

1. SIMATIC S7 中的 S7 通讯

S7 通讯（S7-communication）主要用于 S7-400/400、S7-400/300 PLC 之间的通讯，是 S7 系列 PLC 基于 MPI、PROFIBUS 和工业以太网的一种优化的通讯协议。

MPI 网：MPI 是 Multi-Point-Interface 的缩写，中文意思是“多点接口”。MPI 的设计面向 PG/OP 连接，即连接 PG（调试和测试）和 OP（操作员面板）。此外，MPI 接口还可用于将多台 CPU 联网，进行 S7 基本通讯或 S7 通讯。

PROFIBUS：过程现场总线，开放的、独立于制造商的通信系统。在 SIMATIC 网络中，PROFIBUS 面向单元级和现场级。包含两个不同特性的版本：

- 单元级 PROFIBUS FMS 用于对时间要求不严格的、对等的智能站点之间的通信
- 现场总线 PROFIBUS DP 用于对时间要求严格的、主站和现场设备之间的循环数据交换

工业以太网：工业级的以太网，开放的、独立于制造商的通信系统。在 SIMATIC 中，工业以太网用于管理级和单元级。工业以太网的设计面向对时间要求不严格的大量数据的传送。

2. S7 通讯的特点

- S7 通讯服务集成在所有 SIMATIC S7 控制器中
- 属于 ISO 参考模型第 7 层（应用层）的服务
- 采用客户端-服务器原则（Client-Server-Principle），服务器只能被访问
- 适用于所有的 SIMATIC 子网（MPI, PROFIBUS 和工业以太网）
- 在系统组态期间为 S7 通讯建立 S7 连接，S7 连接属于静态连接
- 可以与同一个通讯伙伴建立多个连接，同一时刻可以访问的通讯伙伴的数量取决于 CPU 以及 CP 的连接资源
- S7-400 控制器使用 SFB BSEND/BRCV 进行数据的安全传送 (每次最大 64 K 字节)，当确认接收方收到数据后，数据传送才算真正完成
- S7-300 CPU 31x-2 PN/DP 以及 CPU 31x 加 CP 模板使用 SIMATIC_NET_CP 库或标准库中的 FB BSEND/BRCV 与其他 S7-300 和 S7-400 进行数据的安全传送
- 使用 SFB USEND/URCV 可以实现数据和信息的快速、非安全传送。S7-400 每次最多传送 4 个数据包，S7-300 最多一个数据包。快速的数据传送无需确认
- 监控通讯方的 CPU 的运行状态，可以控制伙伴 CPU 的起、停（仅限于 S7-400）

3. S7 通讯操作步骤（以一台 S7-400 和一台 S7-300 的工业以太网通讯为例）

3.1 硬件组态

3.1.1 硬件连接

将 S7-400 与 S7-300 PLC 连到同一工业以太网上。将带有以太网网卡的 PC 机连到同一工业以太网上，或将带有 MPI 网卡的 PC 机连到 S7-400/300 的 MPI 接口。如图 1 所示：

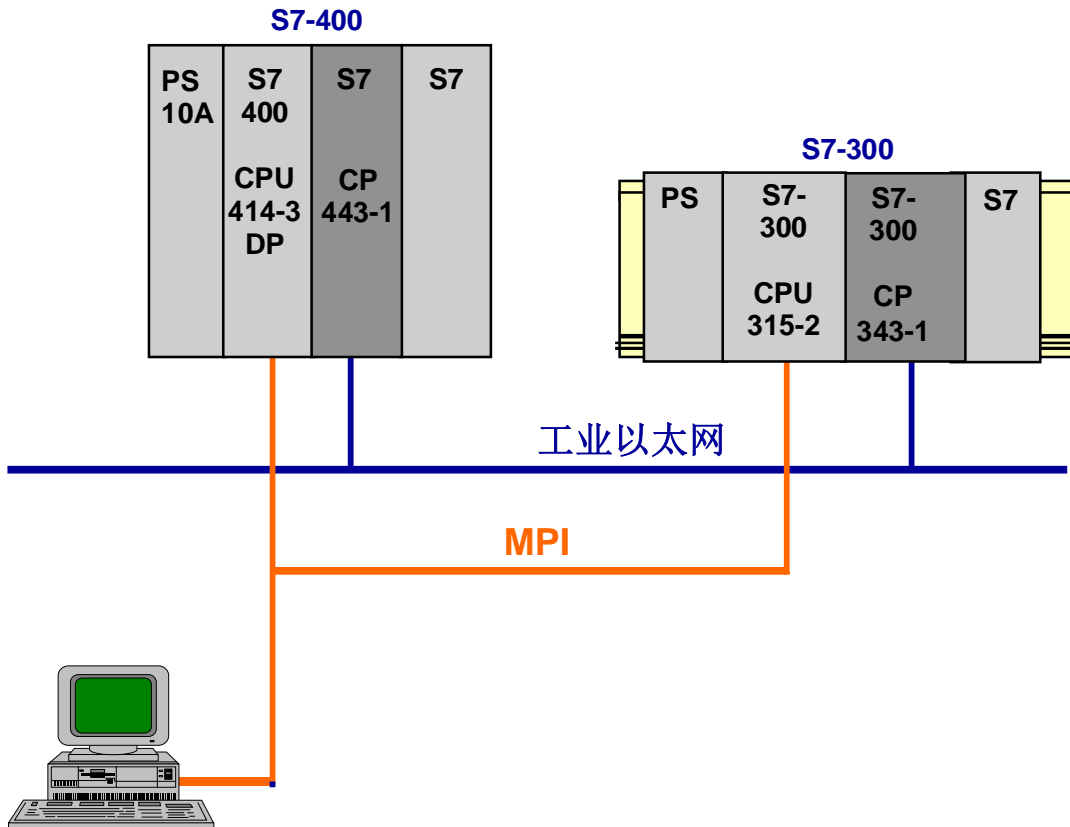


图 1：PC 机、S7-400/300 的连接

3.1.2 新建项目

在 SIMATIC Manager 中新建一个项目，名称为 S7_Comm。如图 2 所示：

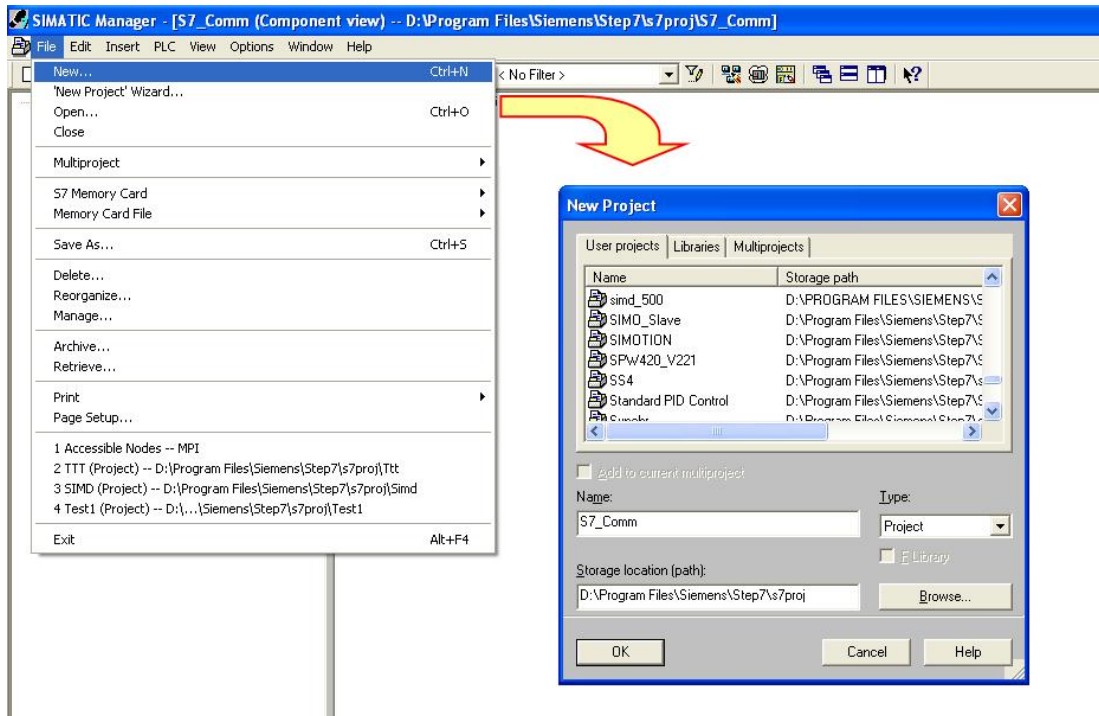


图 2: 新建项目, 名称为 S7_Comm

3. 1. 3 插入一个 S7-400 站和一个 S7-300 站

在项目名称 S7_Comm 下插入 SIMATIC 400 Station 和 S7-300 Station, 然后选中 400 站或 300 站, 双击右侧窗口中的“Hardware”进入 HW Config, 分别对两个站进行硬件组态。从硬件组态目录中依次插入机架、电源、CPU*、以及以太网 CP。在插入以太网 CP 时会弹出网络属性窗口, 设置 CP 上以太网接口的网络参数。以太网模板的 IP 地址分别设置成: 192.168.0.1 和 192.168.0.2。如图 3 和图 4 所示:

* 提示: 可以在 CPU 属性中激活 MB0 作为时钟信号, 以便将来调用程序时使用。

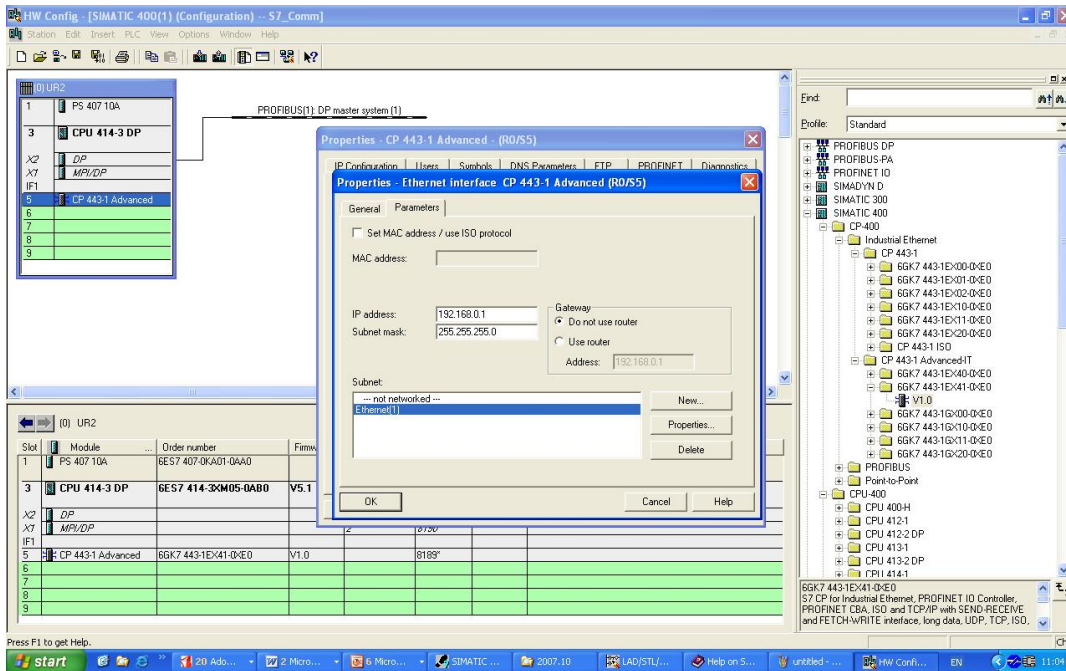


图 3：S7-400 站硬件组态，设置 CP443-1 的 IP 地址

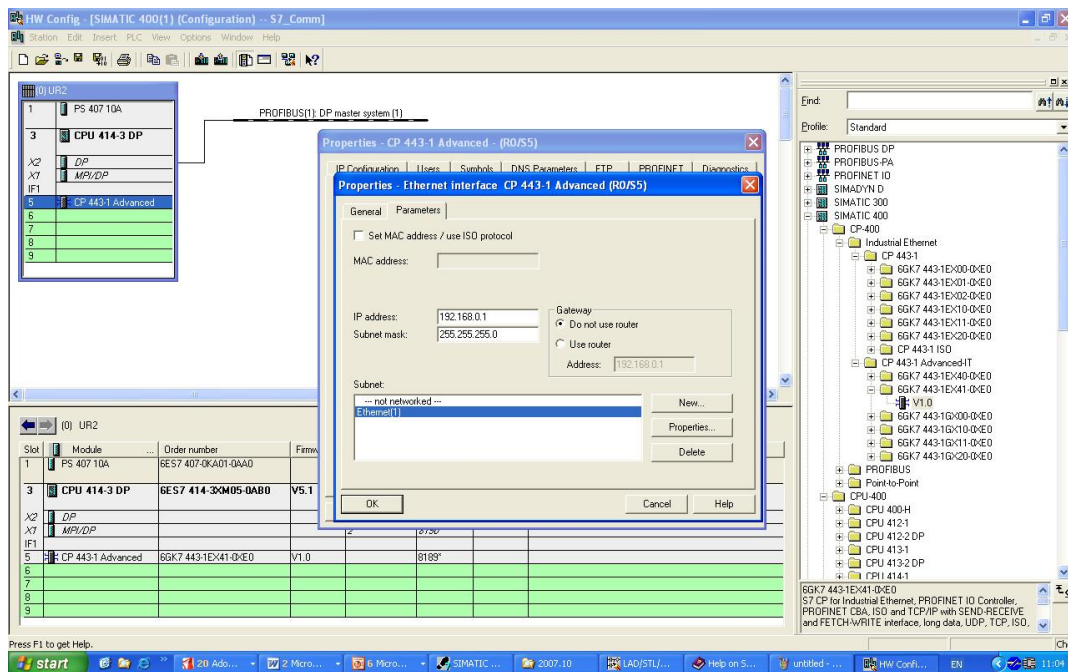


图 4：S7-300 站硬件组态，设置 CP343-1 的 IP 地址

硬件组态完成后，分别进行编译、下载。如果没有错误，接下来进入 NetPro 进行网络组态。

3. 2 建立 S7-连接

从 SIMATIC Manager 或 HW Config 点击网络组态按钮 进入 NetPro 进行网络组态。

用鼠标选中 S7-400 的 CPU，窗口的下半部出现一个表格。在表格的空白处点击鼠标右键，选择 Insert New Connection，插入一个新连接。如图 5 所示：

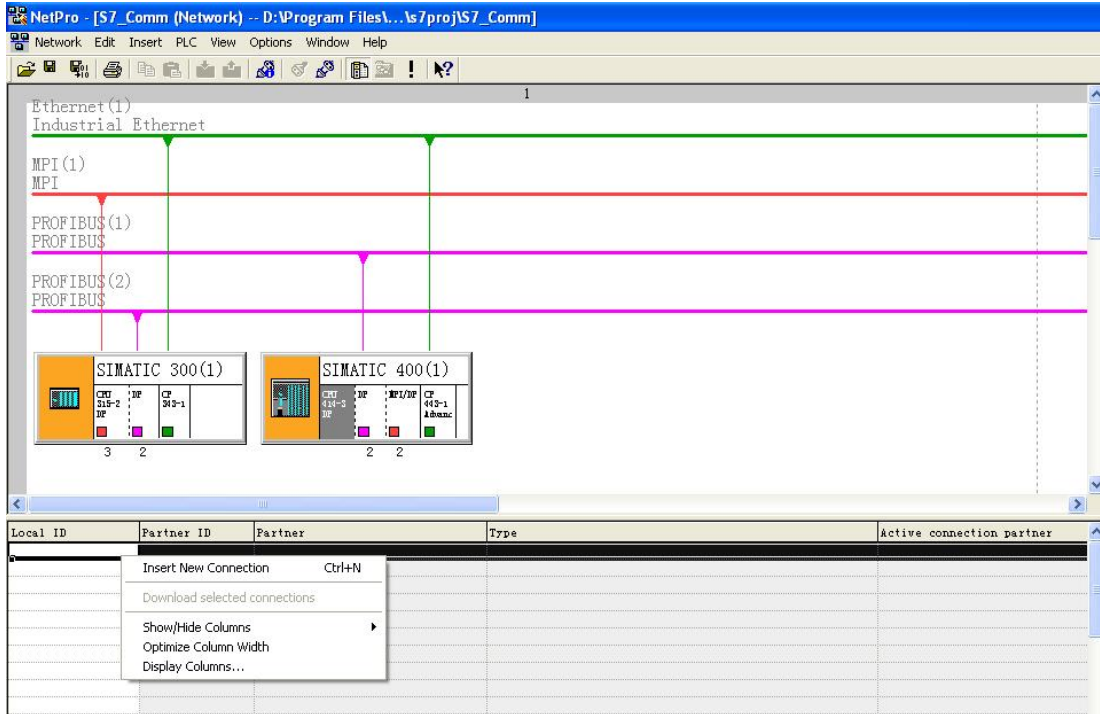


图 5：在 NetPro 中组态 S7-400 CPU 的 S7-连接

选择 Insert New Connection 后弹出插入新连接对话框。

在插入新连接对话框 “Insert New Connection” 的 Connection Partner 中选择连接伙伴 CPU 315-2 DP，在 Connection Type 中选择连接类型 S7 connection。如图 6 所示：

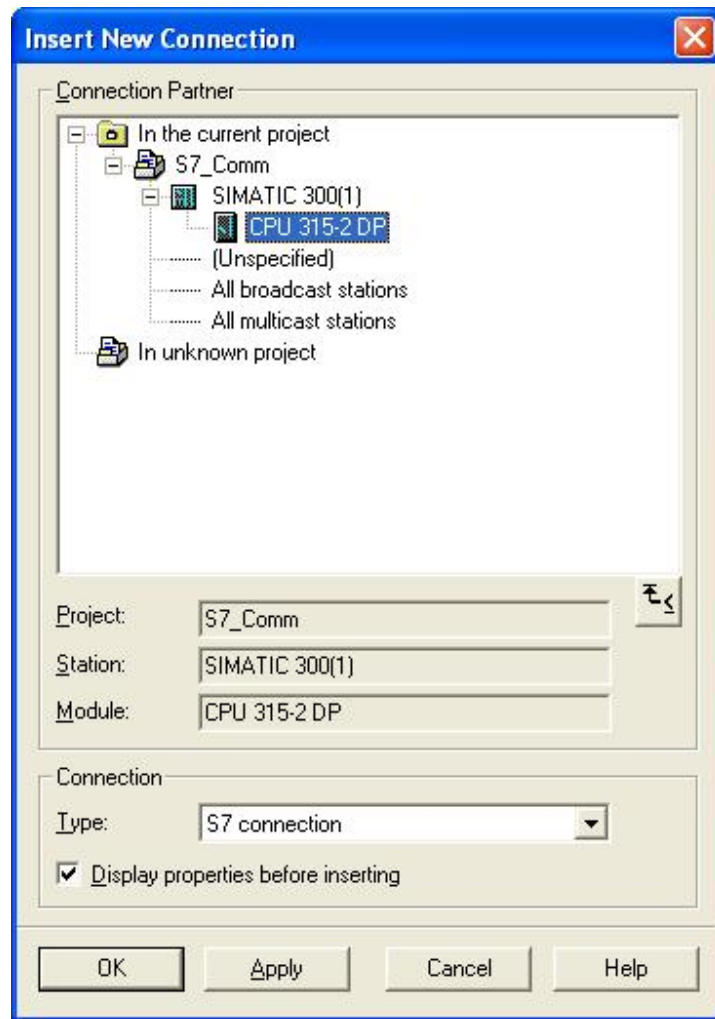


图 6：为 S7-400 CPU 插入新的 S7 连接

保留 “Display properties before inserting”， 点击 OK。

点击 OK 后，弹出 S7 connection 属性窗口，如图 7 所示：

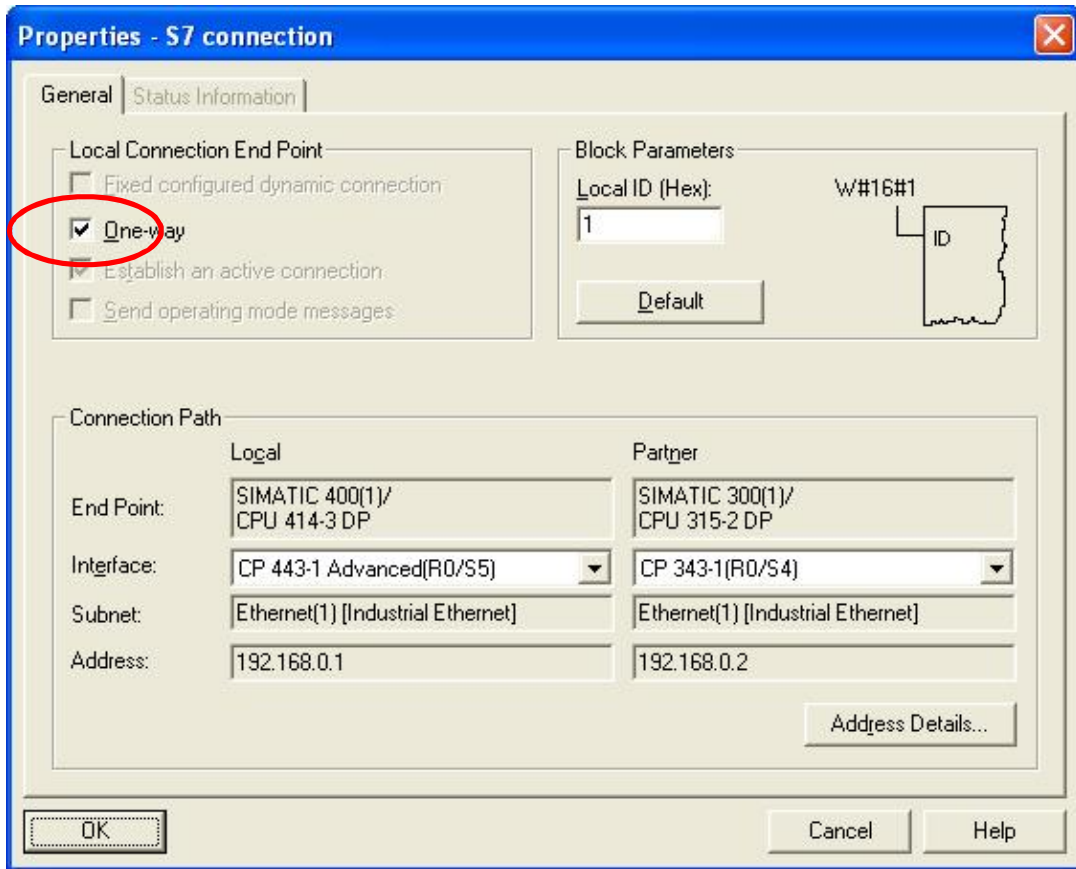


图 7: S7-400 CPU 的 S7 connection 属性，单边

窗口的左上角默认设置为单边（One-way），本地 CPU 作 Client，伙伴 CPU 作 Server，Client 访问 Server。可以利用单边功能块（GET, PUT）进行单边访问。右上角为调用 GET, PUT 功能块时的编程提示，提示编程时怎样填写 ID 输入端。用鼠标点击右下角的“Address Details...”按钮，可以查看详细地址信息。

详细地址信息，如图 8 所示：

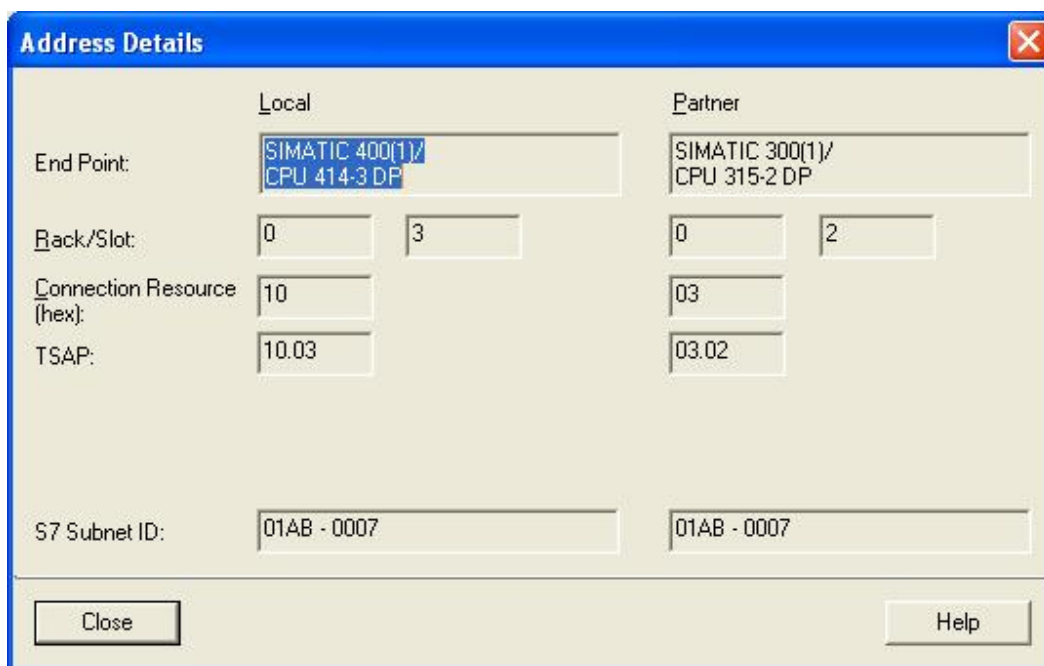


图 8: S7-400 CPU 的 S7 connection 的详细地址信息, 单边

关闭对话框, 表格中出现一个连接:

| Local ID | Partner ID | Partner | Type | Active connection partner |
|----------|------------|-------------------------------|---------------|---------------------------|
| 1 | | SIMATIC 300(1) / CPU 315-2 DP | S7 connection | Yes |

伙伴 CPU 也占用一个连接。但选择伙伴 CPU 后表格中不显示连接 (可以由此识别单边连接)。

点击 存盘编译。然后选中本站, 点击 将连接下载到本 CPU。建立单边连接时伙伴 CPU 下不显示连接, 也无需下载。

提示: 单边连接只需客户端侧单边下载!

若在图 7 中取消左上角的 “One-way” 选择则变成双边 (Two-way), 本地 CPU 和伙伴 CPU 既作 Client, 又作 Server。不但可以利用单边功能块 (GET, PUT) 进行单边访问, 而且可以利用双边功能块 (BSEND/BRCV, USEND/URCV) 进行双边访问。右上角为调用 GET, PUT, BSEND/BRCV, USEND/URCV 功能块时的编程提示, 提示编程时怎样填写 ID 输入端。如图 9 所示:

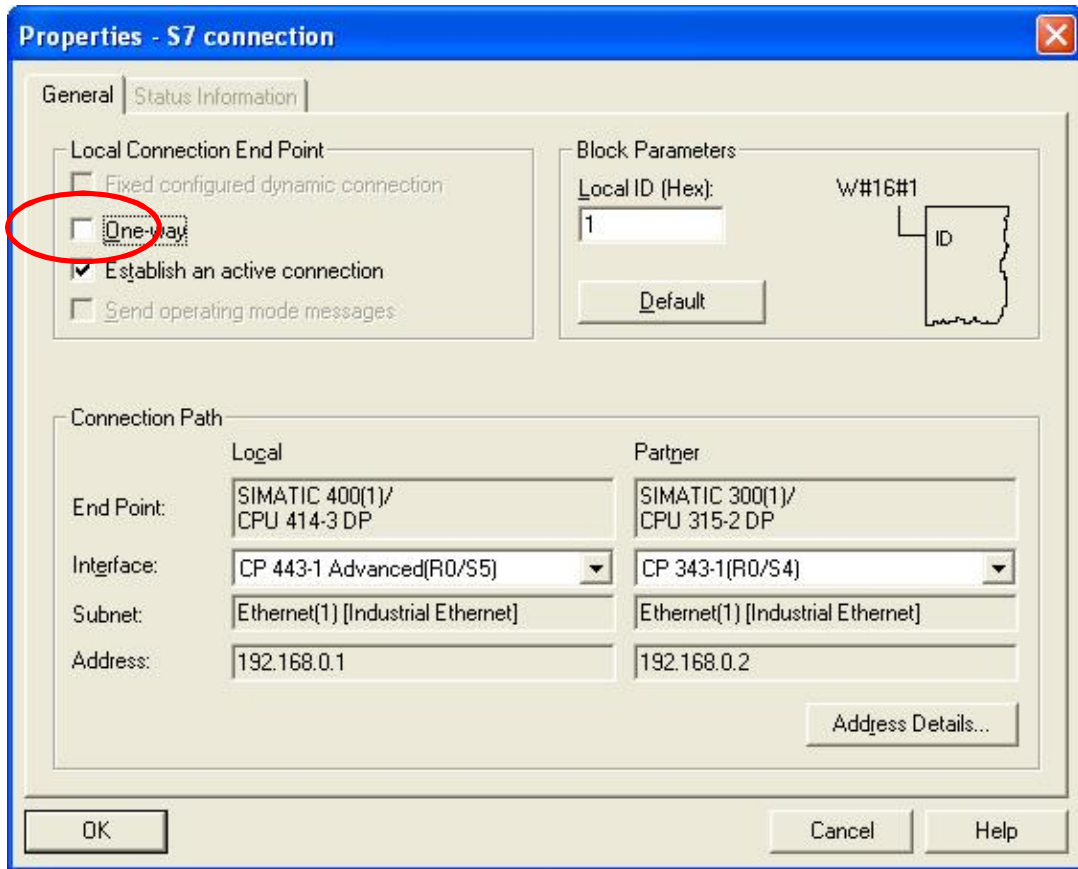


图 9: S7-400 CPU 的 S7 connection 属性，双边

选择双边时，可以选择“Establish an active connection（建立主动连接）”。如果这里取消选择“Establish an active connection”，那么伙伴自动选择。

用鼠标点击右下角的“Address Details...”按钮（若按钮是灰的可以关闭属性窗口，再打开属性窗口），可以查看详细地址信息。

详细地址信息，如图 10 所示：

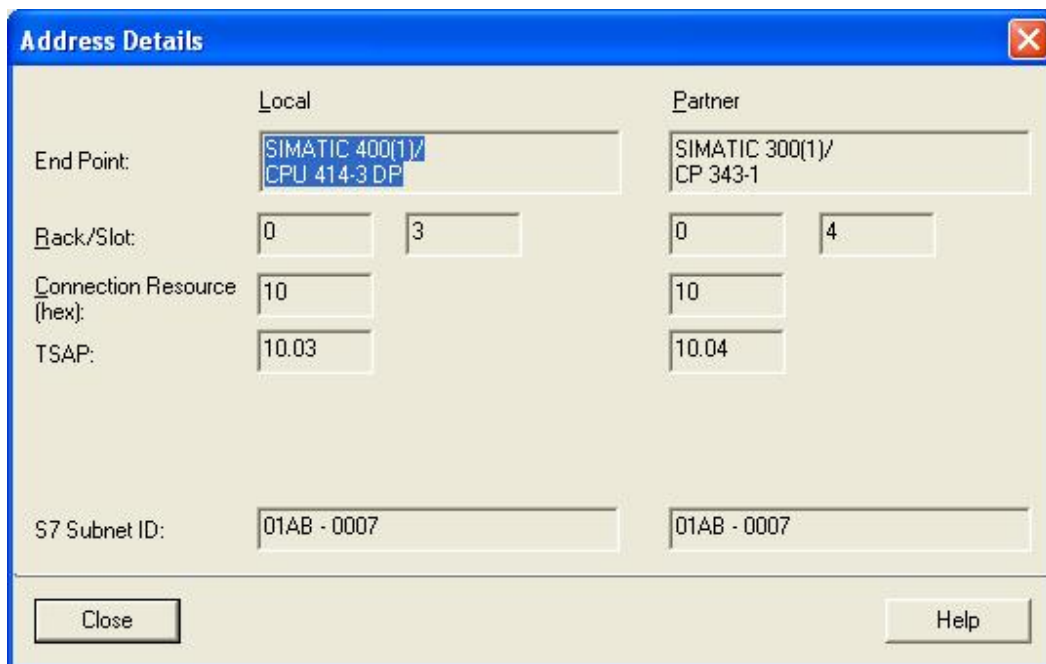




图 10: S7-400 CPU 的 S7 connection 的详细地址信息，双边

关闭对话窗口，表格中出现一个连接：

| Local ID | Partner ID | Partner | Type | Active connection partner |
|----------|------------|-------------------------------|---------------|---------------------------|
| 1 | 1 | SIMATIC 300(1) / CPU 315-2 DP | S7 connection | Yes |

伙伴 CPU 也占用一个连接。选择伙伴 CPU 后表格中也显示一个连接（可以由此识别双边连接）。

| Local ID | Partner ID | Partner | Type | Active connection partner |
|----------|------------|-------------------------------|---------------|---------------------------|
| 1 | 1 | SIMATIC 400(1) / CPU 414-3 DP | S7 connection | No |

点击  存盘编译。然后分别选中本站和伙伴站，分别点击  将连接下载到本 CPU 和伙伴 CPU。

提示：双边连接两个连接伙伴都需要下载！

3. 3 编写 PLC 程序，调用通讯功能块

S7-400 用于 S7 连接的通讯功能块位于标准库下的系统功能块中，如图 11 所示；S7-300 用于 S7 连接的功能块（又叫可装载功能块）位于标准库下的通讯功能块中（用于版本 V2.0 以上的 CPU），如图 12 所示：

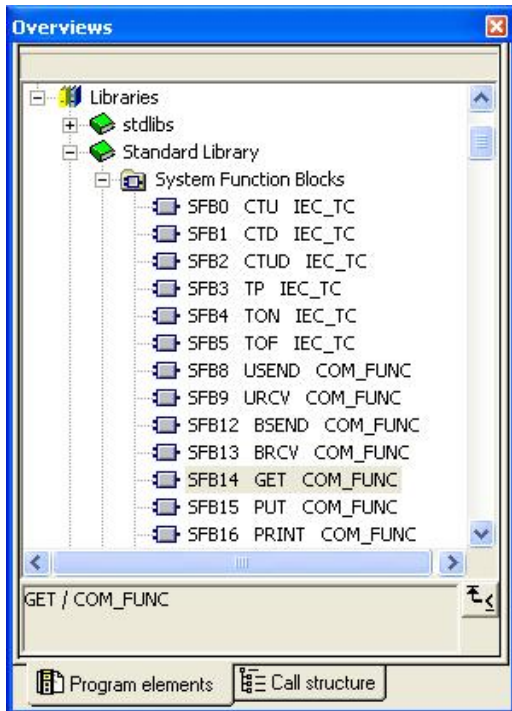


图 11: S7-400 用于 S7 连接的功能块

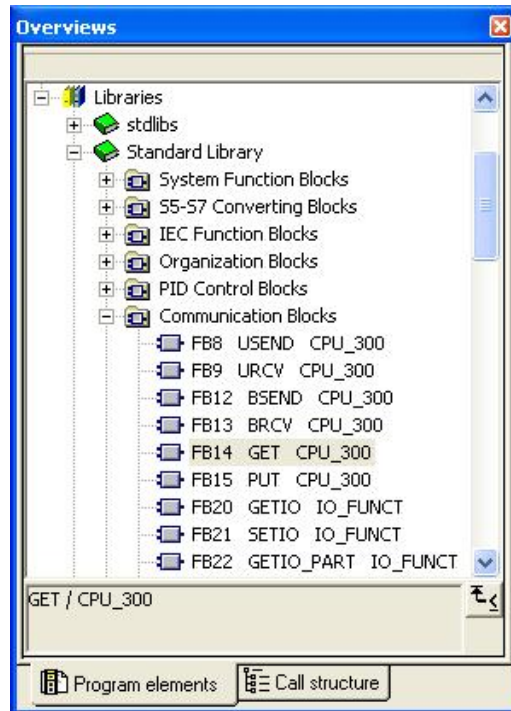


图 12: S7-300 用于 S7 连接的功能块

3. 3. 1 单边功能块 SFB14 GET, 将伙伴 CPU 数据读取到本 CPU 数据区

CALL "GET", DB14

| | | |
|--------|---------------------------|------------------------------|
| REQ | :=M0.5 | //上升沿触发一次传送（时钟脉冲，见第 6 页提示） |
| ID | :=W#16#1 | //指向 S7 连接的编号（见图 7 或图 9 右上角） |
| NDR | :=M100.0 | //上升沿（脉冲）表示从伙伴 CPU 接收到数据 |
| ERROR | :=M100.1 | //上升沿（脉冲）表示数据传送有错误 |
| STATUS | :=MW102 | //包含一个详细的错误描述或警告（十进制） |
| ADDR_1 | :=P#DB101.DBX0.0 BYTE 200 | //指向将读取的伙伴 CPU 中的区域 |
| ADDR_2 | := | |
| ADDR_3 | := | |
| ADDR_4 | := | |
| RD_1 | :=P#DB101.DBX0.0 BYTE 200 | //指向本 CPU 中用于存放数据的区域 |
| RD_2 | := | |
| RD_3 | := | |
| RD_4 | := | |

3. 3. 2 单边功能块 SFB15 PUT, 将本 CPU 数据发送到伙伴 CPU 数据区

```
CALL "PUT", DB14
REQ      :=M0.5           //上升沿触发一次传送（时钟脉冲，见第 6 页提示）
ID       :=W#16#1        //指向 S7 连接的编号（见图 7 或图 9 右上角）
DONE     :=M100.2        //上升沿（脉冲）表示向伙伴 CPU 传送完数据
ERROR    :=M100.3        //上升沿（脉冲）表示数据传送有错误
STATUS   :=MW104         //包含一个详细的错误描述或警告（十进制）
ADDR_1   :=P#DB102.DBX0.0 BYTE 200 //指向将发送到的伙伴 CPU 中的区域
ADDR_2   :=
ADDR_3   :=
ADDR_4   :=
SD_1     :=P#DB102.DBX0.0 BYTE 200 //指向本 CPU 中用于发送数据的区域
SD_2     :=
SD_3     :=
SD_4     :=
```

3. 3. 3 双边功能块 SFB12 BSEND（伙伴 CPU 中调用接收块 BRCV）

```
CALL "BSEND", DB12
REQ      :=M0.7           //上升沿触发一次传送（时钟脉冲，见第 6 页提示）
R        :=               //上升沿终止数据传送，使发送块进入初始状态
ID       :=W#16#1        //指向 S7 连接的编号（见图 7 或图 9 右上角）
R_ID     :=DW#16#1111    //确定发送方和接收方的关系，双方参数必须相同
DONE     :=M110.0        //上升沿（脉冲）表示向伙伴 CPU 传送完数据
ERROR    :=M110.1        //上升沿（脉冲）表示数据传送有错误
STATUS   :=MW112         //包含一个详细的错误描述或警告（十进制）
SD_1     :=P#DB101.DBX0.0 BYTE 160 //指向本 CPU 中用于发送数据的区域
LEN      :=MW2           //欲传送数据的字节数
L        160            //装载欲传送数据的字节数
T        MW      2       //欲传送数据的字节数地址
```

3. 3. 4 双边功能块 SFB13 BRCV（伙伴 CPU 中调用发送块 BSEND）

```
CALL "BRCV", DB12
EN_R     :=TRUE          //置位表示准备接收数据
```

ID :=W#16#1 //指向 S7 连接的编号（见图 7 或图 9 右上角）
R_ID :=DW#16#1111 //确定发送方和接收方的关系，双方参数必须相同
NDR :=M110.0 //上升沿（脉冲）表示从伙伴 CPU 接收到数据
ERROR :=M110.1 //上升沿（脉冲）表示数据传送有错误
STATUS :=MW112 //包含一个详细的错误描述或警告（十进制）
RD_1 :=P#DB101.DBX0.0 BYTE 160 //指向本 CPU 中用于接收数据的区域
LEN :=MW2 //接收到数据的字节数

3. 3. 5 双边功能块 SFB8 USEND 和 SFB9 URCV（参数同 BSEND 和 SRCV，略）

4. S7 通讯传送的数据长度

4. 1 S7-300 与 S7-300/400 通讯时，只有 1 个数据区：

| Data block size | SFB/FB | 1 | 2 | 3 | 4 |
|-----------------|-------------------|-----|---|---|---|
| 240 (S7-300) | PUT/GET/ USEND | 160 | - | - | - |

4. 2 S7-400 与 S7-300 通讯时，有 4 个数据区：

| | | | | | |
|--------------|-------|-----|-----|-----|-----|
| 240 (S7-400) | PUT | 212 | 196 | 180 | 164 |
| | GET | 222 | 218 | 214 | 210 |
| | USEND | 212 | - | - | - |

数据区数据长度的含义（以功能块 PUT 为例）：

仅用一个数据区时，数据长度是 212 字节；

用两个数据区时，数据总长度是 196 字节；

用三个数据区时，数据总长度是 180 字节；

用四个数据区时，数据总长度是 164 字节。

（下同）

4. 3 S7-400 与 S7-400 通讯时，有 4 个数据区：

| | | | | | |
|-----|-------|-----|-----|-----|-----|
| 480 | PUT | 452 | 436 | 420 | 404 |
| | GET | 462 | 458 | 454 | 450 |
| | USEND | 452 | 448 | 444 | 440 |

5. S7-CPU/CP 的连接资源

5.1 CPU 的连接资源

一个 CPU 能够建立多少个连接，一个 CP 允许建立多少个连接是有限的。这个限制叫做连接资源。连接资源可以从样本中查出，例如：S7-CPU 414 的连接资源是 32，如表 1 所示；S7-CPU 315 的连接资源是 16，如表 2 所示。连接资源包括 PG 通讯、OP 通讯、S7 基本通讯和 S7 通讯的连接。PG 通讯至少预留一个连接，OP 通讯至少预留一个连接，有些 S7-300 CPU 还默认预留一些 S7 基本通讯的连接。

| Technical specifications (continued) | | | |
|--------------------------------------|---------------------|---------------------|---------------------|
| | 6ES7 414-2XK05-0AB0 | 6ES7 414-3XM05-0AB0 | 6ES7 414-3EM05-0AB0 |
| Number of connections | | | |
| • overall | 32 | 32 | 32 |

表 1

| Technical specifications (continued) | | | | |
|--------------------------------------|---------------------|---------------------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| | 6ES7 312-1AE13-0AB0 | 6ES7 314-1AG13-0AB0 | 6ES7 315-2AG10-0AB0 | 6ES7 315-2EH13-0AB0 |
| Number of connections | | | | |
| • overall | 6 | 12 | 16 | 16 |
| • usable for PG communication | 5 | 11 | 15 | 15; max. |
| • usable for OP communication | 5 | 11 | 15 | 15 |
| • usable for S7 basic communication | 2 | 8 | 12 | 14 |
| • usable for routing | | | 4 | X1 configured as 1) MPI: max. 10; 2) DP master: max. 24; 3) DP slave (active): max. 14; X2 configured as PROFINET: max. 24 |

表 2

S7-300 CPU 可以通过硬件组态设置预留的连接资源数，预留的连接资源其它连接类型不能占用。如图 13 所示：

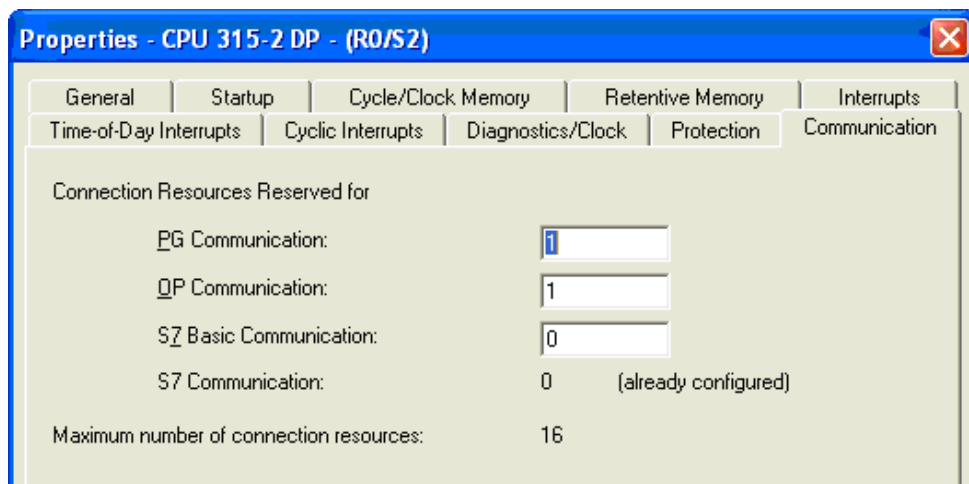


图 13: CPU 315-2 DP 的属性 “ Communication”

5. 2 CP 的连接资源

CP 也有连接资源，例如：CP 443-1 Advanced 的连接资源是 128，如表 3 所示；CP 343-1 的连接资源是 16，如表 4 所示。

| CP 443-1 Advanced | |
|-------------------------|----------|
| Performance data | |
| <u>S7 communication</u> | |
| • Number of connections | max. 128 |

表 3

| CP 343-1 | |
|-------------------------|---------|
| Performance data | |
| <u>S7 communication</u> | |
| • Number of connections | max. 16 |

表 4

5. 3 连接资源的占用

S7-300/400 CPU 可以通过其集成的接口或 CP 上的接口建立连接。

当 S7-400 CPU 通过 CP 接口建立连接时，不论是 Server 还是 Client，都占用 CPU 一个连接，占用 CP 一个连接。

当 S7-300 CPU 通过 CP 接口建立连接时，如果是 Server，那么占用 CPU 一个连接，占用 CP 一个连接；如果是 Client，那么仅占用 CP 一个连接，不单独占用 CPU 连接。整个 CP 仅占用 CPU 一个连接。

可以通过 CPU 的模版信息在线察看 CPU 连接资源的占用情况，如图 14 所示：

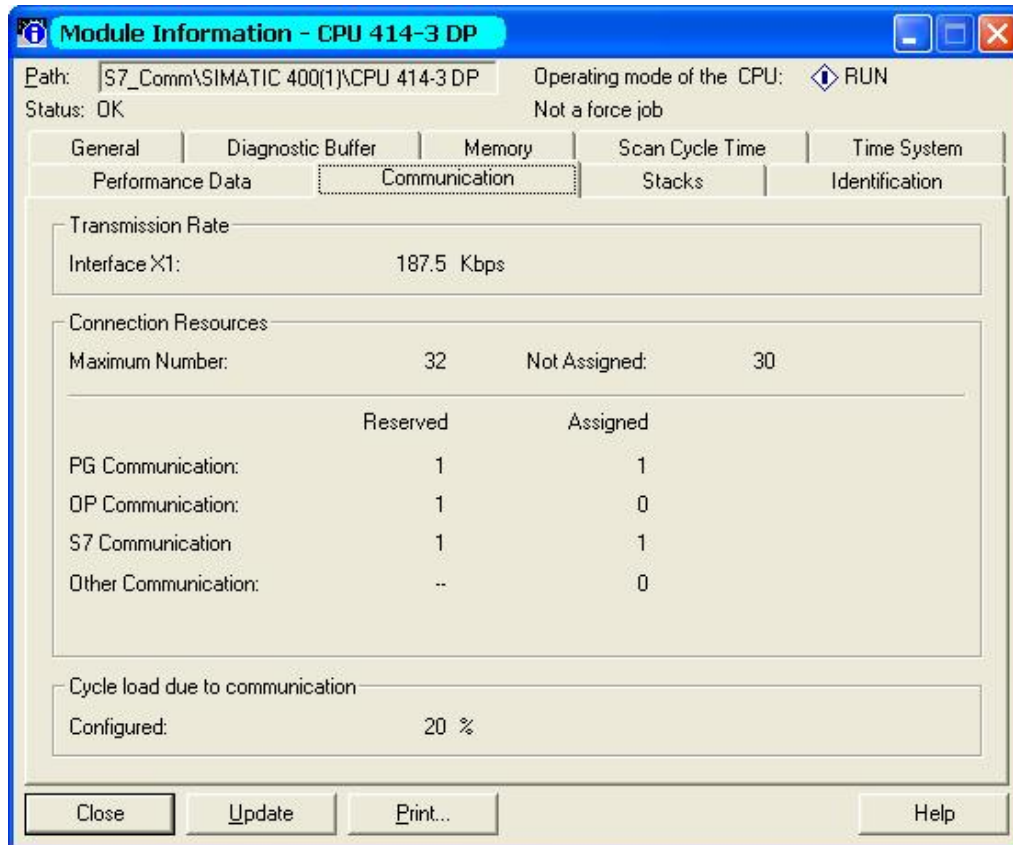



图 14: CPU 414-3 DP 的模板信息 “Communication”

6. 怎样建立与本项目或其它项目中 S7-300/400 通讯的单边连接（以 S7-300 侧为例）

从 SIMATIC Manager 或 HW Config 点击网络组态按钮  进入 NetPro 进行网络组态。

用鼠标选中 S7-300 的 CPU，窗口的下半部出现一个表格。在表格的空白处点击鼠标右键，选择 Insert New Connection，插入一个新连接。如图 15 所示：

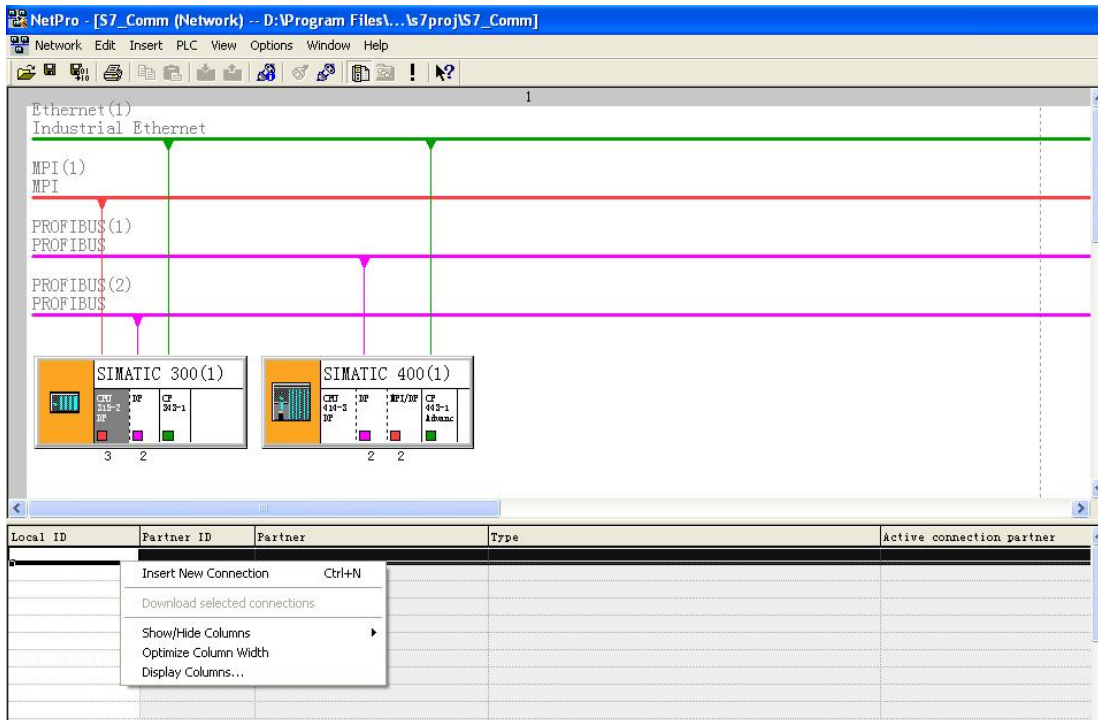


图 15: 在 NetPro 中组态 S7-300 CPU 的 S7-连接

选择 **Insert New Connection** 后弹出插入新连接对话框。

在插入新连接对话框“**Insert New Connection**”的 **Connection Partner** 中选择连接伙伴（**Unspecified**），在 **Connection Type** 中选择连接类型 **S7 connection**。如图 16 所示：

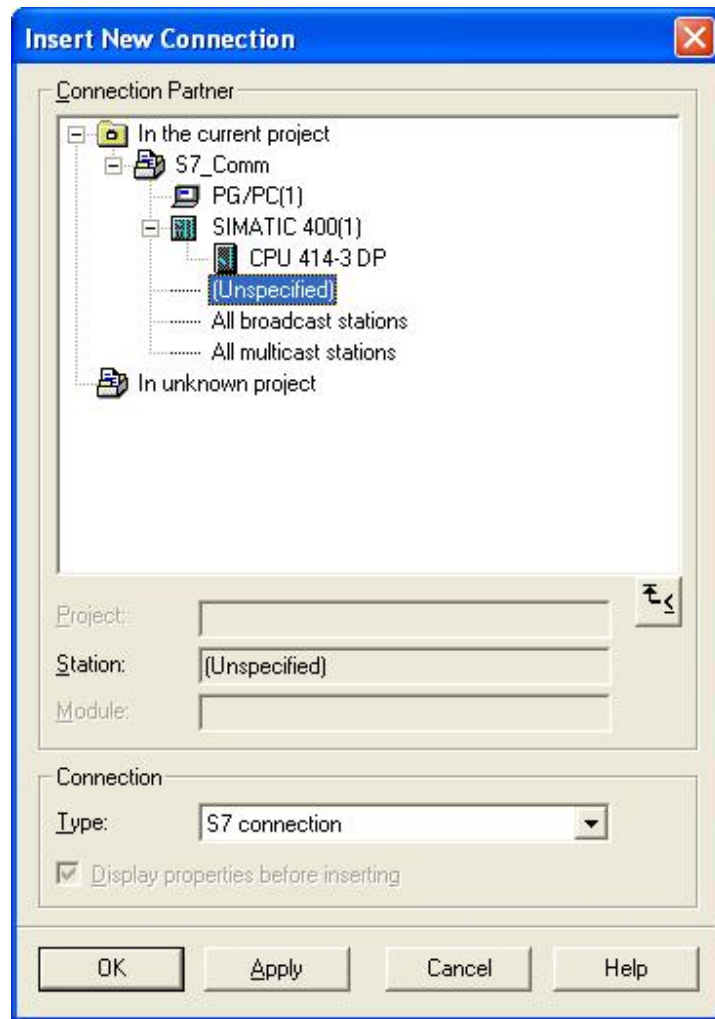


图 16: 为 S7-300 CPU 插入新的 S7 连接

点击 OK。

点击 OK 后，弹出 S7 connection 属性窗口，如图 17 所示：

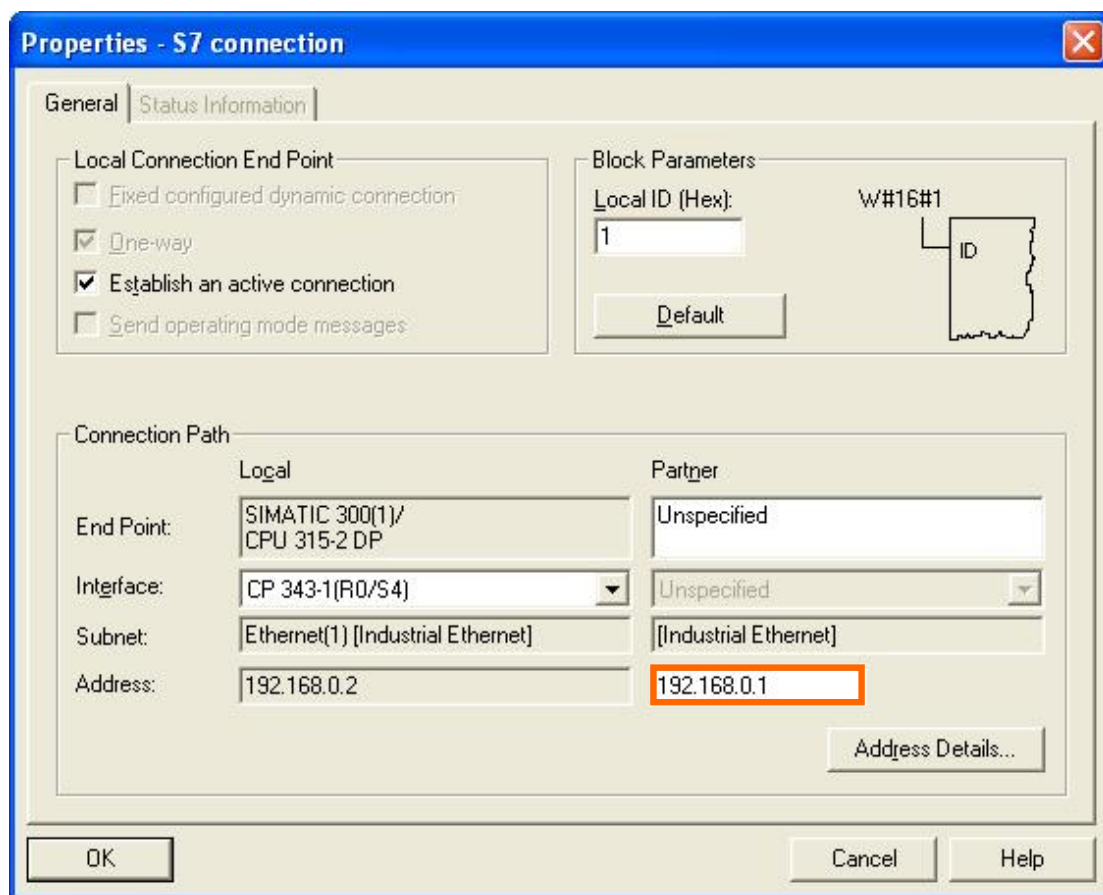


图 17: S7-300 CPU 的 S7 connection 属性，单边

窗口的左上角默认设置为单边（One-way），且不能更改。本地 CPU 作 Client，伙伴 CPU 作 Server，Client 访问 Server。可以利用单边功能块（GET, PUT）进行单边访问。保留选择“Establish an active connection（建立主动连接）”。右上角为调用 GET, PUT 功能块时的编程提示，提示编程时怎样填写 ID 输入端。“Partner”下方的“Address”需要填写伙伴地址，这里应填写 S7-400 CP 的地址：192.168.0.1，参见图 17（上面）。

用鼠标点击右下角的“Address Details...”按钮，填写伙伴的槽口号，如图 18 所示：

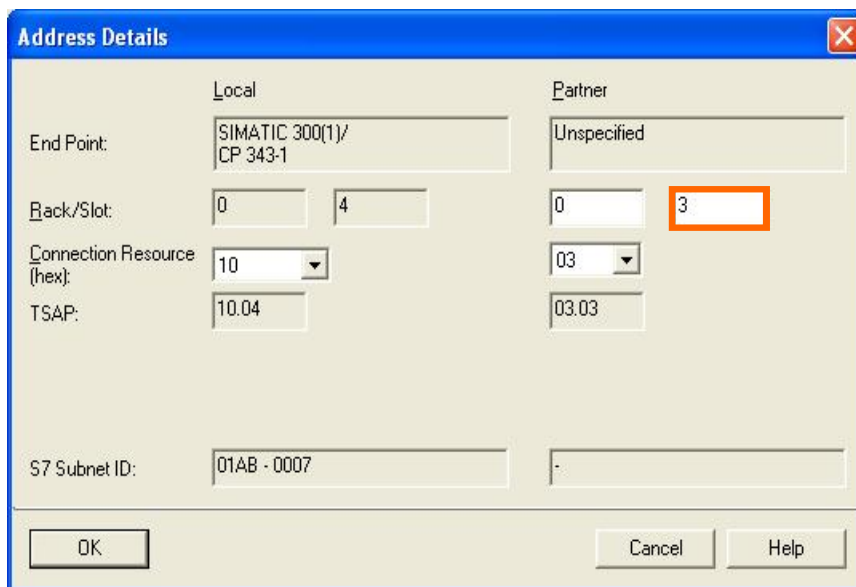




图 18: S7-300 CPU 的 S7 connection 的详细地址信息，单边（没有标出的区域为默认值）

这里伙伴的槽口号应填写 S7-400 CPU 的槽口号：3，连接资源号“Connection Resource” 03 表示自由连接，不指定具体的连接资源号（指定的连接资源号从 10 开始，十六进制）。与伙伴建立单边连接时，必须将伙伴的连接资源号选择成 03 自由连接，参见图 18（上面）。

关闭对话框，表格中出现一个连接：


| Local ID | Partner ID | Partner | Type | Active connection partner |
|----------|------------|---------|---------------|---------------------------|
| 1 | | Unknown | S7 connection | Yes |

伙伴 CPU 也占用一个连接，但不显示连接。伙伴 CPU 可以在也可以不在本项目中。

点击  存盘编译。然后选中本站，点击  将连接下载到本 CPU。建立单边连接时伙伴 CPU 无需建立连接，也无需下载。

提示： 单边连接只需客户端侧单边下载！

7. 怎样建立与其它项目中 S7-300/400 通讯的双边连接

从 SIMATIC Manager 或 HW Config 点击网络组态按钮  进入 NetPro 进行网络组态。

用鼠标选中 S7-300 的 CPU，窗口的下半部出现一个表格。在表格的空白处点击鼠标右键，选择 Insert New Connection，插入一个新连接。如图 19 所示：

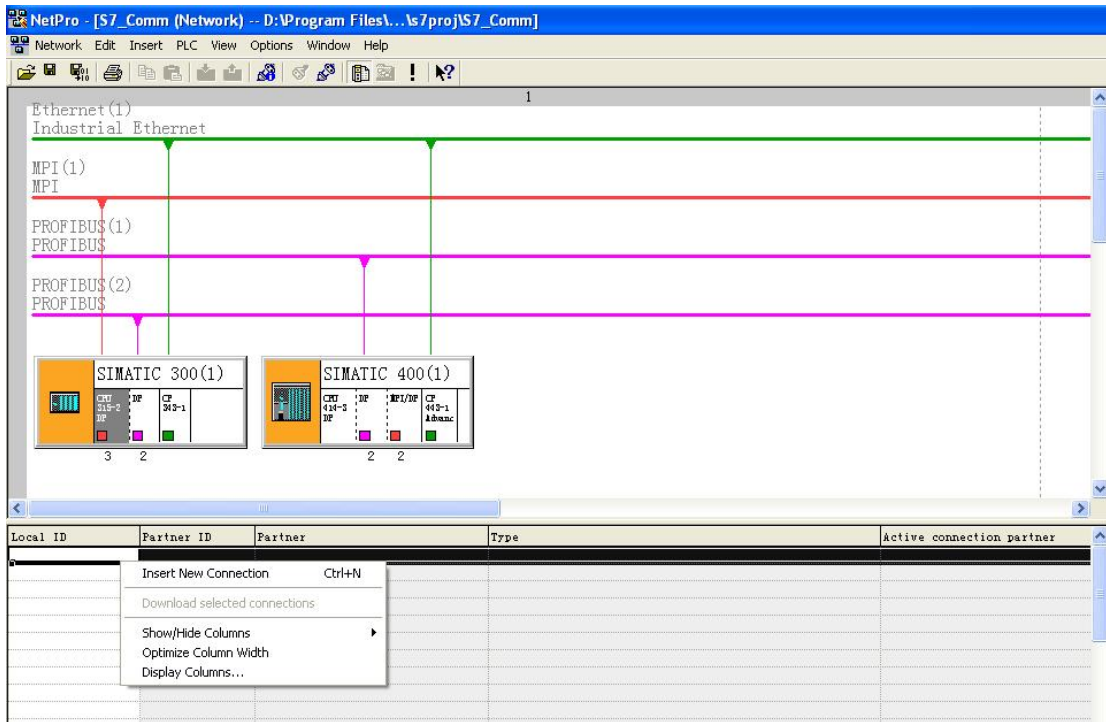


图 19: 在 NetPro 中组态 S7-300 CPU 的 S7-连接

选择 **Insert New Connection** 后弹出插入新连接对话框。

在插入新连接对话框“**Insert New Connection**”的 **Connection Partner** 中选择连接伙伴 (Unspecified)，在 **Connection Type** 中选择连接类型 **S7 connection**。如图 20 所示:

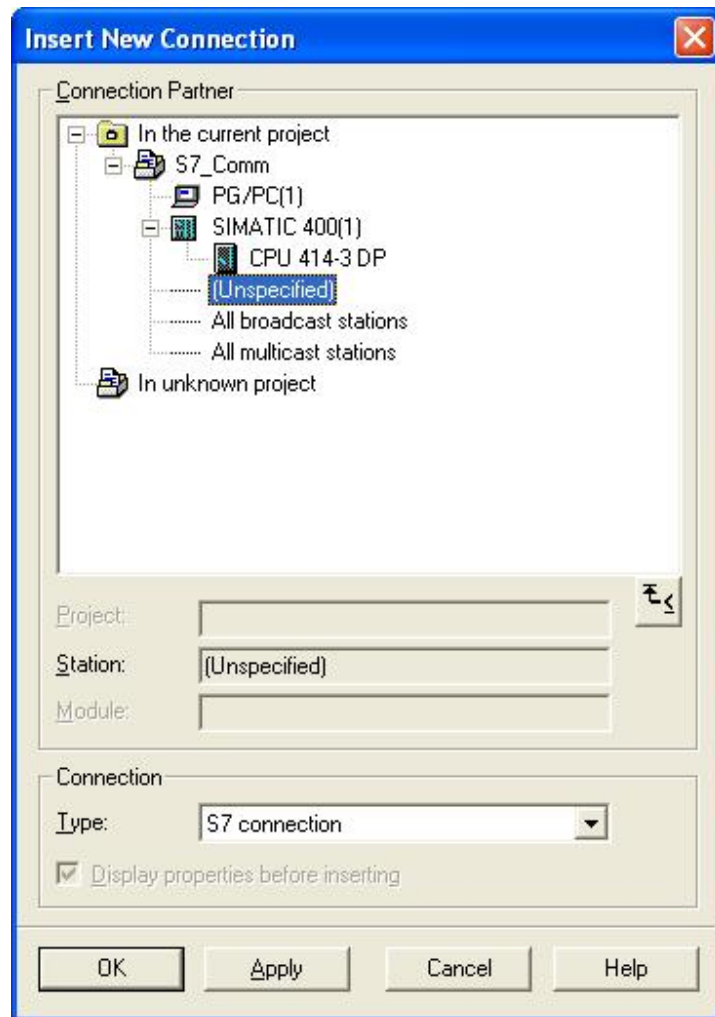


图 20: 为 S7-300 CPU 插入新的 S7 连接

点击 OK。

点击 OK 后，弹出 S7 connection 属性窗口，如图 21 所示：

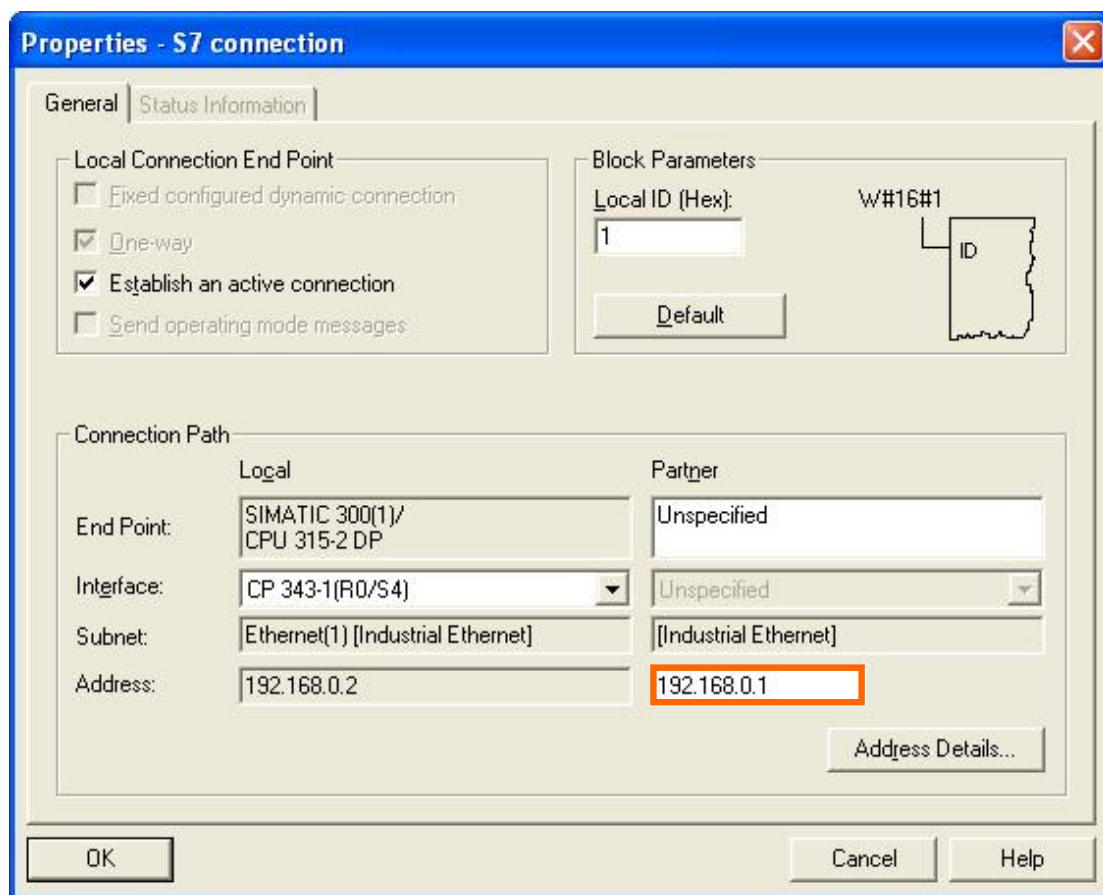


图 21: S7-300 CPU 的 S7 connection 属性，默认为单边

窗口的左上角默认设置为单边（One-way），且不能更改。本地 CPU 作 Client，伙伴 CPU 作 Server，Client 访问 Server。可以利用单边功能块（GET, PUT）进行单边访问。右上角为调用 GET, PUT 功能块时的编程提示，提示编程时怎样填写 ID 输入端。“Partner”下方的“Address”需要填写伙伴地址，这里应填写 S7-400 CP 的地址：192.168.0.1，参见图 21（上面）。

用鼠标点击右下角的“Address Details...”按钮，选择通讯伙伴的连接资源“Connection Resource (hex)”，填写通讯伙伴的槽口号和连接资源号，如图 22 所示：

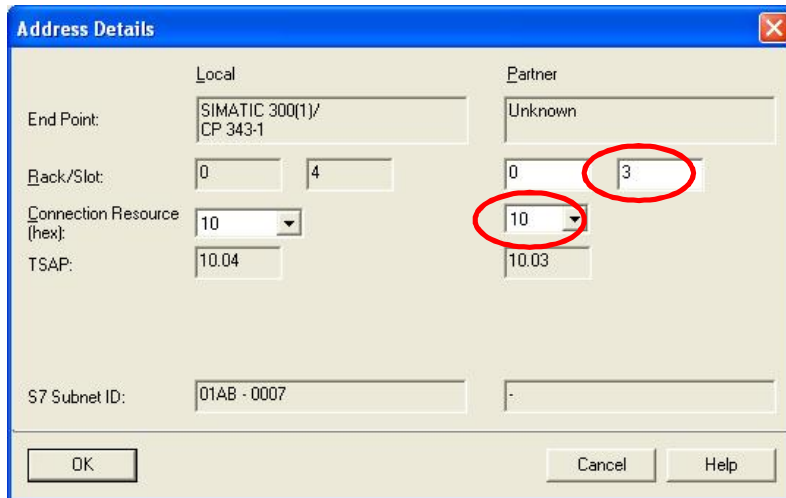


图 22: S7-300 CPU 的 S7 connection 的详细地址信息，双边（没有标出的区域为默认值）
 这里伙伴的槽口号和连接资源号应填写伙伴 CPU（S7-400 CPU）本地“Local”下方的槽口号：3，和连接资源号：10，参见图 22（上面）和图 23:

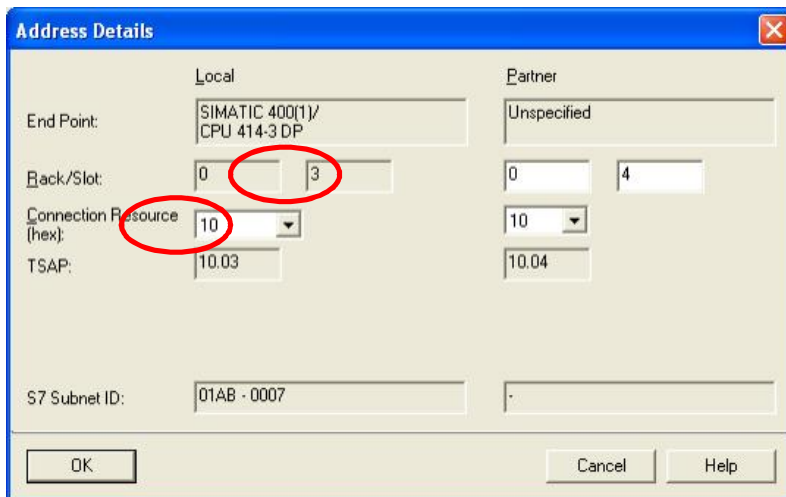


图 23: S7-400 CPU 的 S7 connection 详细地址信息，双边
 这里伙伴的槽口号和连接资源号应填写伙伴 CPU（S7-400 CPU）本地“Local”下方的槽口号：3，和连接资源号：10，参见图 22（上面）和图 23:

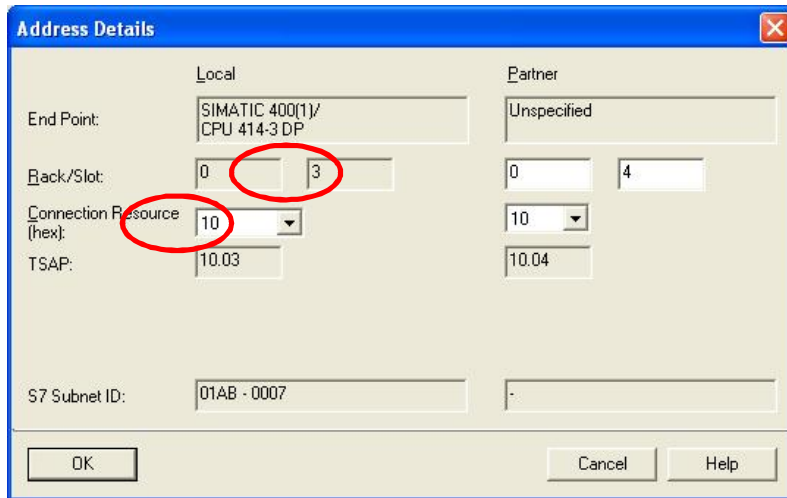


图 23: S7-400 CPU 的 S7 connection 详细地址信息，双边

若伙伴 CPU 也建立这样一个连接，则本地 CPU 和伙伴 CPU 既作 Client，又作 Server。不但可以利用单边功能块（GET, PUT）进行单边访问，而且可以利用双边功能块（BSEND/ BRCV, USEND/URCV）进行双边访问。

注意：双方只能有一方保留选择“Establish an active connection（建立主动连接）”，另一方必须取消选择。

关闭对话框，表格中出现一个连接：

| Local ID | Partner ID | Partner | Type | Active connection partner |
|----------|------------|---------|---------------|---------------------------|
| 1 | | Unknown | S7 connection | Yes |

伙伴 CPU 的连接（需要单独组态，操作同上）。

| Local ID | Partner ID | Partner | Type | Active connection partner |
|----------|------------|---------|---------------|---------------------------|
| 1 | | Unknown | S7 connection | No |

点击  存盘编译。然后选中本站，点击  将连接下载到本 CPU。伙伴 CPU 的操作相同。

提示：双边连接两个连接伙伴都需要下载！

8. 哪些接口支持 S7-Server，哪些接口支持 S7-Client

1. S7-Server 只能被动建立单边 S7 connection；S7-Client 可以主动建立单边 S7 connection，也可以与另一 S7-Client 建立双边 S7 connection。
2. 所有 S7-400 CPU 以及 CP 的接口都可以同时作 S7-Server 和 S7-Client。S7-400 CP 的接口可以看作是 CPU 接口的扩展。
3. S7-300 CPU 分成以下几种情况：

MPI 接口

- S7-300 CPU 的集成 MPI 接口只能作 S7-Server;

PROFIBUS 接口

- S7-300 CPU 的集成 PROFIBUS 接口只能作 S7-Server;
- S7-300 CPU V1.2 以上 + CP 342-5DA02 V5.0 以上的 PROFIBUS 接口可以同时作 S7-Server 和 S7-Client;

以太网接口

- S7-300 CPU 的集成 PN 接口可以同时作 S7-Server 和 S7-Client;
- S7-300 CPU + CP 343-1Lean 的以太网接口只能作 S7-Server;

S7-300 CPU V1.2 以上 + CP 343-1EX11 以上的以太网接口可以同时作 S7-Server 和 S7-Client。