四、西门子

1 西门子 S7-200 PPI 通讯协议

1.1 通信参数

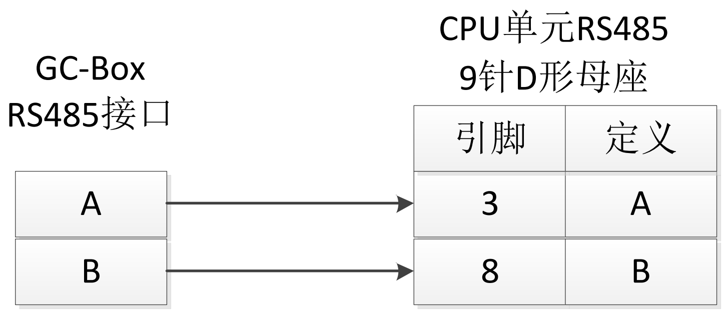
名称	取值	备注
串口号	/dev/ttyO4、/dev/ttyO5	默认/dev/ttyO4
波特率	9600、19200、187500	默认 9600
校验位	NONE、EVEN、ODD	默认 EVEN
数据位	8、7、6、5	默认 8
停止位	1、1.5、2	默认 1

PLC 远程站地址取值范围为 1～126，默认为 2，上位机的本地地址默认为 0。

1.2 通讯寻址类型

设备类型	范围	类型	权限	备注
输入映像寄存器 I	I0.0~I15.7	BIT	读取	
	IB0~IB15	BYTE		
	IW0~IW14	WORD		
	ID0~ID12	DWORD		
输出映像寄存器 Q	Q0.0~I15.7	BIT	读取/写入	
	QB0~QB15	BYTE		
	QW0~QW14	WORD		
	QD0~QD12	DWORD		
变量存储器 V	V0.0~I5119.7	BIT	读取/写入	
	VB0~VB5119	BYTE		
	VW0~VW5118	WORD		
	VD0~VD5116	DWORD		
位存储器 M	M0.0~M31.7	BIT	读取/写入	
	MB0~MB31	BYTE		
	MW0~MW30	WORD		
	MD0~MD28	DWORD		
顺序控制继电器 S	S0.0~S31.7	BIT	读取	
	SB0~SB31	BYTE		
	SW0~SW30	WORD		
	SD0~SD28	DWORD		
特殊存储器 SM	SM0.0~SM179.7	BIT	读取/写入	从地址 0 开始的前 30 个字节为只读区
	SM0~SM179	BYTE		
	SMW0~SMW178	WORD		
	SMD0~SMD176	DWORD		
定时器 T	T0~T255	BIT	读取	暂时不可写入
	T0~T255	WORD	读取/写入	
计数器 C	C0~C255	BIT	读取	暂时不可写入
	C0~C255	WORD	读取/写入	
模拟输入 AI	AIW0~AIW30	WORD	读取	
模拟输出 AQ	AQW0~AQW30	WORD	读取	

1.3 电缆制作



GC-Box
RS485接口

A
B

CPU单元RS485
9针D形母座

引脚	定义
3	A
8	B

2 西门子以太网通讯协议

2.1 概述

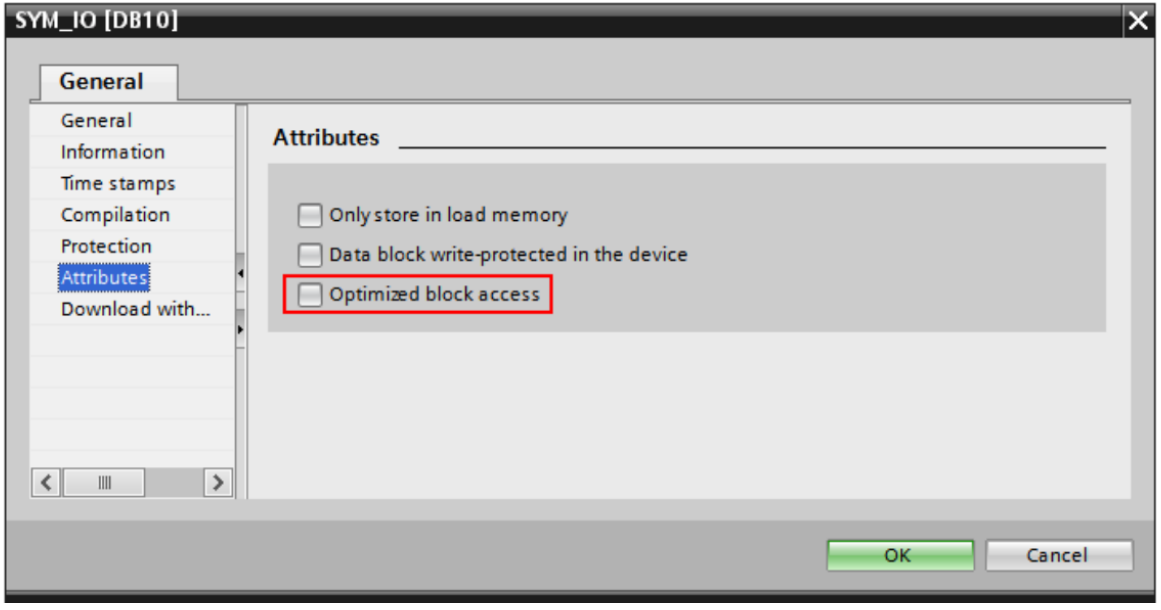
西门子 S7 的 S7-Ethernet 通讯协议与 S7 各个子型号 PLC 通过网口进行连接，支持 S7-300/400/WinAC/1200/1500 等。协议兼容性列表：

	CPU					CP
	300	400	WinAC	1200	1500	343/443
DB 读写	√	√	√	√	√	
EB 读写	√	√	√	√	√	
AB 读写	√	√	√	√	√	
MK 读写	√	√	√	√	√	
CT 读写	√	√	√			
TM 读写	√	√	√			

S7-1200/1500 注意事项：

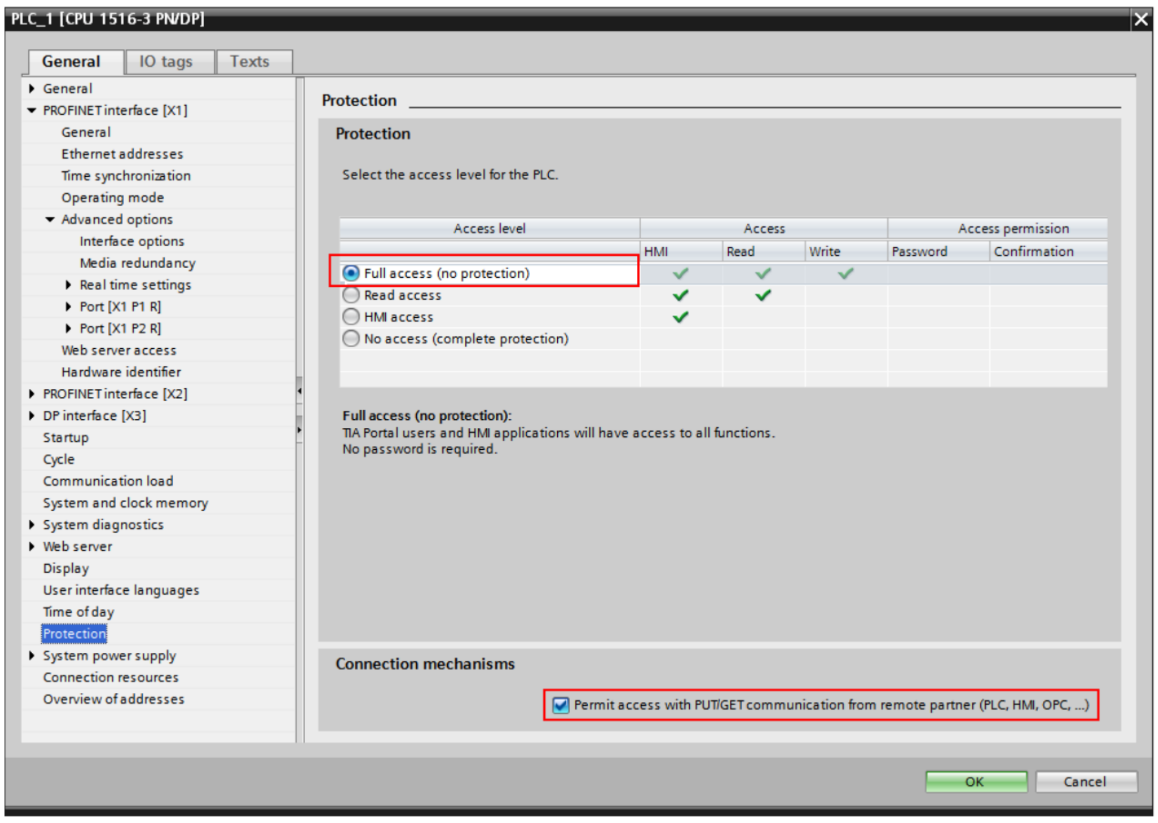
1、S7-1200/1500 只有设置 HMI 接入且只能支持基本的数据传输。特别是 S7-1500 中的 DB 块应该设置为全局，访问权限为完全控制。

2、选择程序块中的 DB，右键选择属性，取消“Optimized block access”选项。



□ Only store in load memory
□ Data block write-protected in the device
□ Optimized block access

3、选择 CPU，右键选择属性，选择左侧的“Protection”条目，选择右侧的“Full access(no protection)”，并将勾选“Permit access with PUT/GET comunication from remote partner(PLC,HMI,OPC,…)”



Select the access level for the PLC.

Access level	Access			Access permission	
	HMI	Read	Write	Password	Confirmation
● Full access (no protection)	✓	✓	✓		
○ Read access	✓	✓			
○ HMI access	✓				
○ No access (complete protection)					

Full access (no protection):
TIA Portal users and HMI applications will have access to all functions.
No password is required.

☑ Permit access with PUT/GET communication from remote partner (PLC, HMI, OPC, ...)

2.2 通讯参数

2.2.1 通用通讯参数

名称	取值	备注
IP	192.168.100.254	局域网中的 PLC 地址
Rack	0	参考说明
Slot	0	参考说明

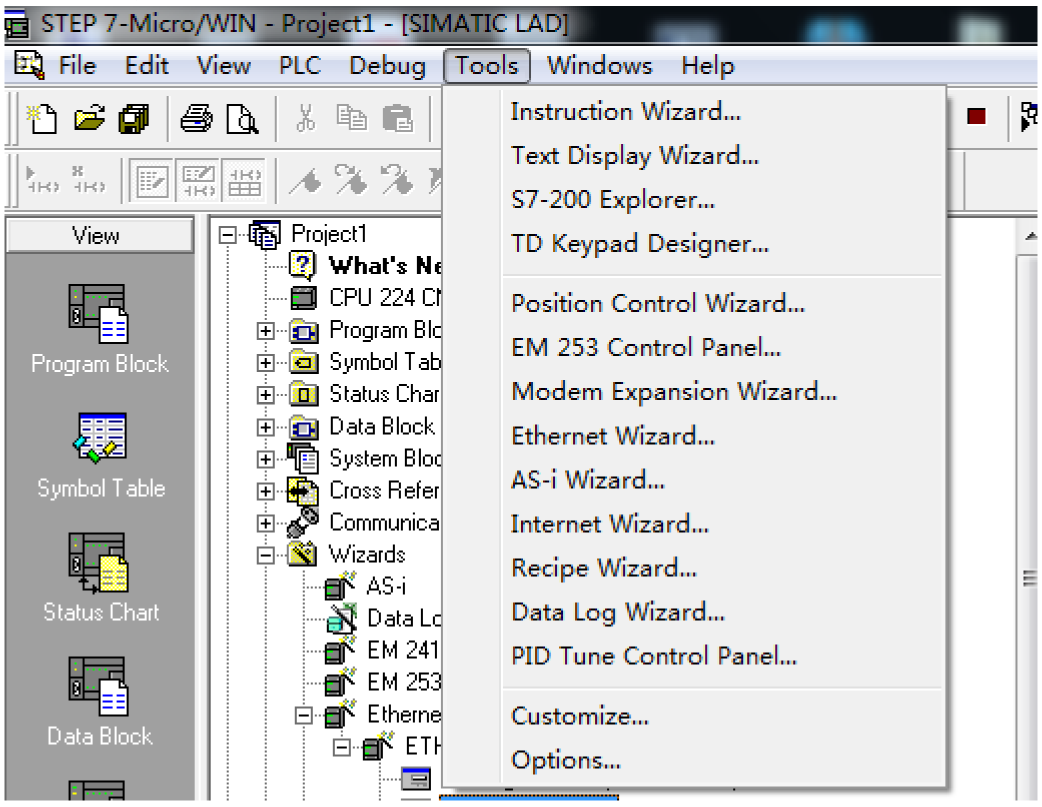
Rack 和 slot 的默认参数如下：

	Rack	Slot	
S7-300	0	2	固定
S7-400	不固定		和硬件配置保持一致
WinAC			和硬件配置保持一致
S7-1200	0	0	或者 0，1
S7-1500	0	0	或者 0，1
S7-200	0	0	

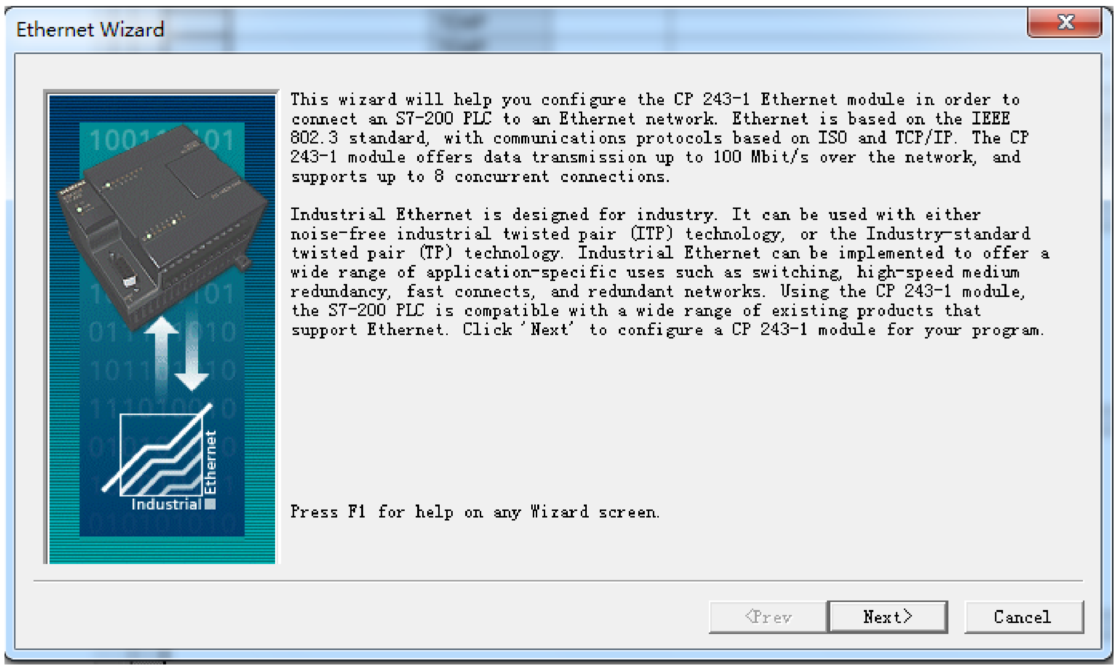
2.2.2 CP243-1 以太网通讯的设置

在 S7-200 PLC 的编程软件中，使用以太网向导，设置以太网模块 CP243-1，使之作为服务器端，具体设置步骤如下：

1、打开 PLC 应用程序→工具→以太网向导，如下图



2、 单击以太网向导,弹出画面如下图。

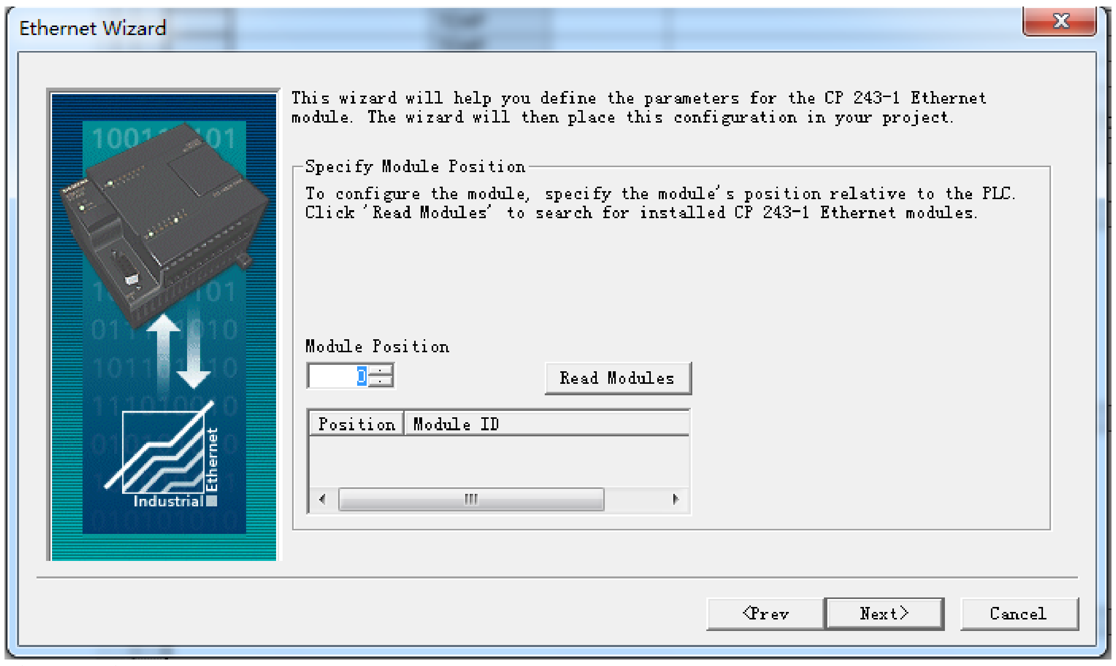


This wizard will help you configure the CP 243-1 Ethernet module in order to connect an S7-200 PLC to an Ethernet network. Ethernet is based on the IEEE 802.3 standard, with communications protocols based on ISO and TCP/IP. The CP 243-1 module offers data transmission up to 100 Mbit/s over the network, and supports up to 8 concurrent connections.

Industrial Ethernet is designed for industry. It can be used with either noise-free industrial twisted pair (ITP) technology, or the Industry-standard twisted pair (TP) technology. Industrial Ethernet can be implemented to offer a wide range of application-specific uses such as switching, high-speed medium redundancy, fast connects, and redundant networks. Using the CP 243-1 module, the S7-200 PLC is compatible with a wide range of existing products that support Ethernet. Click 'Next' to configure a CP 243-1 module for your program.

Press F1 for help on any Wizard screen.

3、直接单击“下一步”，如下图，单击“读取模块”，得到模块的相关信息，注意：模块位置是相对于 PLC 的位置，从索引 0 开始的，一定要与读取模块的位置信息相对应。



This wizard will help you define the parameters for the CP 243-1 Ethernet module. The wizard will then place this configuration in your project.

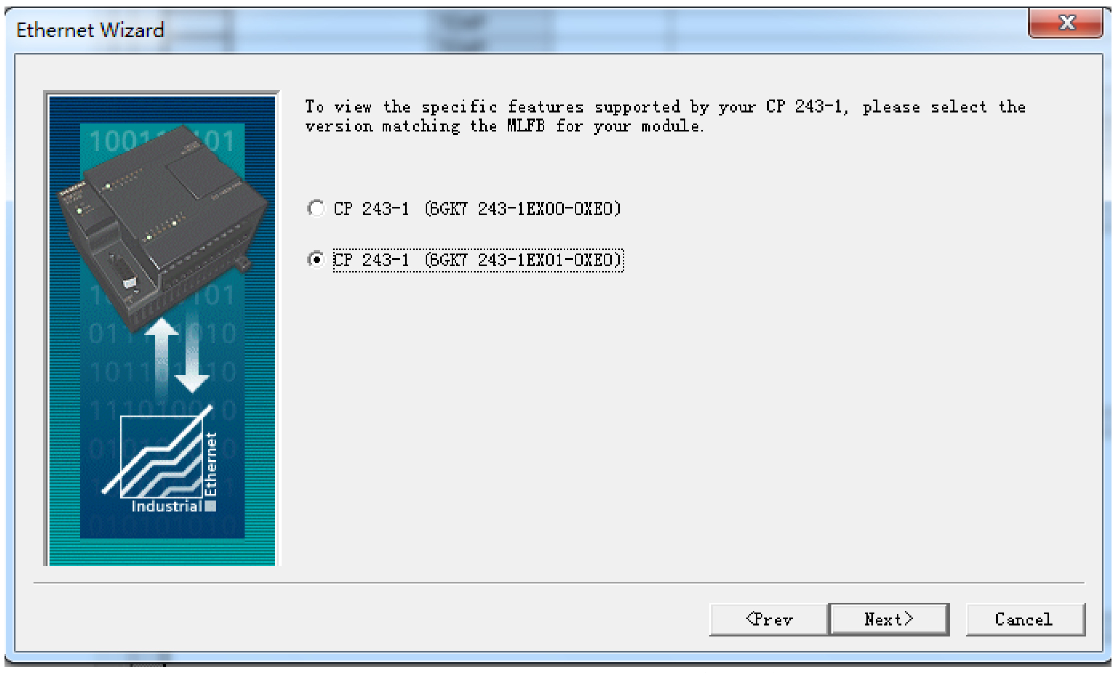
Specify Module Position

To configure the module, specify the module's position relative to the PLC. Click 'Read Modules' to search for installed CP 243-1 Ethernet modules.

Module Position: 0

Position	Module ID

4、 点击下一步，选择选择模块的版本号

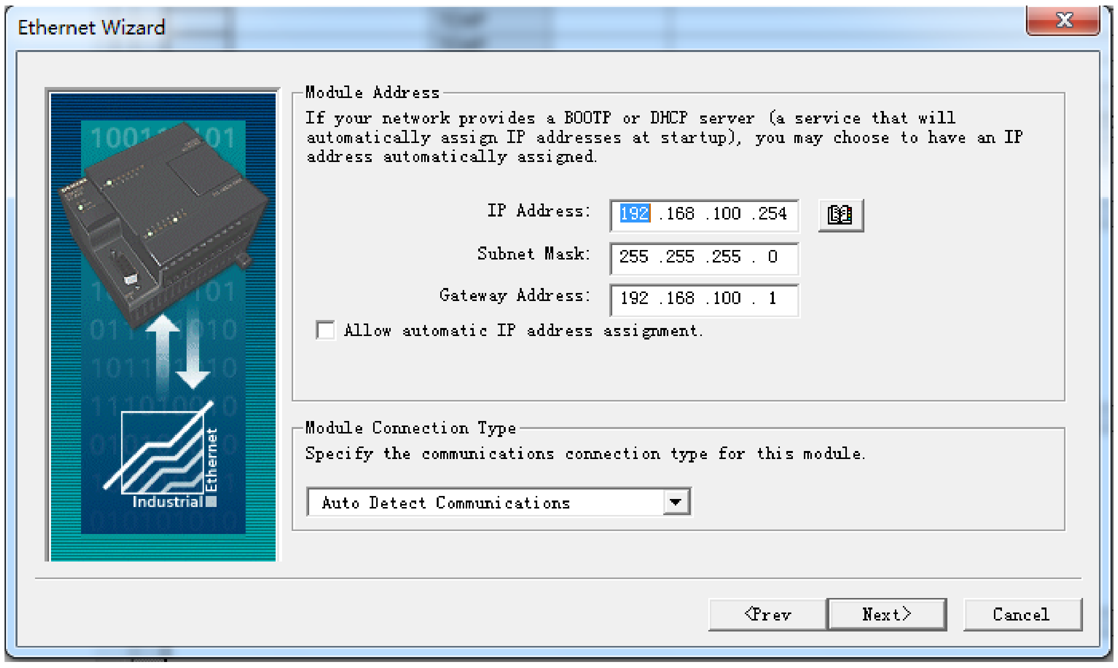


To view the specific features supported by your CP 243-1, please select the version matching the MLFB for your module.

○ CP 243-1 (6GK7 243-1EX00-0XE0)

● CP 243-1 (6GK7 243-1EX01-0XE0)

5、 再单击“下一步”，如下图，分别填入 IP 地址，子网掩码，网关地址。注意正确填写网段。



Module Address

If your network provides a BOOTP or DHCP server (a service that will automatically assign IP addresses at startup), you may choose to have an IP address automatically assigned.

IP Address: 192 .168 .100 .254

Subnet Mask: 255 .255 .255 . 0

Gateway Address: 192 .168 .100 . 1

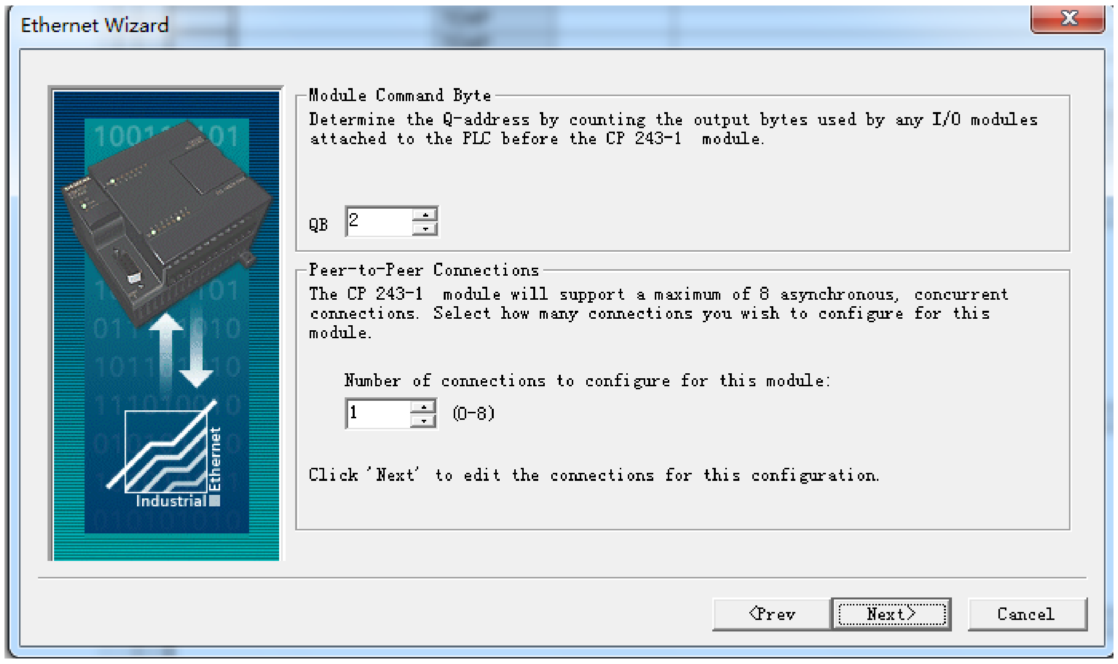
□ Allow automatic IP address assignment.

Module Connection Type

Specify the communications connection type for this module.

Auto Detect Communications

6、 再单击“下一步”，如下图，填写为模块配置的连接数目。



Module Command Byte

Determine the Q-address by counting the output bytes used by any I/O modules attached to the PLC before the CP 243-1 module.

QB 2

Peer-to-Peer Connections

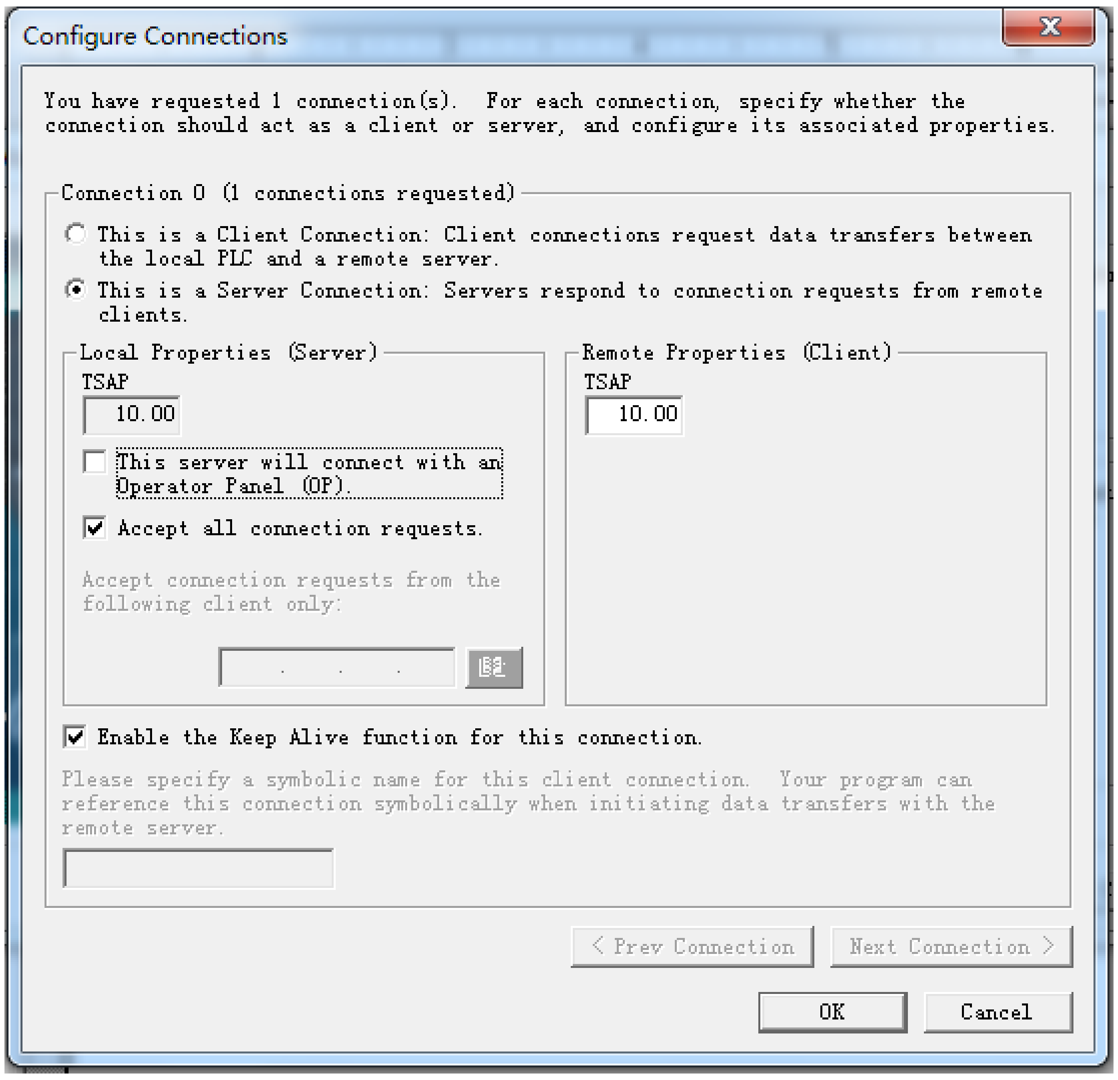
The CP 243-1 module will support a maximum of 8 asynchronous, concurrent connections. Select how many connections you wish to configure for this module.

Number of connections to configure for this module:

1 (0-8)

Click 'Next' to edit the connections for this configuration.

7、 再单击“下一步”，如图下图，设置本地和远程 TSAP。 其他选项按照两图中任一一个勾选。



Configure Connections

You have requested 1 connection(s). For each connection, specify whether the connection should act as a client or server, and configure its associated properties.

Connection 0 (1 connections requested)

○ This is a Client Connection: Client connections request data transfers between the local PLC and a remote server.

● This is a Server Connection: Servers respond to connection requests from remote clients.

Local Properties (Server)

TSAP 10.00

□ This server will connect with an Operator Panel (OP).

☑ Accept all connection requests.

Accept connection requests from the following client only:

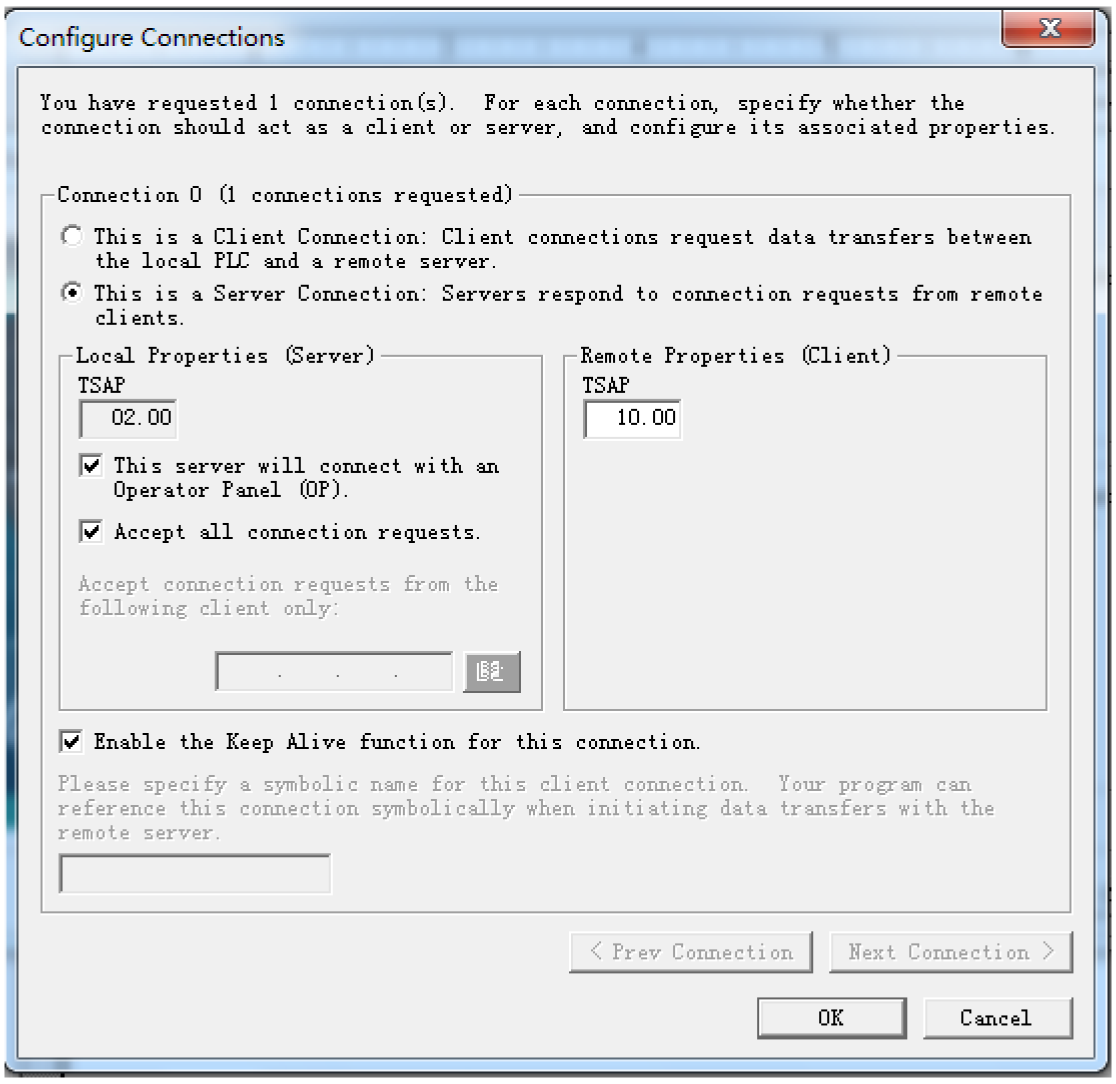
Remote Properties (Client)

TSAP 10.00

☑ Enable the Keep Alive function for this connection.

Please specify a symbolic name for this client connection. Your program can reference this connection symbolically when initiating data transfers with the remote server.

或者



Configure Connections

You have requested 1 connection(s). For each connection, specify whether the connection should act as a client or server, and configure its associated properties.

Connection 0 (1 connections requested)

○ This is a Client Connection: Client connections request data transfers between the local PLC and a remote server.

● This is a Server Connection: Servers respond to connection requests from remote clients.

Local Properties (Server)

TSAP 02.00

☑ This server will connect with an Operator Panel (OP).

☑ Accept all connection requests.

Accept connection requests from the following client only:

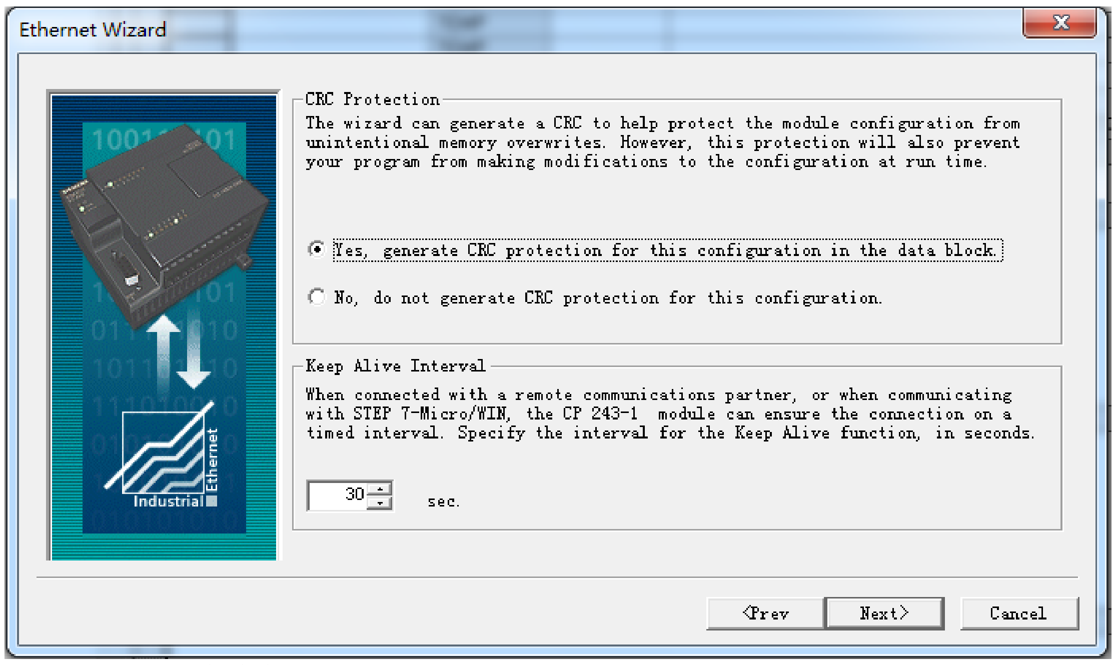
Remote Properties (Client)

TSAP 10.00

☑ Enable the Keep Alive function for this connection.

Please specify a symbolic name for this client connection. Your program can reference this connection symbolically when initiating data transfers with the remote server.

8、再单击“下一步”，如下图，不用填写。



Ethernet Wizard

CRC Protection

The wizard can generate a CRC to help protect the module configuration from unintentional memory overwrites. However, this protection will also prevent your program from making modifications to the configuration at run time.

● Yes, generate CRC protection for this configuration in the data block.

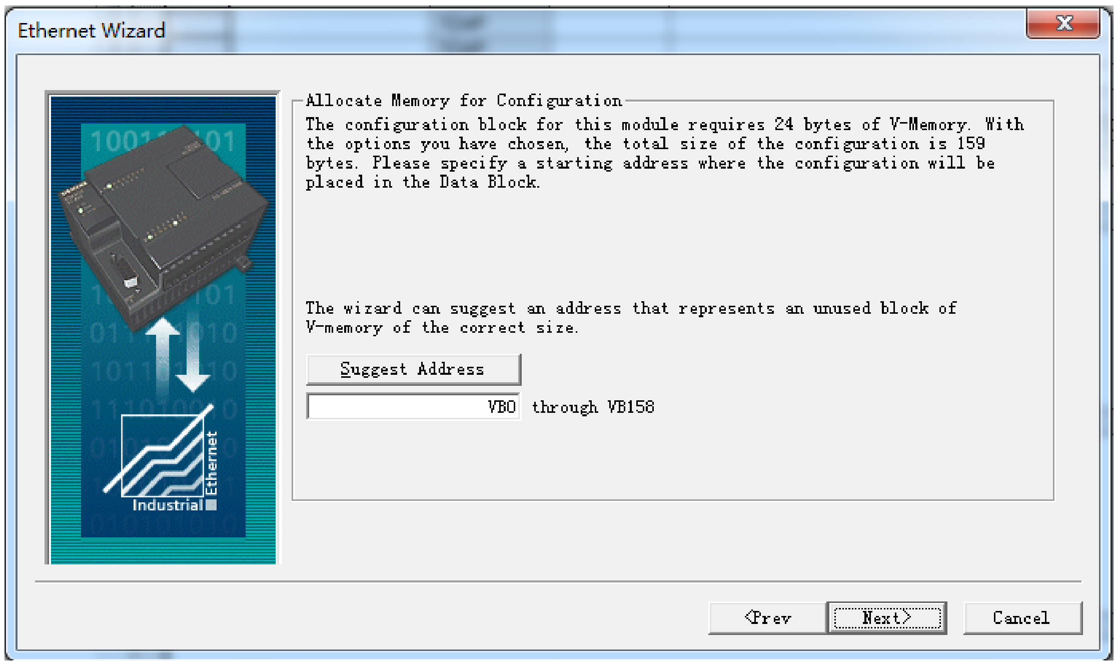
○ No, do not generate CRC protection for this configuration.

Keep Alive Interval

When connected with a remote communications partner, or when communicating with STEP 7-Micro/WIN, the CP 243-1 module can ensure the connection on a timed interval. Specify the interval for the Keep Alive function, in seconds.

30 sec.

9、 再单击“下一步”，如下图，填入程序中为使用的 VB 区首地址，选择建议地址。



Ethernet Wizard

Allocate Memory for Configuration

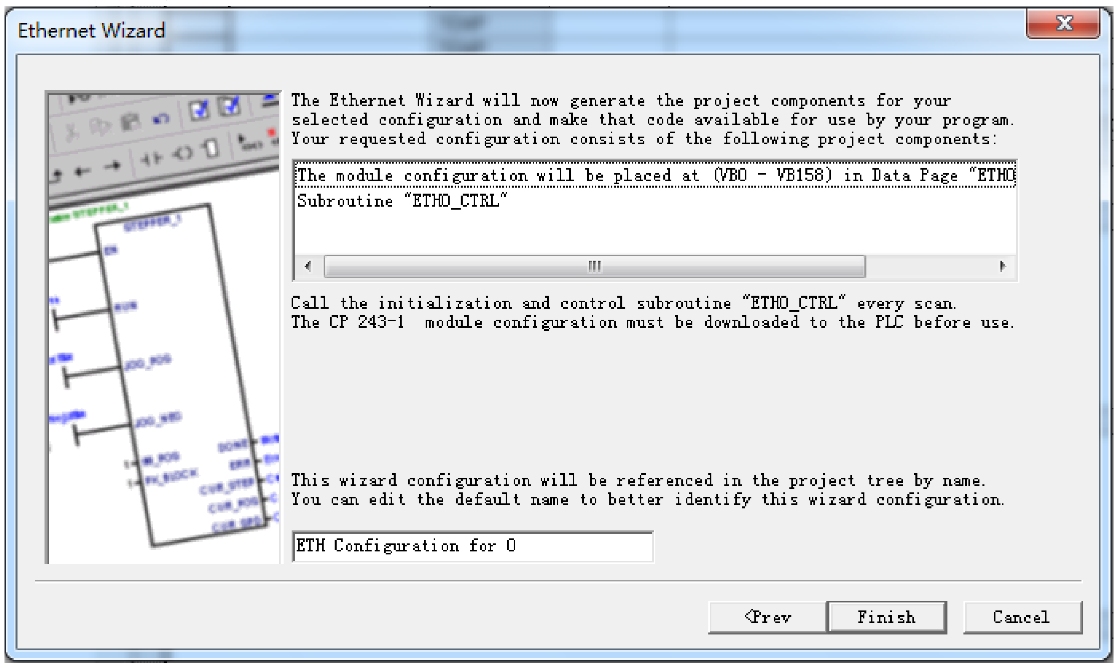
The configuration block for this module requires 24 bytes of V-Memory. With the options you have chosen, the total size of the configuration is 159 bytes. Please specify a starting address where the configuration will be placed in the Data Block.

The wizard can suggest an address that represents an unused block of V-memory of the correct size.

Suggest Address

VB0 through VB158

10、再单击“下一步”，如下图，单击“完成”。



Ethernet Wizard

The Ethernet Wizard will now generate the project components for your selected configuration and make that code available for use by your program. Your requested configuration consists of the following project components:

The module configuration will be placed at (VB0 - VB158) in Data Page "ETH0
Subroutine "ETH0_CTRL"

Call the initialization and control subroutine "ETH0_CTRL" every scan. The CP 243-1 module configuration must be downloaded to the PLC before use.

This wizard configuration will be referenced in the project tree by name. You can edit the default name to better identify this wizard configuration.

ETH Configuration for 0

11、将设置的模块参数下载到 PLC，并断电重启 PLC 生效。

12、将 GC-Box的网络设置和 CP243-1 以太网模块在同一个局域网中，并重启盒子。

13、在 GC-Box上建立西门子以太网采集通道，注意通道参数设置的 IP 地址，本地 TSAP，远程 TSAP 三个参数要于 CP243-1 模块中的相关参数一一对应。

14、添加设备、添加数据项，下发，测试。如果数据项测试 good，表示通信正常，数据采集成功；否则，请检查 CP243-1 模块和 GC-Box 相关通信参数的设置、数据项的地址等信息是否正确。

2.3 通讯寻址类型

表 2 对象标识总表

设备类型	范围	类型	权限	备注
输入映像寄存器 I	I0.0~I65535.7	BIT	读取	
	IB0~IB65535	BYTE		
	IW0~IW65534	WORD		
	ID0~ID65532	DWORD		
输出映像寄存器 Q	Q0.0~Q65535.7	BIT	读取/写入	
	QB0~QB65535	BYTE		
	QW0~QW65534	WORD		
	QD0~QD65532	DWORD		

本地数据 L	L0.0~L65535.5	BIT	读取/写入	
	LB0~LB65535	BYTE		
	LW0~LW6554	WORD		
	LD0~LD6552	DWORD		
位存储器 M	M0.0~M255.7	BIT	读取/写入	
	MB0~MB255	BYTE		
	MW0~MW254	WORD		
	MD0~MD252	DWORD		
存储器 V	V0.0~V255.7	BIT	读取/写入	该区域只针对 200/SMART200 谢列，旧版本需要进行映射： Vm.n->DB1.DBXm.n VBm->DB1.DBBm VWm->DB1.DBWm VDm->DB1.DBDm
	VB0~VB255	BYTE		
	VW0~VW254	WORD		
	VD0~VD252	DWORD		
数据块 DB	DBX0.0~ DBX65535.7	BIT	读取	该区域的格式: DBx.DBX DBx.DBW DBx.DBD 注意 x 是 DB 块的编号
	DBB0~ DBB65535	BYTE		
	DBW0~ DBW65534	WORD		
	DBD0~ DBD65532	DWORD		
定时器 T	T0~T255	BIT	读取	
	T0~T255	WORD	读取/写入	
计数器 C	C0~C255	BIT	读取	
	C0~C255	WORD	读取/写入	

注意：上述各个寄存器地址范围只是示例，具体范围大小是根据实际的硬件确定的，不限于上述范围。

3 西门子 *S7-300/S7-400*

3.1 通讯参数

名称	取值	备注
串口号	COM1	
波特率	9600/19200/115200	默认 9600
网络传输速率	9K/19K/187K/500K	默认 187K

3.2 通讯寻址类型

表 2 对象标识总表

设备类型	范围	类型	权限	备注
输入映像寄存器 I	I0.0~I65535.7	BIT	读取	
	IB0~IB65535	BYTE		
	IW0~IW65534	WORD		
	ID0~ID65532	DWORD		
输出映像寄存器 Q	Q0.0~Q65535.7	BIT	读取/写入	
	QB0~QB65535	BYTE		
	QW0~QW65534	WORD		
	QD0~QD65532	DWORD		
本地数据 L	L0.0~L65535.5	BIT	读取/写入	
	LB0~LB65535	BYTE		
	LW0~LW6554	WORD		
	LD0~LD6552	DWORD		
位存储器 M	M0.0~M255.7	BIT	读取/写入	
	MB0~MB255	BYTE		
	MW0~MW254	WORD		
	MD0~MD252	DWORD		
数据块 DB	DBX0.0~ DBX65535.7	BIT	读取	
	DBB0~ DBB65535	BYTE		
	DBW0~ DBW65534	WORD		
	DBD0~ DBD65532	DWORD		
数据块 DI	DIX0.0~ DIX65535.7	BIT	读取/写入	
	DIB0~DIB65535	BYTE		
	DIW0~DIW65534	WORD		
	DID0~DID65532	DWORD		
定时器 T	T0~T255	BIT	读取	暂时不可写入
	T0~T255	WORD	读取/写入	

计数器 C	C0~C255	BIT	读取	暂时不可写入
	C0~C255	WORD	读取/写入	
变量存储器 V	V0.0~I5119.7	BIT	读取/写入	
	VB0~VB5119	BYTE		
	VW0~VW5118	WORD		
	VD0~VD5116	DWORD		

3.3 PLC 远程站地址

PLC 远程站地址取值范围为 1～126，默认为 2。

3.4 设备类型

系列名	CPU 单元	连接模组	通讯类型	电缆制作	GC-Box中 PLC 型号
S7-300 系列	CPU312 CPU314 CPU315	CPU 单元直接连接	RS485	图 1	
S7-400 系列	CPU412-1 CPU412-2 CPU414-2		RS232	图 2	

3.5 电缆制作

与 S7-300/400 通讯采用 MPI 编程电缆 RS485 接线方式：

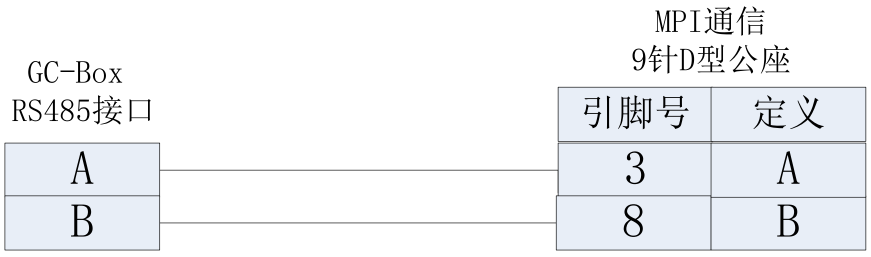


图 1

与 S7-300/400 通讯采用 MPI 编程电缆 RS232 接线方式：

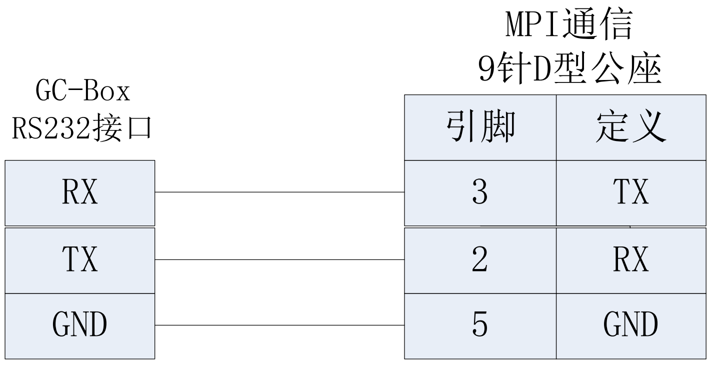


图 2