SIEMENS

操作指南 • 12/2017

基于 S7-300/400 以太网模块 CP343-1 &CP443-1 Modbus TCP 在 STEP7 的使用入门（V6.0）

https://support.industry.siemens.com/cs/cn/zh/view/109754187

Unrestricted

目录

Copyright © Siemens AG Copyright year All rights reserved

1 Modbus TCP 通讯概述 3

1.1 通讯所使用的以太网参考模型 3

1.2 Modbus TCP 数据帧 3

1.3 Modbus TCP 使用的端口号 4

2 S7-300/400 以太网模块 Modbus TCP 通讯概述 5

2.1 软件和硬件 5

2.2 Modbus TCP CP V6.0 软件选项包 5

3 配置以太网模块作为 Modbus TCP Server 与通信伙伴建立通讯 7

3.1 组态硬件 7

3.2 添加 TCP 连接 9

3.3 例程说明 11

3.4 通信测试 16

4 配置以太网模块作为 Modbus TCP Client 与通信伙伴建立通讯 19

4.1 组态硬件 19

4.2 添加 TCP 连接 20

4.3 例程说明 23

4.4 通信测试 28

5 相关资料链接 31

Copyright © Siemens AG Copyright year All rights reserved

1 Modbus TCP 通讯概述

MODBUS TCP 是简单的、中立厂商的用于管理和控制自动化设备的 MODBUS 系列通讯协议的派生产品，显而易见，它覆盖了使用 TCP/IP 协议的“Intranet”和“Internet”环境中 MODBUS 报文的用途。协议的最通用用途是为诸如 PLC 以及连接其它简单域总线或 I/O 模块的网关服务的。

MODBUS TCP 使 MODBUS_RTU 协议运行于以太网，MODBUS TCP 使用 TCP/IP 和以太网在站点间传送 MODBUS 报文，MODBUS TCP 结合了以太网物理网络和网络标准 TCP/IP 以及以 MODBUS 作为应用协议标准的数据表示方法。MODBUS TCP 通信报文被封装于以太网 TCP/IP 数据包中。与传统的串口方式，MODBUS TCP 插入一个标准的 MODBUS 报文到 TCP 报文中，不再带有数据校验和地址。

1.1 通讯所使用的以太网参考模型

Modbus TCP 传输过程中使用了 TCP/IP 以太网参考模型的 5 层：

第一层：物理层，提供设备物理接口，与市售介质/网络适配器相兼容。

第二层：数据链路层，格式化信号到源/目硬件址数据帧。

第三层：网络层，实现带有 32 位 IP 地址报文包。

第四层：传输层，实现可靠性连接、传输、查错、重发、端口服务、传输调度。

第五层：应用层，Modbus 协议报文。

1.2 Modbus TCP 数据帧

Modbus 数据在 TCP/IP 以太网上传输，支持 Ethernet II 和 802.3 两种帧格式，Modbus TCP 数据帧包含报文头、功能代码和数据 3 部分，MBAP 报文头 (Modbus Application Protocol)分 4 个域，共 7 个字节。

Copyright © Siemens AG Copyright year All rights reserved

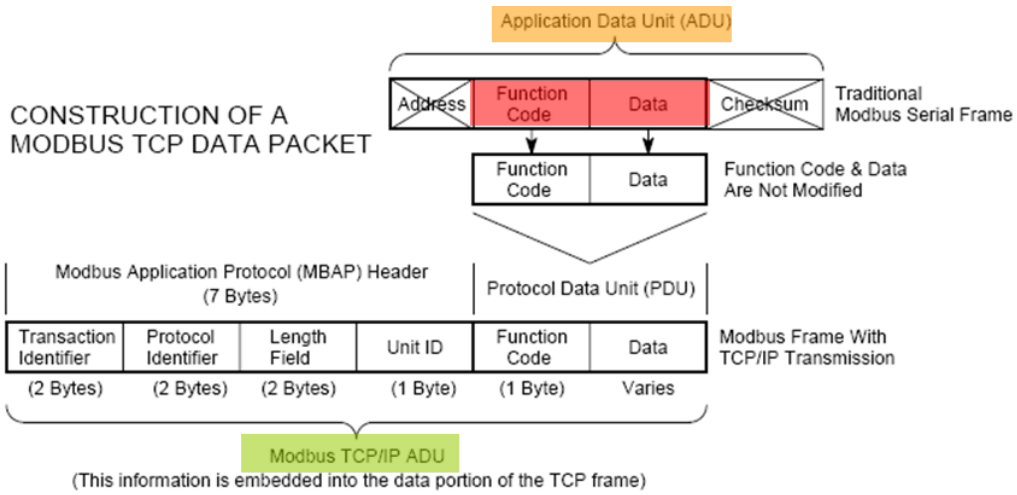


图 1-1 MBAP 报文头

域	长度	描述	客户机	服务器
Transaction ID	2字节	Modbus请求/响应事务处理的识别	客户机启动	服务器从接收的请求中重新复制
Protocol ID	2字节	0=Modbus协议	客户机启动	服务器从接收的请求中重新复制
Length	2字节	随后字节的数量	客户机启动（请求）	服务器（响应）启动
Unit ID	1字节	远程从站的识别ID	客户机启动	服务器从接收的请求中重新复制

图 1-2 MBAP 报文头说明

1.3 Modbus TCP 使用的端口号

（1） PLC 作为 Modbus 服务器时，按缺省协议使用 Port 502 通信端口，在 Modus 客户端程序中设置任意通信端口。

（2） PLC 作为 Modbus 客户端时，无须设置本机端口号；如要指定客户端端口号，为避免与其他通讯协议的冲突一般建议 2000 开始可以使用。

Copyright © Siemens AG Copyright year All rights reserved

2 S7-300/400 以太网模块 Modbus TCP 通讯概述

本文适用于 SIMATIC S7-300、S7-400 CPU 带以太网模块 CP343-1 或 CP443-1 的软件产品。相关指令允许在带有以太网模块 CP343-1 或 CP443-1 的 S7-300、S7-400 系统和支持 Modbus TCP 协议的设备之间进行通信。

根据客户端——服务器原理进行数据传输。传输过程中，可以将 SIMATIC S7 用作客户端，也可以用作服务器。

2.1 软件和硬件

在 STEP7 软件中使用 Modbus TCP 的指令，需要安装 MODBUS TCP CP 指令库，才可将 SIMATIC S7-300、S7-400 CPU 带以太网模块 CP343-1 或 CP443-1 与支持 Modbus TCP 的通信伙伴进行通信，如下图 2-1 所示：

Product	Identification number	As of version
SIMATIC Modbus/TCP CP	6AV6676-6MB00-6AX0	6.0
FB 905 "MODBUSCP"		5.0
FB 906 "MB_CPSRV"		3.0
FB 908 "MB_CPCLI"		3.0

图 2-1 指令版本

下面例子将分别介绍如何配置 315-2DP+CP343-1 为 Modbus TCP 的 Server，Client 与通信伙伴建立通信，测试例程中用到的软硬件如图 2-2 所示：

名称	数量	订货号
SIMATIC CPU315-2DP(FW V3.3)	1	6ES7 315-2AH14-0AB0
SIMATIC CP343-1(FW V3.0)	1	6GK7 343-1EX30-0XE0
SIMATIC STEP7 V5.6	1	6ES7 822-4CC11-0YA5
Modbus TCP CP software	1	6AV6 676-6MB00-6AX0
Modscan32 用于在 PC 中模拟 Modbus Client	1	网上免费下载
Modsim32 用于在 PC 中模拟 Modbus Server	1	网上免费下载

图 2-2 例程中用到的软硬件列表

2.2 Modbus TCP CP V6.0 软件选项包

当将软件包安装完集成到 Step7 时，可以在 Step7 安装文件的相应目录中找到块库、例程、英文手册，如下图所示，在实际的项目调试过程中由于例子程序的各项功能比较完善，因此可以直接使用例子程序，根据项目的实际情况修改相应

Copyright © Siemens AG Copyright year All rights reserved

的参数即可，可以节省大量的参数设置时间，以下主要描述了使用软件包“Modbus TCP CP V6.0” 配置 S7-300/400 站，通过以太网模块 CP343-1 或 CP443-1 进行 Modbus TCP 通讯的详细配置和编程步骤。

- "Modbus_TCP_CP" library in \Program Files\Siemens\Step 7\S7LIBS
- 2 sample projects in \Program Files\Siemens\Step 7\EXAMPLES
- The programming manual in \Program Files\Siemens\Step 7\S7MANUAL\S7Comm

图 2-3 块库、例程、英文手册的文件夹位置

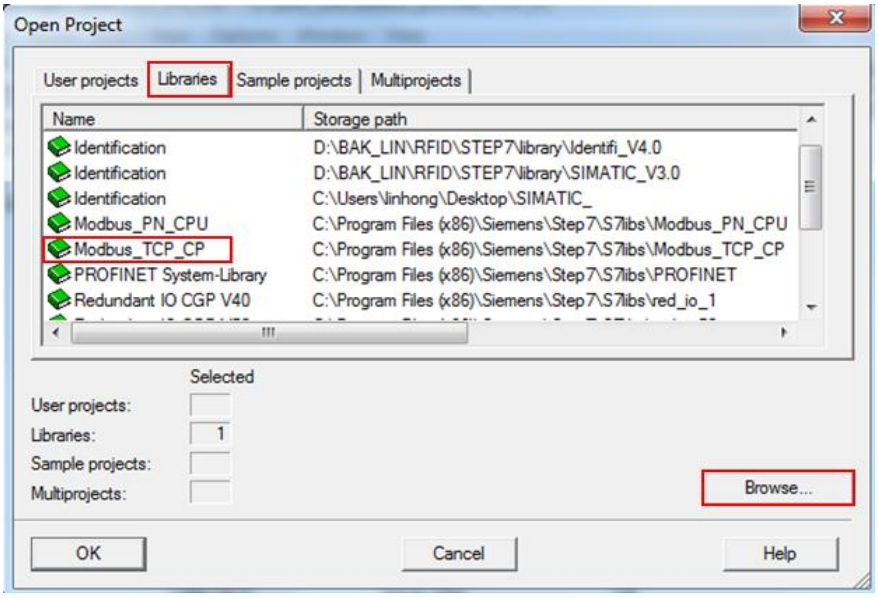


图 2-4 指令库(注：当找不到块库时，可以通过”Browse..”按钮来进行查找)

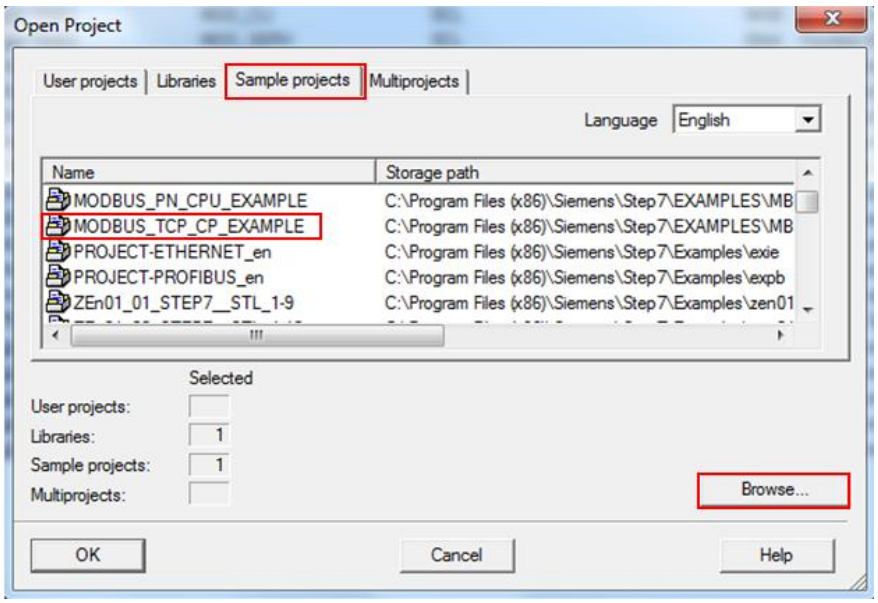


图 2-5 例程(注：当找不到例程时，可以通过”Browse..”按钮来进行查找)

Copyright © Siemens AG Copyright year All rights reserved

3 配置以太网模块作为 Modbus TCP Server 与通信伙伴建立通讯

下面以 S7-300 单站系统及 Modscan32 软件为例，详细介绍如何将 S7-300 单站系统通过以太网模块 CP343-1 配置为 Modbus TCP Server，与作为 Client 的 Modscan32 进行 Modbus TCP 通讯。

3.1 组态硬件

在 STEP7 中创建一个新项目（项目名称：MB_TCP_CP_V60），如图 3-1 所示：

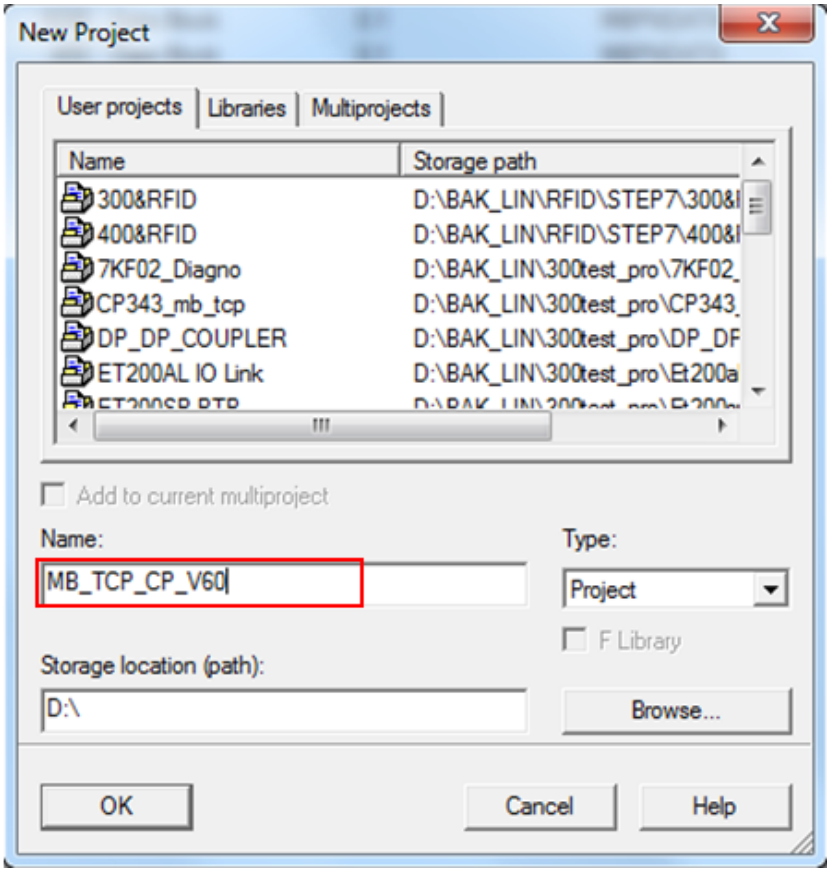


图 3-1 创建新项目

然后，插入一个新的“SIMATIC 300 Station”，如图 3-2 所示：

Copyright © Siemens AG Copyright year All rights reserved

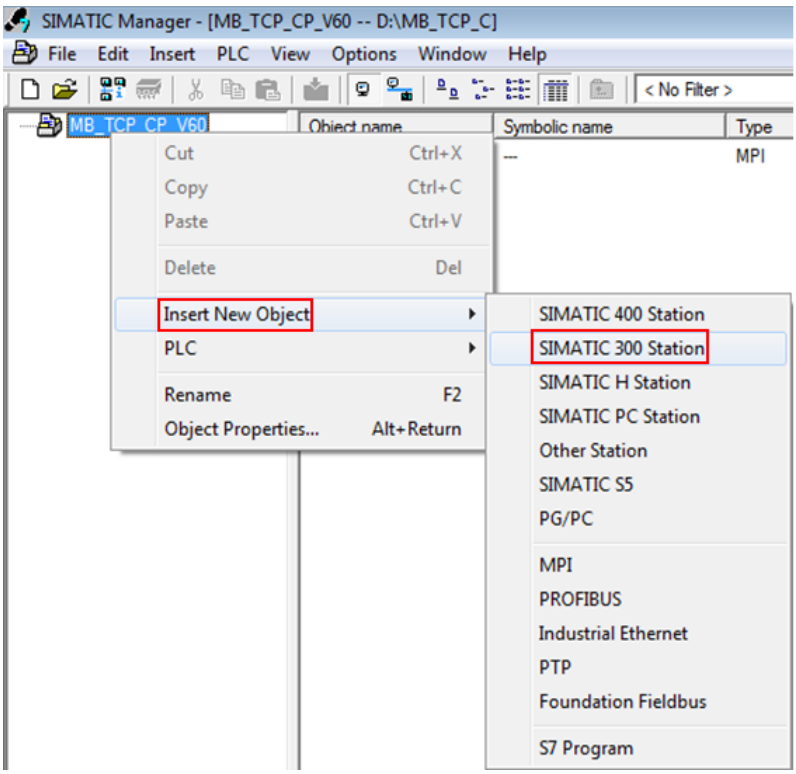


图 3-2 插入 PLC 站点

接着，打开硬件组态视图，插入 CPU 315-2DP 和 CP343-1，设置 IP 地址，如图 3-3 所示：

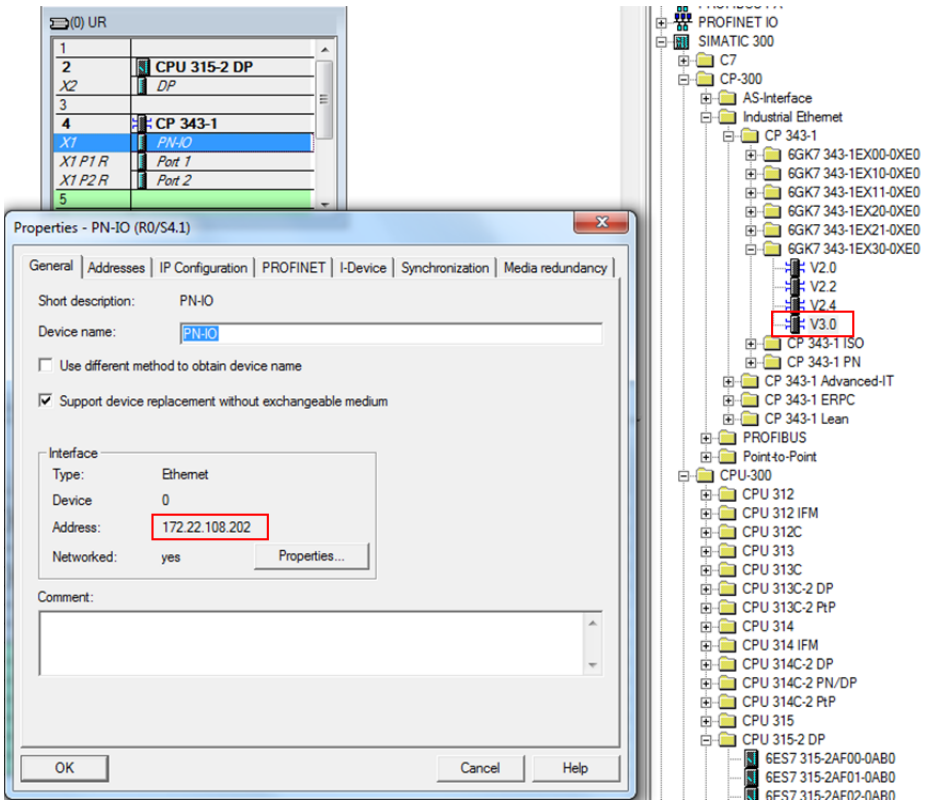


图 3-3 硬件组态

Copyright © Siemens AG Copyright year All rights reserved

3.2 添加 TCP 连接

在“硬件组态”界面，菜单“Options”下点击“Configure Network”进入网络配置界面，如图 3-4 所示：

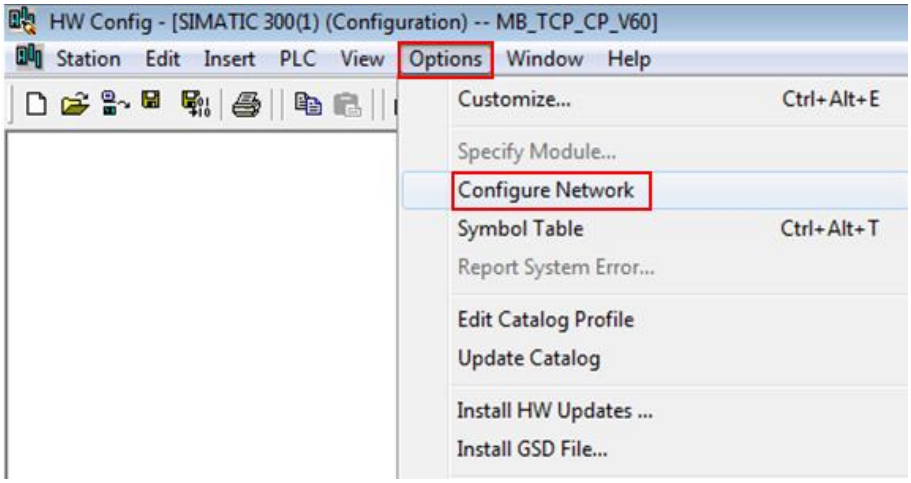


图 3-4 进入网络配置界面

接着，选择 CPU，在下方表格中，鼠标右键选择“Insert New Connection”添加 TCP 连接，如图 3-5 所示：

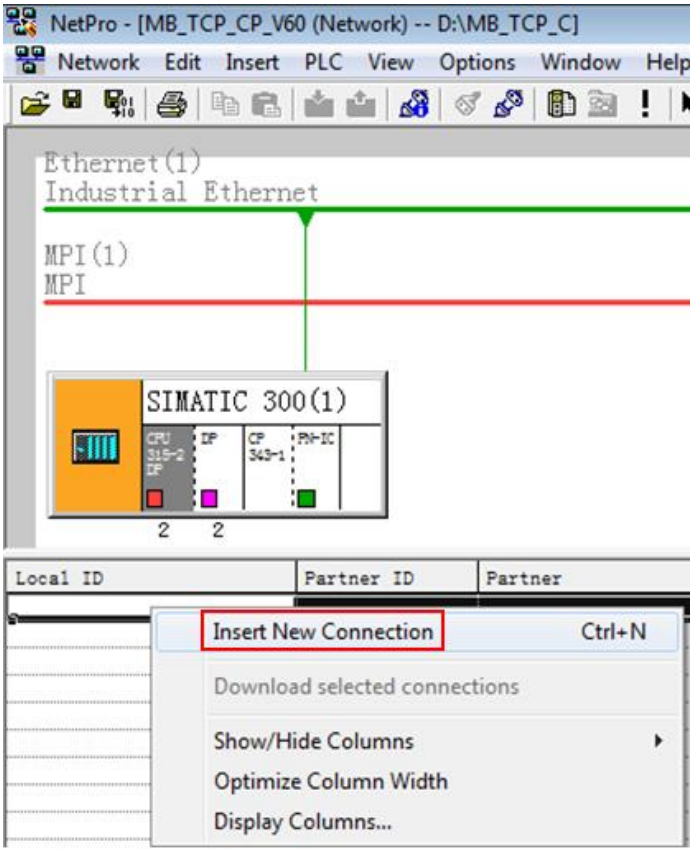


图 3-5 添加 TCP 连接

Copyright © Siemens AG Copyright year All rights reserved

选择通信伙伴为“Unspecified”，连接类型为“TCP connection”，如图 3-6 所示：

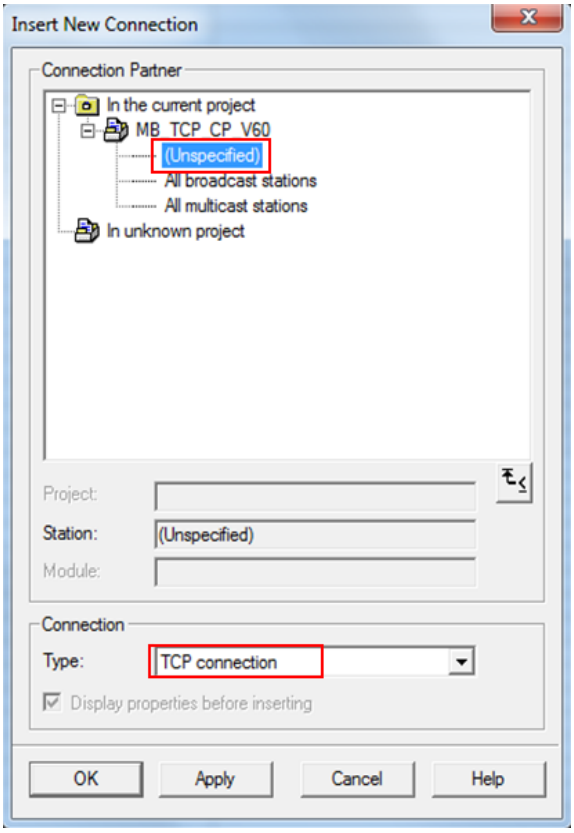


图 3-6 选择通信伙伴和连接类型

选择本地连接资源号（默认 ID=1），PLC 作为 server。注意，不要勾选“Active connection establishment”，如图 3-7 所示：

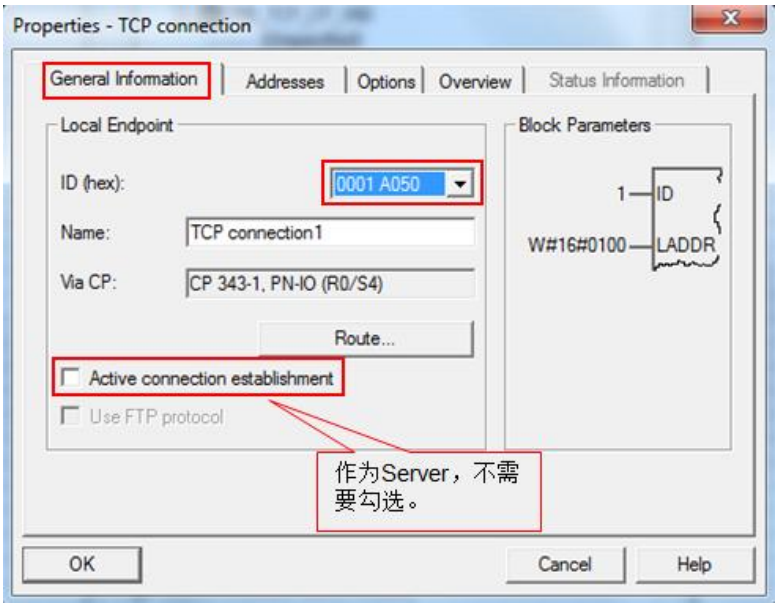


图 3-7 设置连接 ID 号和连接属性

Copyright © Siemens AG Copyright year All rights reserved

点击“Addresses”页面，设置本地端口号为 502，如图 3-8 所示：

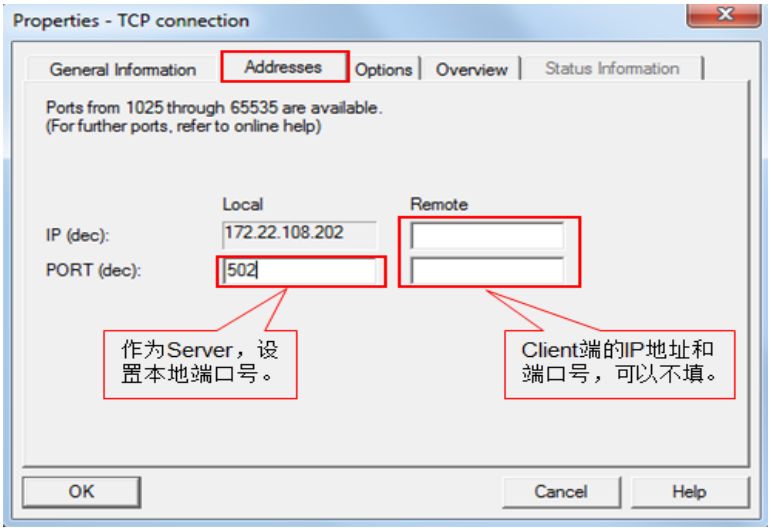


图 3-8 设置端口信息

3.3 例程说明

打开例程，从站点“SIMATIC 300（Server）”中拷贝所有程序块（注意，不要拷贝“System data”）到新建项目“MB_TCP_CP_V60”的站点“SIMATIC 300（1）”的 Blocks 中，如图 3-9 所示：

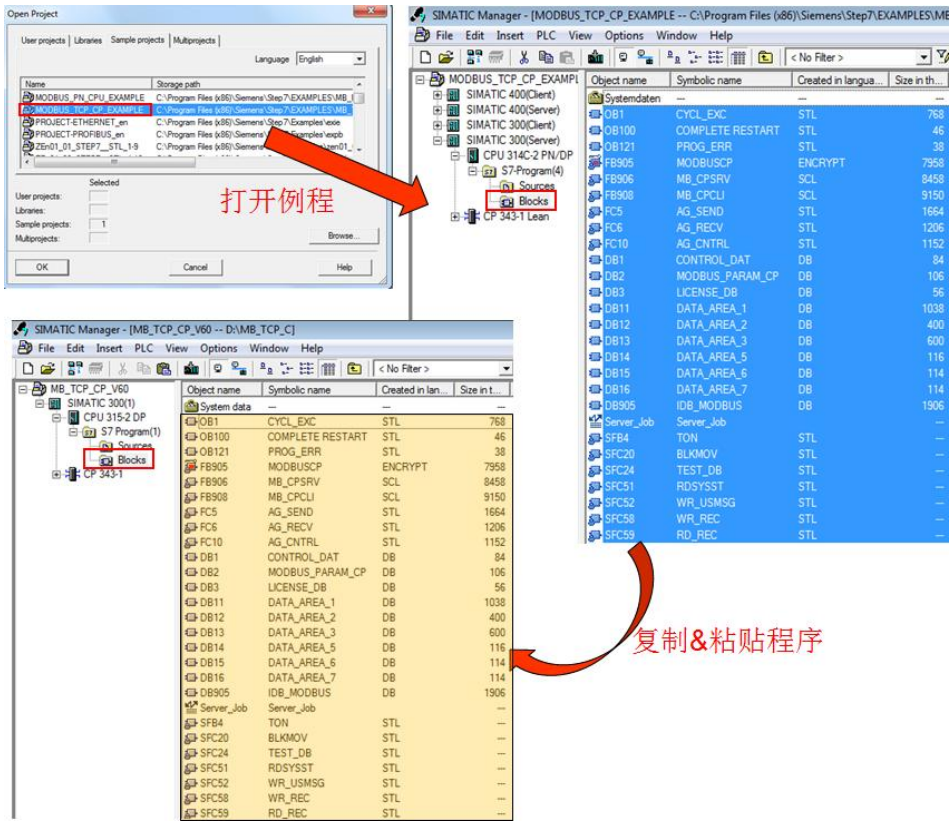


图 3-9 拷贝例程程序

Copyright © Siemens AG Copyright year All rights reserved

（1）打开 OB1，查看指令“MODBUSCP”

在项目的 OB1 组织块中调用了 Modbus TCP 指令，如图 3-10 所示：

```
OB1 :  "Main Program Sweep (Cycle)"
Comment:

Network 1: cyclic call of FB MODBUSCP - S7 is Server
      A     "CONTROL_DAT".Init                    DB1.DBX24.1
      =     #Init_save                            #Init_save

      A     #Init_save                            #Init_save
      R     "CONTROL_DAT".ENQ_ENR                 DB1.DBX4.0

      CALL  "MODBUSCP" , "IDB_MODBUS"             FB905 / DB905
       id           :="MODBUS_PARAM_CP".ID2_ID    DB2.DBW0
       db_param     :="MODBUS_PARAM_CP"           DB2
       REG_KEY_DB   :="LICENSE_DB"                DB3
       MONITOR      :="CONTROL_DAT".MONITOR       DB1.DBD0
       ENQ_ENR      :="CONTROL_DAT".ENQ_ENR       DB1.DBX4.0
       LICENSED     :="CONTROL_DAT".LICENSED      DB1.DBX4.1
       BUSY         :="CONTROL_DAT".BUSY          DB1.DBX4.2
       DONE_NDR     :="CONTROL_DAT".DONE_NDR      DB1.DBX4.3
       ERROR        :="CONTROL_DAT".ERROR         DB1.DBX4.4
       STATUS       :="CONTROL_DAT".STATUS        DB1.DBW6
       STATUS_FUNC  :="CONTROL_DAT".STATUS_FUNC   P#DB1.DBX8.0
       IDENT_CODE   :=
       Init_Error   :="CONTROL_DAT".Init_Error    DB1.DBX24.2
       Init_Status  :="CONTROL_DAT".Init_Status   DB1.DBW26
       UNIT         :="CONTROL_DAT".UNIT          DB1.DBB18
       DATA_TYPE    :="CONTROL_DAT".DATA_TYPE     DB1.DBB19
       START_ADDRESS:="CONTROL_DAT".START_ADDRESS DB1.DBW20
       LENGTH       :="CONTROL_DAT".LENGTH        DB1.DBW22
       WRITE_READ   :="CONTROL_DAT".WRITE_READ    DB1.DBX24.0
       Init         :="CONTROL_DAT".Init          DB1.DBX24.1
```

图 3-10 调用 Modbus TCP 指令

以下为部分管脚说明（其它管脚信息请查看指令库手册）：

id：为 “Configure Network”中的已组态连接的 ID。连接 ID 是 CPU 与连接伙伴之间通过 CP 实现的连接的唯一标识。在此处输入连接组态的数字。该参数的取值范围为 1 到 64。

db_param：参数数据块，包含 modbus 块实例的 modbus 数据参数。CPU 决定该参数的取值范围。DB 编号 0 为系统保留，不允许使用。以纯文本格式输入 DB 编号“DBxy”。如果要实施多个连接，则参数数据块可以按顺序包含所有连接所需的参数。

REG_KEY_DB：用于授权的注册密钥。

MONITOR：监视时间 MONITOR 用于监视来自连接伙伴的进入数据。采用时间格式 T# 指定监视时间，建议采用 1.5 s 左右的监视时间。

Copyright © Siemens AG Copyright year All rights reserved

在“S7 用作服务器”模式下，帧第二部分的输入通过 MONITOR 时间进行监视。如果超出监视时间，则会报错。该时间从接收到 MODBUS/TCP 特定的报文报头开始算起，并在完整地接收到请求后结束。

Init：在参数中有上升沿时，初始化 Modbus 块。只有当前没有作业正在运行时，才能执行初始化。必须通过 ENQ_ENR = FALSE 和 BUSY = FALSE 在程序中确保此条件。

（2）参数数据块 DB2

参数数据块 DB2（名称 MODBUS_PARAM_CP），该参数 DB 块用于 modbus 数据区域的设置。

注意，如需修改 DB 块中的数据，请将 DB 块切换到数据视图“Data view”，在“Actual value”列中进行修改。

本例中，根据图 3-7 的连接设置需将 DB2 的“ID2_ID”修改为“16#1”，为方便后续通信测试的地址对应，将 modbus 寄存器的起始和结束地址分别修改为“16#0”和“16#1F3”，如图 3-11 所示：

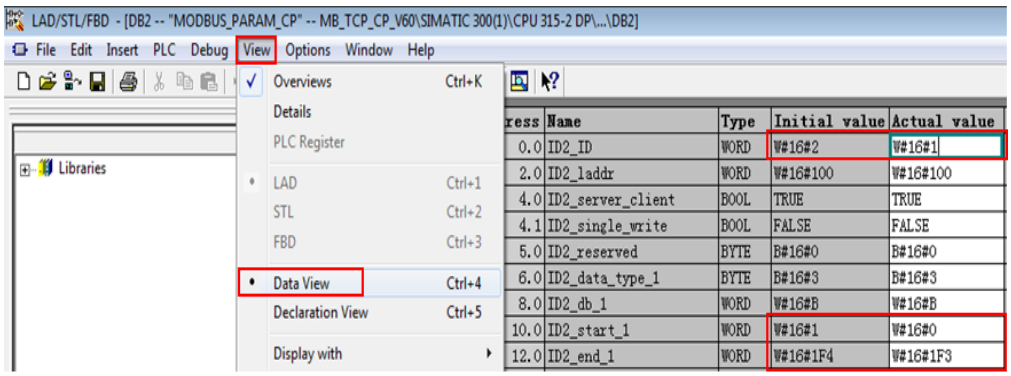


图 3-11 将 DB 块切换到数据视图并修改参数

以下为部分参数说明（其它参数信息请查看指令库手册）：

ID2_ID：为 “Configure Network”中的已组态连接的 ID。连接 ID 是 CPU 与连接伙伴之间通过 CP 实现的连接的唯一标识。在此处输入连接组态的数字。该参数的取值范围为 1 到 64。

ID2_laddr：为硬件组态中的 CP 基址（I 地址）。在此处输入组态的值。该参数的取值范围取决于 CPU。“ID”和“laddr”参数还可以从 TCP 连接的“属性 > 常规”(Properties > General Information) 中获取。如图 3-7 所示。

ID2_server_client：该参数用于区分客户端和服务器模式。如果输入为 TRUE，则使用“S7 用作服务器”模式。如果设置为 FALSE，则使用“S7 用作客户端”模式。

Copyright © Siemens AG Copyright year All rights reserved

ID2_single_write：在“客户端”操作模式模式才有效。

ID2_data_type_x：用于指定在该 DB 中映射的 Modbus/TCP 数据类型。如果在 ID2_data_type_x 中输入值 0，则不使用相应的数据区。

标识符	数据类型	数据宽度
16#0	未使用区域	
16#1	线圈	Bit
16#2	输入	Bit
16#3	保持寄存器	Word
16#4	输入寄存器	Word

Modbus 数据类型	DATA_TYPE	功能	长度	功能代码
线圈	1	读取	任意	1
线圈	1	写入	1	5
线圈	1	写入	1	15
线圈	1	写入	> 1	15
输入	2	读取	任意	2
保持寄存器	3	读取	任意	3
保持寄存器	3	写入	1	6
保持寄存器	3	写入	1	16
保持寄存器	3	写入	> 1	16
输入寄存器	4	读取	任意	4

图 3-12 不同的数据类型与所用 modbus 功能代码的关系

ID2_db_x：指定用于映射 Modbus/TCP 寄存器或下面所定义位值的数据块。使用全局 DB 时，DB 编号 0 为系统保留，因而不允许使用。

DB 编号 1 到 65535（W#16#0001 到 W#16#FFFF）

ID2_start_x / end_x：“ID2_start_x”用于指定 DB 的数据字 0 中映射的第一个 Modbus/TCP 地址。“ID2_end_x”参数用于定义最后一个 Modbus/TCP 地址。

对于寄存器访问，带有最后一个 Modbus 地址输入的 S7 DB 中的数据字编号如下计算：DBW 编号 = (end – start) * 2

对于位访问，带有最后一个 Modbus 地址输入的 S7 DB 中的数据字节编号如下计算：DBB 编号 = (end – start + 7) / 8

Copyright © Siemens AG Copyright year All rights reserved

定义的数据区不得重叠。“ID2_end_x”参数不能小于“ID2_start_x”。如果出错，则会中止 FB 的启动过程并提示错误。如果两个值相同，将分配一个 Modbus/TCP 地址（1 个寄存器或 1 个位值）。

例程中设置的 DB 块和 modbus 地址的对应关系，如图 3-13 所示：

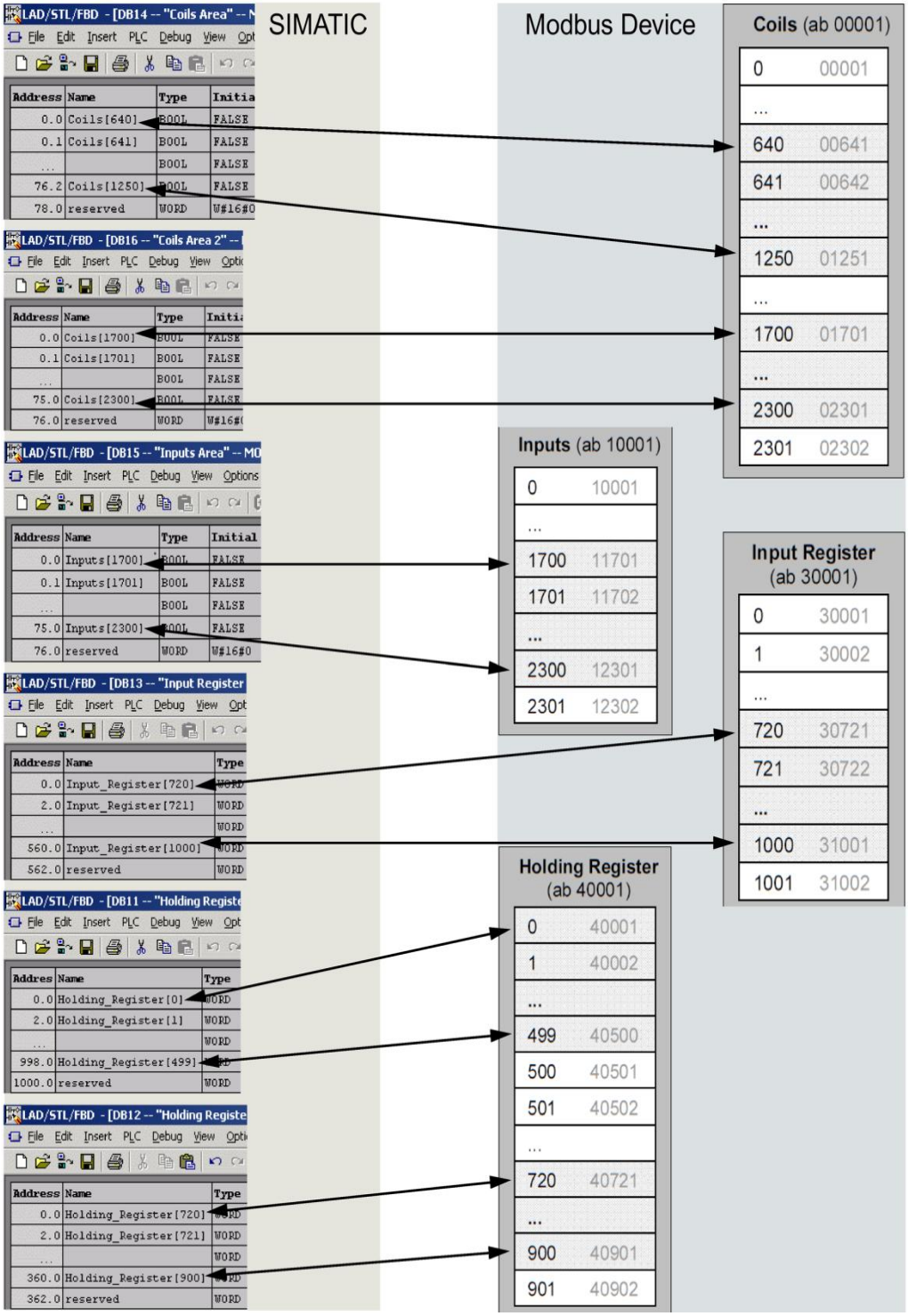


图 3-13 DB 块和 modbus 地址的对应关系

Copyright © Siemens AG Copyright year All rights reserved

（3）授权密钥数据块

DB3 为授权密钥数据块（名称 LICENSE_DB），用于填写通过西门子授权中心申请到的 17 个字符，如图 3-14 所示：

Address	Name	Type	Initial value	Actual value	Comment
0.0	REG_KEY	STRING [17]	'insert REG_KEY'	'insert REG_KEY'	Registration Key

图 3-14 授权密钥数据块

授权密钥的申请方法，请查看指令库手册“SIMATIC Modbus/TCP communication using CP 343-1 and CP 443-1 of the Manual”的第 5 章。

由于在获取授权密钥前，“MODBUSCP”指令是无授权状态，会使 CPU 报错而停机。而为了读取 CPU 的“IDENT_CODE”码，需要 CPU 运行起来，则必须添加编程错误组织块 OB121。

（4）启动组织块

启动组织块 OB100（名称 COMPLETE RESTART），该 OB 块在 CPU 启动时置位“MODBUSCP”指令的初始化位 Init，如图 3-15 所示：

```
OB100 :  "Complete Restart"
Comment:

Network 1: Initialization of "MODBUSCP"
    // for initialization
          SET
          S     "CONTROL_DAT".Init          DB1.DBX24.1
```

图 3-15 置位“MODBUSCP”指令的初始化位 Init

3.4 通信测试

将项目下载到 CPU 中，打开 Modsan32 应用程序，下面以保持寄存器为例介绍通信测试过程。

首先，在 ModScan32 的 Connection 菜单下选择 connect，并设置 ModScan32 访问作为 server 端的 PLC 的 IP 地址和端口号，如图 3-16 所示：

Copyright © Siemens AG Copyright year All rights reserved

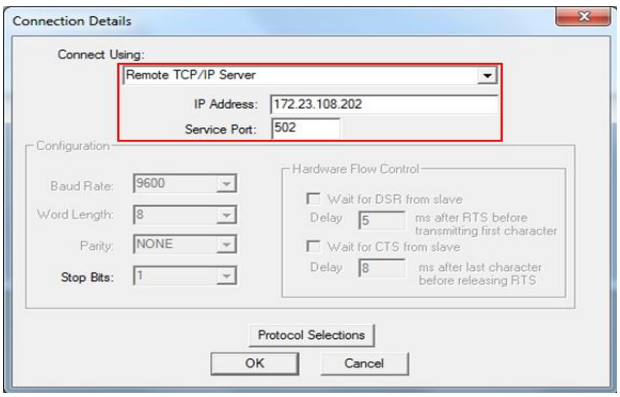


图 3-16 Connection 菜单下选择 connect

最后，在 Modscan32 软件中设置需要访问的 Modbus 起始地址及长度（本测试中，Modscan32 使用数据类型 3，访问保持寄存器起始地址为 40001 的 10 个字），建立与 PLC 的通信连接，并进行数据读取，如图 3-17 所示：

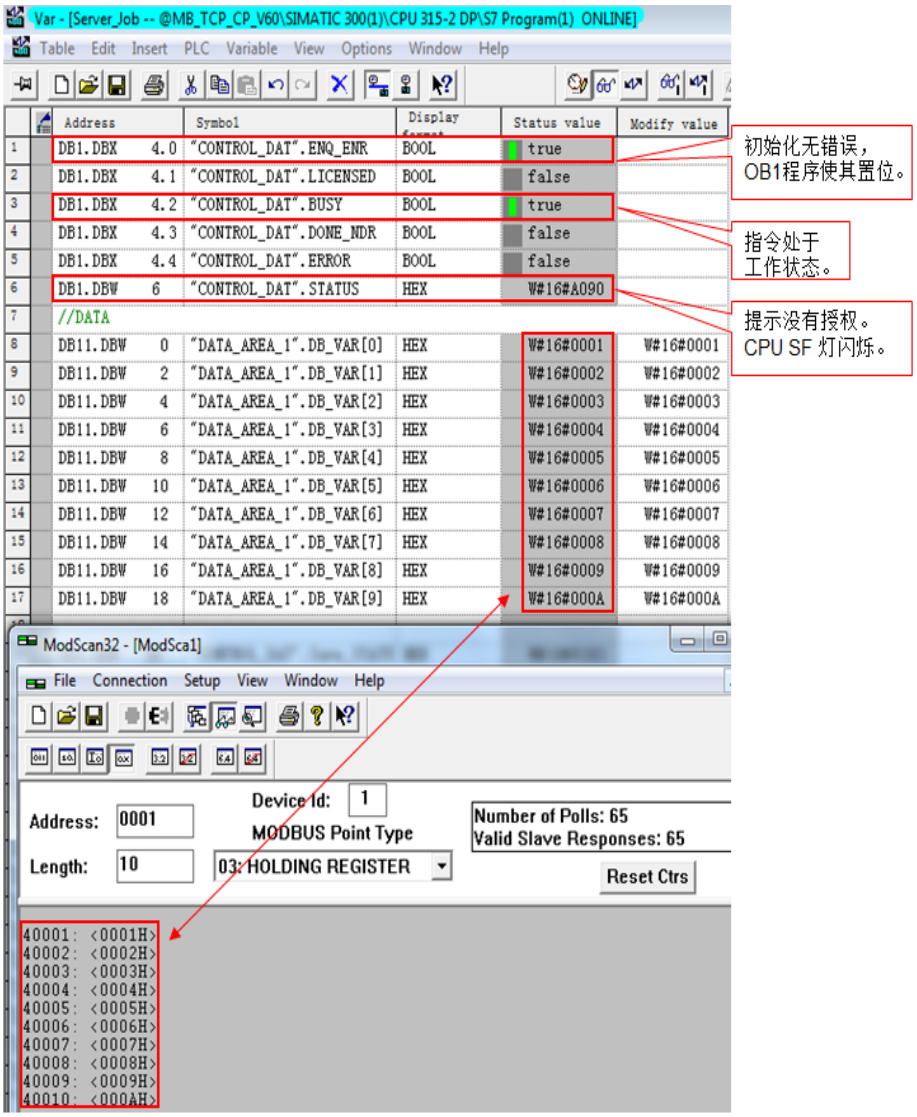


图 3-17 通信测试

Copyright © Siemens AG Copyright year All rights reserved

可以通过网络配置窗口，查看通信状态，如图 3-18 所示：

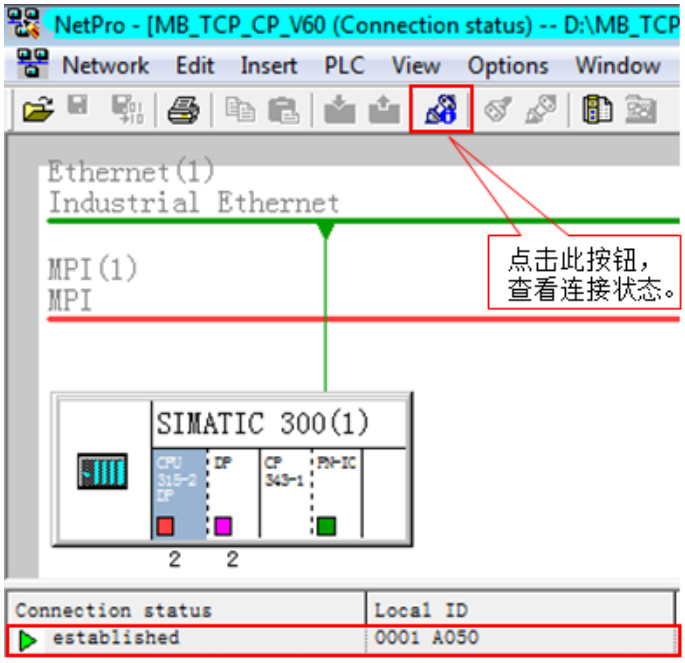


图 3-18 通信状态

使用功能块“MODBUSCP”的一些注意事项：

1）S7-300CPU 通过以太网模块 CP343-1 的功能块“MODBUSCP”支持与多个 Modbus 客户端的通信，支持的个数取决于 CP343-1 所支持的 TCP 连接数，必须为每一个客户端连接分别调用一次功能块“MODBUSCP”，其背景数据块、ID、端口号等参数必须唯一。

2）S7-300CPU 通过以太网模块 CP343-1 可以同时作为 Modbus TCP 的 Server 及 Client。

3）S7-300CPU 通过以太网模块 CP343-1 支持多协议，除了运行 Modbus TCP 协议外，同时可以运行 PROFINET、TCP/IP、S7 等协议。

Copyright © Siemens AG Copyright year All rights reserved

4 配置以太网模块作为 Modbus TCP Client 与通信伙伴建立通讯

下面以 S7-300 单站系统及 ModSim32 软件为例，详细介绍如何将 S7-300 单站系统通过以太网模块 CP343-1 配置为 Modbus TCP Client，与作为 Server 的 Modsim32 进行 Modbus TCP 通讯。

4.1 组态硬件

插入一个新的“SIMATIC 300 Station”，如图 4-1 所示：

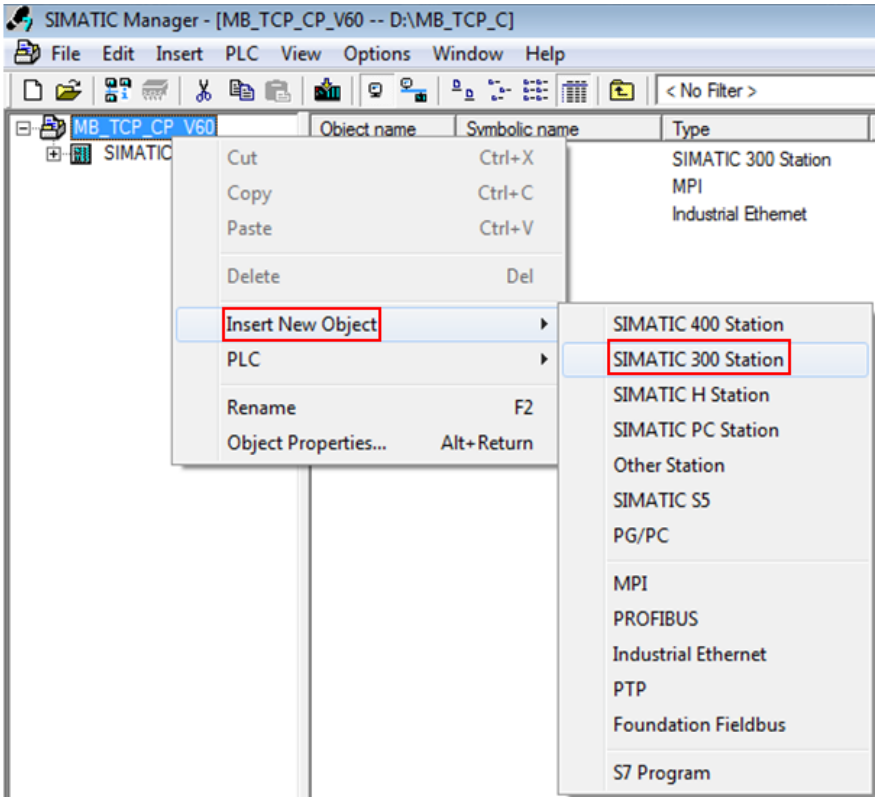


图 4-1 插入 PLC 站点

接着，打开硬件组态视图，插入 CPU 315-2DP 和 CP343-1，设置 IP 地址，如图 4-2 所示：

Copyright © Siemens AG Copyright year All rights reserved

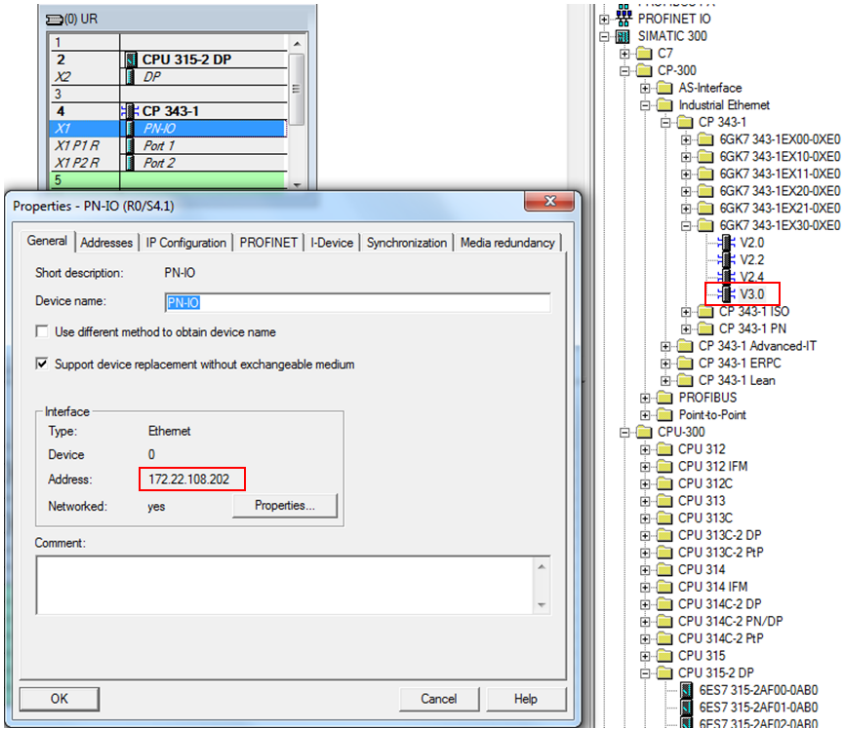


图 4-2 硬件组态

4.2 添加 TCP 连接

在“硬件组态”界面，菜单“Options”下点击“Configure Network”进入网络配置界面，如图 4-3 所示：

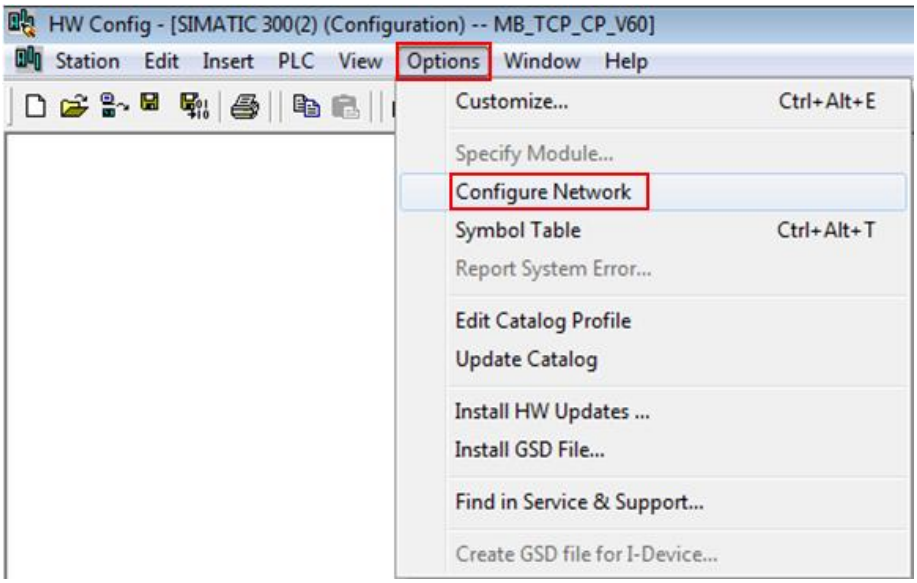


图 4-3 进入网络配置界面

接着，选择 CPU，在下方表格中，鼠标右键选择“Insert New Connection”添加 TCP 连接，如图 4-4 所示：

Copyright © Siemens AG Copyright year All rights reserved

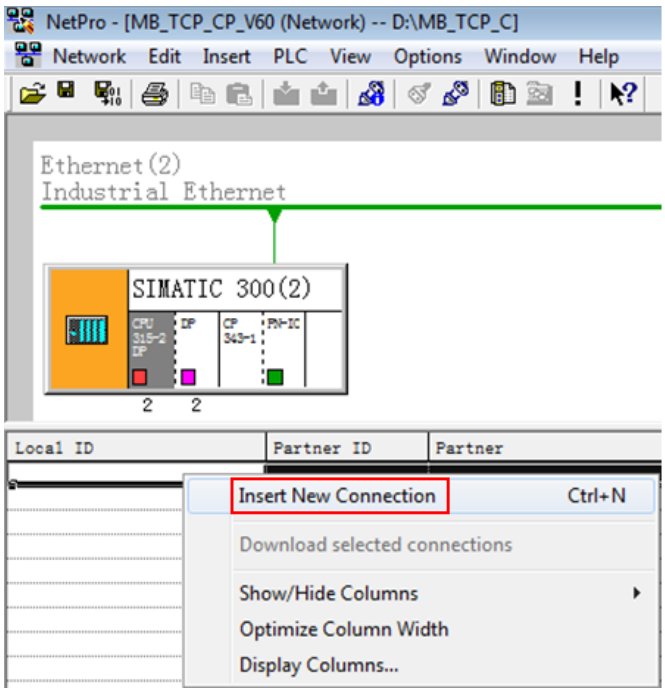


图 4-4 添加 TCP 连接

选择通信伙伴为“Unspecified”，连接类型为“TCP connection”，如图 4-5 所示：

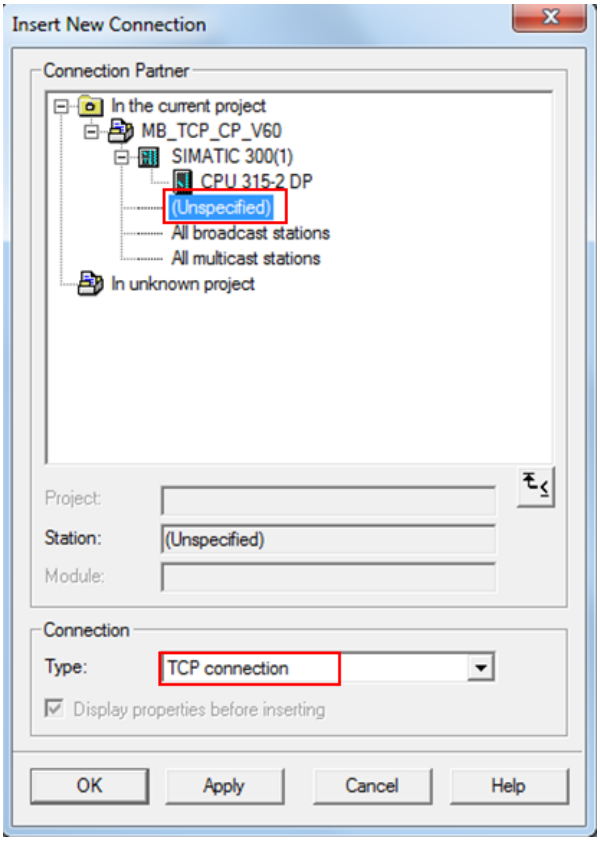


图 4-5 选择通信伙伴和连接类型

Copyright © Siemens AG Copyright year All rights reserved

选择本地连接资源号（默认 ID=1），PLC 作为 server。注意，不要勾选“Active connection establishment”，如图 4-6 所示：

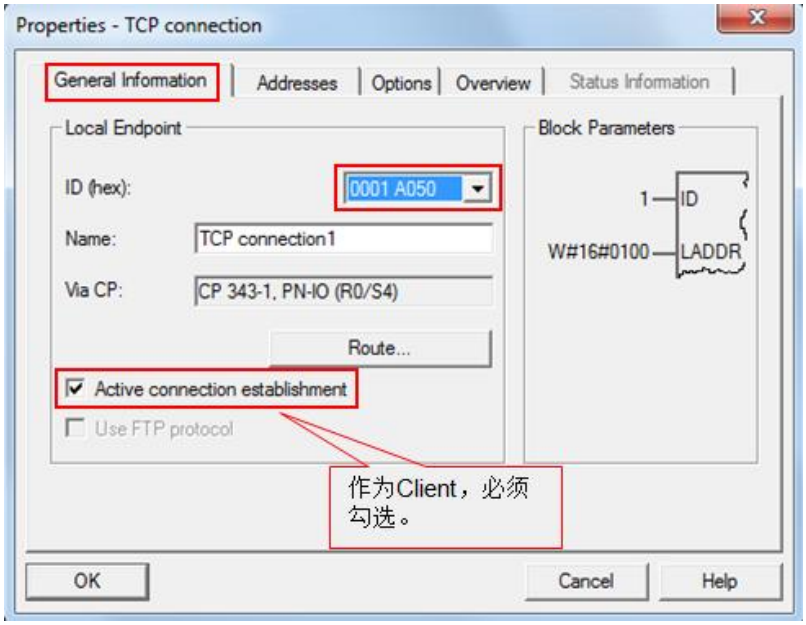


图 4-6 设置连接 ID 号和连接属性

点击“Addresses”页面，设置本地端口号为 502，如图 4-7 所示：

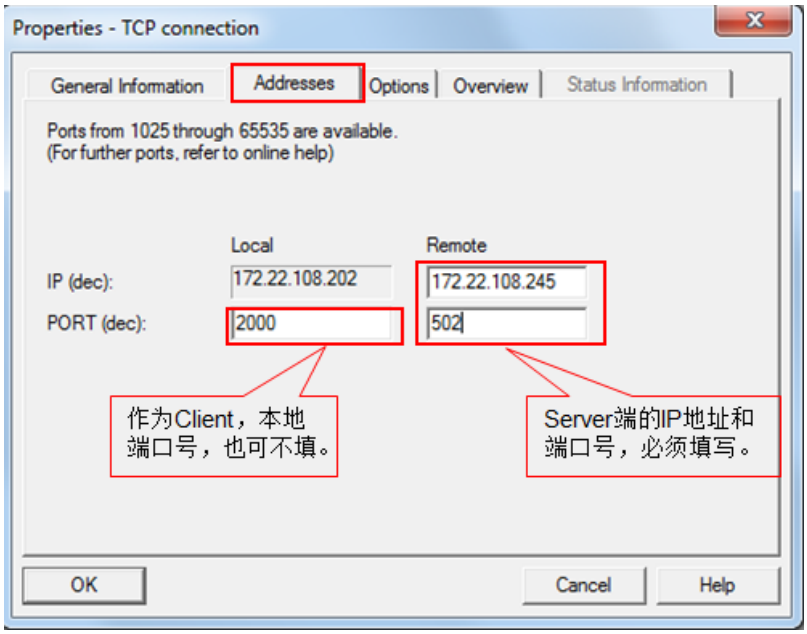


图 4-7 设置端口信息

Copyright © Siemens AG Copyright year All rights reserved

4.3 例程说明

打开例程，从站点“SIMATIC 300（Client）”中拷贝所有程序块（注意，不要拷贝“System data”）到新建项目“MB_TCP_CP_V60”的站点“SIMATIC 300（2）”的 Blocks 中，如图 4-8 所示：

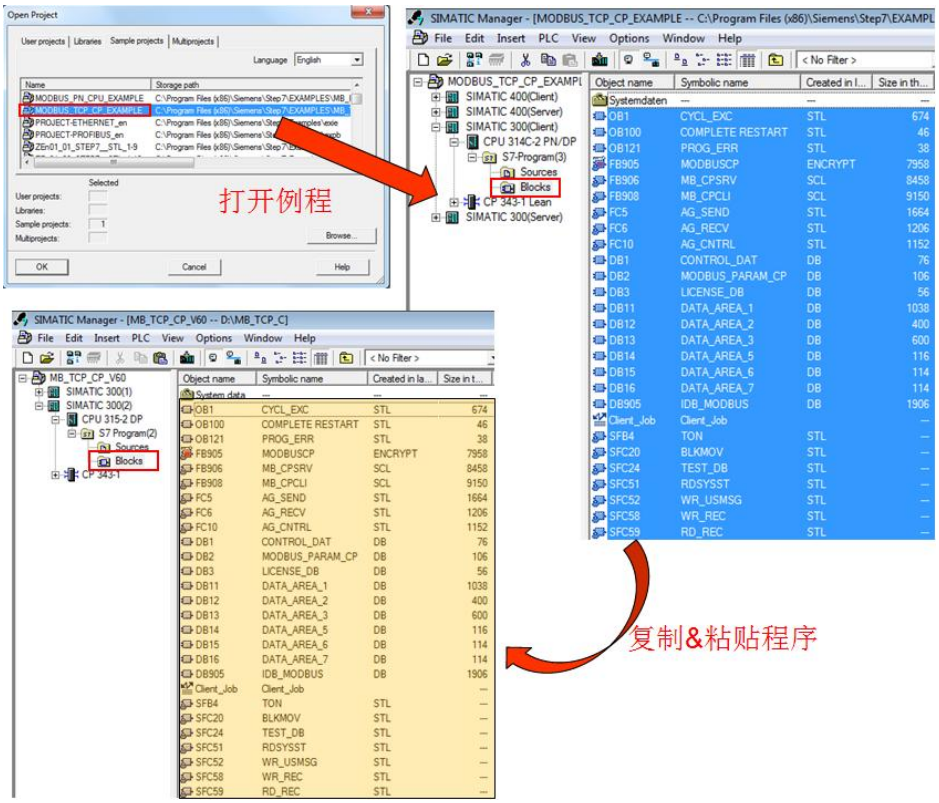


图 4-8 拷贝例程程序

（1）打开 OB1，查看指令“MODBUSCP”

在项目的 OB1 组织块中调用了 Modbus TCP 指令，如图 4-9 所示：

Copyright © Siemens AG Copyright year All rights reserved

```
OB1 :  "Main Program Sweep (Cycle)"
Comment:
Network 1: cyclic call of FB MODBUSCP - S7 is client

CALL  "MODBUSCP" , "IDB_MODBUS"                    FB905 / DB905
 id            :="MODBUS_PARAM_CP".ID1_ID          DB2.DBW0
 db_param      :="MODBUS_PARAM_CP"                 DB2
 REG_KEY_DB    :="LICENSE_DB"                      DB3
 MONITOR       :="CONTROL_DAT".MONITOR             DB1.DBD0
 ENQ_ENR       :="CONTROL_DAT".ENQ_ENR             DB1.DBX4.0
 LICENSED      :="CONTROL_DAT".LICENSED            DB1.DBX4.1
 BUSY          :="CONTROL_DAT".BUSY                DB1.DBX4.2
 DONE_NDR      :="CONTROL_DAT".DONE_NDR            DB1.DBX4.3
 ERROR         :="CONTROL_DAT".ERROR               DB1.DBX4.4
 STATUS        :="CONTROL_DAT".STATUS              DB1.DBW6
 STATUS_FUNC   :="CONTROL_DAT".STATUS_FUNC         P#DB1.DBX8.0
 IDENT_CODE    :=
 Init_Error    :="CONTROL_DAT".Init_Error          DB1.DBX24.2
 Init_Status   :="CONTROL_DAT".Init_Status         DB1.DBW26
 UNIT          :="CONTROL_DAT".UNIT                DB1.DBB18
 DATA_TYPE     :="CONTROL_DAT".DATA_TYPE           DB1.DBB19
 START_ADDRESS:="CONTROL_DAT".START_ADDRESS        DB1.DBW20
 LENGTH        :="CONTROL_DAT".LENGTH              DB1.DBW22
 WRITE_READ    :="CONTROL_DAT".WRITE_READ          DB1.DBX24.0
 Init          :="CONTROL_DAT".Init                DB1.DBX24.1
```

图 4-9 调用 Modbus TCP 指令

以下为部分管脚说明（其它管脚信息请查看指令库手册）：

id：为 “Configure Network”中的已组态连接的 ID。连接 ID 是 CPU 与连接伙伴之间通过 CP 实现的连接的唯一标识。在此处输入连接组态的数字。该参数的取值范围为 1 到 64。

db_param：参数数据块，包含 modbus 块实例的 modbus 数据参数。CPU 决定该参数的取值范围。DB 编号 0 为系统保留，不允许使用。以纯文本格式输入 DB 编号“DBxy”。如果要实施多个连接，则参数数据块可以按顺序包含所有连接所需的参数。

REG_KEY_DB：用于授权的注册密钥。

MONITOR：监视时间 MONITOR 用于监视来自连接伙伴的进入数据。采用时间格式 T# 指定监视时间，建议采用 1.5 s 左右的监视时间。

在“S7 用作客户端”模式下，MONITOR 时间用于监视服务器的完整响应的到达时间。如果超出监视时间，激活的作业将结束执行并提示错误。该时间从发送请求后开始算起，并在完整地接收到响应后结束。

Copyright © Siemens AG Copyright year All rights reserved

Init：在参数中有上升沿时，初始化 Modbus 块。只有当前没有作业正在运行时，才能执行初始化。必须通过 ENQ_ENR = FALSE 和 BUSY = FALSE 在程序中确保此条件。

（2）参数数据块 DB2

参数数据块 DB2（名称 MODBUS_PARAM_CP），该参数 DB 块用于 modbus 数据区域的设置。

注意，如需修改 DB 块中的数据，请将 DB 块切换到数据视图“Data view”，在“Actual value”列中进行修改。

本例中，为方便后续通信测试的地址对应，将 modbus 寄存器的起始和结束地址分别修改为“16#0”和“16#1F3”，如图 4-10 所示：

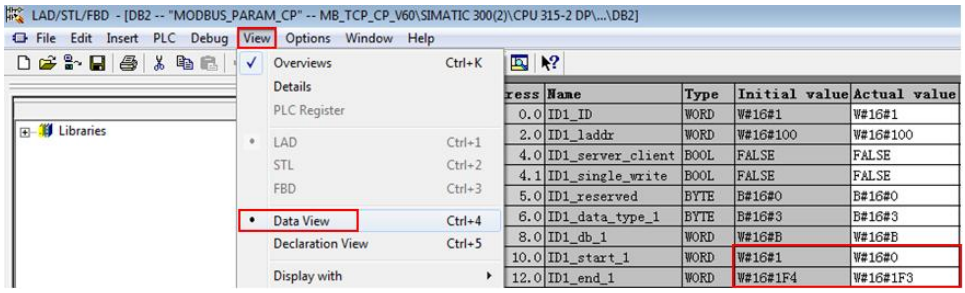


图 4-10 将 DB 块切换到数据视图并修改参数

以下为部分参数说明（其它参数信息请查看指令库手册）：

ID1_ID：为 “Configure Network”中的已组态连接的 ID。连接 ID 是 CPU 与连接伙伴之间通过 CP 实现的连接的唯一标识。在此处输入连接组态的数字。该参数的取值范围为 1 到 64。

ID1_laddr：为硬件组态中的 CP 基址（I 地址）。在此处输入组态的值。该参数的取值范围取决于 CPU。“ID”和“laddr”参数还可以从 TCP 连接的“属性 > 常规”(Properties > General Information) 中获取。如图 4-6 所示。

ID1_server_client：该参数用于区分客户端和服务器模式。如果输入为 TRUE，则使用“S7 用作服务器”模式。如果设置为 FALSE，则使用“S7 用作客户端”模式。

ID1_single_write：在“客户端”操作模式下，如果参数 ID1_single_write = TRUE，则功能代码 5 和 6 用于执行长度为 1 的写入作业。如果 ID1_single_write = FALSE，则功能代码 15 和 16 用于所有写入作业。

ID1_data_type_x：用于指定在该 DB 中映射的 Modbus/TCP 数据类型。如果在 ID1_data_type_x 中输入值 0，则不使用相应的数据区。

Copyright © Siemens AG Copyright year All rights reserved

标识符	数据类型	数据宽度
16#0	未使用区域	
16#1	线圈	Bit
16#2	输入	Bit
16#3	保持寄存器	Word
16#4	输入寄存器	Word

Modbus 数据类型	DATA_TYPE	功能	长度	功能代码
线圈	1	读取	任意	1
线圈	1	写入	1	5
线圈	1	写入	1	15
线圈	1	写入	> 1	15
输入	2	读取	任意	2
保持寄存器	3	读取	任意	3
保持寄存器	3	写入	1	6
保持寄存器	3	写入	1	16
保持寄存器	3	写入	> 1	16
输入寄存器	4	读取	任意	4

图 4-11 不同的数据类型与 modbus 功能代码的关系

ID1_db_x：指定用于映射 Modbus/TCP 寄存器或下面所定义位值的数据块。使用全局 DB 时，DB 编号 0 为系统保留，因而不允许使用。

DB 编号 1 到 65535（W#16#0001 到 W#16#FFFF）

ID1_start_x / end_x： “ID1_start_x”用于指定 DB 的数据字 0 中映射的第一个 Modbus/TCP 地址。“ID1_end_x”参数用于定义最后一个 Modbus/TCP 地址。

对于寄存器访问，带有最后一个 Modbus 地址输入的 S7 DB 中的数据字编号如下计算：DBW 编号 = (end – start) * 2

对于位访问，带有最后一个 Modbus 地址输入的 S7 DB 中的数据字节编号如下计算：DBB 编号 = (end – start + 7) / 8

定义的数据区不得重叠。“ID1_end_x”参数不能小于“ID1_start_x”。如果出错，则会中止 FB 的启动过程并提示错误。如果两个值相同，将分配一个 Modbus/TCP 地址（1 个寄存器或 1 个位值）。

例程中设置的 DB 块和 modbus 地址的对应关系，如图 4-12 所示：

Copyright © Siemens AG Copyright year All rights reserved

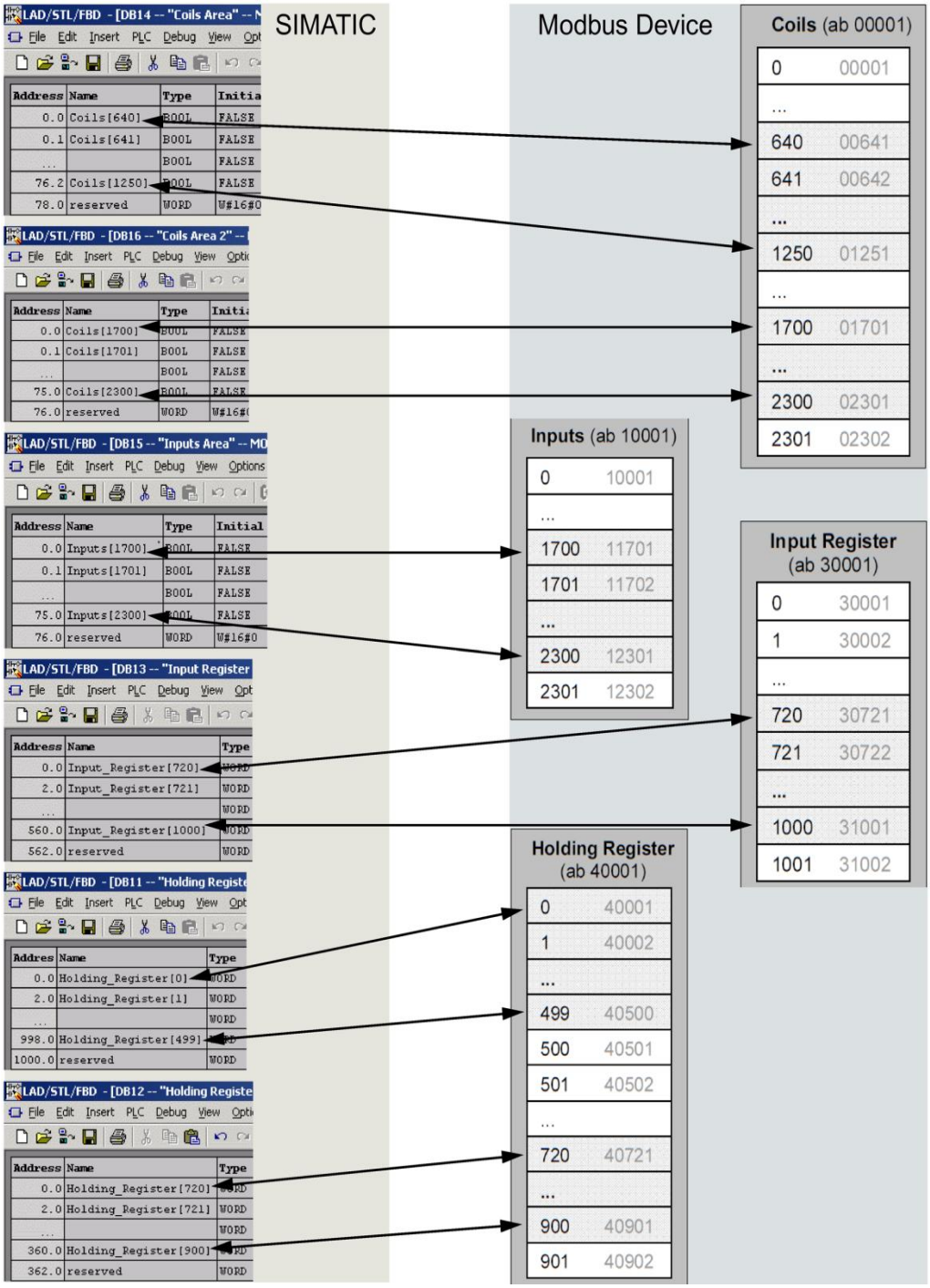


图 4-12 DB 块和 modbus 地址的对应关系

（3）授权密钥数据块

DB3 为授权密钥数据块（名称 LICENSE_DB），用于填写通过西门子授权中心申请到的 17 个字符，如图 4-13 所示：

Address	Name	Type	Initial value	Actual value	Comment
0.0	REG_KEY	STRING [17]	'insert REG_KEY'	'insert REG_KEY'	Registration Key

图 4-13 授权密钥数据块

Copyright © Siemens AG Copyright year All rights reserved

授权密钥的申请方法，请查看指令库手册“SIMATIC Modbus/TCP communication using CP 343-1 and CP 443-1 of the Manual”的第 5 章。

由于在获取授权密钥前，“MODBUSCP”指令是无授权状态，会使 CPU 报错而停机。而为了读取 CPU 的“IDENT_CODE”码，需要 CPU 运行起来，则必须添加编程错误组织块 OB121。

（4）启动组织块

启动组织块 OB100（名称 COMPLETE RESTART），该 OB 块在 CPU 启动时置位“MODBUSCP”指令的初始化位 Init，如图 4-14 所示：

```
OB100 :  "Complete Restart"
Comment:
Network 1: Initialization of "MODBUSCP"
    // for initialization
        SET
        S     "CONTROL_DAT".Init          DB1.DBX24.1
```

图 4-14 置位“MODBUSCP”指令的初始化位 Init

4.4 通信测试

将项目下载到 CPU 中，打开 ModSim32 应用程序，下面以保持寄存器为例介绍通信测试过程。

首先，在 ModSim32 的 Connection 菜单下选择 Connect——>Modbus/TCP Svr，并设置 ModSim32 作为 server 端的端口号，如图 4-15 所示：

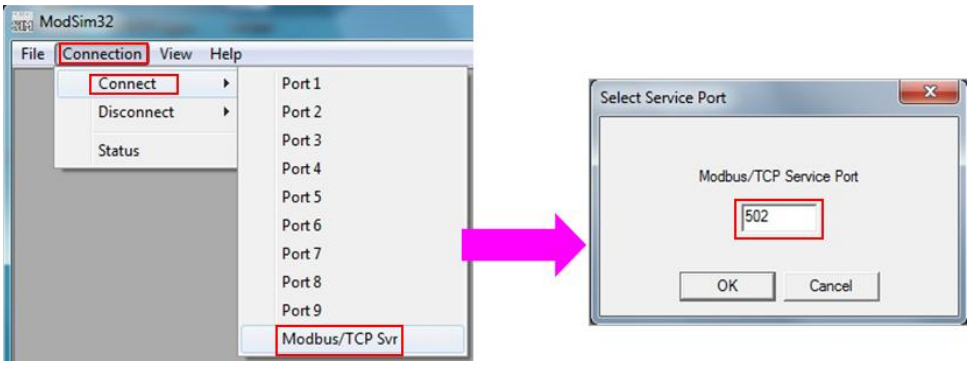


图 4-15 设置 ModSim32 作为 server 端的端口号

然后，需要置位“ENQ_ENR”，作为 modbus TCP 的 client 端的 PLC 将创建连接，并发送读取寄存器的请求（本测试中，PLC 访问 Modsim32 定义的数据类型 3，保持寄存器起始地址为 40001 开始的 10 个字），并进行数据读取，如图 4-16 所示：

Copyright © Siemens AG Copyright year All rights reserved

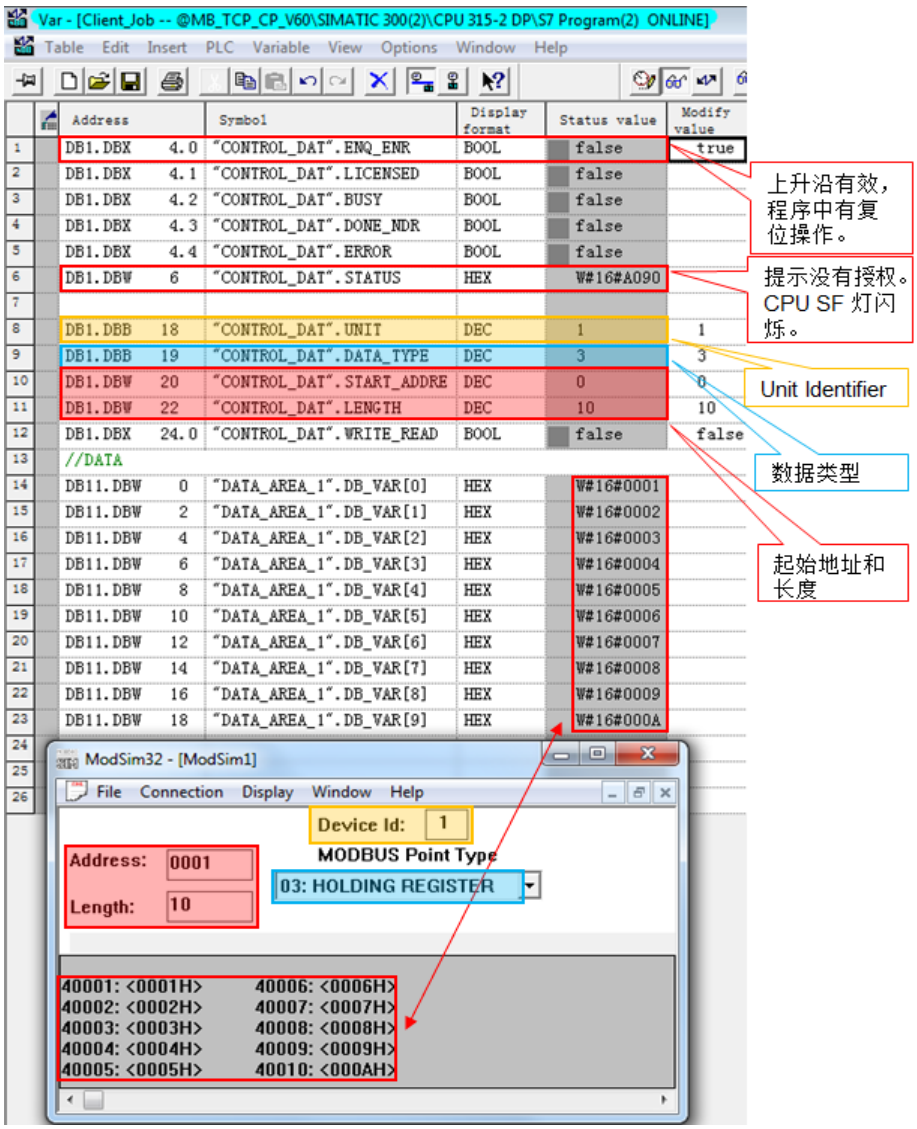


图 4-16 通信测试

可以通过网络配置窗口，查看通信状态，如图 4-17 所示：

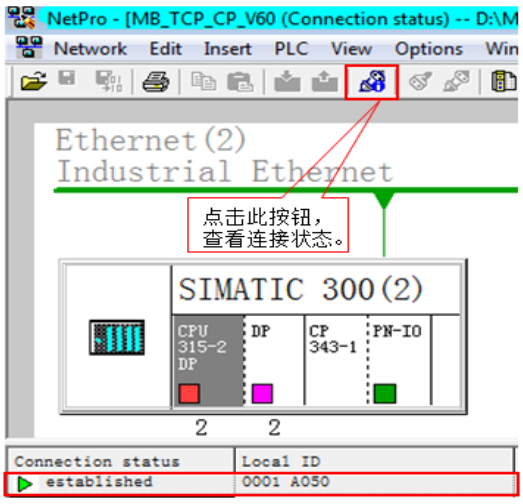


图 4-17 通信状态

Copyright © Siemens AG Copyright year All rights reserved

使用功能块“MODBUSCP”的一些注意事项：

1）S7-300CPU 通过以太网模块 CP343-1 的功能块“MODBUSCP”支持与多个 Modbus 服务器的通信，支持的个数取决于 CP343-1 所支持的 TCP 连接数，必须为每一个客户端连接分别调用一次功能块“MODBUSCP”，其背景数据块、ID、端口号等参数必须唯一。

2）S7-300CPU 通过以太网模块 CP343-1 可以同时作为 Modbus TCP 的 Server 及 Client。

3）S7-300CPU 通过以太网模块 CP343-1 支持多协议，除了运行 Modbus TCP 协议外，同时可以运行 PROFINET、TCP/IP、S7 等协议。

5 相关资料链接

Copyright © Siemens AG Copyright year All rights reserved

S7-300/S7-400 中 Modbus/TCP 块需要多少个授权?

http://support.automation.siemens.com/CN/view/zh/103709414

如何在 SIMATIC S7 上建立 OPEN MODBUS/TCP 通讯，如何查找相关信息?

http://support.automation.siemens.com/CN/view/zh/22660304

Simatic S7-300/S7-400：创建 Modbus/TCP 通信连接数据的向导

https://support.industry.siemens.com/cs/cn/zh/view/60735352

SIMATIC Modbus/TCP communication using CP 343-1 and CP 443-1 of the Manual

http://support.automation.siemens.com/WW/view/en/103447617

Block library for Modbus/TCP communication over CP343-1 or CP443-1

https://support.industry.siemens.com/cs/cn/en/view/109749851