：6ES7288-1ST20-0AA0 固件：V2.4版本交换机：CSM 127 6GK7 277-1AA10-0AA0 |

表2.通信任务

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **硬件** | **通信角色** | **IP地址** | **端口号** | **读/写** | **数据区域** |
| **SR60** | 客户端 | 192.168.0.60 | 0 | 读 | VB20-VB31 |
| **ST20** | 服务器 | 192.168.0.20 | 502 | 响应 | VB0-VB11 |

#### 客户端侧指令编程

1、系统块中设置客户端的IP地址，以确保IP地址设置无误。此步骤为可选，如果确定IP地址设置无误，可忽略此步骤。设置方法如图2.所示。



图2.系统块设置IP地址

2、鼠标点击 MAIN 主程序的程序段1的编程区域，从库文件夹下找到 Modbus TCP 客户端指令 MBUS\_CLIENT，鼠标双击，指令出现在程序段1中，操作如图3.所示。



图3.添加客户端指令

3、填写客户端指令参数，如图4.所示。



图4.填写客户端参数

程序块具体参数详细解释介绍见表3.

|  |  |  |
| --- | --- | --- |
| **参数及类型** | **数据类型** | **说明** |
| **Req** | **IN** | BOOL | =1：表示向服务器发送Modbus 请求 |
| **Connect** | **IN** | BOOL | =1：尝试与分配的IP地址及端口号建立连接；=0：尝试断开已经建立的连接，忽略Req的任何请求 |
| **IPAddr1-4** | **IN** | BYTE | 填写 Modbus TCP 服务器的IP地址IPAddr1-4为高到低字节 |
| **IP\_Port** | **IN** | BYTE | 填写Modbus TCP 服务器的端口号 |
| **RW** | **IN** | BYTE | 指定操作模式 =0：读；=1写 |
| **Addr** | **IN** | DWORD | 要进行读写的参数的 Modbus 起始地址 |
| **Count** | **IN** | INT | 要进行读写的参数数据长度；数字量输入/输出Count=1表示1 bit，最大1920位对于模拟量输入和保持寄存器，最大 Count 值为 120 字。 |
| **DataPtr** | **IN\_OUT** | DWORD | 数据寄存器地址指针，指向本地用于读/写操作的数据地址区域的首地址 |
| **Done** | **OUT** | BOOL | TRUE：以下任一条件时为真：客户端已与服务器建立连接；客户端已与服务器断开连接；客户端已接收 Modbus 响应；发生错误FALSE：客户端正忙于建立连接或等待来自服务器的 Modbus 响应。 |
| **Error** | **OUT** | BOOL | 出现错误，仅一个周期有效 |

4、鼠标选中程序块文件夹，单击右键，下拉菜单中选择库存储器，如图5.所示。



图5.点击库存储器

5、在库存储区分配对话框中手动输入存储区的起始地址。此实例为VB5000开始，以使指令库可以正常工作。确保库存储区与程序中其他已使用的地址不冲突。使用建议地址无法确定是否有地址重叠，所以推荐手动输入正确的库存储区首地址。如图6.所示。



图6.库存储区地址分配

6、编译项目，下载程序。

#### 通信测试结果

将M0.0置位为1，然后在状态图表中创建变量，VW20-VW30 共6个字，监视值如图7.所示。



图7.读取服务器数据

#### 关于Modbus地址与CPU中数据区域地址对应关系说明

S7-200 SMART 做 Modbus TCP 通信，可以支持的功能码及功能描述及所占用的地址区，如表4.所示。客户端会主动的发送请求，服务器响应。在通信指令填写参数中没有直接填写功能码，而是通过多个参数填写共同确定功能码的。

表4.功能码概况说明

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **功能码（十进制）** | **功能描述** | **RW** | **Addr** | **Count** | **CPU地址** |
| **01** | 读数字量输出 位 | 0 | 00001-09999 | 1-1920 位 | Q0.0-1151.7 |
| **02** | 读数字量输入 位 | 0 | 10001-19999 | 1-1920 位 | I0.0-1151.7 |
| **03** | 读寄存器 字 | 0 | 40001-49999400001-465535 | 1-120 字 | V区 |
| **04** | 读模拟量输入 字 | 0 | 30001-39999 | 1-120 字 | AIW0-AIW110 |
| **05** | 写数字量输出 单个位 | 1 | 00001-09999 | 1位 | Q0.0-Q1151.7 |
| **06** | 写寄存器 单个字 | 1 | 40001-49999400001-465535 | 1个字 | V区 |
| **15** | 写数字量输出 多个位 | 1 | 00001-09999 | 1-1920 位 | Q0.0-1151.7 |
| **16** | 写寄存器 多个字 | 1 | 40001-49999400001-465535 | 1-120 字 | V区 |

举例：

和Modbus TCP服务器交换数据参数支持功能码：03，在客户端指令中设置两个参数确定03功能码：

RW=0：确定读取数据，（筛选出可能会使用的功能码:01,02,03,04），

Addr：40001-49999/400001-465535，表示交换数据为寄存器类型的数据。