SIEMENS

# 西门子 PLC 实现基于 CP 的 FETCH WRITE 使用入门

| Getting-started | Edition 09/02 |
| --- | --- |

**摘　要** 西门子的以太网通信模板提供了一种基于 TCP 的 FETCH WRITE 通信方式，该方式无需在 PLC 侧编程就可以得到 PLC 内的所有数据，可以用来与 S5 设备或者 PC 进行数据交换，本文对使用方式进行简要介绍

**关键词** TCP, FETCH , WRITE

**Key Words** TCP, FETCH , WRITE

# 目　　录

# 目　　录

1. PLC 侧通信准备

1.1 模块需求

在进行此类通信时，需要使用带有 FETCH WRITE 功能的模块，如下图：

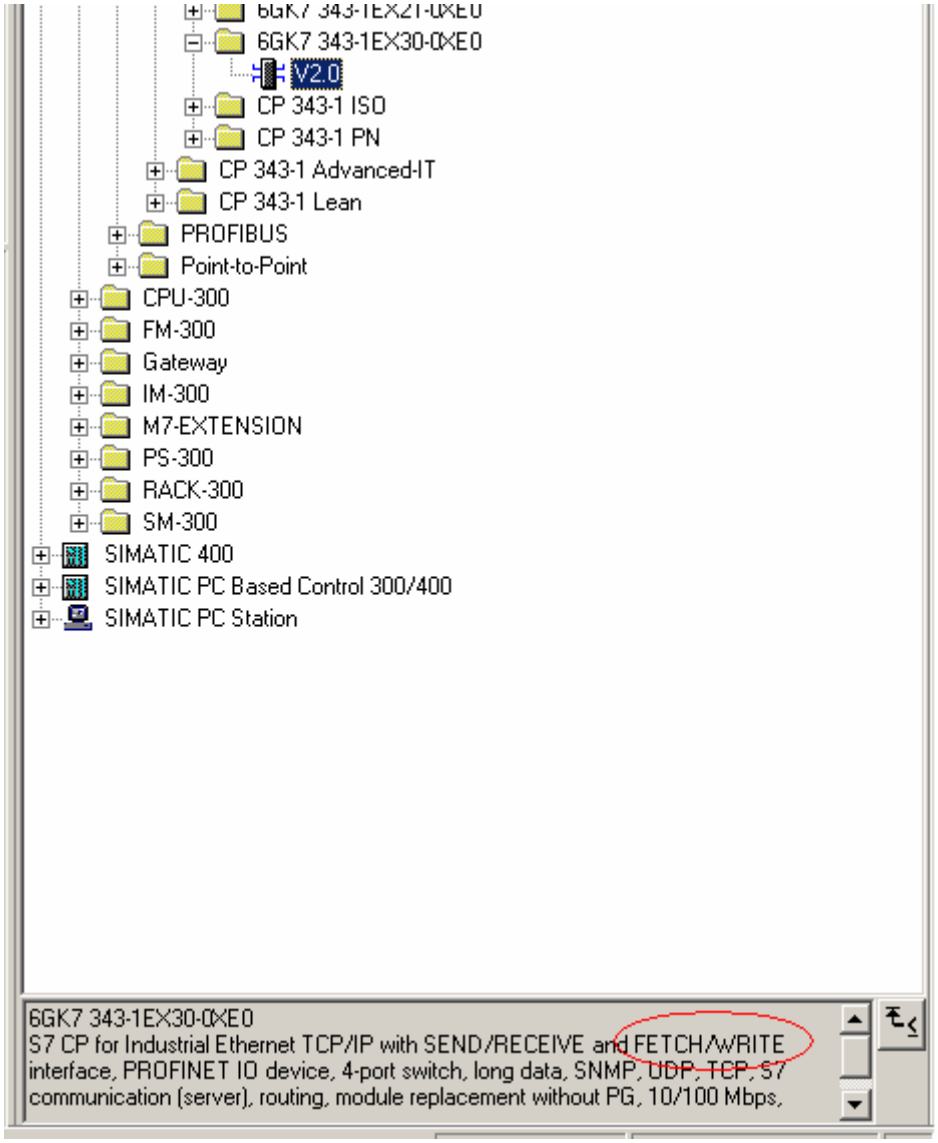


图 01：CP 模块需求

您需要组态一个 S7 300 或者 400 站点，进行硬件组态并保存编译。

硬件组态完成后，进入 netpro:

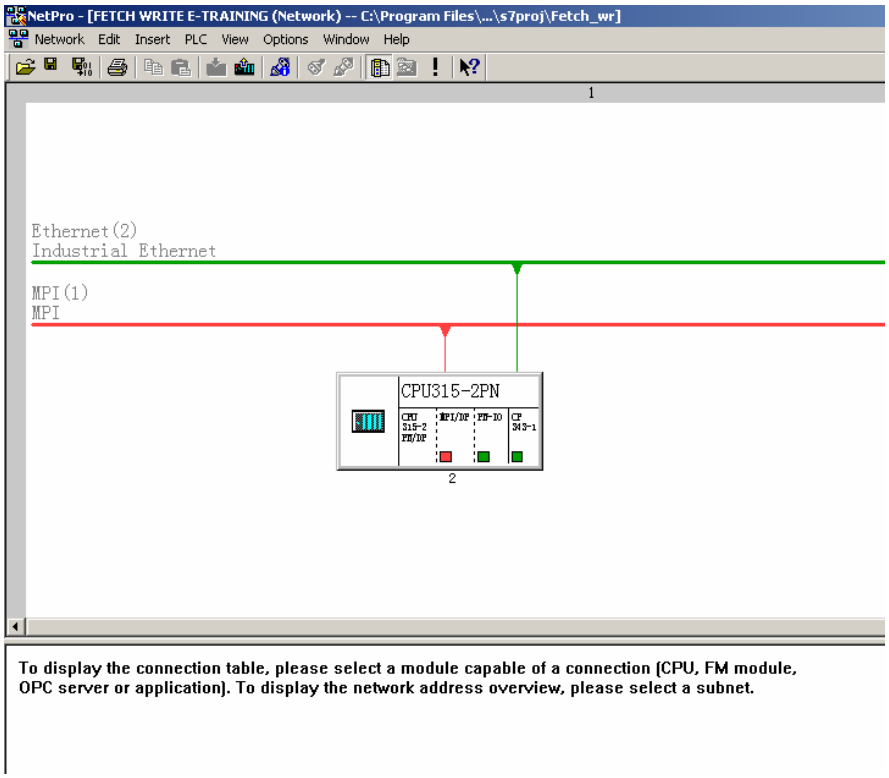


图 02：Netpro 中进行连接的建立

单击 CPU 后，双击下方表格区 local id 空白处：

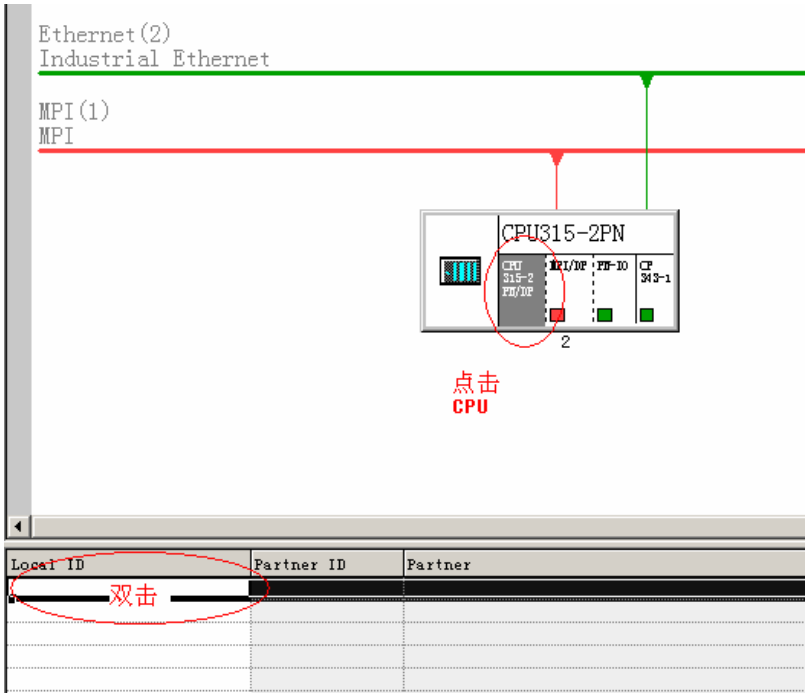


图 03：插入新的连接

1.2 FETCH 连接

双击完成后会弹出如下窗口，选择通信对象为 unspecified，通信类型选择为 TCP connection：

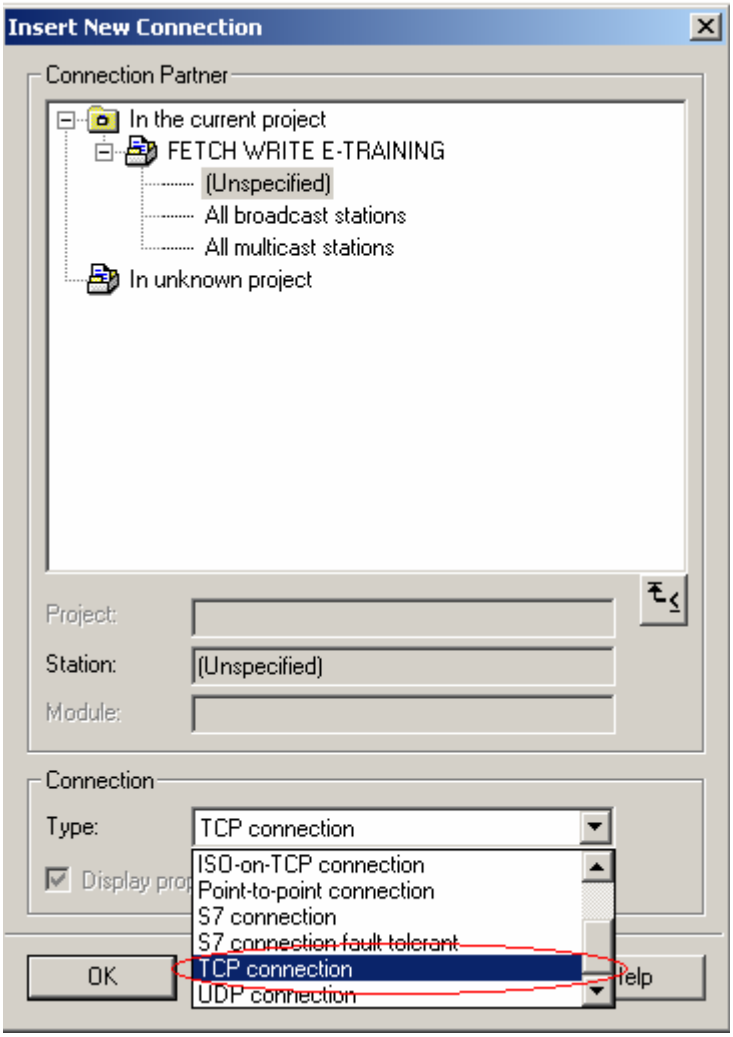


图 04：插入新的连接

点击 “OK”确认后会出现属性窗口的设置，在这里不需要设置通信对方的 IP 和端口号，仅需要指定 FETCH 功能对应的本地端口号。

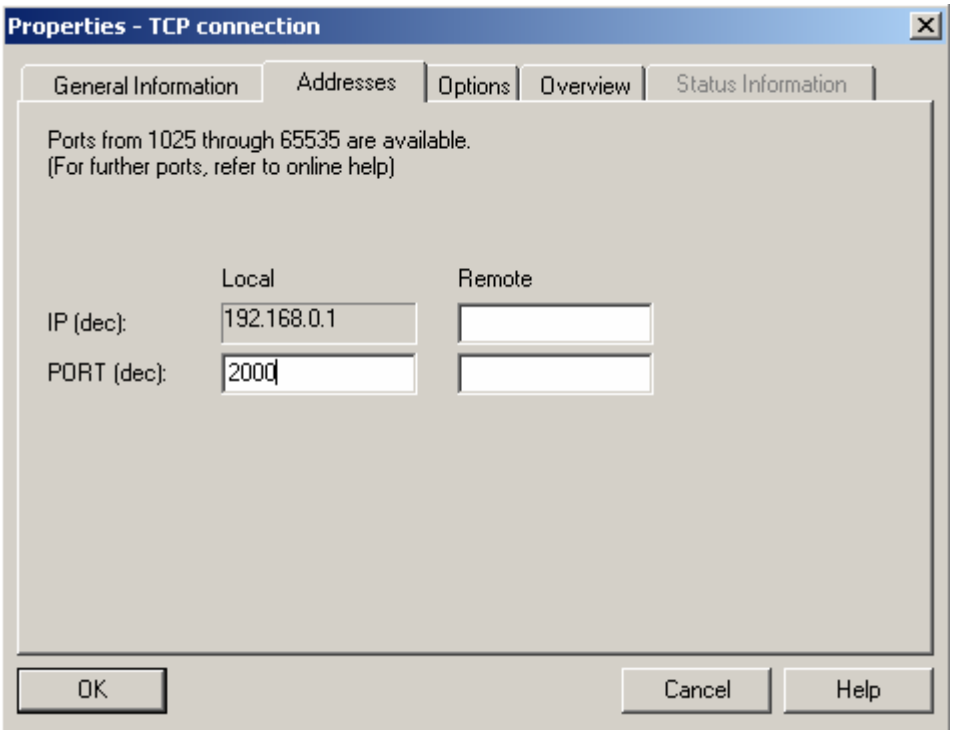


图 05：指定 FETCH 功能对应的端口号

在 Options 标签内设置 mode （模式）为 Fetch passive：

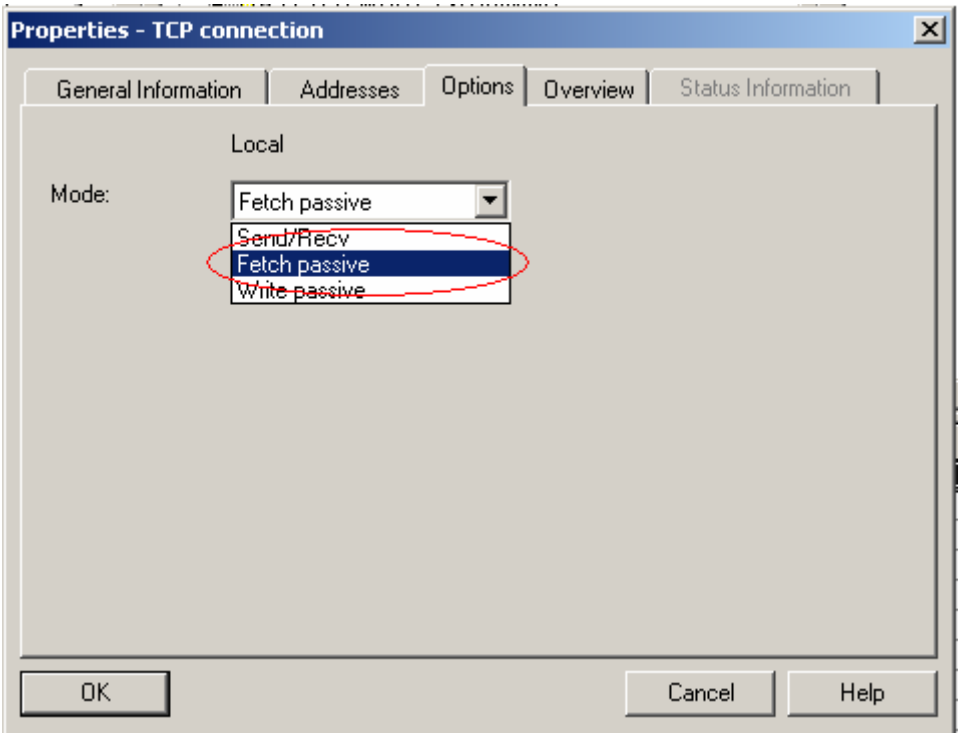


图 05：指定此链接为 FETCH 功能

1.2 WRITE 连接

继续双击表格区 local id 空白处会弹出如下窗口，选择通信对象为 unspecified，通信类型选择为 TCP connection：

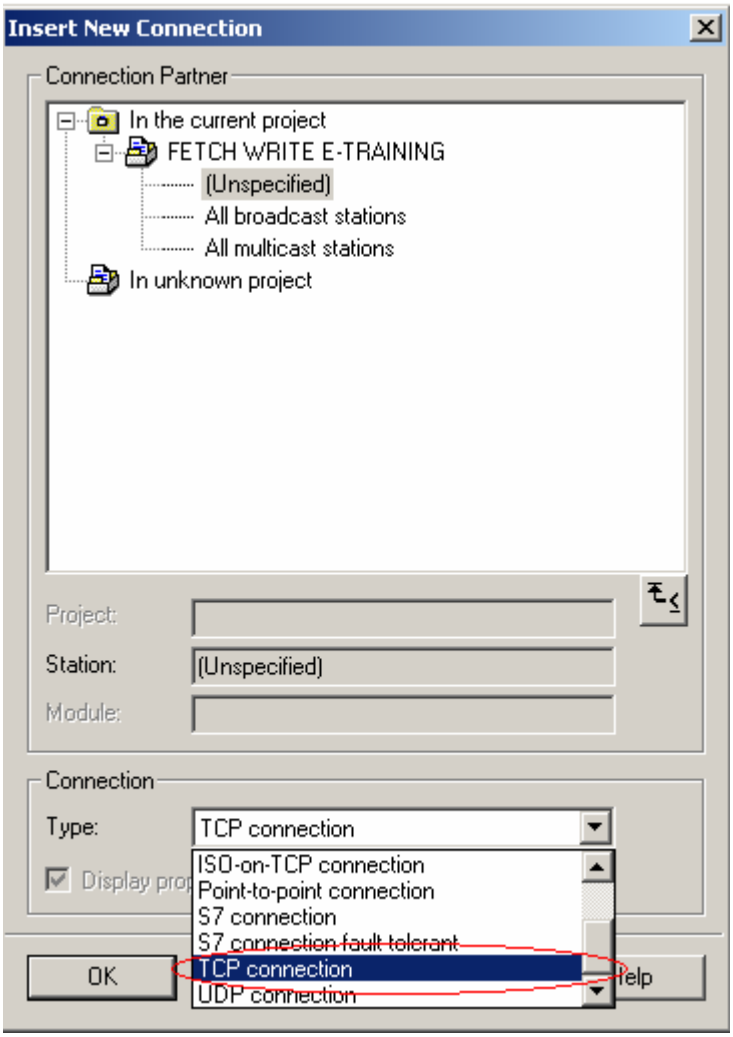


图 06：插入新的连接

点击 “OK”确认后会出现属性窗口的设置，在这里不需要设置通信对方的 IP 和端口号，仅需要指定 WRITE 功能对应的本地端口号。

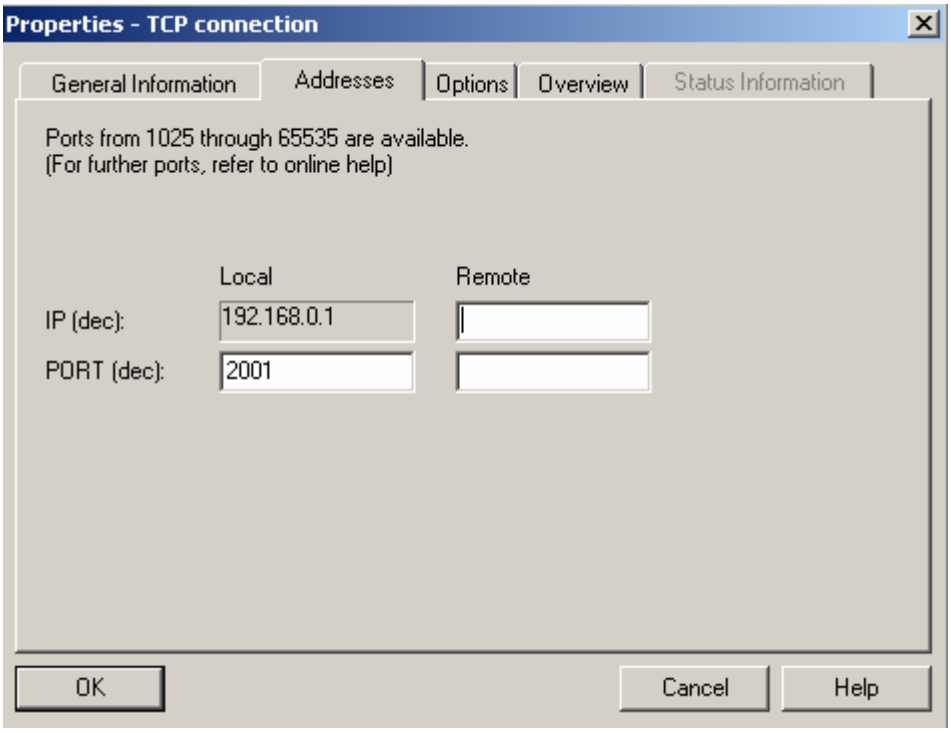


图 07：指定 WRITE 功能对应的端口号

在 Options 标签内设置 mode （模式）为 Write passive：

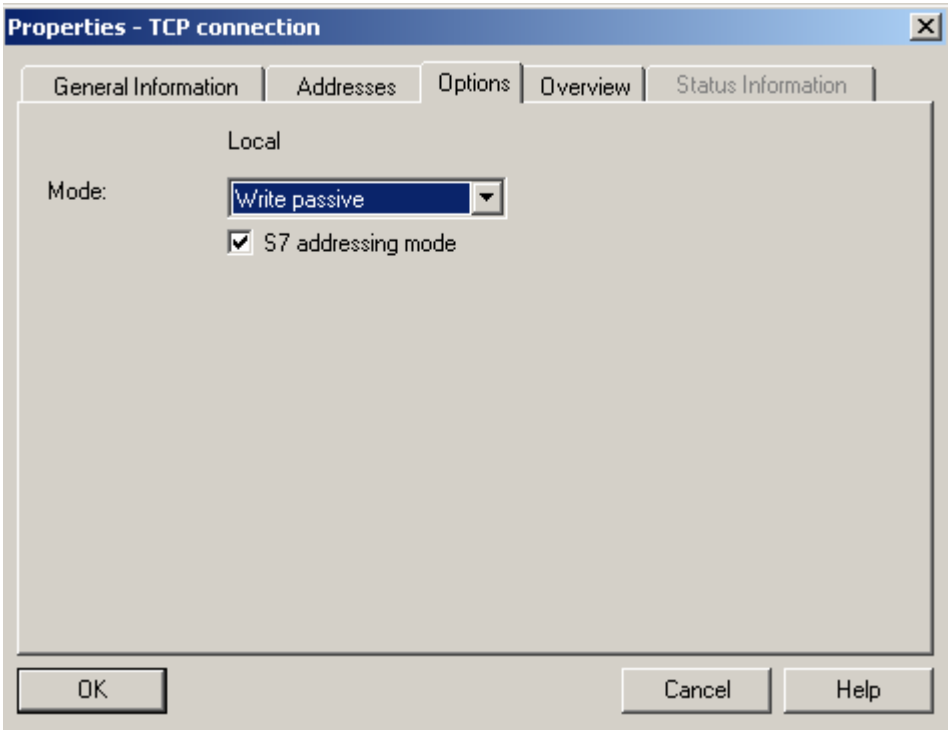


图 08：指定此链接为 FETCH 功能

**此处的地址模式如果与 s5 通信不勾选，默认是勾选的。**

1.4 编译保存并下载

当完成以上操作后，在 netpro 中保存并编译，无误后下载到 PLC 中，PLC 侧的准备工作结束：

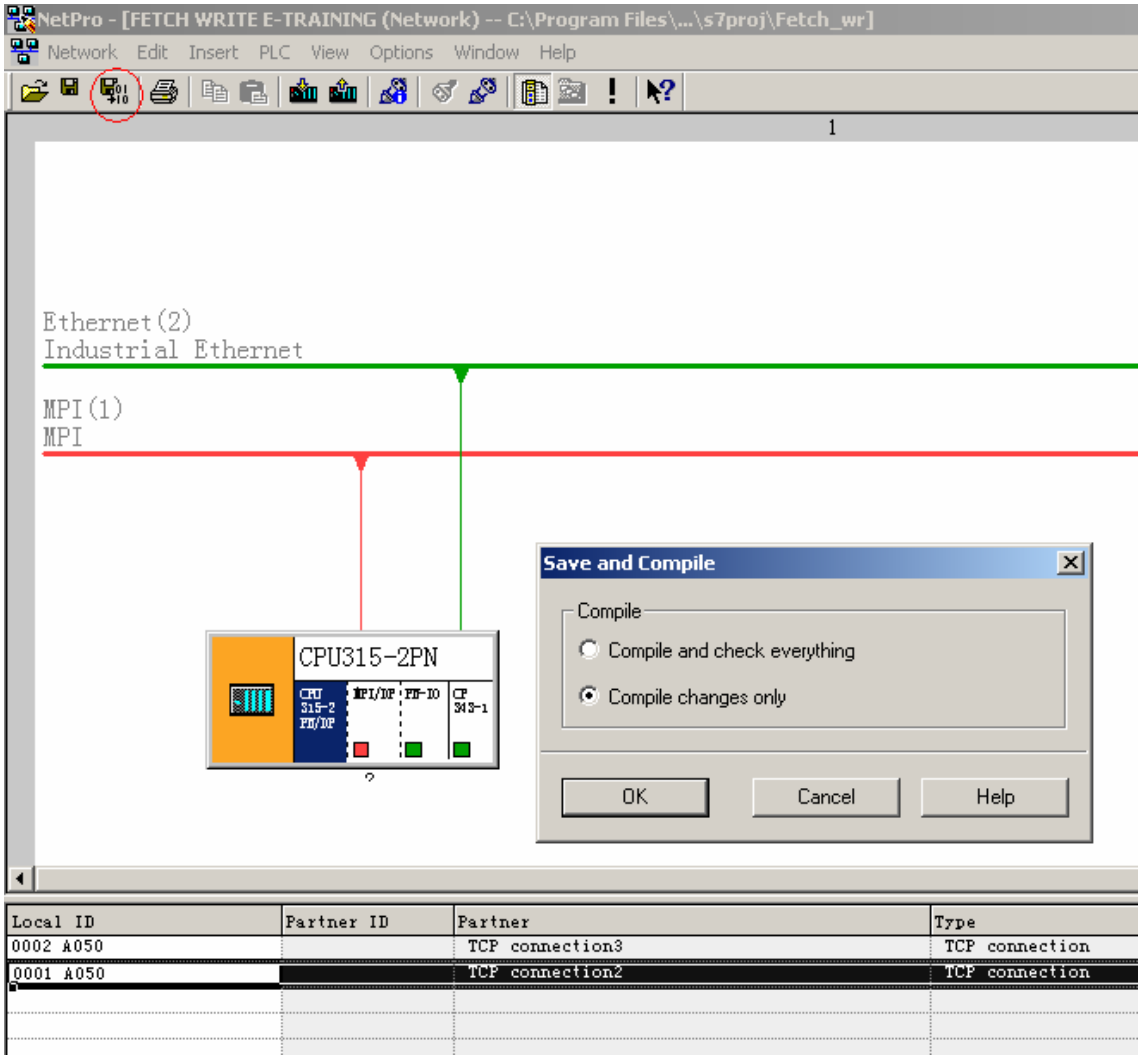


图 09：保存并编译

2.PC 侧通信准备

PC 侧需要进行 TCP 通信连接准备，在通信过程中 PC 侧需要作为 client 去连接 PLC,首先需要建立 TCP 连接，该连接需要使用“三次握手”的方式进行。

2.1 FETCH 报文

连接建立成功后需要按照如下结构发送报文，共 16 个字节：

**FETCH request frame**

| | | |
|---|---|---|
| 0 | System ID | ="S" |
| 1 | | ="5" |
| 2 | Length of header | =16d. |
| 3 | ID OP code | =01 |
| 4 | Length OP code | =03 |
| 5 | OP code | =05 |
| 6 | ORG field | =03 |
| 7 | Length ORG field | =08 |
| 8 | ORG ID | |
| 9 | DBNR | |
| A | Start address | High Byte |
| B | | Low Byte |
| C | Length | High Byte |
| D | | Low Byte |
| E | Empty field | =FFh. |
| F | Length empty field | =02 |

图 10：FETCH 时 PC 需要发送的报文

说明如下：

0，1 字节为’S’,’5’的 asc 码值，即十六进制的 53，35。

2 字节为长度描述，值为 16 进制的 10。

3 到 7 字节为固定的 16 进制数值 ：01 03 05 03 08

8，9 字节为变化的参数，用来描述读取的 PLC 地址区，数值选择按下表进行：

表一 ORG ID,DBNR 值：

| S7 Address Area | DB | M | I | Q |
|---|---|---|---|---|
| ORG ID | $01_H$<br>Source/dest. data from/to data block in main memory | $02_H$<br>Source/dest. data from/to flag area | $03_H$<br>Source/dest. data from/to process image of the inputs (PII) | $04_H$<br>Source/dest. data from/to process image of the outputs (PIQ) |
| DBNR | DB, from which the source data are taken or to which the dest data are transferred | irrelevant | irrelevant | irrelevant |
| permitted range | 1...255 | | | |
| Start address | DW number, from which the data are taken or written to | Flag byte no., from which the data are taken or written to | Input byte no., from which the data are taken or written to | Output byte no., from which the data are taken or written to |
| permitted range | 0...2047 | 0...255 | 0...127 | 0...127 |
| Length | Length of the source/dest. data field in words | Length of the source/dest. data field in bytes | Length of the source/dest. data field in bytes | Length of the source/dest. data field in bytes |
| permitted range | 1...2048 | 1...256 | 1...128 | 1...128 |

| ORG ID | $05_H$<br>Source/dest. data from/to in I/O modules. With source data input modules, with dest data output modules | $06_H$<br>Source/dest data from/to counter cells | $07_H$<br>Source/dest data from/to timer cells |
|---|---|---|---|
| DBNR | irrelevant | irrelevant | irrelevant |
| Start address | I/O byte no., from which the data are taken or written to | Number of the counter cell from which the data are taken or written to | Number of the timer cell from which the data are taken or written to |
| permitted range | 0...127<br>digital I/Os<br>128...255<br>analog I/Os | 0...255 | 0...255 |
| Length | Length of the source/dest. data field in bytes | Length of the source/dest. data field in words (counter cell = 1 word) | Length of the source/dest. data field in words (counter cell = 1 word) |
| permitted range | 1...256 | 1 | 1 |

字节 A，B，为起始地址，字节 C，D，为长度，字节 E，F,为固定的 FF 和 02。

因此例如您需要读取 MB0 与 MB1，需要发送的报文为(16 进制)：

53 35 10 01 03 05 03 08 02 00 00 00 00 02 ff 02

当发送成功后可以接收到如下响应：

FETCH response frame

| | | |
|---|---|---|
| 0 | System ID | =”S” |
| 1 | | =”5” |
| 2 | Length of header | =16d. |
| 3 | ID OP code | =01 |
| 4 | Length OP code | =03 |
| 5 | OP code | =06 |
| 6 | Ack field | =0Fh |
| 7 | Length ack field | =03 |
| 8 | Error field | =No |
| 9 | Empty field | =FFh |
| A | Length empty field | =07 |
| B | free | |
| C | | |
| D | | |
| E | | |
| F | | |
| | Data up to 64 K but only if Error no. =0 | |

图 11：FETCH 时 PLC 响应的报文

因此可以看出，数据存放于接收到的报文第 17 个字节开始的区域。

、

2.2 WRITE 报文

**WRITE request frame**

| | | |
|---|---|---|
| 0 | System ID | ="S" |
| 1 | | ="5" |
| 2 | Length of header | =16d. |
| 3 | ID OP code | =01 |
| 4 | Length OP code | =03 |
| 5 | OP code | =03 |
| 6 | ORG field | =03 |
| 7 | Length ORG field | =08 |
| 8 | ORG ID | |
| 9 | DBNR | |
| A | Start address | High Byte |
| B | | Low Byte |
| C | Length | High Byte |
| D | | Low Byte |
| E | Empty field | =FFh. |
| F | Length empty field | =02 |
| Data up to 64 K | | |

图 12：write 时 PC 发送的报文

WRITE 与 FETCH 类似，只是在 16 个字节后附带上要写入 PLC 的数据，如果写入成功则可以得到如下的报文响应：

WRITE acknowledgment frame

| | | |
|---|---|---|
| 0 | System ID | =”S” |
| 1 | | =”5” |
| 2 | Length of header | =16d. |
| 3 | ID OP code | =01 |
| 4 | Length OP code | =03 |
| 5 | OP code | =04 |
| 6 | Ack field | =0Fh |
| 7 | Length ack field | =03 |
| 8 | Error field | =No |
| 9 | Empty field | =FFh |
| A | Length empty field | =07 |
| B | free | |
| C | | |
| D | | |
| E | | |
| F | | |

图 13：write 时 PLC 响应的报文

# 附录一推荐网址

**自动化系统**
西门子（中国）有限公司
工业自动化与驱动技术集团 客户服务与支持中心
网站首页：www.4008104288.com.cn
自动化系统 **下载中心**：
http://www.ad.siemens.com.cn/download/DocList.aspx?TypeId=0&CatFirst=1
自动化系统 **全球技术资源**：
http://support.automation.siemens.com/CN/view/zh/10805045/130000
**“找答案”**自动化系统版区：
http://www.ad.siemens.com.cn/service/answer/category.asp?cid=1027

## 注意事项

应用示例与所示电路、设备及任何可能结果没有必然联系，并不完全相关。应用示例不表示客户的具体解决方案。它们仅对典型应用提供支持。用户负责确保所述产品的正确使用。这些应用示例不能免除用户在确保安全、专业使用、安装、操作和维护设备方面的责任。当使用这些应用示例时，应意识到西门子不对在所述责任条款范围之外的任何损坏/索赔承担责任。我们保留随时修改这些应用示例的权利，恕不另行通知。如果这些应用示例与其它西门子出版物(例如，目录)给出的建议不同，则以其它文档的内容为准。

## 声明

我们已核对过本手册的内容与所描述的硬件和软件相符。由于差错难以完全避免，我们不能保证完全一致。我们会经常对手册中的数据进行检查，并在后续的版本中进行必要的更正。欢迎您提出宝贵意见。



**西门子（中国）有限公司**