BT-ESM-P

快速启动手册

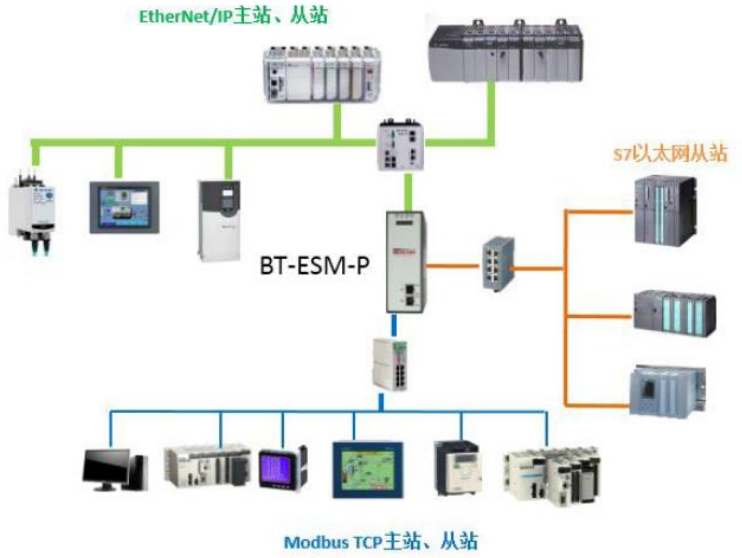
BEACON GLOBAL TECHNOLOGY

目录

模块简介：

BT-ESM-P系列网关是EtherNet/IP、Modbus TCP、Siemens S7以太网相互通讯的网关模块，支持在EtherNet/I、Modbus TCP和Siemens S7 Ethernet网络设备之间的双向数据交换，最大10000个16位字数据交换区。

- EtherNet/IP协议可支持通讯的典型设备主要有罗克韦尔1756系列、1769系列、1746系列、PLC-2系列、PLC-5系列、SLC500系列、Micrologix 系列PLC。以及PowerFlex系列变频器，E300智能马达保护器，PowerMonitor智能电力监控仪，上位机RSView SE软件等。
- S7以太网协议可支持通讯的典型设备为各类西门子PLC，包括S7-200，S7-300，S7-400，S7-1200，S7-1500，
- Modbus TCP协议可支持通讯的设备包括各种PLC, DCS, 上位机软件，数显仪表，传感器等。
- 三种以太网协议设备可在相同网段或者不同网段进行通讯。
- 不同以太网协议在同一个网段时，可选择模块上任意一个以太网接口和交换机连接（注意：不能同时把模块E1和E2接口设置成相同的网段），再把同一网段下两种协议的设备同时也接入交换机。
- 不同以太网协议设备如果在不同网段通讯时，需要选用模块的两个以太网口进行通讯，可把模块E1和E2设置成不同的网段，两种协议的设备分别接入E1和E2口即可。



E1 端口 == 可选择配置为设置为 3 种以太网协议，同时支持主从站
E2 端口 == 可选择配置为设置为 3 种以太网协议，同时支持主从站

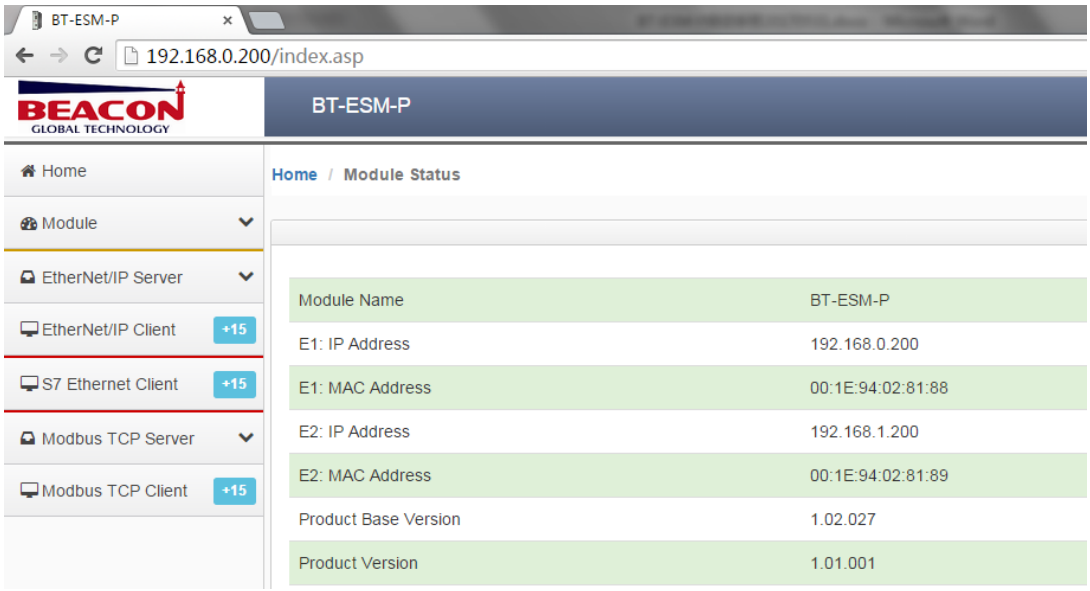
模块初始配置

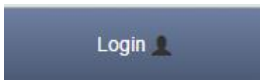
E1 以太网接口出厂 IP 地址为 192.168.0.200。模块上电后，OLED 显示屏上会滚动显示 IP 地址。

BT系列模块全部采用网页配置形式组态，无需安装其他多余的组态软件，推荐采用如下浏览器及以上版本（更好的支持HTML5的功能）对于模块进行配置：IE10，GOOGLE Chrome 35，FIREFOX 35，Safari 7 及以上的版本。

通过以太网配置模块：

1. 把本地电脑的IP地址与所连接的模块端口配置成相同的IP网段，例如本案例采用E1接口进行配置，本地电脑配置成192.168.0.177，然后在GOOGLE Chrome浏览器的地址框里面输入192.168.0.200，点击回车键后，进入到模块的配置页面如下图。



2. 在配置页面的导航条内，点击Login，将打开如图所示。 

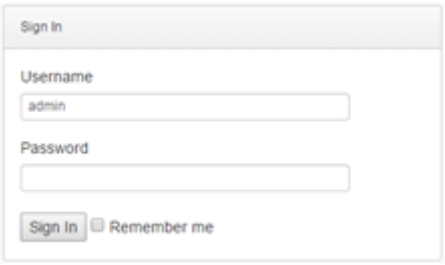
3. 按照界面提示，输入用户名和密码进入模块配置。

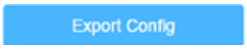
用户名(Username):admin

密码(Password): admin

点击登录(Sign In)

请注意：如果不登录，只能浏览配置，无法进行配置修改。

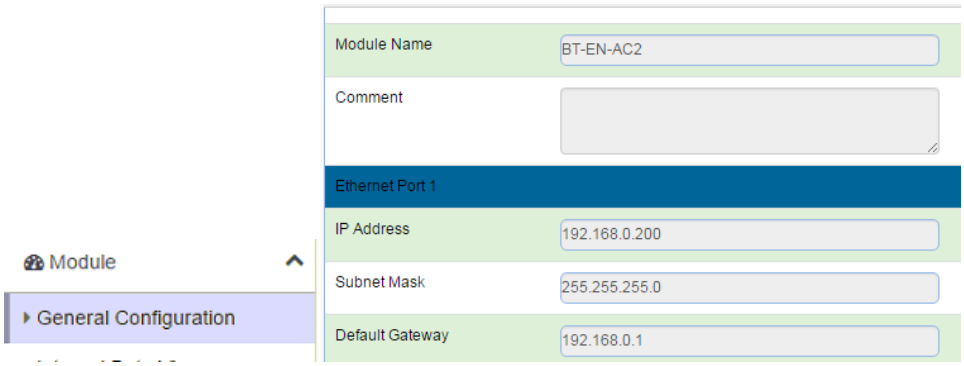


4. 登录后看到导出配置文件 

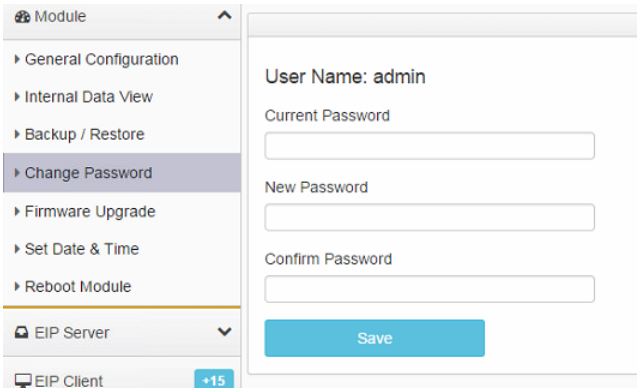
和恢复配置文件 

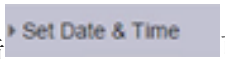
5. 查看模块 IP 地址，点击 

，修改模块的 IP 地址。

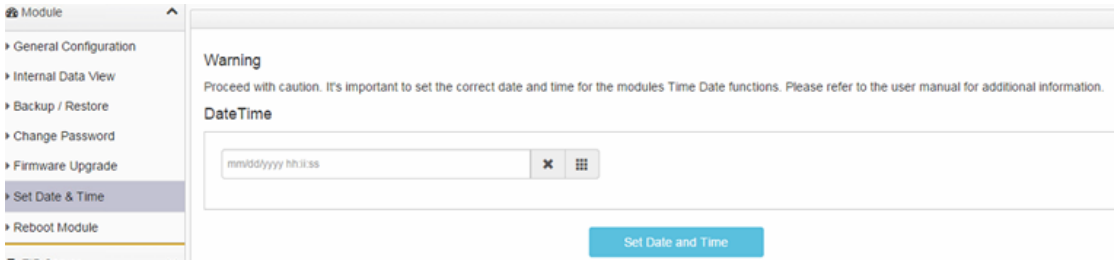


6. 点击修改密码，可以修改模块的登录密码。 

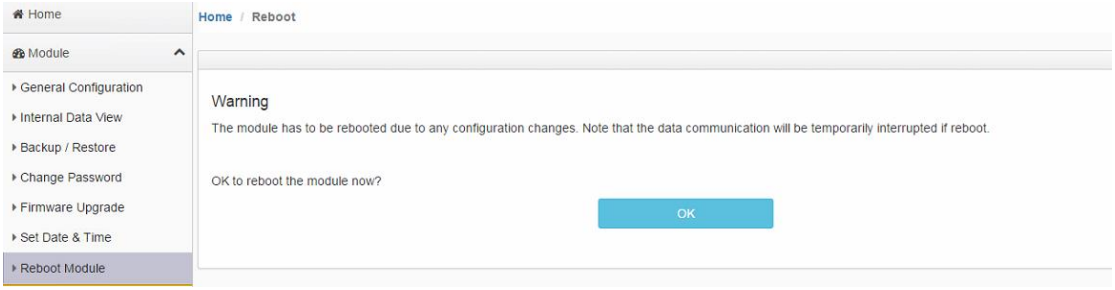


7. 点击 

可以设置模块的日期和时间。

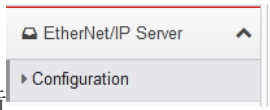


8. 点击 Reboot Module 表示重启模块。（不是复位）



配置模块做 EtherNet/IP Server

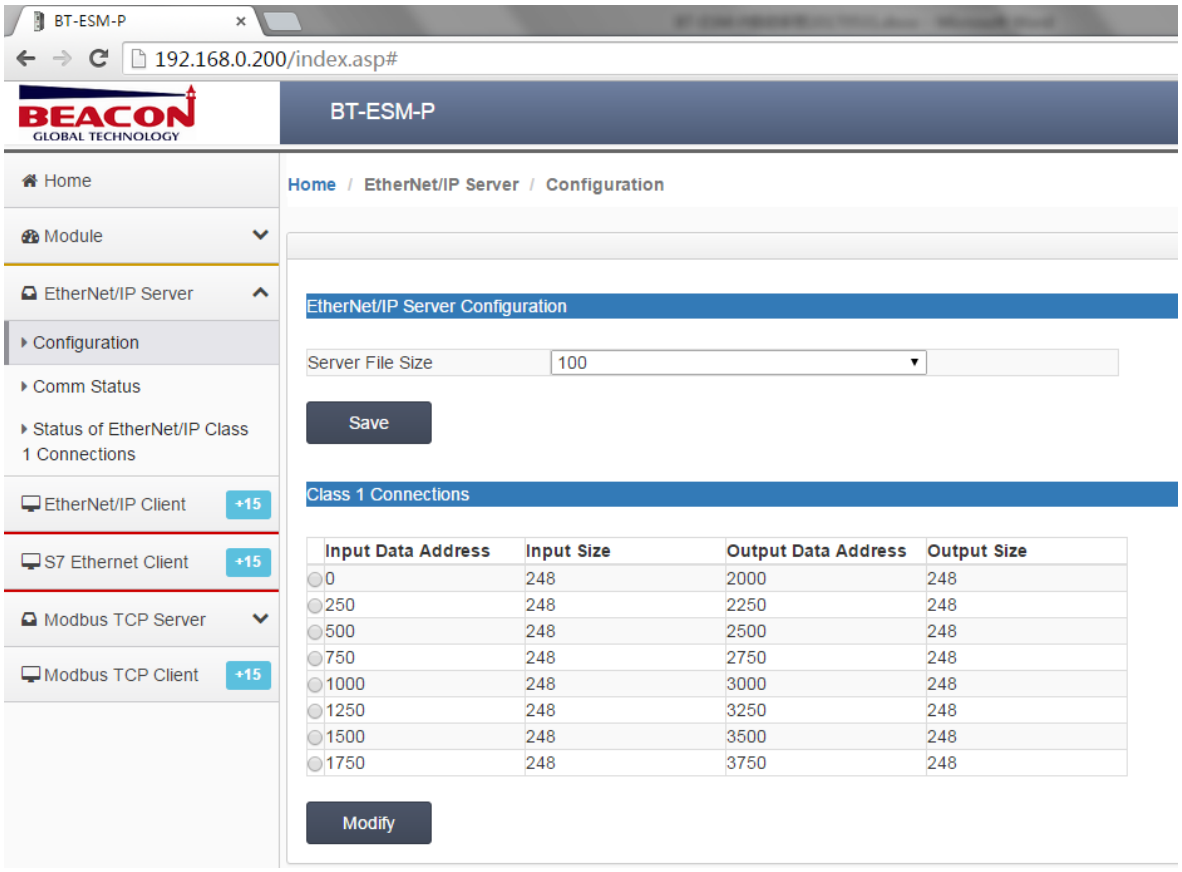
这是模块通过以太网和罗克韦尔 PLC 通讯的最主要方式，本章内容关键在于搞清楚内部数据区和 CIP 标签组的对应关系。通过浏览器，进入模块主页面。

在左侧菜单中，点击 

，查看 EtherNet/IP Server Configuration 的链接数，不同型号的模块的 EtherNet/IP Server Configuration链接数不同。

可以看到当前模块有多组Class 1 Connections的链接，这多组 Class 1 Connections的链接可以在 Logix5000软件里进行配置全部采用或者根据需要部分采用。

每组Class 1 Connections提供248个 INT数据类型的输入和248个INT数据类型的输出。



模块做为 EtherNet/IP Server时候，可以被多个罗克韦尔PLC 同时访问。

注意，不同型号模块可使用的内部寄存器数量不同，本节内容中举例只使用了 4 组 CIP 链接，在配置模块时请根据实际情况选择模块内部数据区。

使用了 4 组 CIP 链接时的数据对应关系：

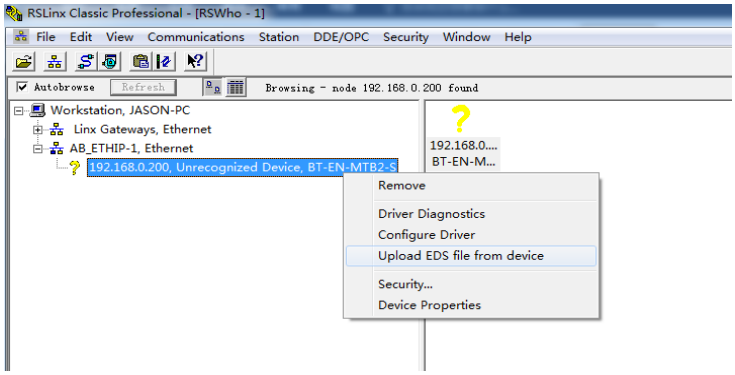
Input Data Address 表示罗克韦尔 PLC 采集模块数据（对 PLC 一侧为输入）的内部寄存器地址范围，0 是指模块内部第 0 个寄存器，输入起始地址为 0，数量 248，表示模块对 PLC 的第一组输入数据，所占用的模块内部寄存器地址范围。

Output Data Address 表示罗克韦尔 PLC 写给模块数据（对 PLC 一侧为输出）的内部寄存器地址范围，1000 是指模块内部第 1000 个寄存器，输出起始地址为 1000，数量 248，表示 PLC 对模块的第一组输出数据，所占用的模块内部寄存器地址范围。

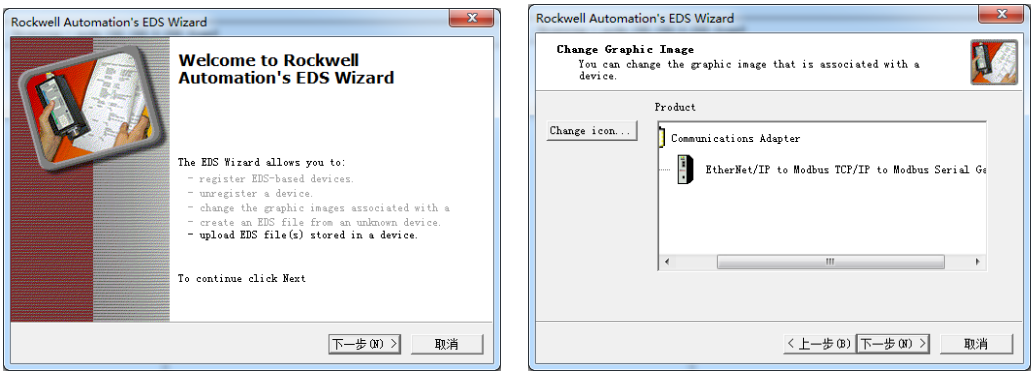
此处 248 个输入寄存器的数量要与 Logix5000 里面的 Class 1 Connections 对应。并且输入输出的起始位置和数量可以任意更改。注：模块默认做 EtherNet/IP 从站，不需要任何设置。

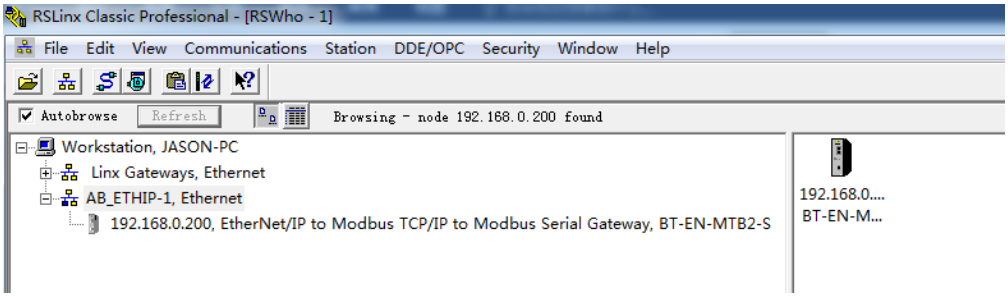
如下步骤为在 Logix5000 配置软件中添加模块：

将网关E1端口和电脑，以及Logix PLC以太网接口相连接。在电脑中使用RSLinx扫描模块，然后在RSLogix5000中添加该模块的EDS文件，如下图：

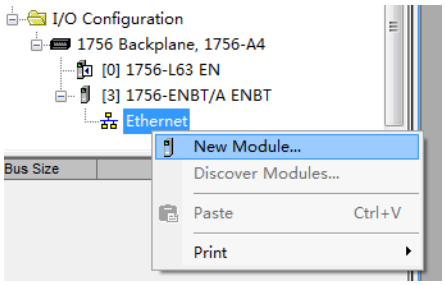


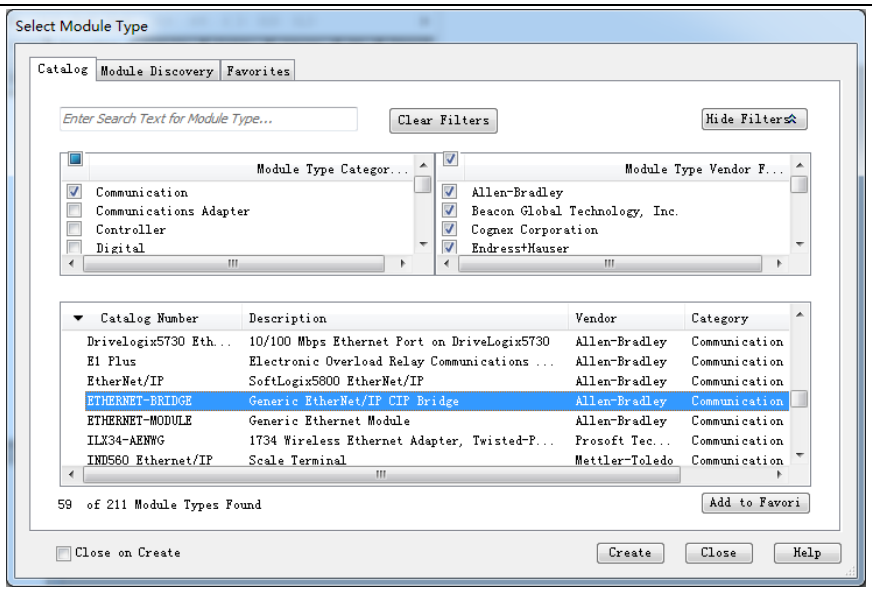
选择从设备上传 EDS 文件，如下图：



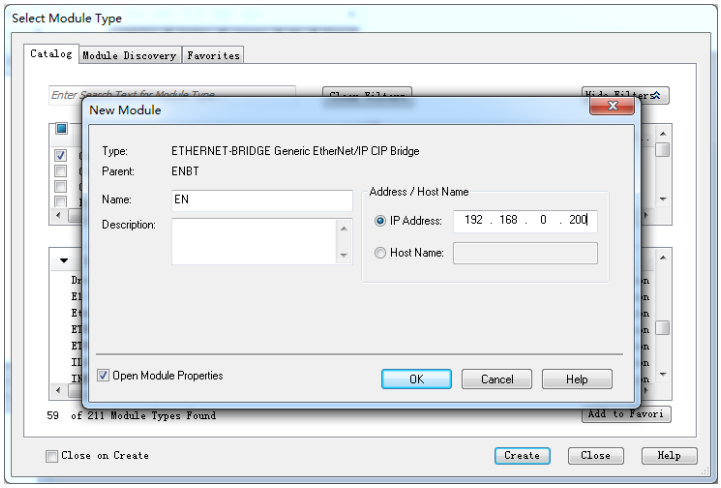


下一步通过添加“Generic EtherNet Bridge”完成 PLC 和模块的通讯，如下图.

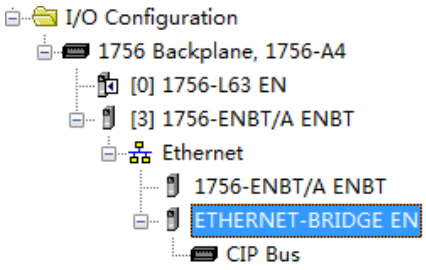


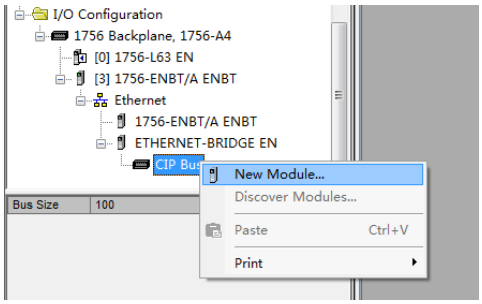


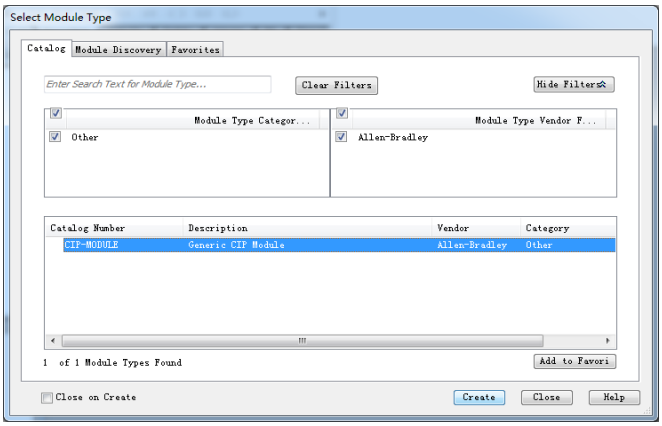
设定模块的 IP 地址，该地址为 E1 端口地址



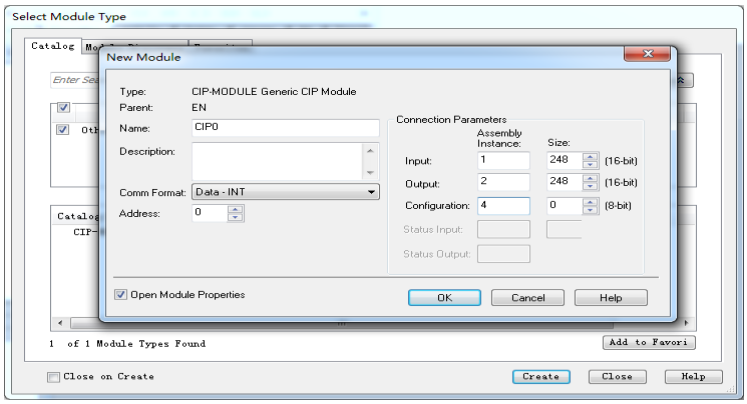
在 Generic EtherNet Bridge 下添加一个新模块，再添加一个新的 CIP-Connection.







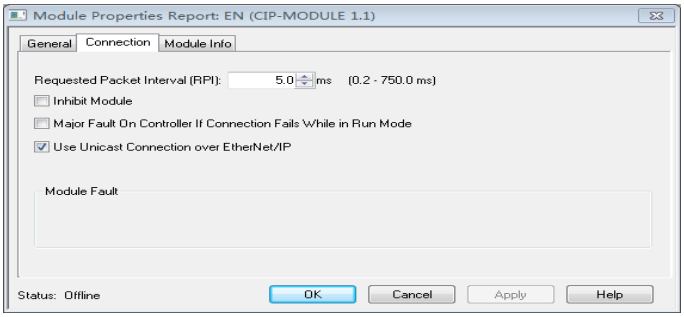
之后开始设定 PLC I/O connection 的参数，如下图：



请使用 Input 和 Output 都为 248 个字，Configuration 为 0。Comm format 需要选择 Data INT。

Assembly instances 设定方式：input 为"1",output 为"2",configuration 为"4"。

每一个 I/O connection 都需要进行如上的配置，之后点击 Create，来设定 I/O connection 的 RPI time 时间.单机 PLC 结构，Use Unicast Connection over EtherNet/IP 要勾选，RPI 时间可以使用 5ms 或者 20ms。冗余 PLC 结构，Use Unicast Connection over EtherNet/IP 不要勾选，RPI 时间可以使用 20ms 或者 40ms。



以上步骤完成后，在模块侧，可以通过诊断来查看：

前文已经提到过，采用 4 组 CIP 数据连接，数据对应关系如下，

从 AB 的 PLC 对模块 internal data base 进行读写。

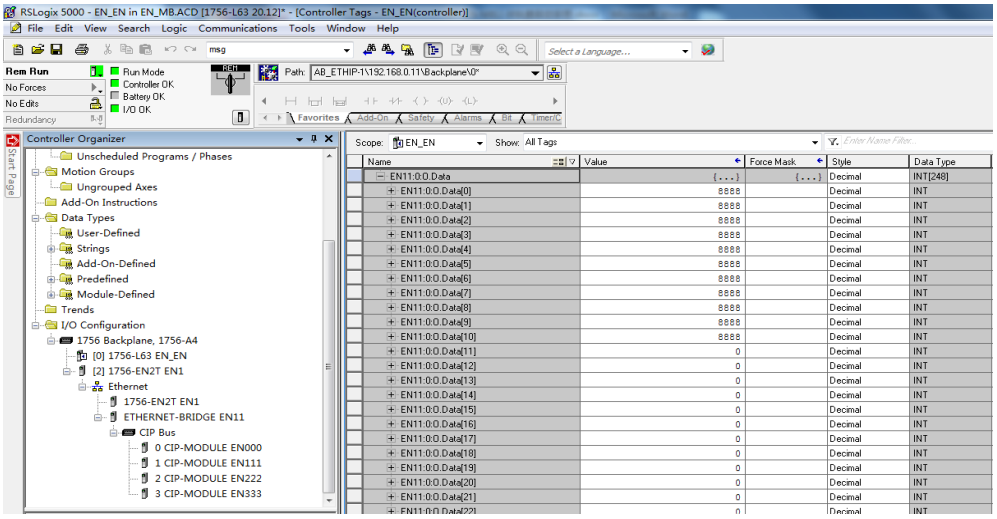
EN:0:I.Data[0]-EN:0:I.Data[247]对应模块内部寄存器 0-247 的地址　　输入

EN:0:O.Data[0]-EN:0:O.Data[247]对应模块内部寄存器 1000-1247 的地址　　输出

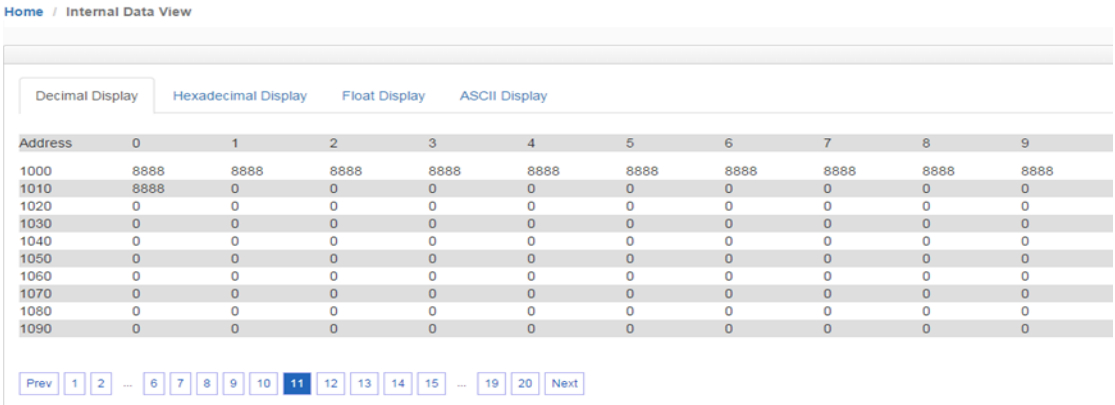
EN:1:I.Data[0]-EN:1:I.Data[247]对应模块内部寄存器 250-497 的地址　　输入

EN:1:O.Data[0]-EN:1:O.Data[247]对应模块内部寄存器 1250-1497 的地址　　输出

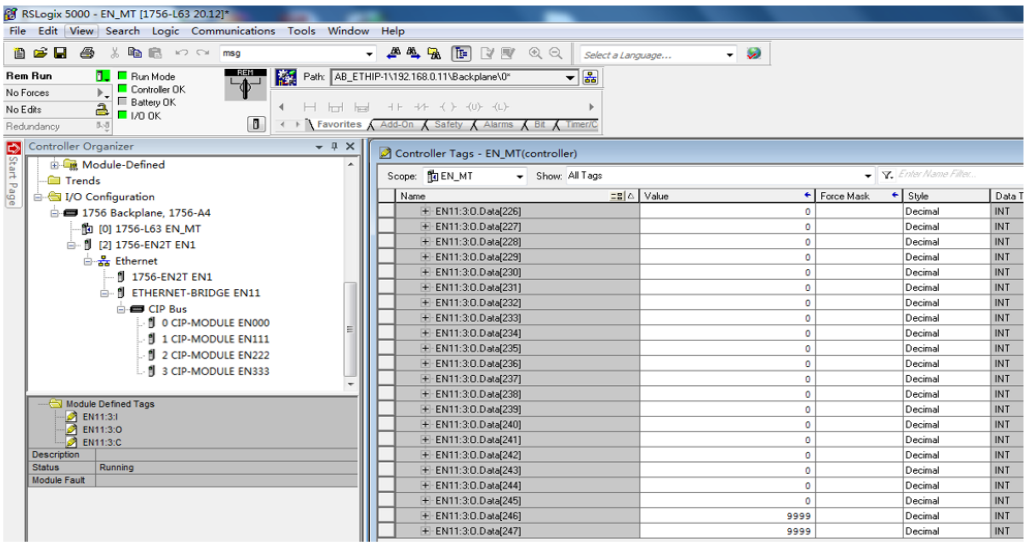
以此类推。如下图，在 RSLogix5000 第一个 CIP I/O 链接的输出标签的开头写一些数据。



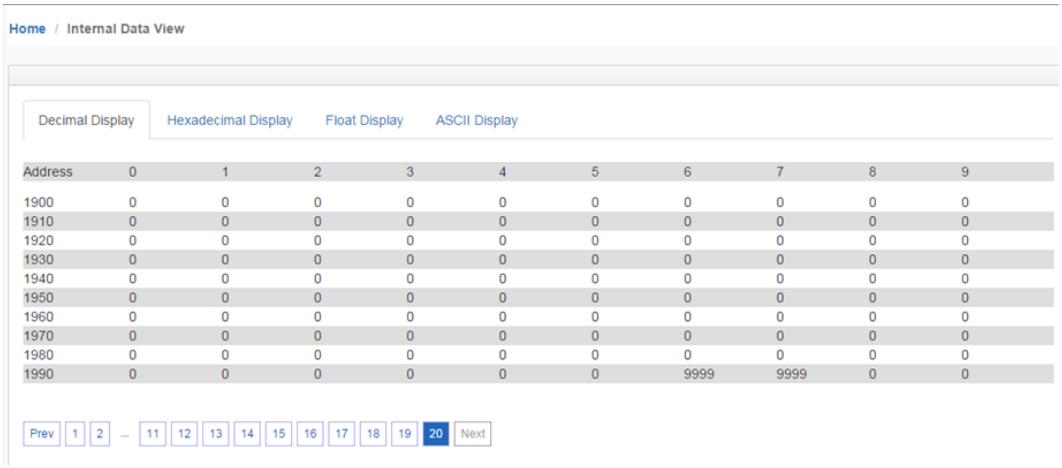
网关Internal Data Base 从地址1000开始的数据的变化。



在RSLogix 5000第4个CIP I/O链接的输出标签的结尾写一些数据。



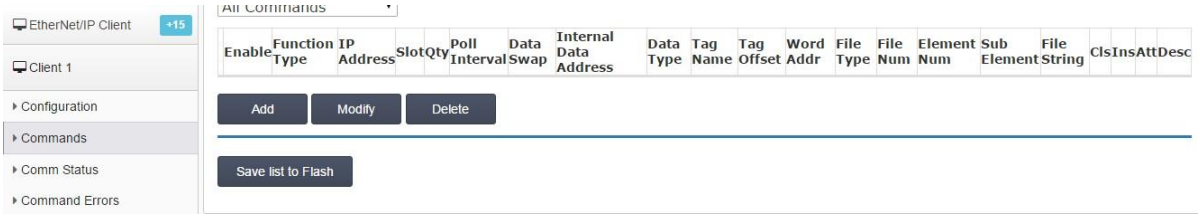
网关Internal Data Base地址1996和1997的数据值的变化。



配置模块做 EtherNet/IP Client

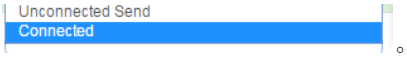
模块正常和 Logix 系列 PLC 通讯都是作为 server 从站，不过也可以同时支持作为 Client 和 Server 和 PLC 交换数据。在前一章介绍“模块做 Ethernet/IP server”的时候，很重要的一点是介绍了如何分配模块内部数据区的内容。

如果模块同时作为 EtherNet/IP 的 Client 和 Server 则要特别注意，读写数据区冲突的问题，以免造成数据混乱。



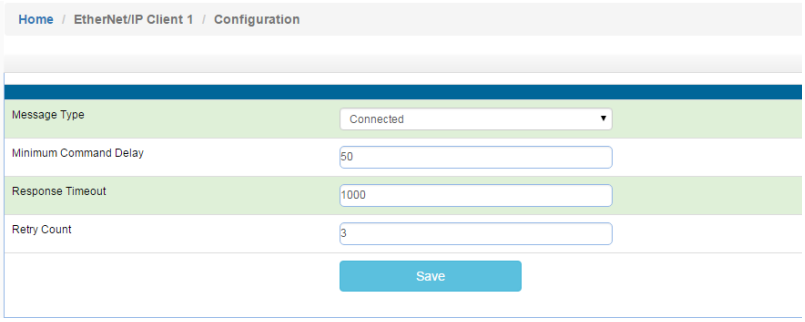
如上图，点击 EtherNet/IP Client ---Client1---Commands。

点开Configuration，查看默认的配置。

Message Type: 

。

连接罗克韦尔 1756 系列，1769 系列，1746 系列，PLC-2 系列，PLC-5 系列，SLC500 系列，Micrologix PLC 系列，PowerFlex 变频器系列，连接 E300 智能马达保护器，PowerMonitor 智能电力监控仪等需要选择 Connected。



此处用于连接 1756 PLC，因此选择 Connected.

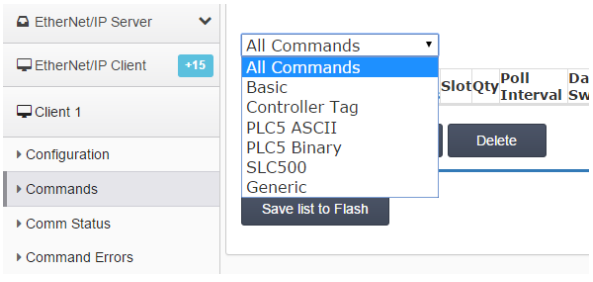
Minimum Command Delay：每个 Client 执行指令的轮询时间，单位 ms，　　范围 0-65535

注：该时间越小,发送命令越快，但并非越小越好，需要先查看从站设备的说明书，确定从站响应时间是否能及时接受和反馈，主站发送命令的间隔。

Response Timeout：所连接设备的响应时间，单位 ms，　　范围 0-65535

Retry Count：重新尝试连接次数 ，　　范围 0-65535

之后选择指令的类型：



Basic 命令用于罗克韦尔 PLC-5, ControlLogix 数据的读写；

Controller Tag 命令用于罗克韦尔 CompactLogix，ControlLogix 数据标签或标签数组的读写

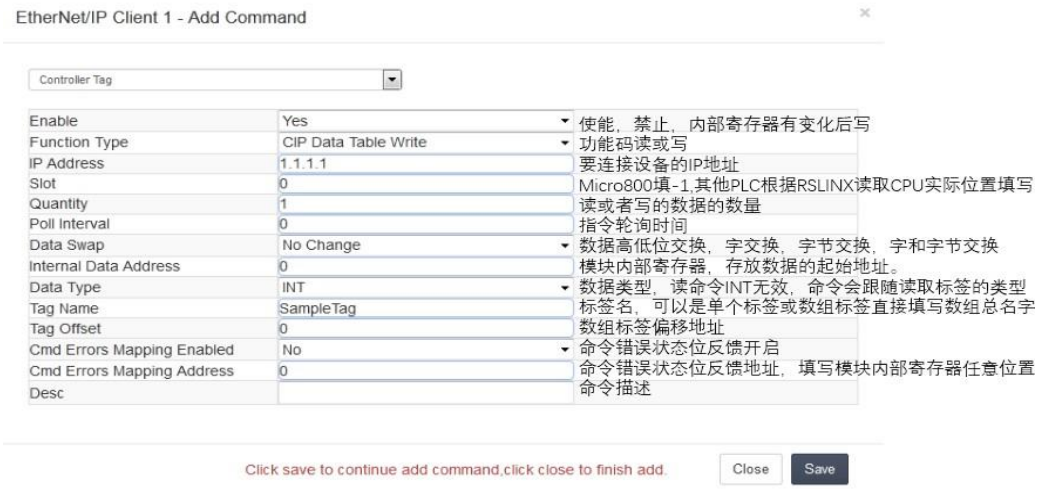
PLC5 ASCII 命令用于罗克韦尔 PLC-5，ControlLogix 数据的读写；

PLC5 Binary 命令用于罗克韦尔 PLC-5，ControlLogix 数据的读写；

SLC500 命令用于罗克韦尔 SLC500，MicroLogix，PowerFlex 变频器数据的读写；

Generic 命令用于罗克韦尔 PowerFlex 变频器，E300 智能马达保护器，PowerMonitor 智能电力监控仪数据的读写。

选择要连接的种类，选择相应的命令。点击 Add 可以增加命令行。

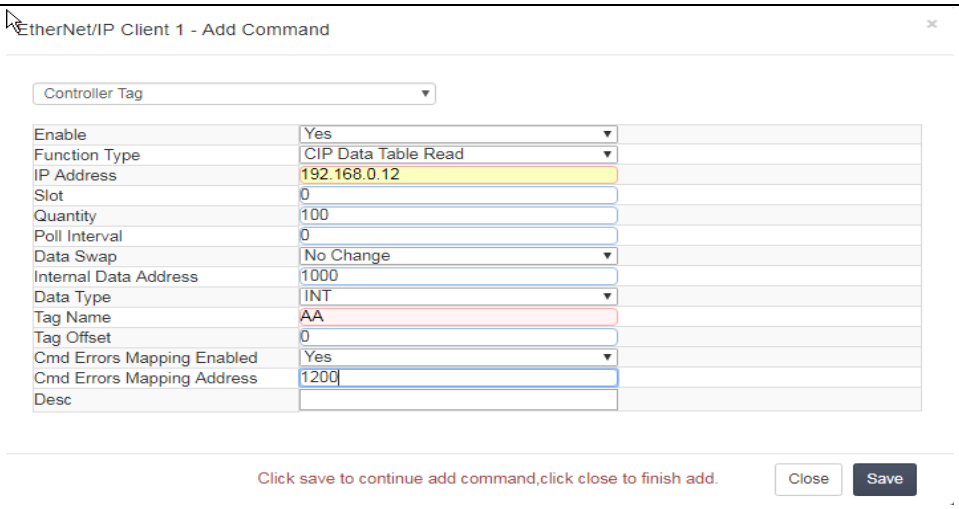


以下按照和 1756 PLC 通讯举例，和其他罗克韦尔产品的通讯指令详细内容，可另外参考其他手册或者咨询 BEACON 当地经销商和办事处。

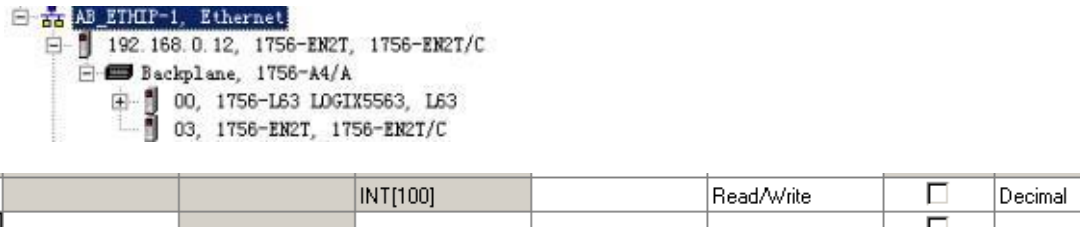
如下举例中，仅针对 EtherNet/IP Client 指令部分内容进行介绍，暂不考虑上一章中提到的 PLC CIP 标签和模块内部数据区地址映射的关系，以及内部数据区大小范围。

在实际操作中，因为不同产品型号的模块内部数据区大小不同，请务必注意模块数据区的实际大小，并根据实际数据寄存器的地址范围来配置指令，同时还请注意相同地址是否重复被多种协议写入数据。

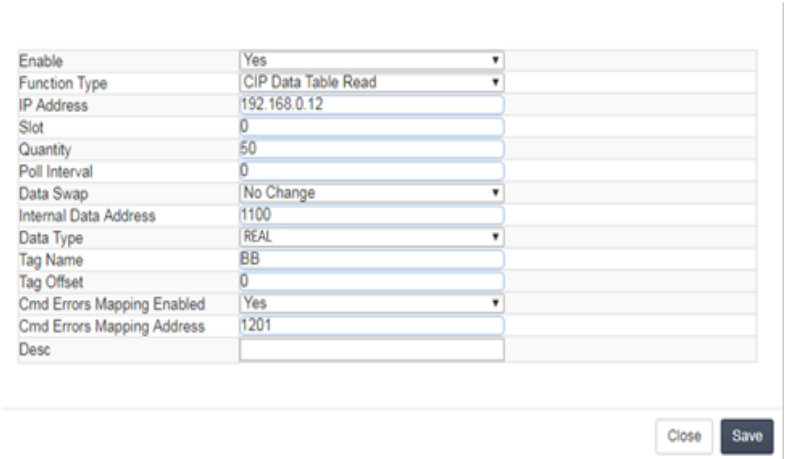
此选项用于罗克韦尔 PLC 在不能停机的情况下，对 Logix5000 或者 Studio 5000 软件里面标签或者标签数组进行读或写的操作。



举例一：如上图，读取 IP 地址为 192.168.0.12，CPU 位于 0 槽位的 L63 CPU 里面的全局变量标签数组 AA，数组是 INT 格式，数量 100 个 INT(每条命令最大 100 个 INT,或者 50 个 DINT/REAL),放到模块内部寄存器 1000-1099 里面，如果命令检测不到 AA 的数组有 100 个 INT 或者没有 AA 数组，或者 IP 地址不对，槽位不对等，就会在模块内部寄存器 1200 的位置报一个非零值，显示这条命令有错误，工程师可以使用 Cmd Errors Mapping 反馈来查看所连接设备的状态。（注：对于读来说 Data：Type 始终是 INT,不可修改，但是会随着数组的类型自动调整）

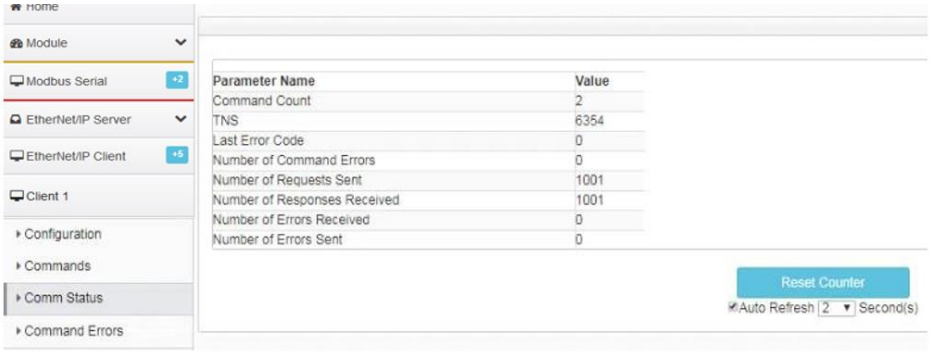


读取 IP 地址为 92.168.0.12，CPU 位于 0 槽位的 L63 CPU 里面的全局变量标签数组 BB，数组是 REAL 格式，数量 50 个 REAL(每条命令最大 100 个 INT，或者 50 个 DINT/REAL)，放到模块内部寄存器 1100-1199 里面，如果命令检测不到 BB 的数组有 50 个 REAL 数据，或者 IP 地址不对，槽位不对等，就会在模块内部寄存器 1201 的位置报一个非零值，显示这条命令有错误，工程师可以使用 Cmd Errors Mapping 反馈来查看所连接设备的状态。

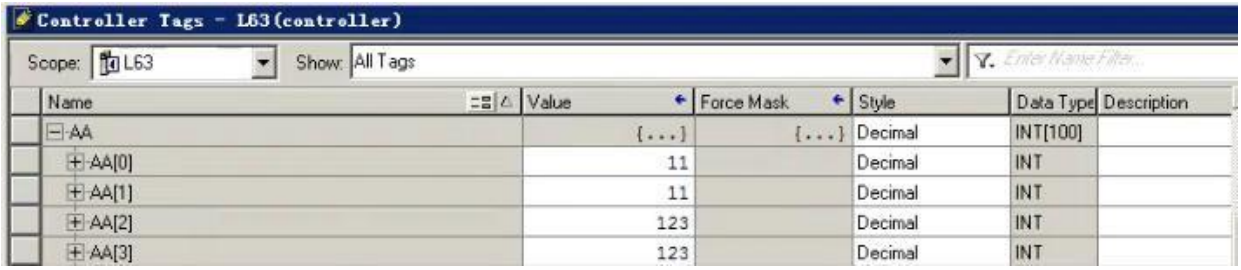


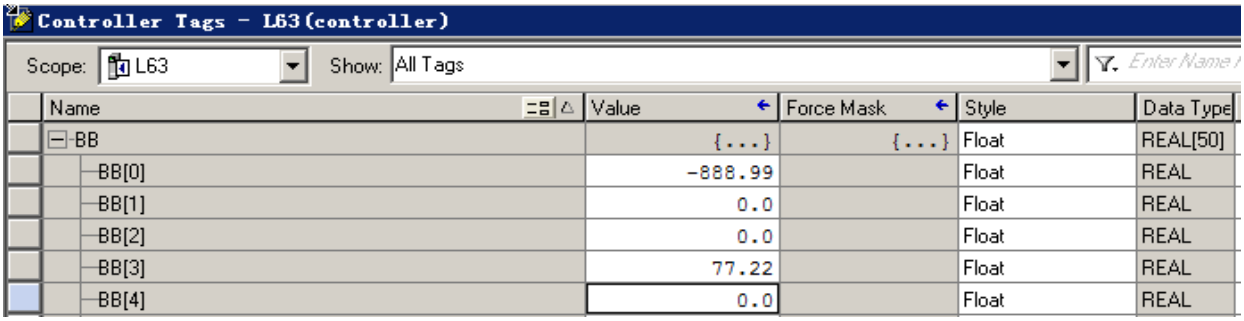
	⊞-BB			REAL[50]		Read/Write	Float

检查命令状态，点击 Comm Status 如下图，可以看发送和接收的次数，最后的错误代码等。

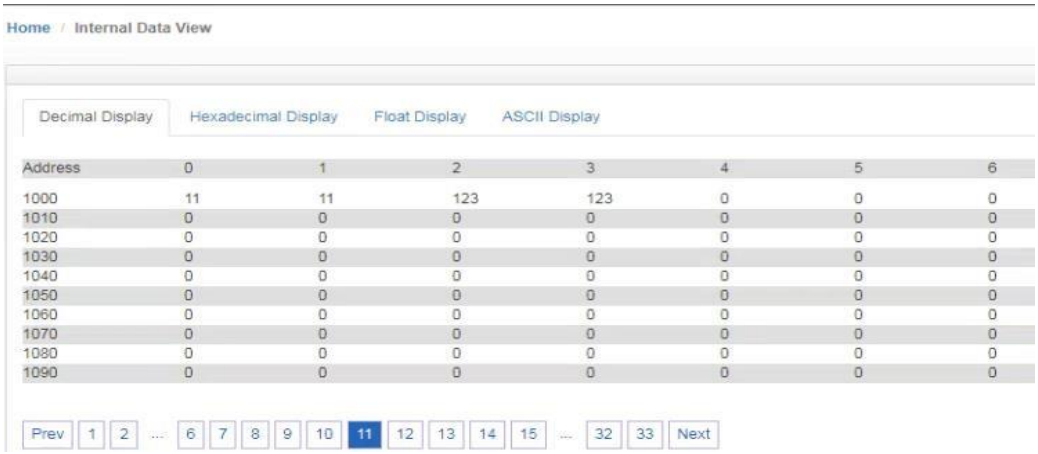


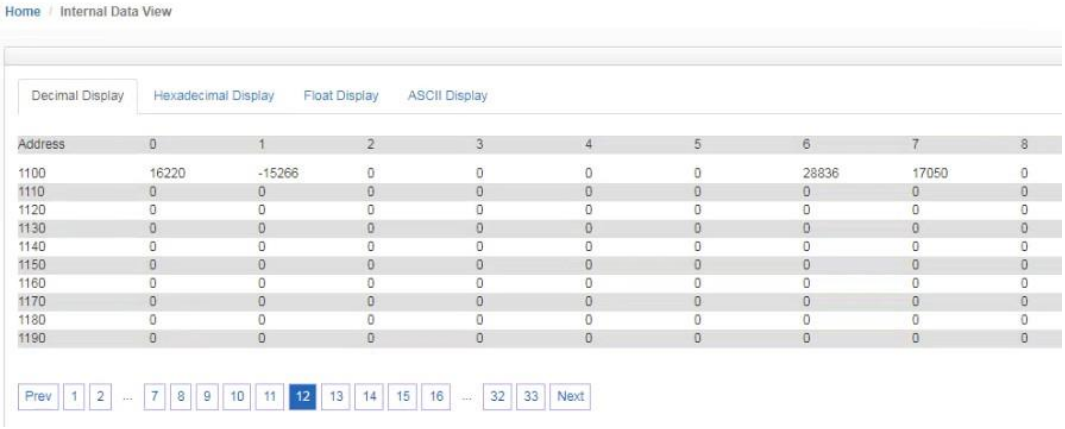
在 AA 和 BB 输入些数据：



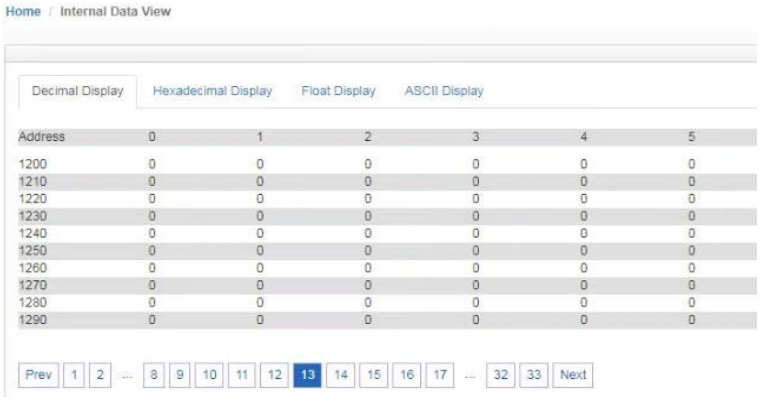


查看内部寄存器 1000 和 1100 的数据，此处说明 1 个 REAL 的浮点数占 2 个内部寄存器，虽然命令是 50 个浮点数，放到 1100 开始的内部寄存器，实际上是 1100-1199 这 100 个寄存器存放着 50 个浮点数

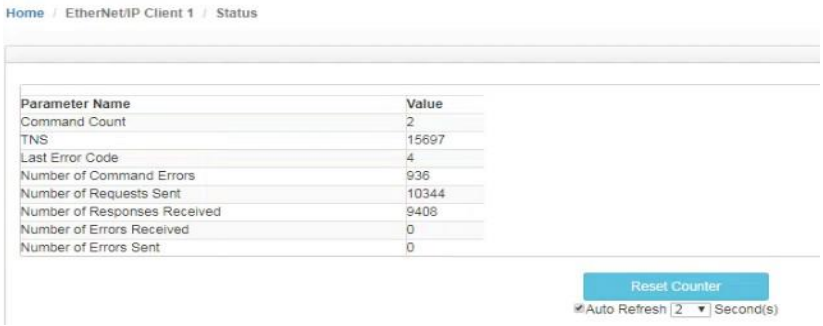


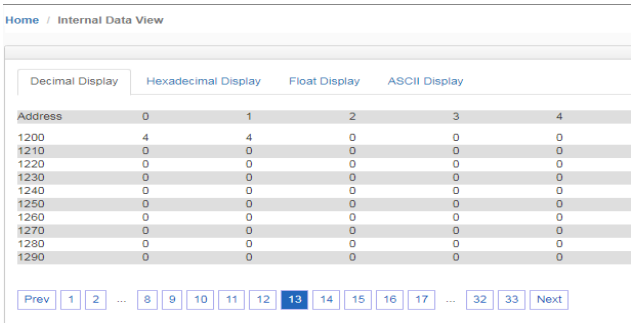


可以看到内部寄存器 1200 和 1201 没有错误反馈：



如果我们从 Logix5000 里面删除掉 AA 或者 BB 数组标签的时候，命令检测不到有这两个数组，就会在内部寄存器 1200 和 1201 里面报错误，其他协议可以采集存放错误标签寄存器来反馈命令的执行情况。也可以查看命令状态。这里可以看到错误代码 4 产生，这里面错误代码含义很多种，如果命令检测不到 AA 的数组有 100 个 INT 或者没有 AA 数组，或者 IP 地址不对，槽位不对等，就会在模块内部寄存器 1200 的位置报一个非 0 值，工程师编程时，此地址不等于 0 就表示命令没有执行下去，因为错误代码组合种类非常多，例如 IP 地址不对，又没有检测不到 AA 数组，这时候就会产生 IP 和检测不到 AA 数组的错误代码组合。这里不再详细介绍。





举例：连接 E300 马达保护器，请先查看 E300 用户手册，了解关于以太网连接的方法，E300 自带有 3 个输出继电器，如果控制输出继电器 1，继电器 2，继电器 3，就需要使用 CLASS CODE9,3 个继电器分别对应着 Instance1，Instance2，Instance3。Attribute 选择 3 是对这个继电器写值，0=OFF 1=ON。

Discrete Output Point Object — CLASS CODE 0x0009

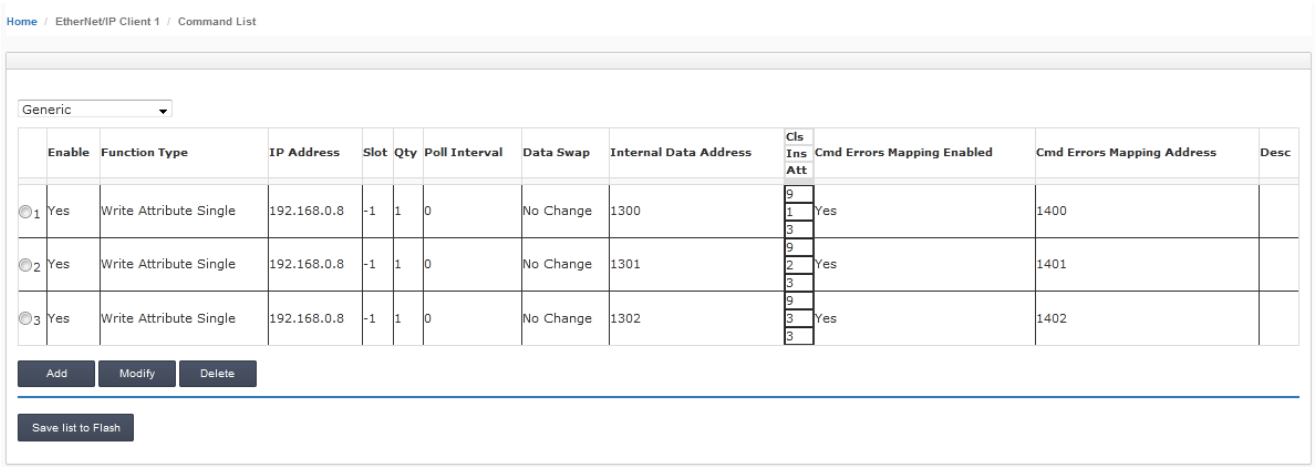
The following class attributes are supported for the Discrete Output Point Object:

Instance	Name	Description
1	OutputPt00	Control Module Output 0
2	OutputPt01	Control Module Output 1
3	OutputPt02	Control Module Output 2
4	OutDigMod1Pt00	Digital Expansion Module 1 Output 0
5	OutDigMod1Pt01	Digital Expansion Module 1 Output 1
6	OutDigMod2Pt00	Digital Expansion Module 2 Output 0
7	OutDigMod2Pt01	Digital Expansion Module 2 Output 1
8	OutDigMod3Pt00	Digital Expansion Module 3 Output 0
9	OutDigMod3Pt01	Digital Expansion Module 3 Output 1
10	OutDigMod4Pt00	Digital Expansion Module 4 Output 0
11	OutDigMod4Pt01	Digital Expansion Module 4 Output 1

All instances contains the following attributes.

Table 619 - Discrete Output Point Object Instance Attributes

Attribute ID	Access Rule	Name	Data Type	Value
3	Get/Set	Value	BOOL	0=OFF, 1=ON
5	Get/Set	Fault Action	BOOL	0=Fault Value attribute, 1=Hold Last State
6	Get/Set	Fault Value	BOOL	0=OFF, 1=ON
7	Get/Set	Idle Action	BOOL	0=Fault Value attribute, 1=Hold Last State
8	Get/Set	Idle Value	BOOL	0=OFF, 1=ON
113	Get/Set	Pr Fault Action	BOOL	0=Pr Fault Value attribute, 1=Ignore
114	Get/Set	Pr Fault Value	BOOL	0=OFF, 1=ON
115	Get/Set	Force Enable	BOOL	0=Disable, 1=Enable
116	Get/Set	Force Value	BOOL	0=OFF, 1=ON
117	Get/Set	Input Binding	STRUCT: USINT Array of USINT	Size of appendix I encoded path Appendix I encoded path: NULL path means attribute 3 drives the output. Otherwise, this is a path to a bit in an instance of the DeviceLogix Data Table.



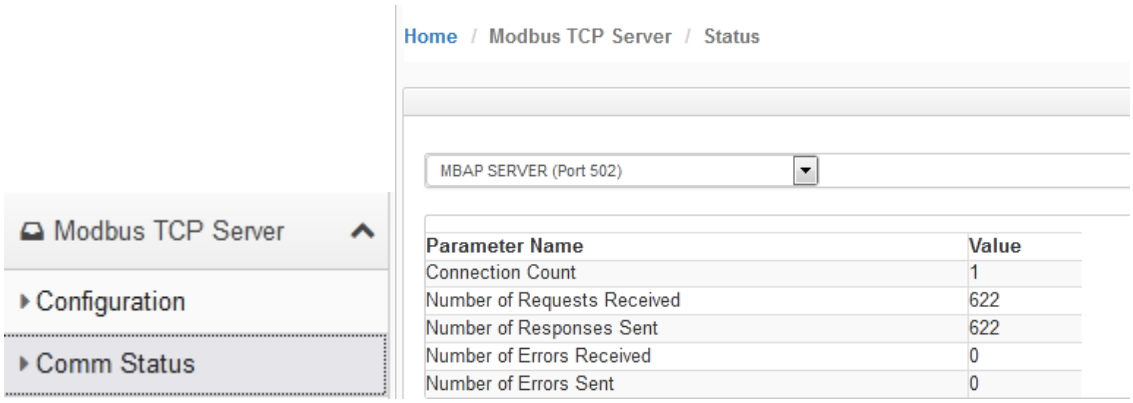
如上建立的 3 条指令，表示对 IP 地址为 192.168.0.8 的 E300 马达保护器 3 个输出继电器进行输出操作，如果内部寄存器 1300，1301，1302 值为 1 的时候，3 个输出继电器会进行闭合动作，如果内部寄存器 1300，1301，1302 值为 0 的时候，3 个输出继电器会进行分开动作，如果 3 条命令没有正确执行，内部寄存器 1400，1401，1402 会报一个非零值。注：模块作为 EtherNet/IP Client 可以支持的内容非常多，根据需要连接的设备的不同（Logix 控制器，PowerFlex 变频器，E300 马达保护器，PowerMonitor 电力仪表），可以和我们联系，获取进一步的详细技术支持。联系方式请见手册最后一页。

配置模块做 Modbus TCP server

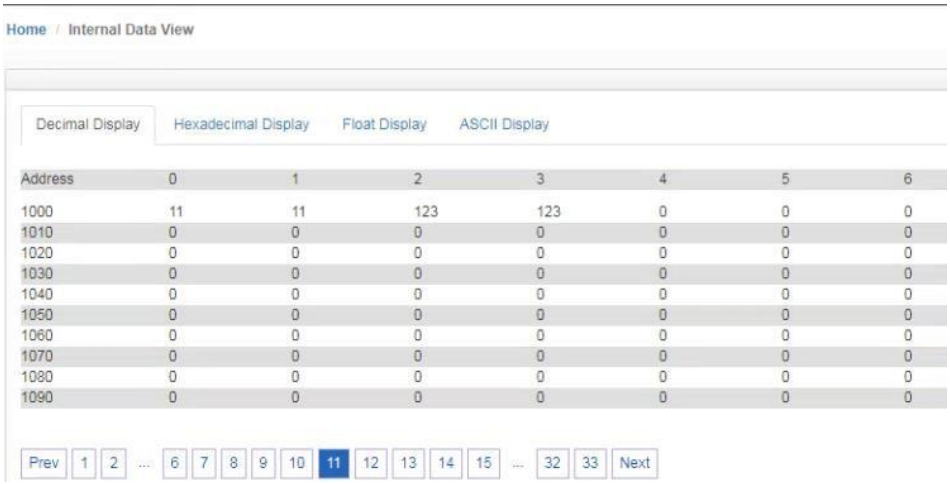
点击 Modbus TCP仿真软件连接模块的Modbus TCP Server，先修改本地电脑IP地址为192.168.0.177。打开浏览器，进入模块主配置页面

在左侧导航栏点击 Modbus TCP Server ---Comm Status 如下图

注：模块默认做 Modbus TCP 从站，不需要任何设置，可同时被多个Modbus TCP主站访问。



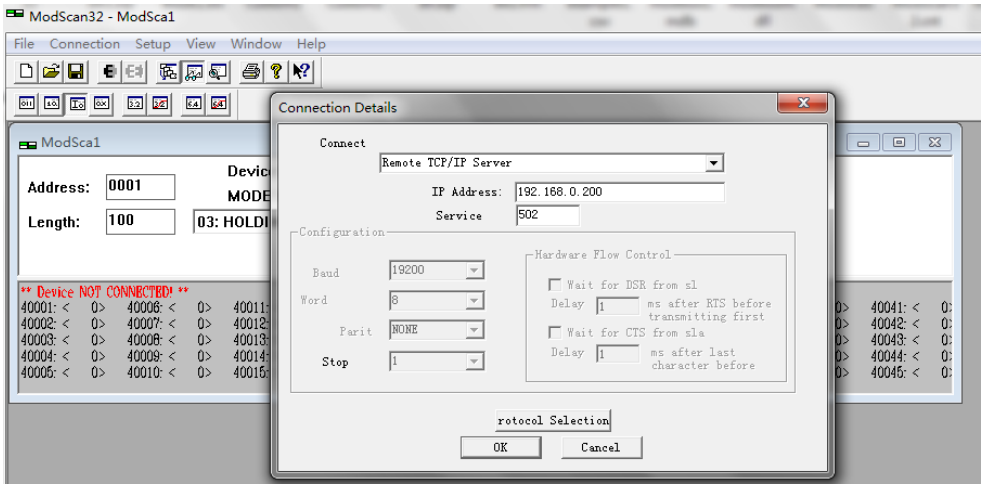
点击模块 Module---internal Data View 可以查看模块内部数据区，本型号有 10000 个字的数据区可供使用。



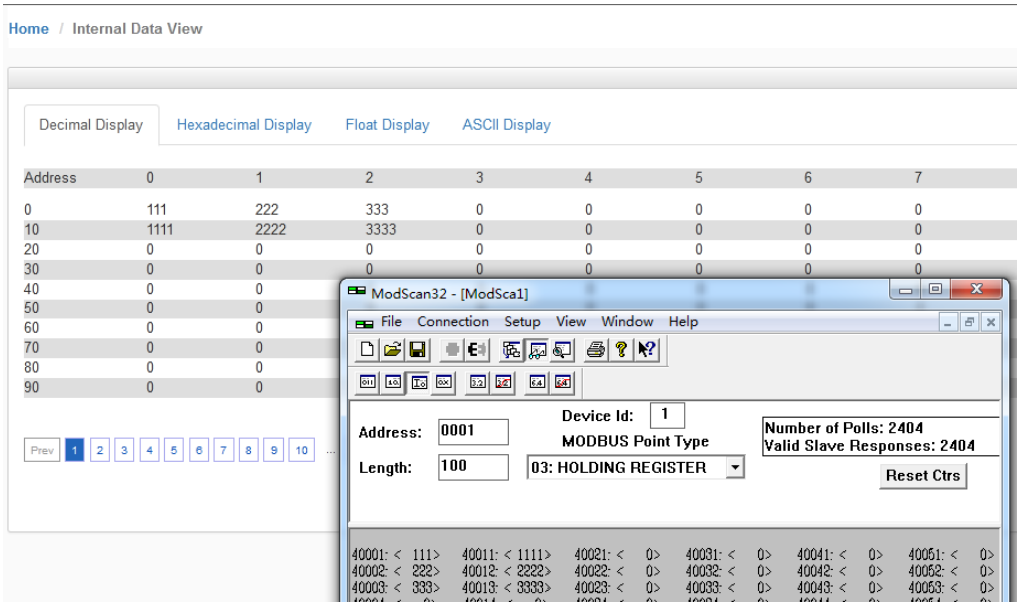
模块内部寄存器对应着Modbus TCP 地址如下：Internal Data模块内部寄存器同时提供 Modbus 4区 ，3 区，1 区，0 区的访问。模块内部寄存器0对应着40001，同时对应着30001，同时对应着10001-10016，同时对应着00001-00016。 注意先要确认模块的内部寄存器数据区大小：

模块内部寄存器地址	等于	Modbus4区地址	等于	Modbus3区地址	等于	Modbus1区地址	等于	Modbus1区地址	等于	Modbus0区地址	等于	Modbus0区地址
0	=	40001	=	30001	=	10001	至	10016	=	00001	至	00016
1	=	40002	=	30002	=	10017	至	10032	=	00017	至	00032
10	=	40011	=	30011	=	10161	至	10176	=	00161	至	00176
11	=	40012	=	30012	=	10177	至	10192	=	00177	至	00192
20	=	40021	=	30021	=	10321	至	10336	=	00321	至	00336
30	=	40031	=	30031	=	10481	至	10496	=	00481	至	00496
99	=	40100	=	30100	=	11585	至	11600	=	01585	至	01600
100	=	40101	=	30101	=	11601	至	11616	=	01601	至	01616
220	=	40221	=	30221	=	13521	至	13536	=	03521	至	03536
1000	=	41001	=	31001	=	26001	至	26016	=	16001	至	16016
1001	=	41002	=	31002	=	26017	至	26032	=	16017	至	16032
1999	=	42000	=	32000	=	41985	至	42000	=	31985	至	32000
2000	=	42001	=	32001	=	42001	至	42016	=	32001	至	32016
2001	=	42002	=	32002	=	42017	至	42032	=	32017	至	32032
3000	=	43001	=	33001	=	58001	至	58016	=	48001	至	48016

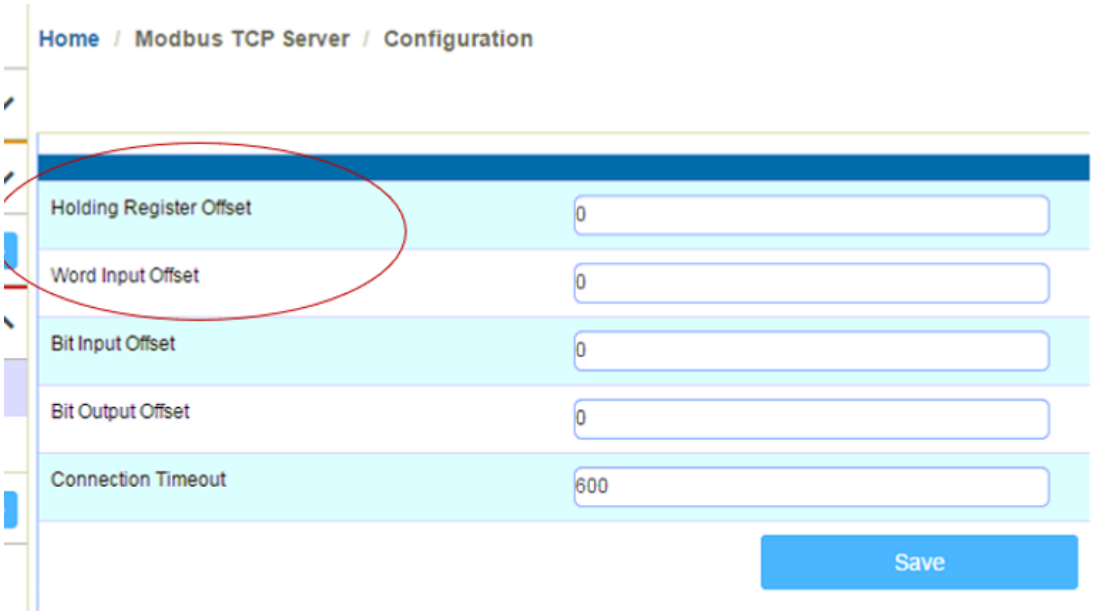
打开 Modbus TCP仿真软件MODSCAN32,作用是仿真 Modbus TCP主站。使用功能码FC03，读写模块内部数据区0-99 的连续 100 个字的数据，40001 对应着内部寄存器 0 ,40100 对应着内部寄存器 99 ,以此类推。选择 Connection，选择 Remote TCP/IP Server ，填写模块 E1 口的 IP 地址 192.168.0.200，端口号默认 502。 然后点击OK。



ModScan32 软件可以对内部寄存器读写同时进行，在 40001，40002，40003 写一些数据，查看模块内部寄存器 0-2 里面的数据情况。数据能完整对应，同时可以看到 ModScan32 软件右上角发送了 2404 次，接收了 2404 次。如果有错误，发送和接收的数据次数会不相等。

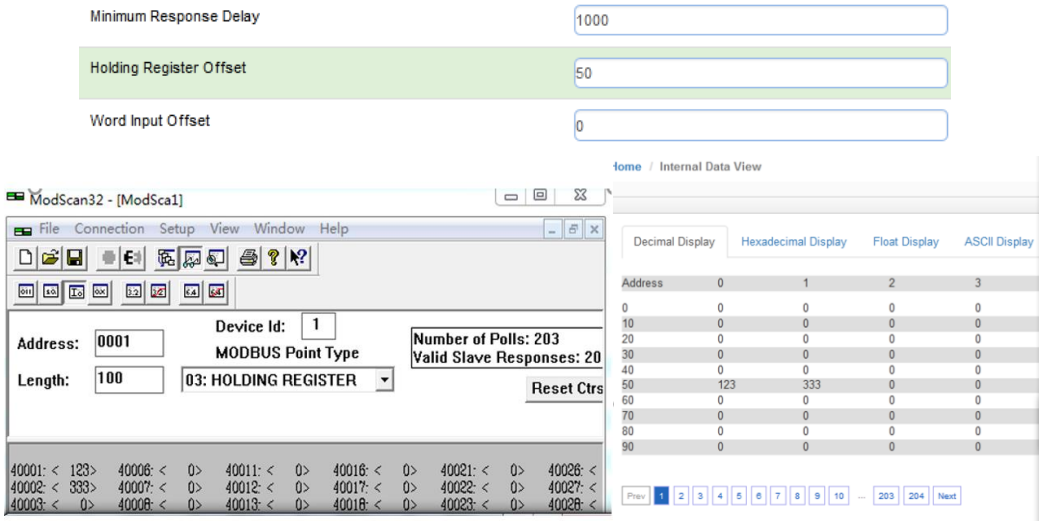


模块设置成为Modbus TCP从站的时候，在configuration界面中，可以看到下图两个选项。

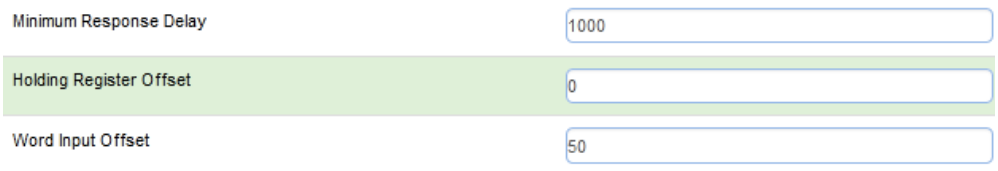


Holding Register Offset使用方法：

Modbus TCP主站对模块写数据，在40001和40002输入两个数据，正常情况下，这两个数据应该会被写入到模块内部寄存器0-1当中去。如果此处偏移量设置成50(如下图)，则数据会直接偏移写入模块内部寄存器50-51里面。4区，3区，1区，0区同样遵循这个原理。



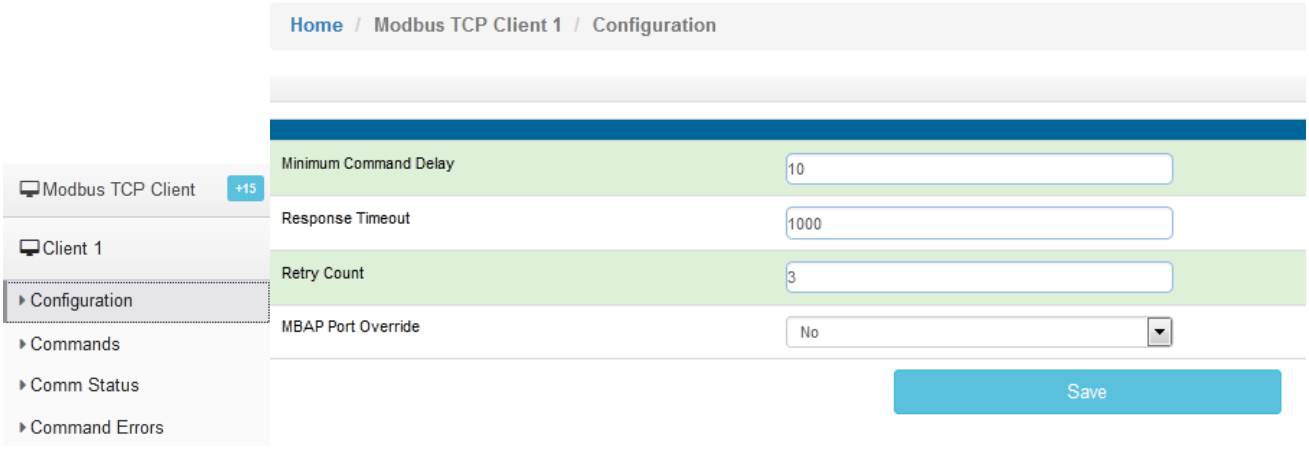
Word Input Offset使用方法：如果此处偏移量设置成50(如下图)，Modbus TCP主站一侧在3区对30001和30002输入两个数据，数据会直接向后偏移放到模块内部寄存器50-51里面，ModScan32仿真软件不能载入3区的数值，请以现场设备实际数据区域来填写。



配置模块做 Modbus TCP Client

注：模块的 Modbus TCP 端口可以同时支持作为主站和从站，做主站功能适用于连接另外的 Modbus TCP 的从站设备。

如下图点击 Modbus TCP Client ---Client1 ---Configuration



点开Configuration。查看默认的配置。此配置默认就可以使用。

Minimum Command Delay：每个Client执行指令的轮询时间，单位ms　　0-65535

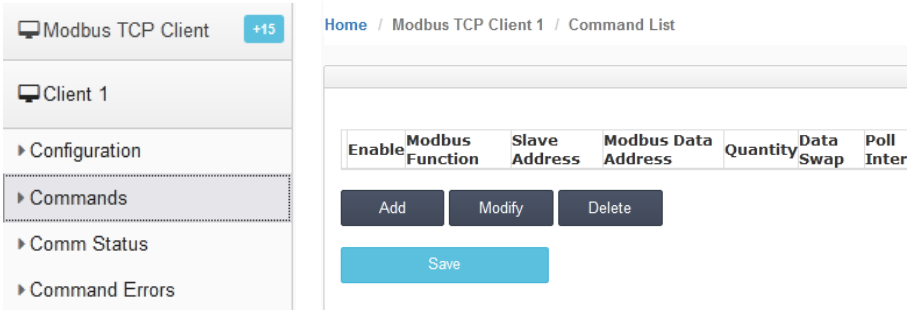
注：该时间越小,发送命令越快，但并非越小越好，需要先查看从站设备的说明书，确定从站响应时间是否能及时接受和反馈，主站发送命令的间隔。

Response Timeout：所连接设备的响应时间，单位 ms　　0-65535

Retry Count：重新尝试连接次数　　0-65535

MBAP Port Override 端口 502 覆盖　　NO/YES

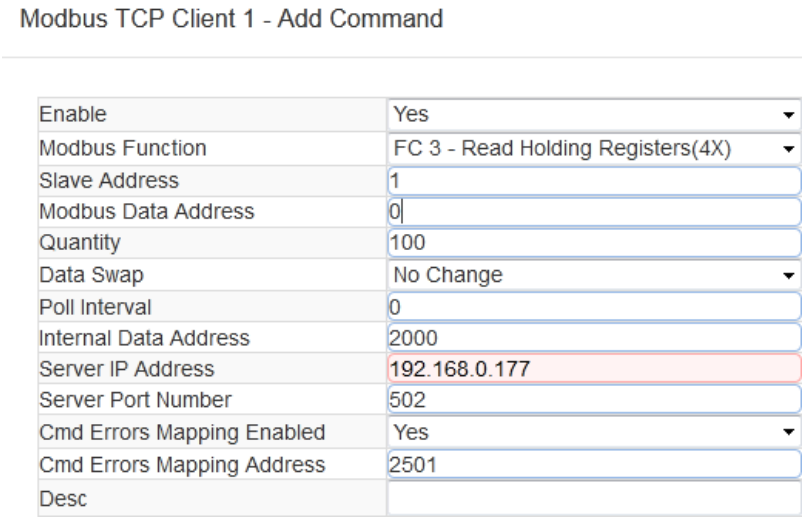
点击 Modbus TCP Client ---Client1---Commands



点击 Add，可以增加一条命令，命令如下

命令解释：采用功能码控制读写区域，模块内部寄存器是16位的INT格式，读写位的时需要注意16倍关系。

注意先要确认模块的内部寄存器数据区大小, 本型号模块可用数据区为 10000 个字。



以上指令含义如下：模块使用功能码 FC3，从站数据起始地址是 0 等于 40001。读取数量是 100。 模块内部寄存器起始地址 2000。表示读 IP 地址为 192.168.0.177 的从站，从站数据地址范围为 40001-40100 的 100 个字，放到模块内部寄存器 2000-2099，命令没有正确返回在内部寄存器 2051 报错。

如果功能码是 FC4 时（只读），从站数据起始地址是 0 等于 30001。读取数量是 100.模块内部寄存器起始地址 2000，表示读 IP 地址为 192.168.0.177 的从站，从站数据地址范围为 30001-30100，放到模块内部寄存器2000-2099，命令没有正确返回，会在内部寄存器2051报错。

Modbus TCP Client 1 - Add Command

Enable	Yes
Modbus Function	FC 1 - Read Coil (0X)
Slave Address	1
Modbus Data Address	0
Quantity	16
Data Swap	No Change
Poll Interval	0
Internal Data Address	32000
Server IP Address	192.168.0.177
Server Port Number	502
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2501
Desc	

以上指令含义如下：模块使用功能码 FC1 时，从站数据起始地址是 0 等于 00001，读取数量是 16（此处读取 16 个位等于读取一个字）。模块内部寄存器起始地址 32000（此处为位地址，读取 16 个位等于读取一个字，模块内部寄存器是字，所以实际上模块内部寄存器的起始地址为 32000/16=2000）。表示读 IP 地址为 192.168.0.177 的从站，从站数据地址范围为00001-00016，放到模块内部寄存器起始地址为2000（因为读取到 16 个位数据，等于 1 个字数据，所以只占用模块内部寄存器一个地址），命令没有正确返回在内部寄存器2051报错。

如果是功能码FC2时（只读），从站数据起始地址是0。读取数量是16。模块内部寄存器32000，同上表示读 IP 地址为 192.168.0.177 的从站，从站数据地址范围为00001-00016，放到模块内部寄存器2000，命令没有正确返回，会在内部寄存器2051报错。

Modbus TCP Client 1 - Add Command

Enable	Conditional
Modbus Function	FC 16 - Preset (Write) Multiple Register
Slave Address	1
Modbus Data Address	50
Quantity	20
Data Swap	No Change
Poll Interval	0
Internal Data Address	2000
Server IP Address	192.168.0.177
Server Port Number	502
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2501
Desc	

以上指令含义如下：Conditional 表示有条件情况下，模块使用功能码 FC6 或者 FC16 时，写出数量是 20。模块内部寄存器起始地址为 2000，表示当模块内部寄存器范围 2000-2019 的任意寄存器发生数据发生变化时候，触发一条写的命令，数据从模块写到 IP 地址为 192.168.0.177 的从站，从站接收数据地址范围为 40051-40070，命令没有正确执行，会在内部寄存器2051报错。

Modbus TCP Client 1 - Add Command

Enable	Yes
Modbus Function	FC 16 - Preset (Write) Multiple Register
Slave Address	1
Modbus Data Address	50
Quantity	20
Data Swap	No Change
Poll Interval	0
Internal Data Address	2000
Server IP Address	192.168.0.177
Server Port Number	502
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2051
Desc	

以上指令含义如下：模块功能码FC6或者FC16时，写入数量是20。模块内部寄存器起始地址2000。表示内部寄存器范围 2000-2019 的数据，一直连续的写出到 IP 地址为 192.168.0.177 的从站，从站接收数据的地址范围为40051-40070，命令没有正确执行，会在内部寄存器2051报错。

Cmd Errors Mapping Enabled和Cmd Errors Mapping Address这两个参数介绍；

Cmd Errors Mapping Enabled表示命令错误是否映射，选择YES表示使用，选择NO，表示不使用；

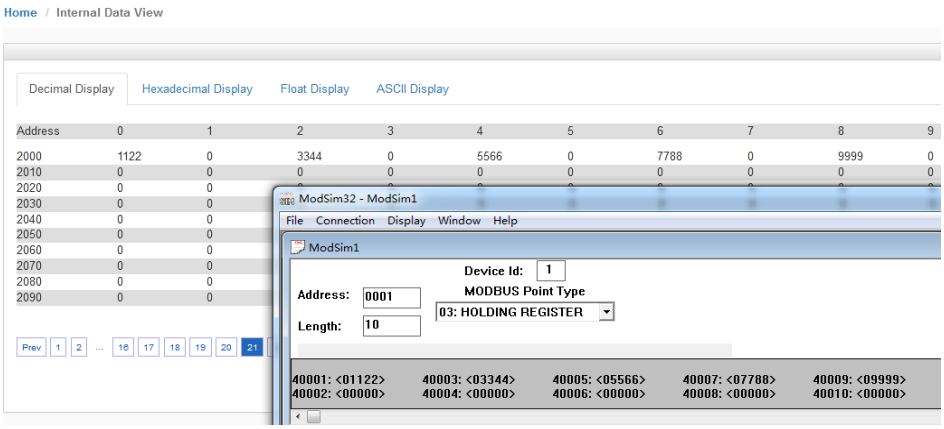
Cmd Errors Mapping Address 表示命令错误映射的地址。

Modbus TCP Client 1 - Add Command

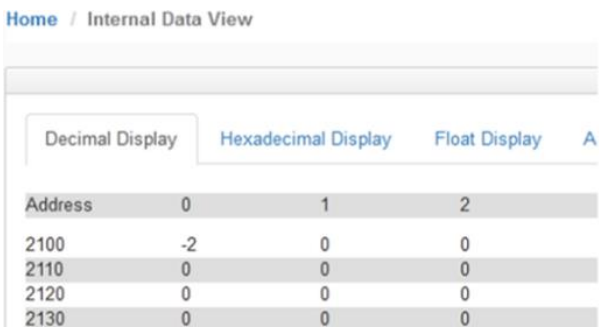
Enable	Yes
Modbus Function	FC 3 - Read Holding Registers(4X)
Slave Address	1
Modbus Data Address	0
Quantity	10
Data Swap	No Change
Poll Interval	0
Internal Data Address	2000
Server IP Address	192.168.0.177
Server Port Number	502
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2100
Desc	

以上指令含义如下：模块使用功能码 FC3，从站数据起始地址是 0 等于 40001。读取数量是 10。 模块内部寄存器起始地址 2000。表示读 IP 地址为 192.168.0.177 的从站，从站数据地址范围为 40001-40010 的 10 个字，放到模块内部寄存器 2000-2009，命令没有正确执行，返回在内部寄存器 2100 报错。

指令正确执行的效果如下图显示：

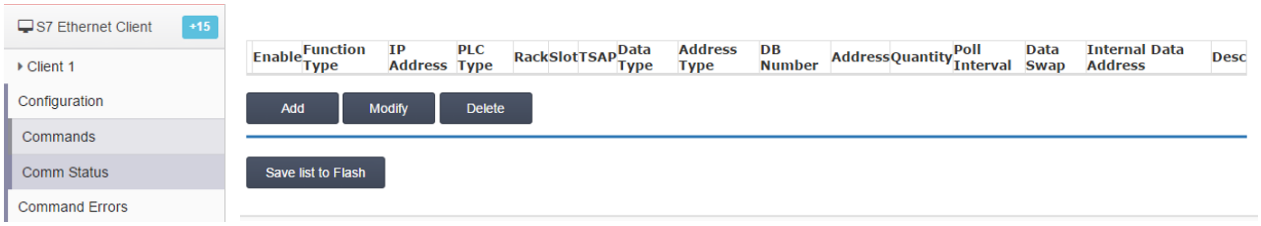


如果这条指令没有执行成功，例如：IP地址为192.168.0.177的从站，从站IP地址错误，从站掉线等等。如果开启了Cmd Errors Mapping Enabled，就会在Cmd Errors Mapping Address（本指令中选择了模块内部寄存器2100）的位置报一个非零值，显示这条命令有错误，工程师可以调用这个寄存器的数据到控制系统中，查看所连接设备的状态。



配置模块做 Siemens S7 以太网主站

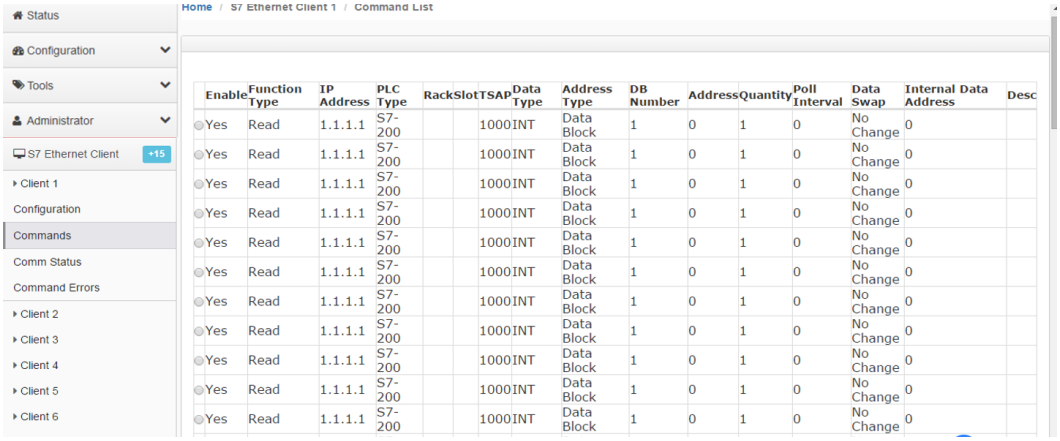
1. 点击 S7 Ethernet Client ---Client1 ---Commands



2. 点击 S7 Ethernet Client,可以看到+15.表示可以支持作为最多 15 个主站.
   点开 Configuration.查看默认的配置
   Minimum Command Delay：最小通讯延时 0-65535
   Response Timeout：西门子 PLC 响应时间 0-65535
   Retry Count：重新尝试连接次数 0-65535

3. 配置命令参数， 

用来读或写西门子 PLC 的命令。每个主站支持最大 32 条指令。如果同时连接 5 个西门子 PLC，建议在 Client1-Client5 配置每一个主站分别对每个西门子 PLC 的读写。可以减小指令执行时间，以及设备掉线后对于其他设备的影响。



点击 Add ，可以增加新的命令，如下为针对不同种类西门子 PLC 添加指令的配置界面：

S7 Ethernet Client 1 - Add Command

Enable	Yes	是否启用命令
Function Type	Read	读/写
IP Address	1.1.1.1	西门子S7-200的以太网模块IP地址
PLC Type	S7-200	西门子PLC的种类
TSAP	1000	西门子S7-200的TSAP参数
Data Type	INT	数据类型
Address Type	Data Block (DB)	地址类型
DB Number	1	DB块的号码
Address	0	起始地址
Quantity	1	数量
Data Swap	No Change	数据是否交换高地位
Poll Interval	0	每条命令发送间隔的时间
Internal Data Address	0	网关内部数据库寄存器地址
Desc		命令描述

Click save to continue add command,click close to finish add. Close Save

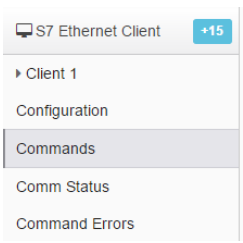
undefined - Add Command

Enable	Yes	是否启用命令
Function Type	Read	读/写
IP Address	1.1.1.1	西门子S7-300, S7-400, S7-1200以太网接口的IP地址
PLC Type	S7-300/S7-400/S7-1200	西门子PLC的种类
Rack	0	西门子CPU所在的机架号
Slot	1	西门子CPU所在的槽位号
Data Type	INT	数据类型
Address Type	Data Block (DB)	地址类型
DB Number	1	DB块的号码
Address	0	起始地址
Quantity	1	数量
Data Swap	No Change	数据是否交换高地位
Poll Interval	0	每条命令发送的间隔时间
Internal Data Address	0	网关内部数据库寄存器地址
Desc		命令描述

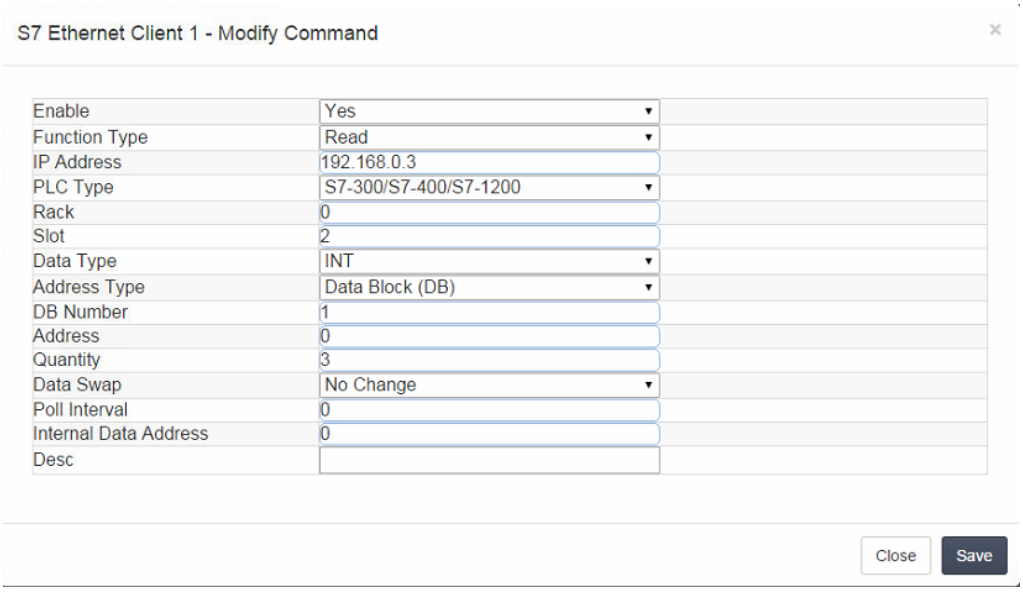
Click save to continue add command,click close to finish add. Close Save

举例读写西门子 PLC 整型数据

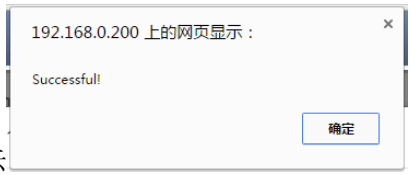
配置 S7-Eethernet Client 主站指令，点击 S7-Eethernet Client----Commands 建立指令，读或写西门子 DB 数据块的数据。



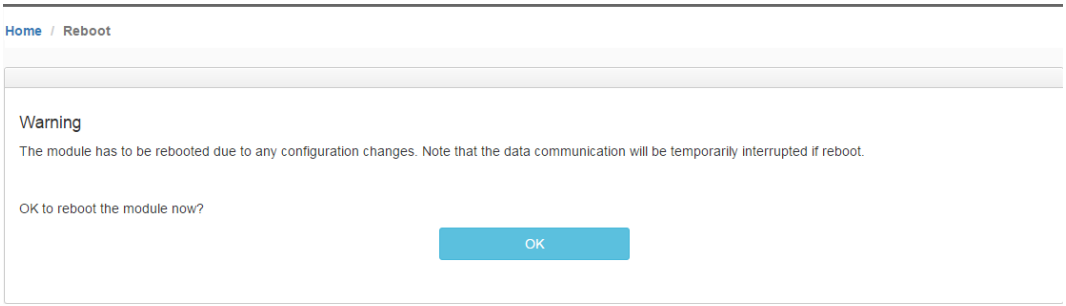
读指令解释如下，读取 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器，把其中的 DB1 数据块里面的 3 个 INT 读到模块内部数据寄存器地址 0-2 中.



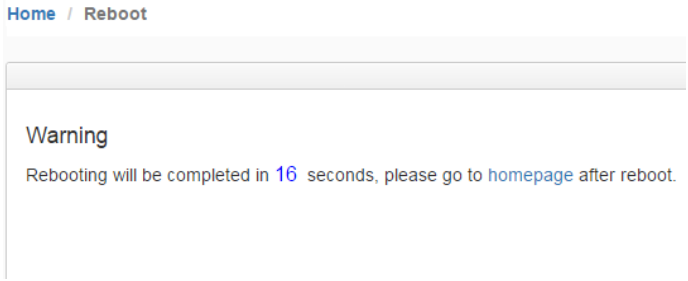
命令的要注意的地方，Slot 是指西门子 CPU 的槽位，Address 是指 DB 数据的起始地址，Quantity 是指要传输几个数据，Data Swap 是指传输的数据是否进行高低位交换，Internal Data Address 是指模块内部寄存器的起始地址。

点击 Save 保存，提示 

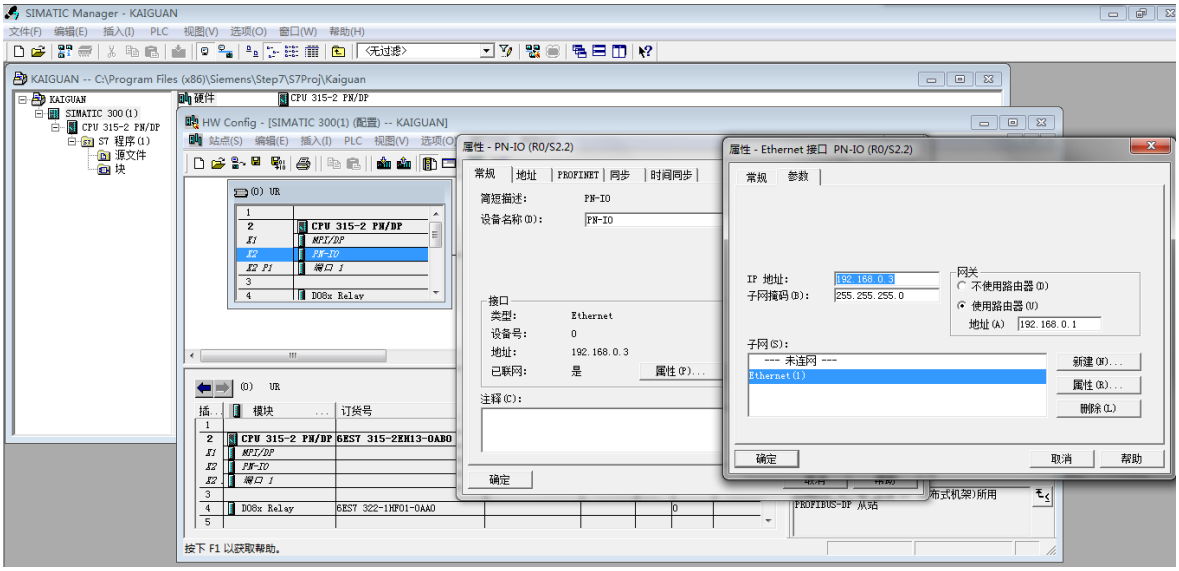
，然后点击 Close 关闭这个命令。接着点击 Save list to Flash 把这个命令保存到模块里面。

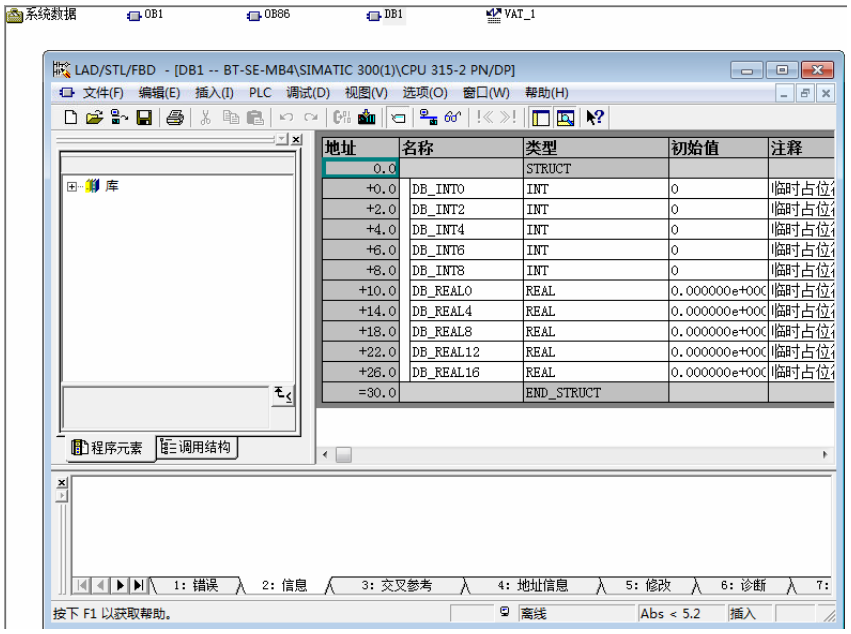


提示重启模块，点击 OK 完成重启。

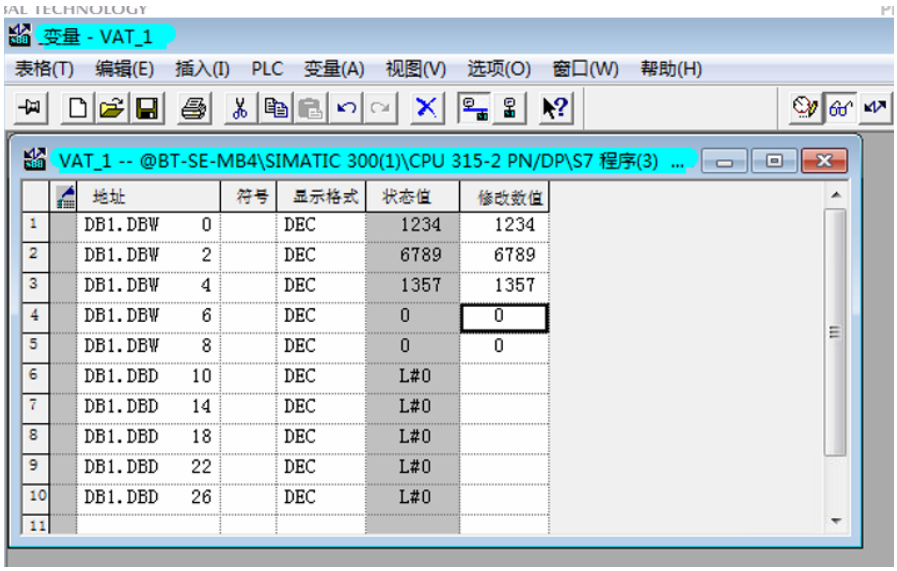


配置西门子 PLC 一侧，建立 DB 块



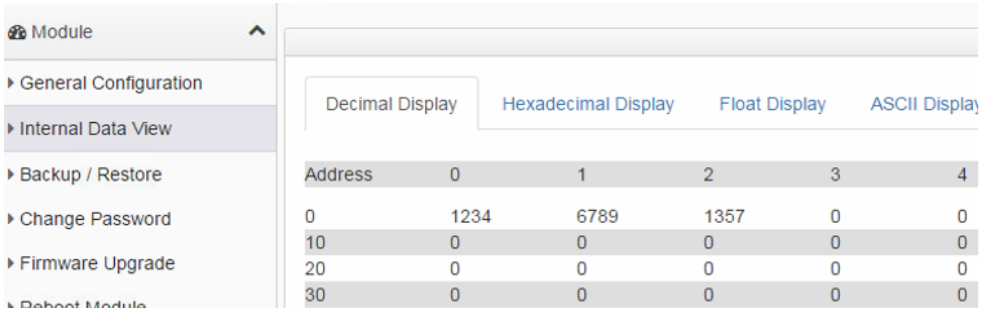


在 DB1.DBW0，DB1.DBW2，DB1.DBW4 里面写点数据。点击  赋值。



	地址	符号	显示格式	状态值	修改数值
1	DB1.DBW 0		DEC	1234	1234
2	DB1.DBW 2		DEC	6789	6789
3	DB1.DBW 4		DEC	1357	1357
4	DB1.DBW 6		DEC	0	0
5	DB1.DBW 8		DEC	0	0
6	DB1.DBD 10		DEC	L#0	
7	DB1.DBD 14		DEC	L#0	
8	DB1.DBD 18		DEC	L#0	
9	DB1.DBD 22		DEC	L#0	
10	DB1.DBD 26		DEC	L#0	
11					

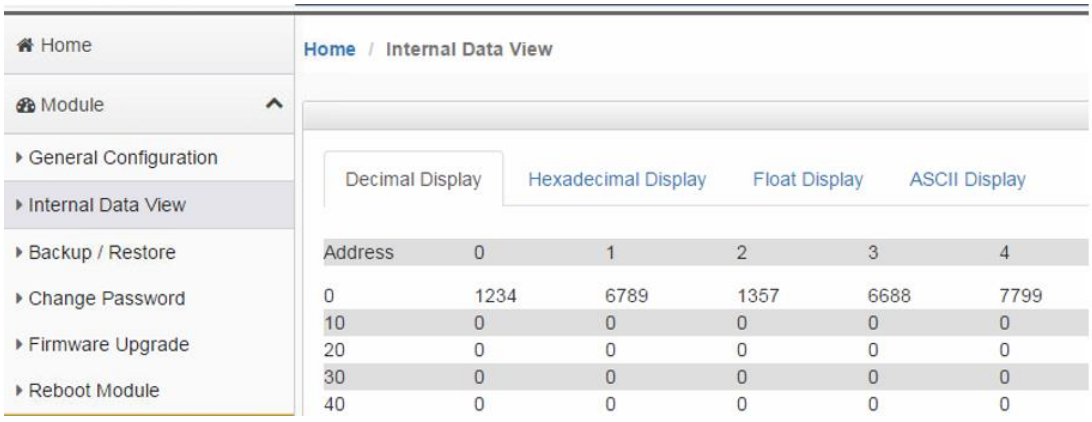
返回模块网页查看内部数据寄存器地址 0-2 中读入了相同的数据。



Address	0	1	2	3	4
0	1234	6789	1357	0	0
10	0	0	0	0	0
20	0	0	0	0	0
30	0	0	0	0	0

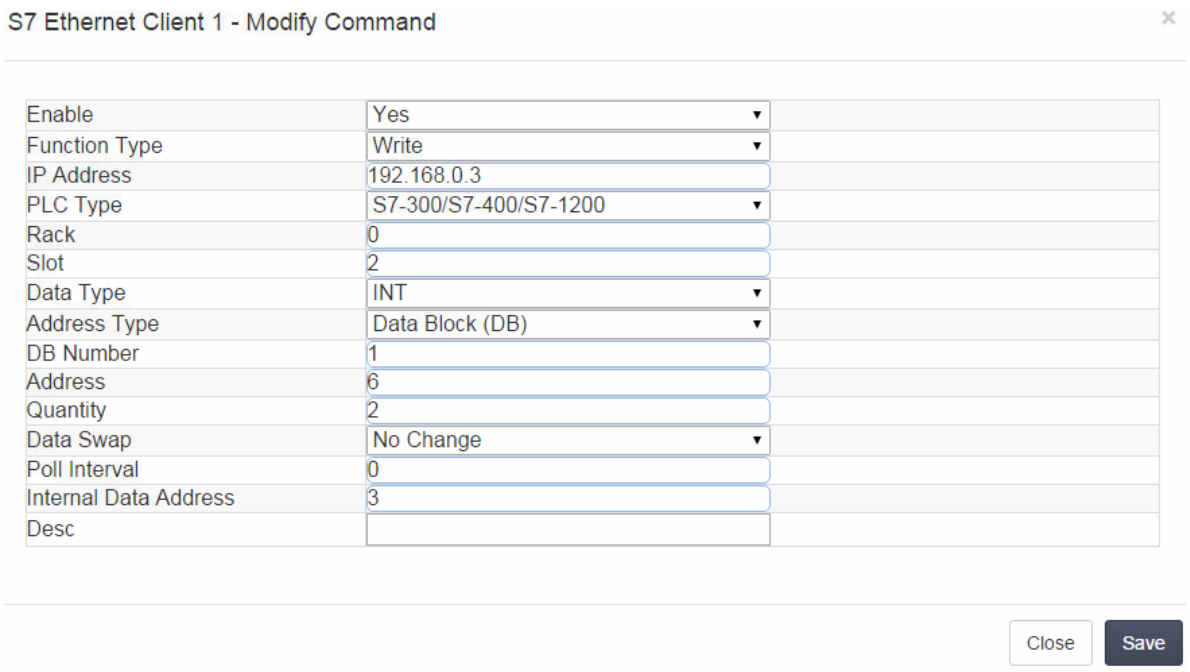
为模块内部寄存器赋值（不同型号模块，可使用不同的驱动协议为模块数据区赋值），再配置命令写给西门子 DB1.DBW6 和 DB1.DBW8。

模块内部数据寄存器地址 3-4 被赋值数据，地址 0-2 是从西门子读到的数据。

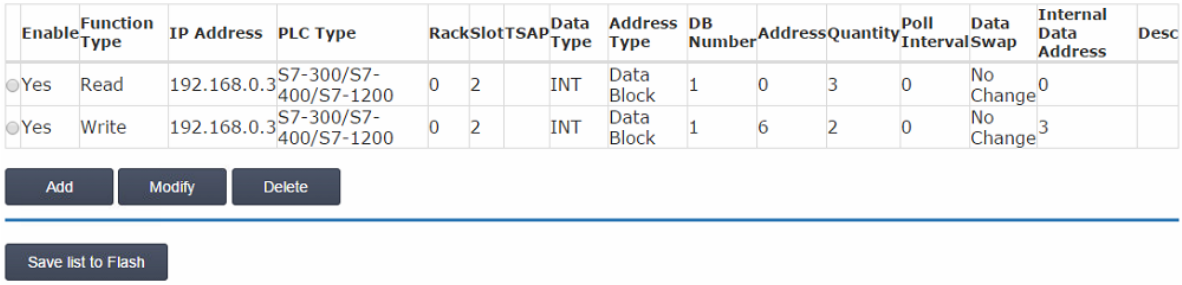


Address	0	1	2	3	4
0	1234	6789	1357	6688	7799
10	0	0	0	0	0
20	0	0	0	0	0
30	0	0	0	0	0
40	0	0	0	0	0

在模块 S7 以太网一侧配置写出指令如下

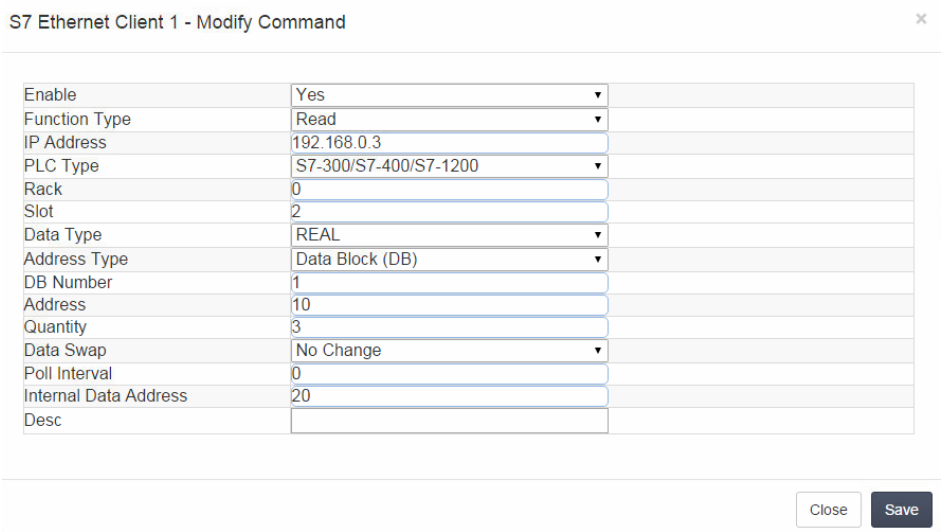


以上指令含义为，从模块内部数据区起始地址 3 开始，调用 2 个整型数，写给 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器，写入 DB1 数据块里面的 DBW6 和 DBW8.保存该指令，重启模块。



查看西门子 PLC 的数据，可以看到 DB1.DBW6 和 DB1.DBW8 的状态值，和模块内部数据区一致。

举例：读写西门子 PLC 浮点数



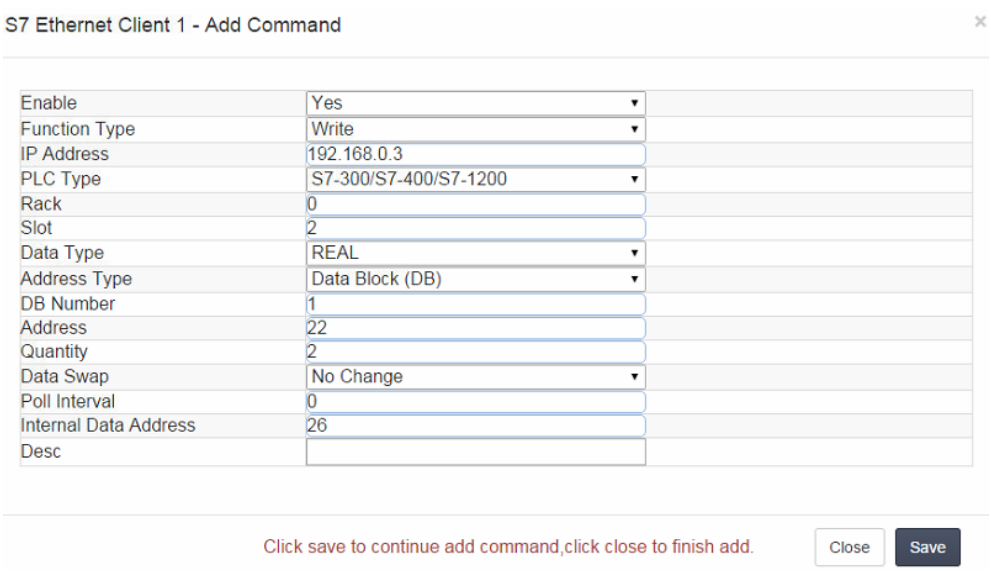
以上指令解释如下，读取 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器，把其中的 DB1 数据块里面，从 DBD10 开始的 3 个 REAL 类型数据，读到模块内部数据寄存器起始地址为 20 的区域中. 因为模内部数据寄存器为 16 位的字，所以 3 个浮点数会占用 6 个寄存器，也就是存放到模块内部地址 20-25 中

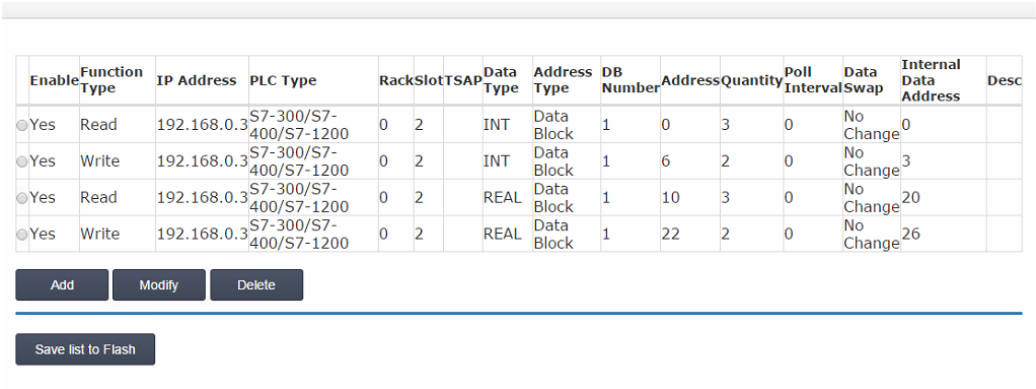
如下图，在西门子 PLC 中 DB1.DBD10/14/18 中赋值

模块内部数据区 20-25 的 6 个寄存器将会读取到了相同的数值。

之后再次为模块内部寄存器 26-29 赋值 2 个浮点数，998.5432 和 -99.1111。（不同型号模块，可使用不同的驱动协议为模块数据区赋值）。

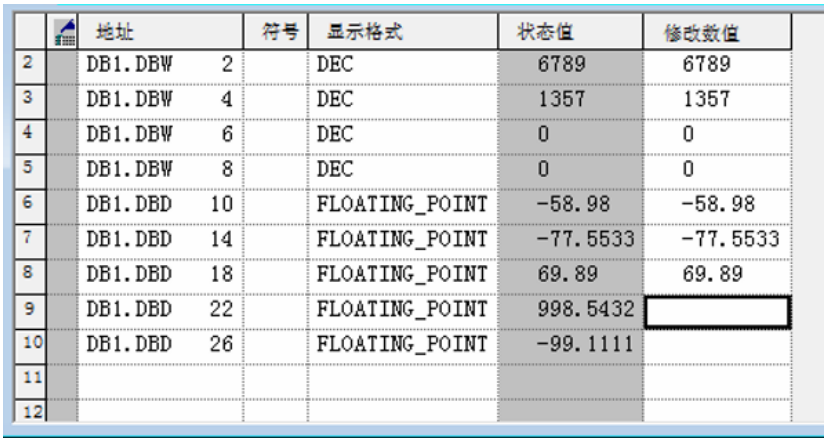
在模块 S7 以太网主站建立一条写指令含义为，从模块内部数据区起始地址 26 开始，调用 2 个 REAL 类型数据，写给 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器，写入 DB1 数据块里面的 DBD22 和 DBD26.保存该指令，重启模块。





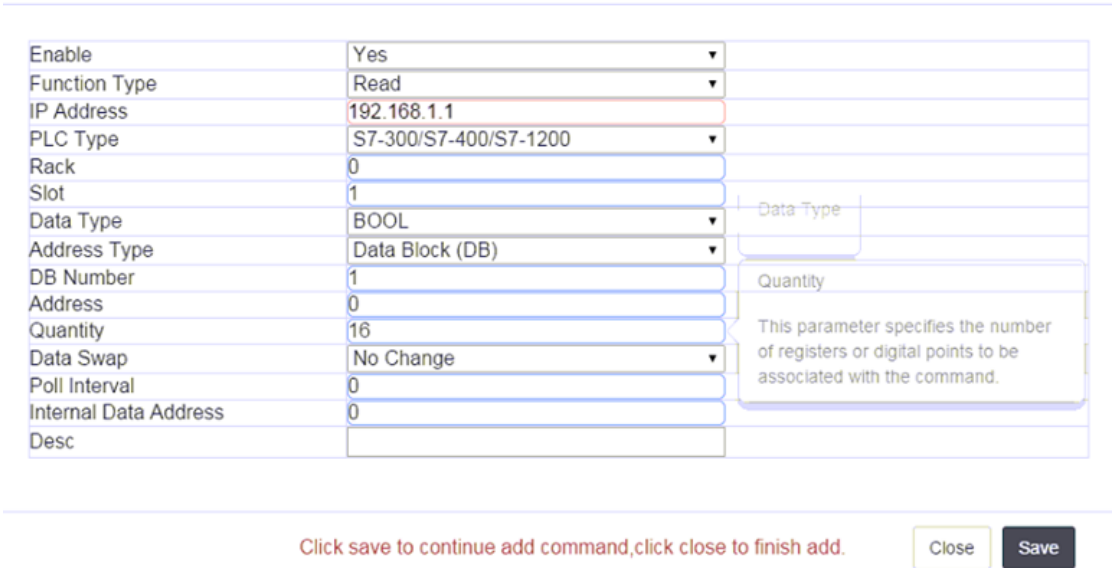
点击 Save list to Flash 重启网关，让命令生效。

如下图查看西门子 PLC 的数据，可以看到 DB1.DBD22 和 DB1.DBD26 的数据值，和模块内部数据区一致。

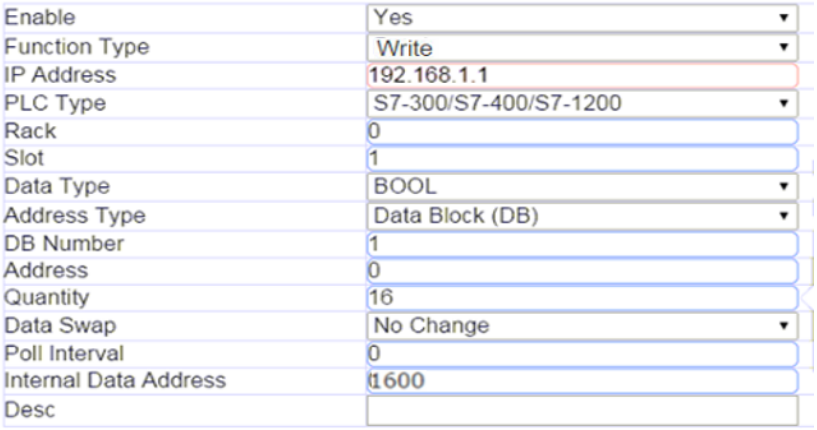


	地址	符号	显示格式	状态值	修改数值
2	DB1.DBW 2		DEC	6789	6789
3	DB1.DBW 4		DEC	1357	1357
4	DB1.DBW 6		DEC	0	0
5	DB1.DBW 8		DEC	0	0
6	DB1.DBD 10		FLOATING_POINT	-58.98	-58.98
7	DB1.DBD 14		FLOATING_POINT	-77.5533	-77.5533
8	DB1.DBD 18		FLOATING_POINT	69.89	69.89
9	DB1.DBD 22		FLOATING_POINT	998.5432	
10	DB1.DBD 26		FLOATING_POINT	-99.1111	
11					
12					

举例. 读写西门子 PLC 的布尔量



以上读指令解释如下，读取 IP 地址为 192.168.1.1 的西门子 1200 系列控制器的位数据，读取 DB1 数据块里面的前两个字节中的 16 个布尔量，放进模块内部数据寄存器起始地址为 0 的区域。
此处需要注意，模块内部寄存器都是 16 位的字，所以 16 个布尔量占用 1 个寄存器地址。



以上指令解释如下，调用模块内部数据寄存器起始地址为 100 的连续 16 个布尔量数据，写入到 IP 地址为 192.168.1.1 的西门子 S7-300 系列控制器中，写入的位置为 DB1 数据块里面的前两个字节中的 16 个位。
此处需要注意，模块内部寄存器都是 16 位的字，所以写出布尔量时，内部寄存器的起始地址的真实位置为 1600/16=100，写出 16 个布尔量，正好写出一个寄存器内的数据。

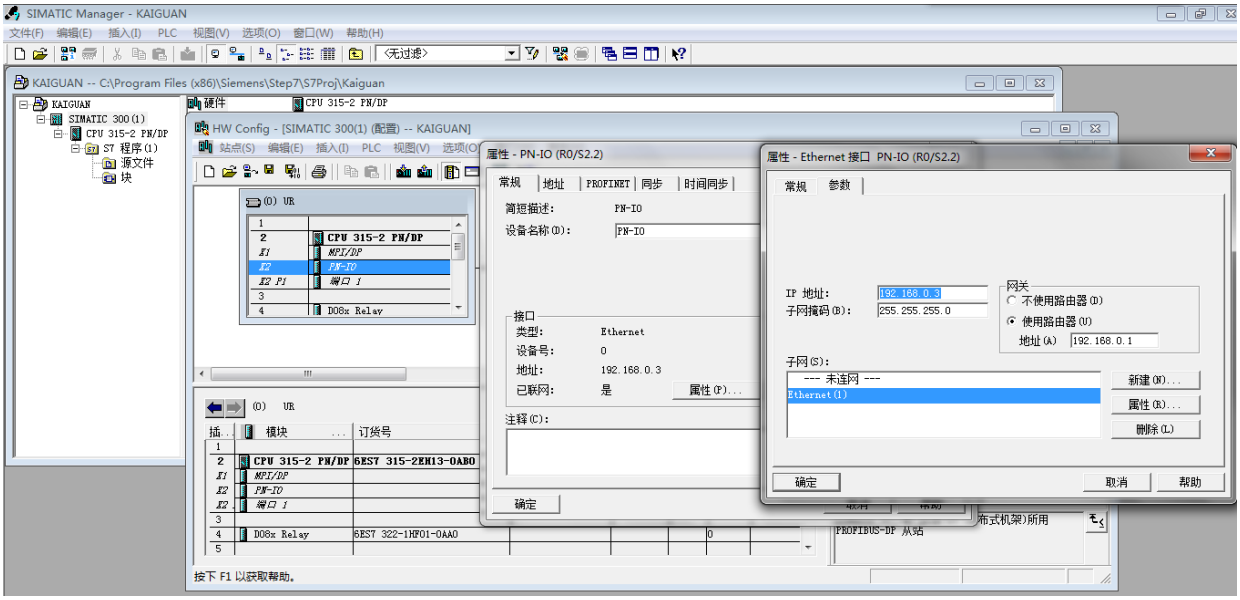
以上介绍了 S7 以太网主站指令对 INT 类型，REAL 类型，BOOL 类型数据读写操作指令。
此外 S7 以太网主站指令，还可以对 BYTE，DINT 进行操作，此处不再详细举例。

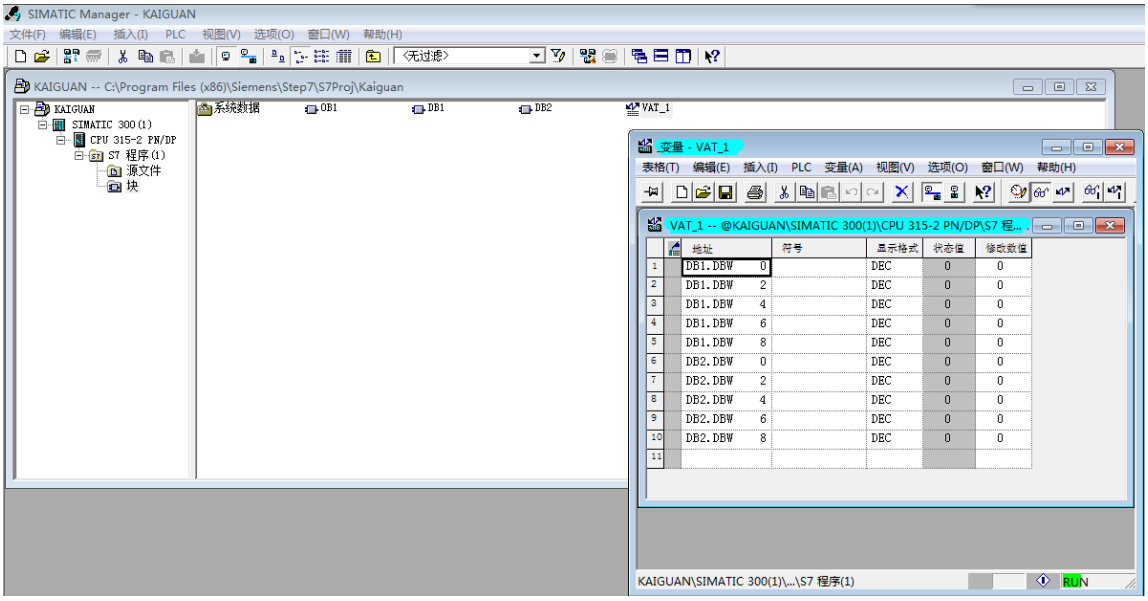
举例 1.罗克韦尔 1756PLC 和西门子 PLC 315-2DP/PN 通讯

本案例中配置模块做 EtherNet/IP server，做 S7 以太网 client

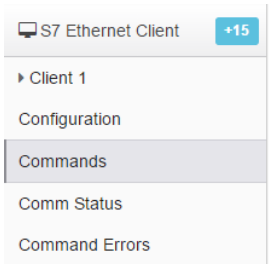
西门子多个 DB 块的数据可以被读取，本例以 DB1 和 DB2 为例。每个 DB 块包含 5 个数据，由模块进行读取。

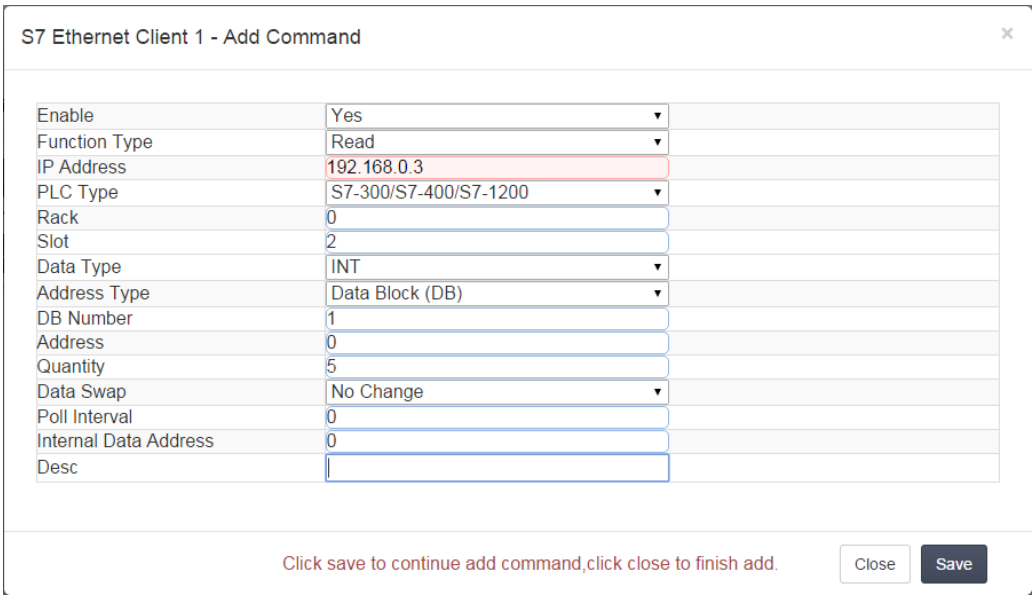
西门子 PLC 内部配置如下：





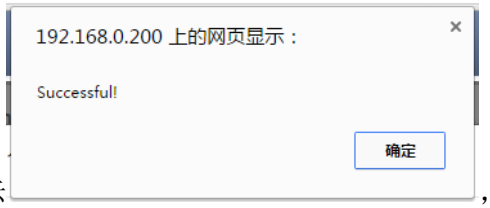
之后在模块中选择S7 Ethernet Client这里做配置，点击S7-Eethernet Client-Commands 建立两条读指令



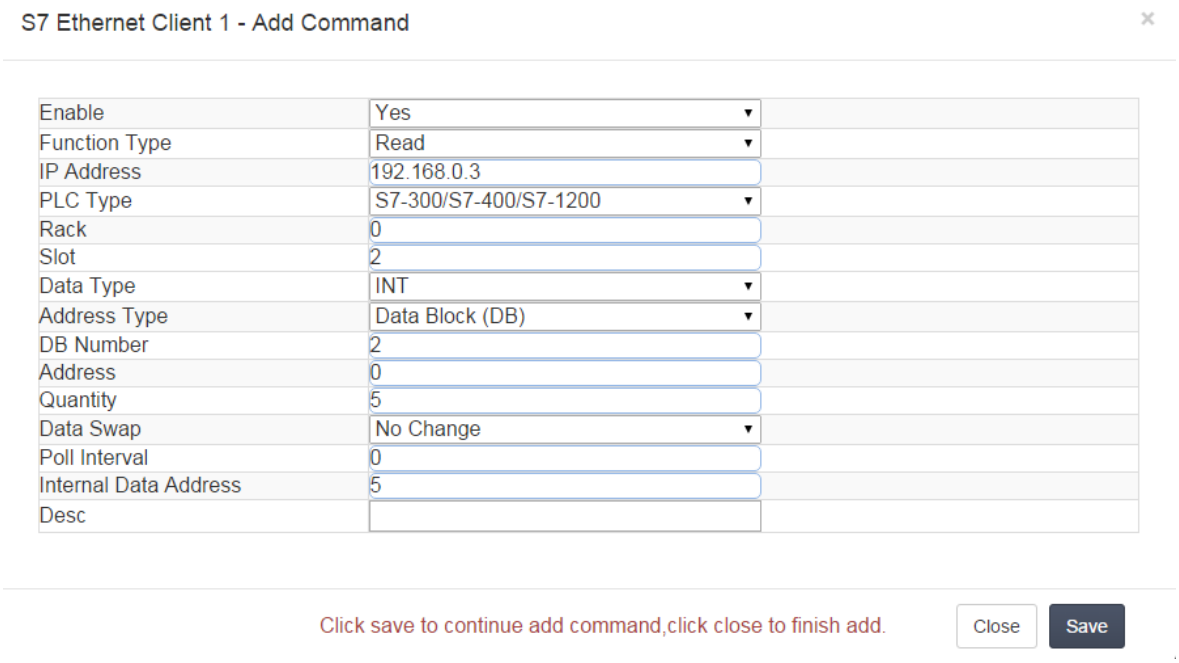


第一条命令的要注意的地方，Slot 是指西门子 CPU 的槽位，Address 是指 DB 数据的起始地址，Quantity 是指要传输几个数据，Data Swap 是指传输的数据是否进行高低位交换，Internal Data Address 是指读到的数据存放在模块内部寄存器起始地址。

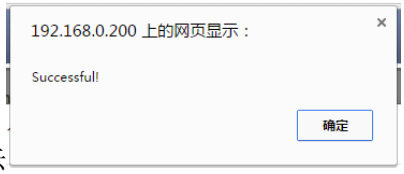
第一条命令的含义是模块读取 IP 地址为 192.168.0.3 的西门子 PLC DB1 内的前 5 个 INT 字，存入模块内部寄存器地址 0-4，总共 5 个寄存器里面。

点击 Save 保存，提示 

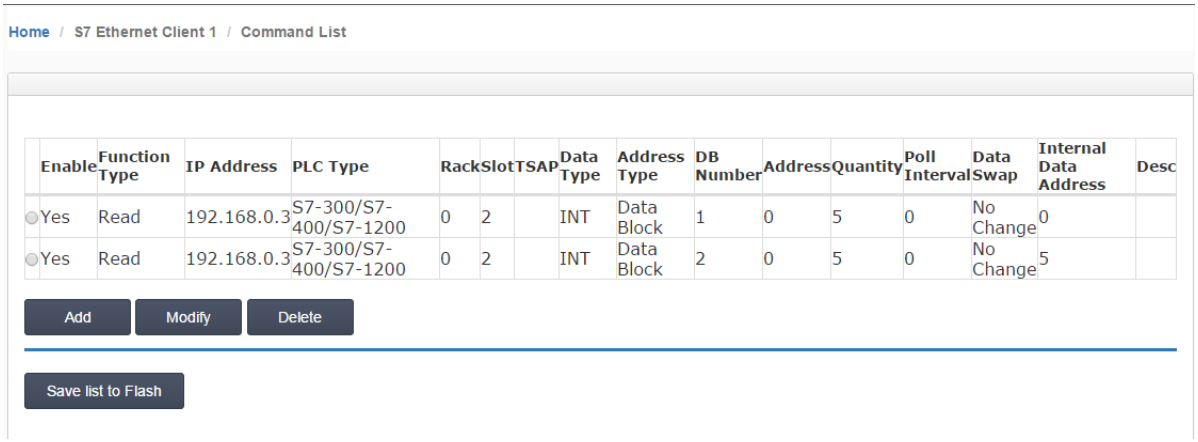
，接着写第二条指令，

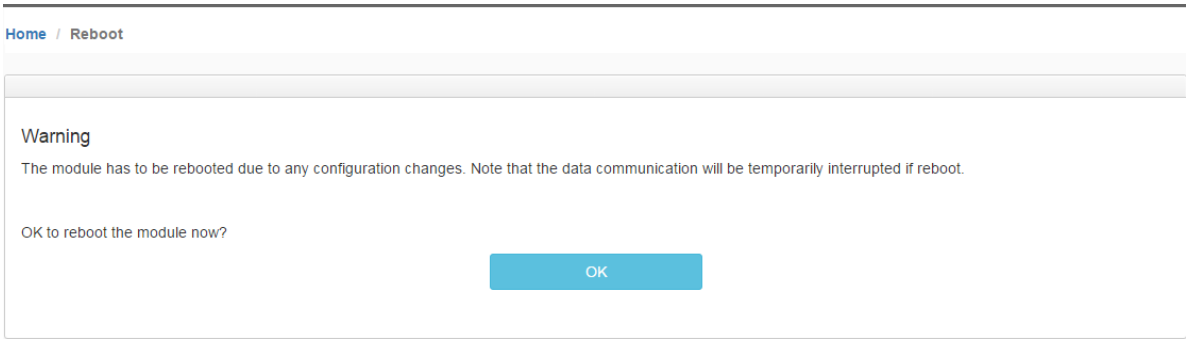


第二条命令的含义是模块读取 IP 地址为 192.168.0.3 的西门子 PLC DB2 内的前 5 个字，存入模块内部寄存器地址 5-9，总共 5 个寄存器里面。

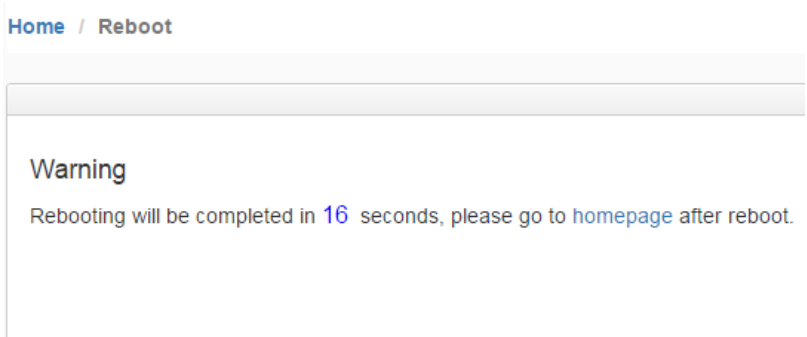


点击 Save 保存，提示，然后点击 Close 关闭这个命令。接着点击 Save list to Flash 把这个命令保存到模块里面。

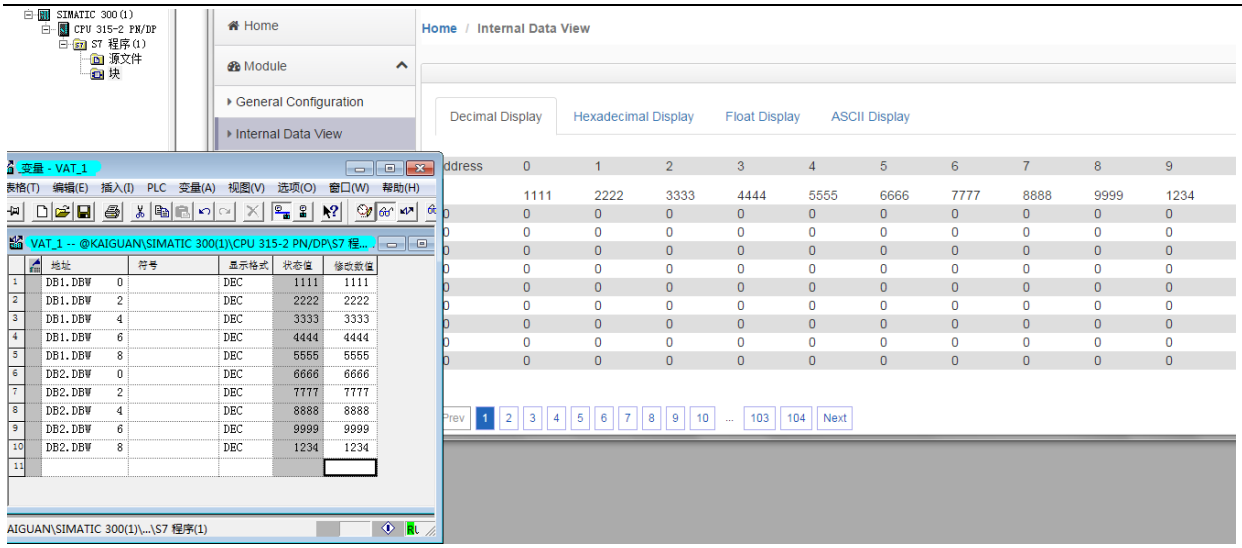




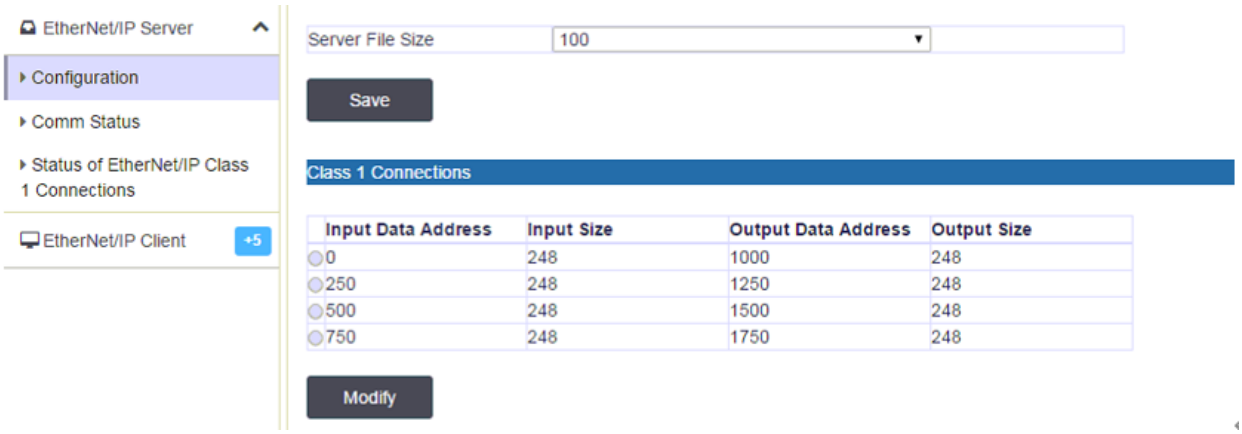
提示重启模块，点击 OK 完成重启。



在西门子 PLC 变量表里面写入一些数据，可以看到模块寄存器 0-9 总共 10 个寄存器显示有数据被读取到。



配置模块做 EtherNet/IP Class 1 Server 从站，根据下图分配输入输出寄存器区域



在 Logix50000 内建立 CIP 输入输出数组，具体内容请见前文“配置模块做 EtherNet/IP server”对应关系如下

PLC 输入数据标签组

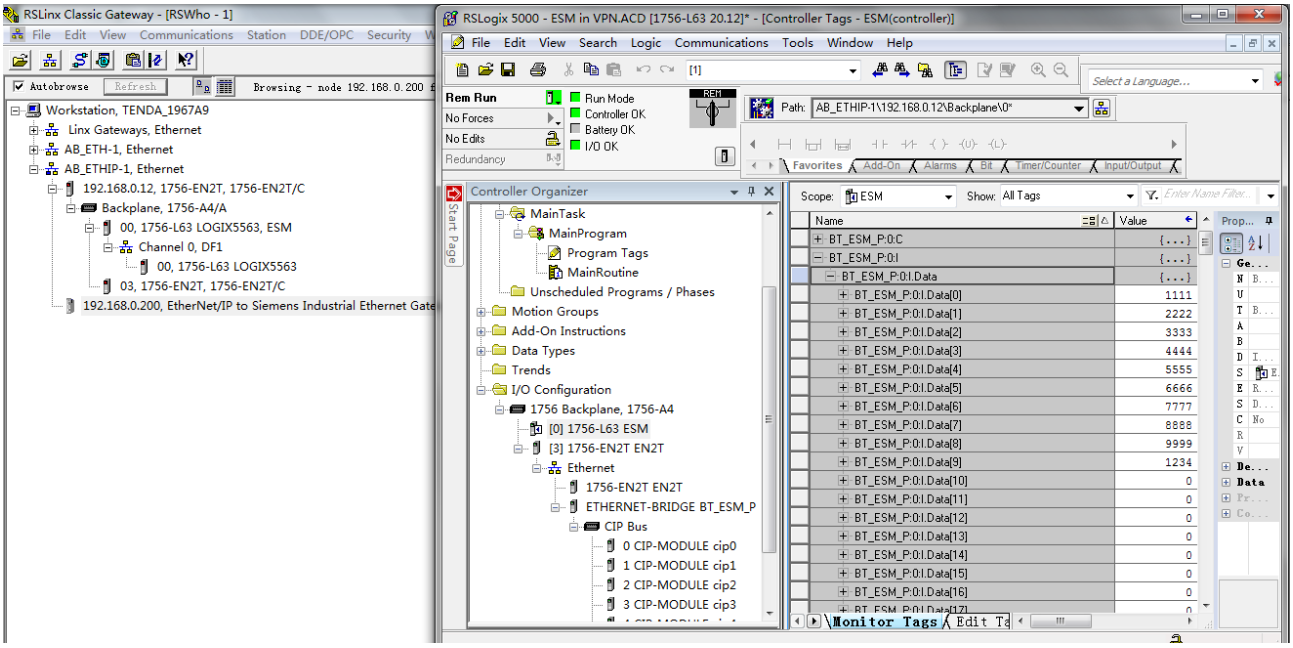
BT_ESM_P:0:I.Data[0]- [247]对应模块内部寄存器地址 0-247，

BT_ESM_P:1:I.Data[0] -[247]对应模块内部寄存器地址 250-497

BT_ESM_P:0:O.Data[0] -[247]对应模块内部寄存器地址 1000-1247，

BT_ESM_P:1:O.Data[0] -[247]对应模块内部寄存器地址 1250-1497

配置完成后，可以看到 PLC 内的输入标签组 BT_ESM_P:0:I 有数据从模块传输过来，与之前在西门子 PLC 内部键入的数据一致。



举例 2.罗克韦尔 1756PLC 和西门子 PLC 315-2DP/PN 通讯

本案例中配置模块做 EtherNet/IP Client，做 S7 以太网 client

模块可以同时做 EtherNet/IP Client 和 server，所以这种方式无需修改 PLC 原有配置，适用于改造项目中不停机传输数据。

首先在罗克韦尔 PLC 程序内建立一个标签“S7_READ”，包含 10 个 INT 数据

S7_READ			INT[10]
S7_READ[0]			INT
S7_READ[1]			INT
S7_READ[2]			INT
S7_READ[3]			INT
S7_READ[4]			INT
S7_READ[5]			INT
S7_READ[6]			INT
S7_READ[7]			INT
S7_READ[8]			INT
S7_READ[9]			INT

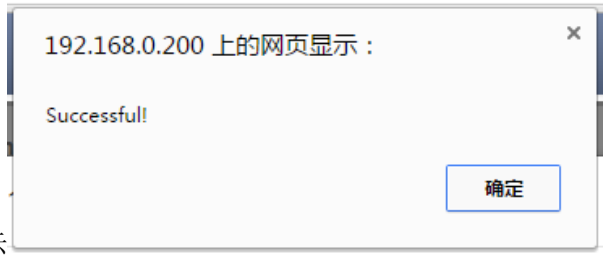
再配置模块 EtherNet/IP Client---Client 1—Commands，含义为从模块内部数据区 0 开头的 10 个连续数据写给罗克韦尔 PLC 标签“S7_READ”，写入的区域起始地址为“S7_READ[0]”

EtherNet/IP Client 1 - Add Command

Controller Tag

Enable	Yes
Function Type	CIP Data Table Write
IP Address	192.168.0.12
Slot	0
Quantity	10
Poll Interval	0
Data Swap	No Change
Internal Data Address	0
Data Type	INT
Tag Name	S7_READ
Tag Offset	0
Desc	

Click save to continue add command,click close to finish add. Close Save



点击 Save，提示，然后点击 Close 关闭这个命令。接着点击 Save list to Flash 把这个命令保存到模块里面。

同时仍然继续使用上一个案例中配置完成的两条 S7 以太网主站的指令，如下图。

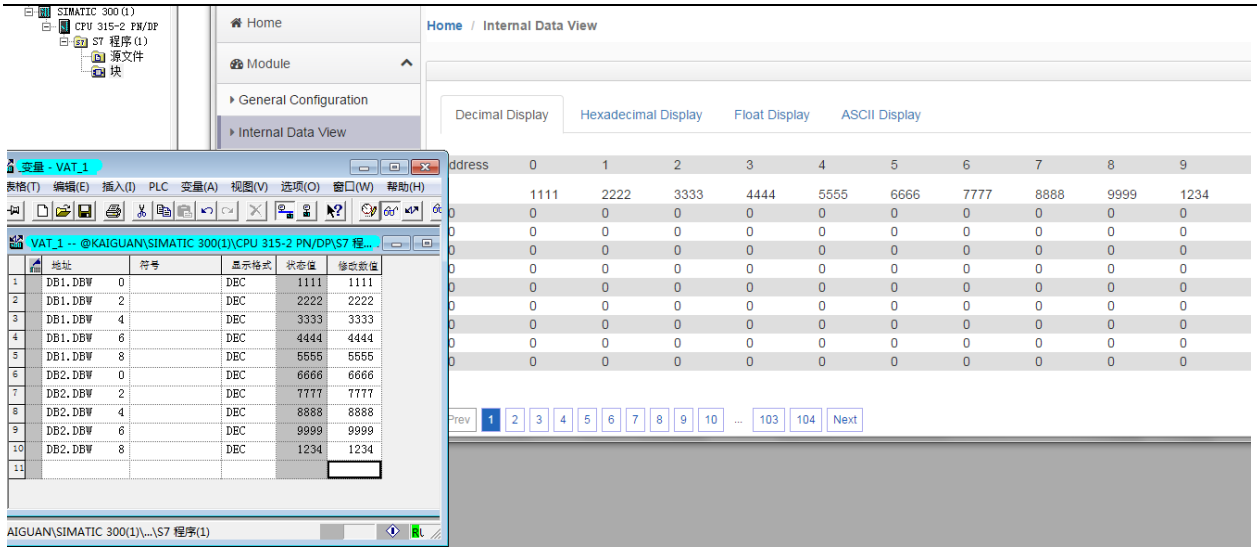
Home / S7 Ethernet Client 1 / Command List

Enable	Function Type	IP Address	PLC Type	Rack	Slot	TSAP	Data Type	Address Type	DB Number	Address	Quantity	Poll Interval	Data Swap	Internal Data Address	Desc
Yes	Read	192.168.0.3	S7-300/S7-400/S7-1200	0	2		INT	Data Block	1	0	5	0	No Change	0	
Yes	Read	192.168.0.3	S7-300/S7-400/S7-1200	0	2		INT	Data Block	2	0	5	0	No Change	5	

Add Modify Delete

Save list to Flash

前文中介绍了，模块配置好的 S7 以太网指令，已经将西门子 PLC 变量已经读取到了模块内部数据 0-9，可以看到模块寄存器地址 0-9 总共 10 个寄存器显示有数据被读入。



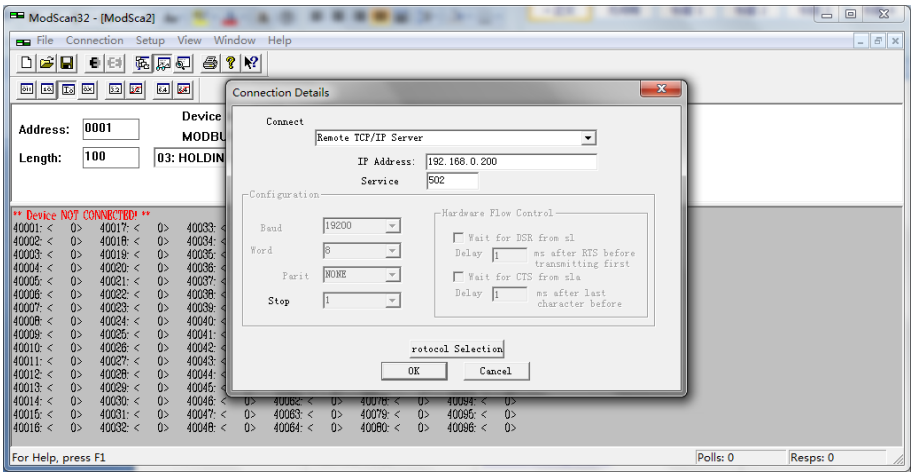
再查看罗克韦尔 PLC 建立的标签，可以看到数据从模块写入进来，与之前西门子 PLC 键入数据一致。

S7_READ	{...}	{...}	Decimal	INT[10]
S7_READ[0]	1111		Decimal	INT
S7_READ[1]	2222		Decimal	INT
S7_READ[2]	3333		Decimal	INT
S7_READ[3]	4444		Decimal	INT
S7_READ[4]	5555		Decimal	INT
S7_READ[5]	6666		Decimal	INT
S7_READ[6]	7777		Decimal	INT
S7_READ[7]	8888		Decimal	INT
S7_READ[8]	9999		Decimal	INT
S7_READ[9]	1234		Decimal	INT

举例 3. Modbus TCP 设备和罗克韦尔 PLC 交换数据

本案例中配置模块做 Modbus TCP server，做 EtherNet/IP server

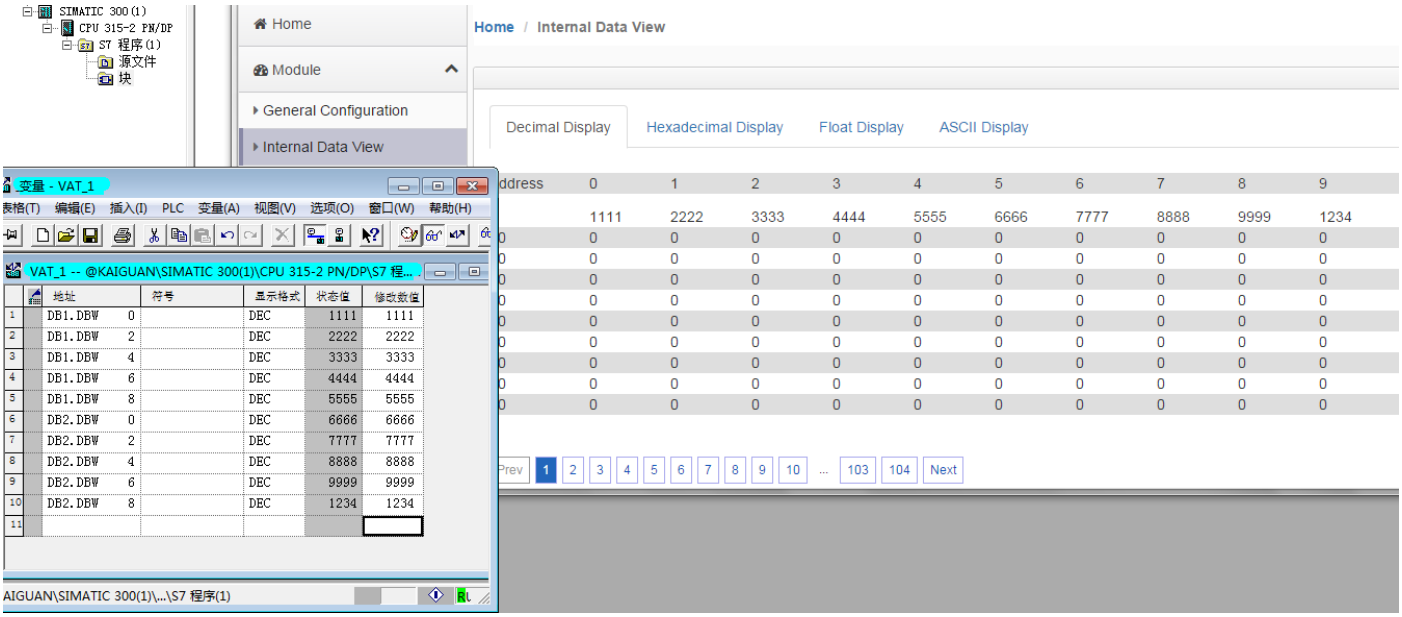
通过 Modscan32 仿真 Modbus TCP 主站，连接模块作为 Modbus TCP Server。模块默认配置是 Modbus TCP Server，不做任何设定。点击连接，选择 Remote TCP/IP Server. 192.168.0.200 是模块的 IP 地址。



模块内部寄存器地址区和 Modbus TCP 主站地址映射关系如下：

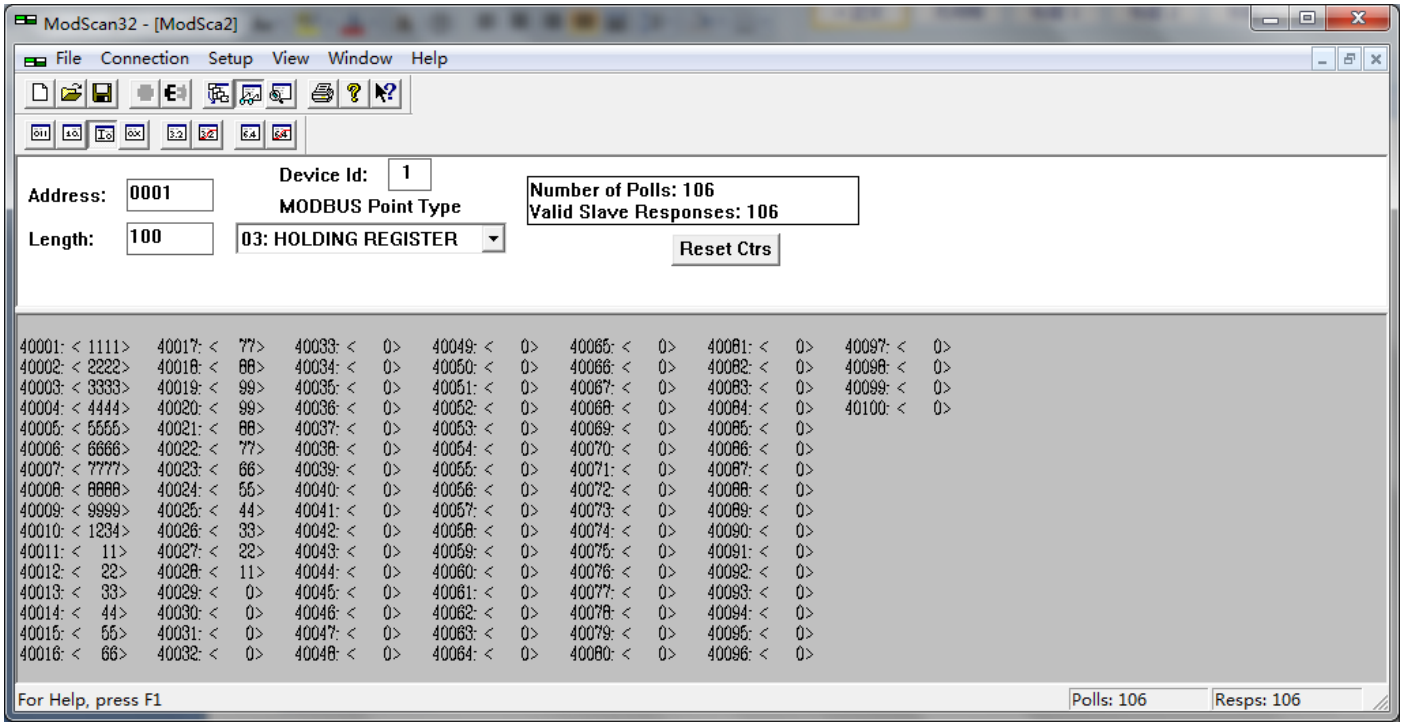
模块内部寄存器地址	等于	Modbus4区 地址
0	=	40001
1	=	40002
10	=	40011
11	=	40012
20	=	40021
30	=	40031
99	=	40100
100	=	40101

模块可以同时支持三种以太网协议之间相互传输数据，所以模块和仿真软件连接后，Modscan 读取模块 4 区的地址位 40001-40010，就可以读取到模块的内部数据区 0-9 的数据，由此可以看到，在之前的测试中模块从西门子 PLC 读到的数据，这时候仍然存储在模块内部数据区 0-9，同时也可以被仿真软件读取到 40001-40010 里面。

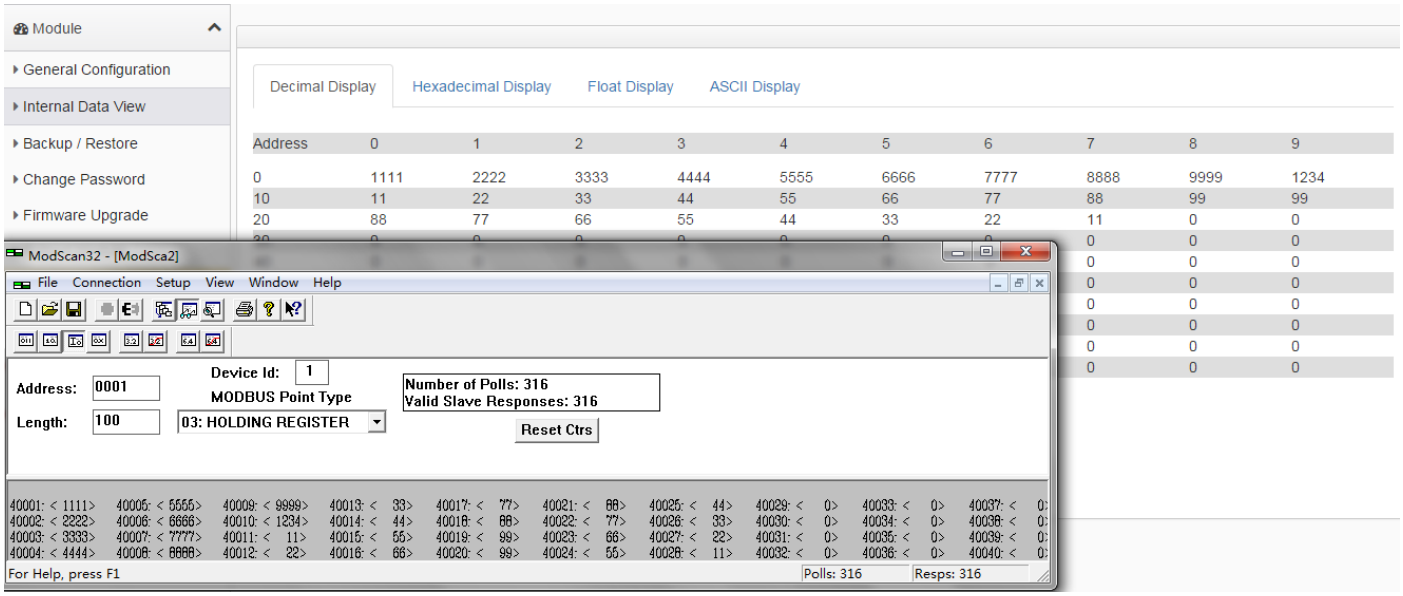


之后在仿真软件的地址区 40011 到 40028 里面写数据，可以看到模块里的内部寄存器 10-27 中相应的变化。

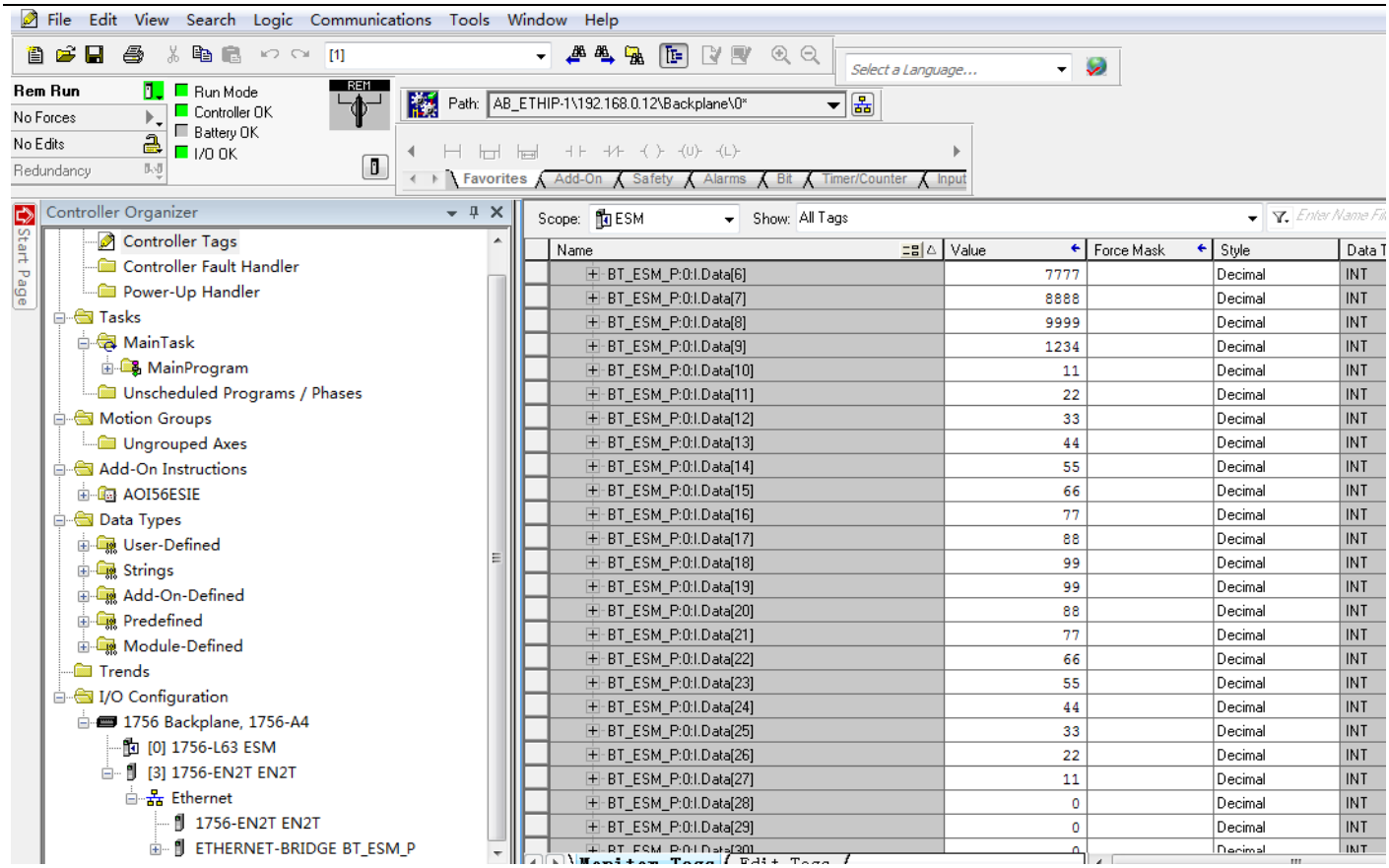
下图为仿真软件中地址位 40011 到 40028 键入数据



下图为模块里的内部寄存器 10-27 中相应的变化：



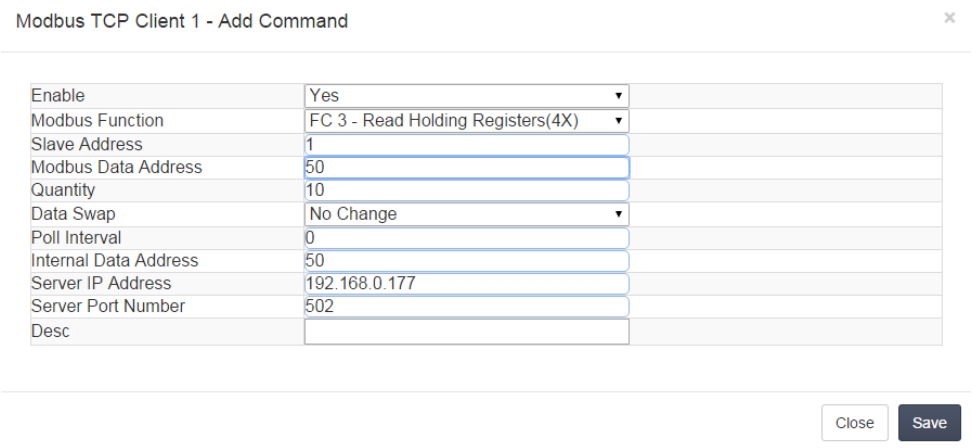
同时，由于在之前的测试中，已经对于模块内部数据区和罗克韦尔 PLC 之间地址区之间建立了 CIP 映射，所以从仿真软件地址区 40011 到 40028 写到模块内部寄存器地址 10-27 的数据，就通过模块被读取到了罗克韦尔 PLC BT_ESM_P:0:I.Data[10]- BT_ESM_P:0:I.Data[27]里面。



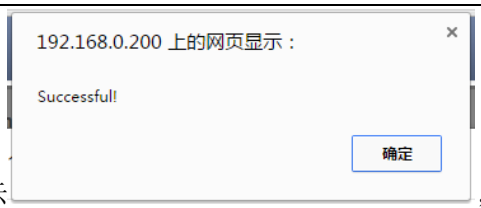
举例 4.Modbus TCP 设备和罗克韦尔 PLC 交换数据

本案例中配置模块做 Modbus TCP Client，做 EtherNet/IP server

通过 Modsim32 仿真做 Modbus TCP 从站，模块作为 Modbus TCP Client 读取数据 ,选择模块 Modbus TCP Client --Client 1—Commands 中配置命令。

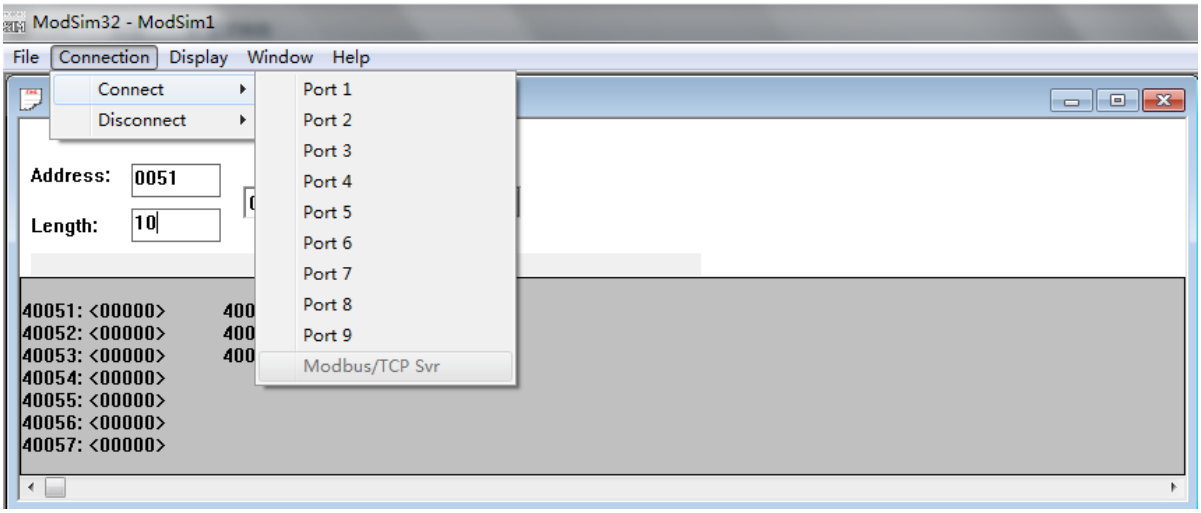


命令含义，模块读取 IP 地址为 192.168.0.177 的 Modsim32（DCS）中连续 10 个数据，地址范围是 40051-40060，存入到模块内部寄存器 50-59 里面。

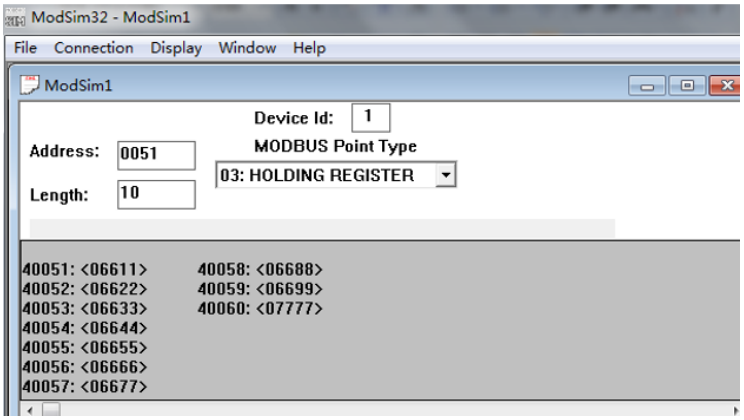


点击 Save， 提示，然后点击 Close 关闭这个命令。接着点击 Save list to Flash 把这个命令保存到模块里面。

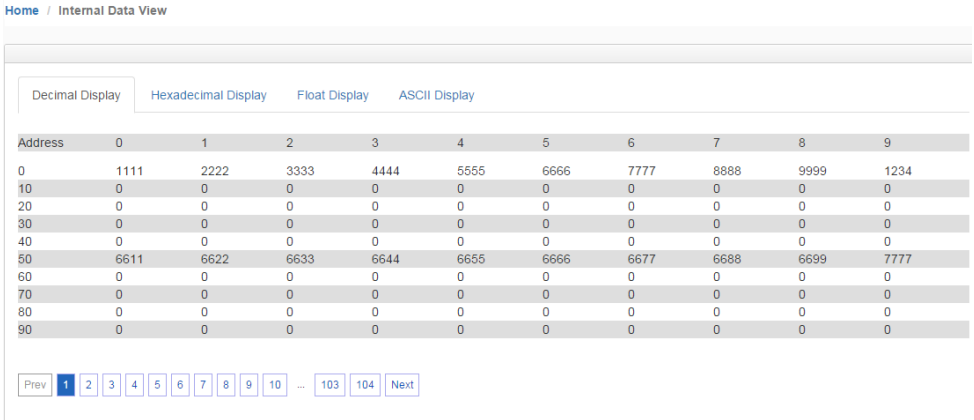
打开 Modsim32,点击 Connection - Connect---Modbus/TCP Svr



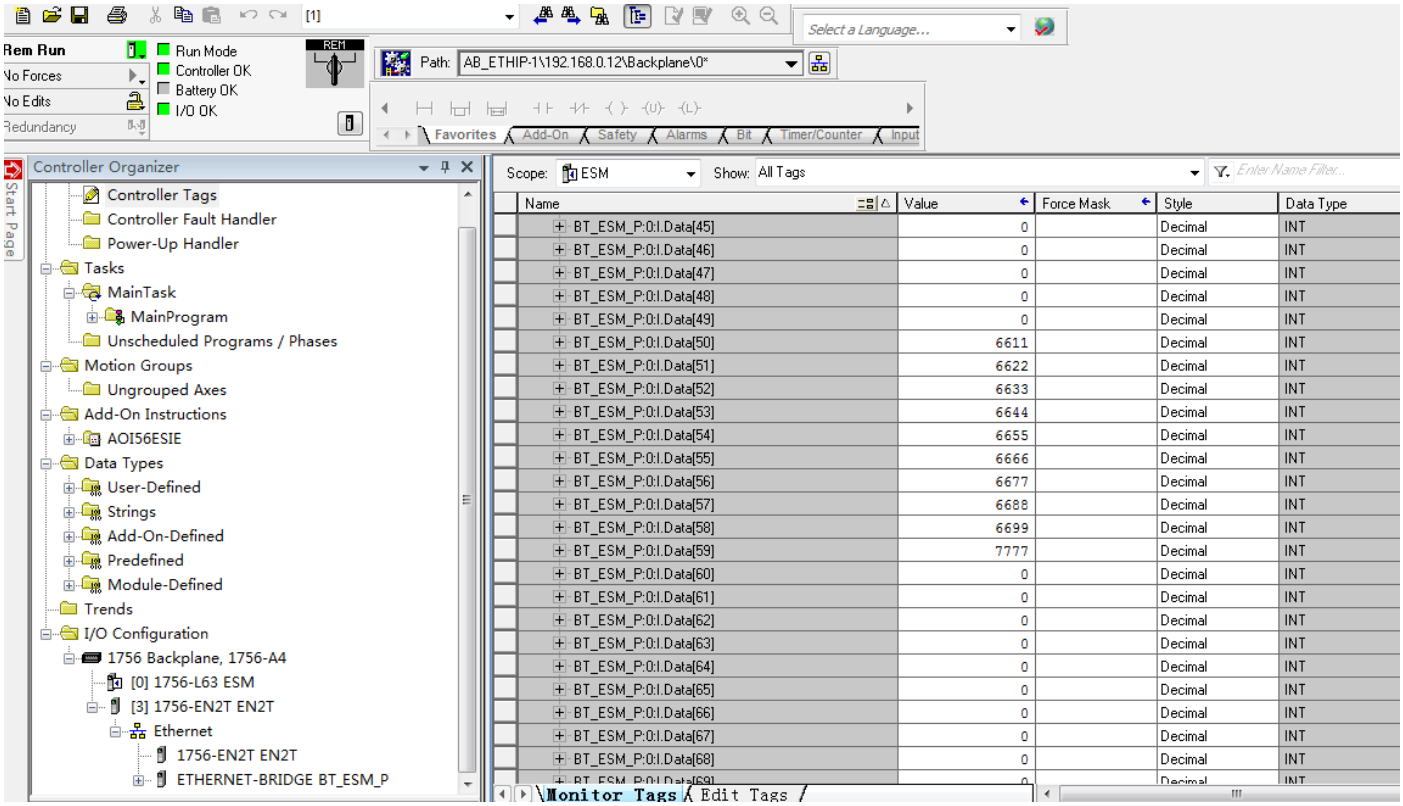
在仿真软件地址区 40051-40060 里面写任意数据。



查看模块内部寄存器地址 50-59 的情况，可以看到有相应的数据变化，说明模块从仿真中成功读取到了数据。



由于在之前的测试中，已经对于模块内部数据区和罗克韦尔 PLC 之间地址区之间建立了 CIP 连接映射，此时再检查罗克韦尔 PLC BT_ESM_P:0:I.Data[50]- BT_ESM_P:0:I.Data[59]的数据情况，也有相应的变化，这说明数据经过模块成功的被读取到了 ControlLogix PLC 中。



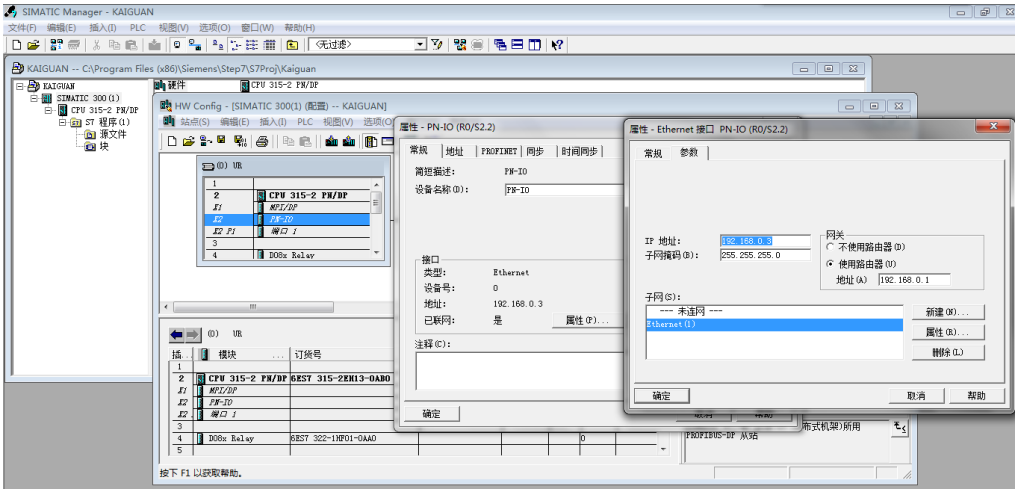
举例 5.Modbus TCP 和西门子 PLC 交换数据

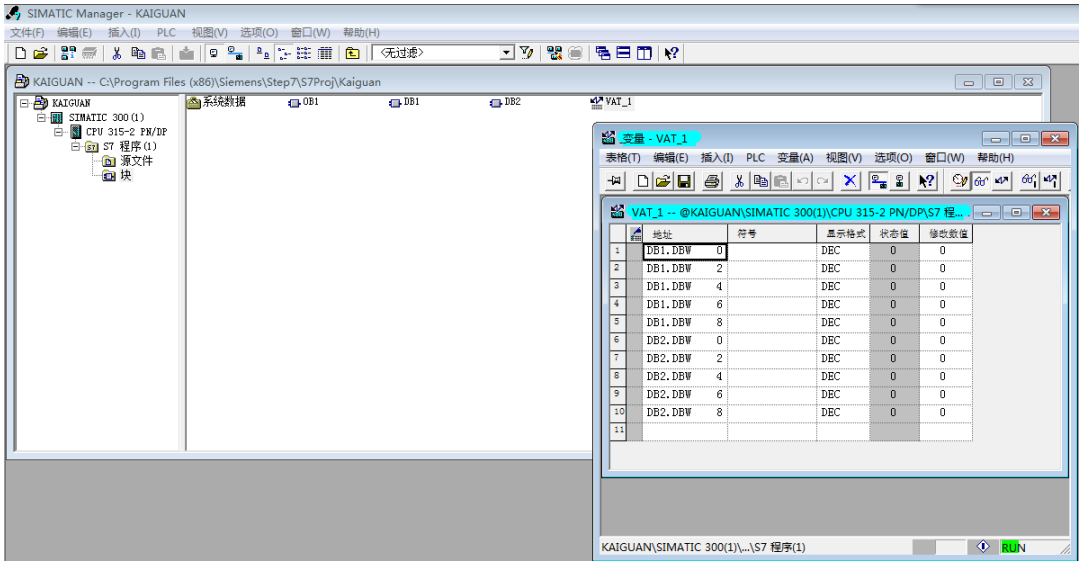
本案例中，模块Modbus TCP配置为Server和Client， S7 Ethernet配置成为Client

模块可以采集西门子多个 DB 块的数据，本例以 DB1 和 DB2 为例。从每个 DB 块采集 5 个数据给模块。

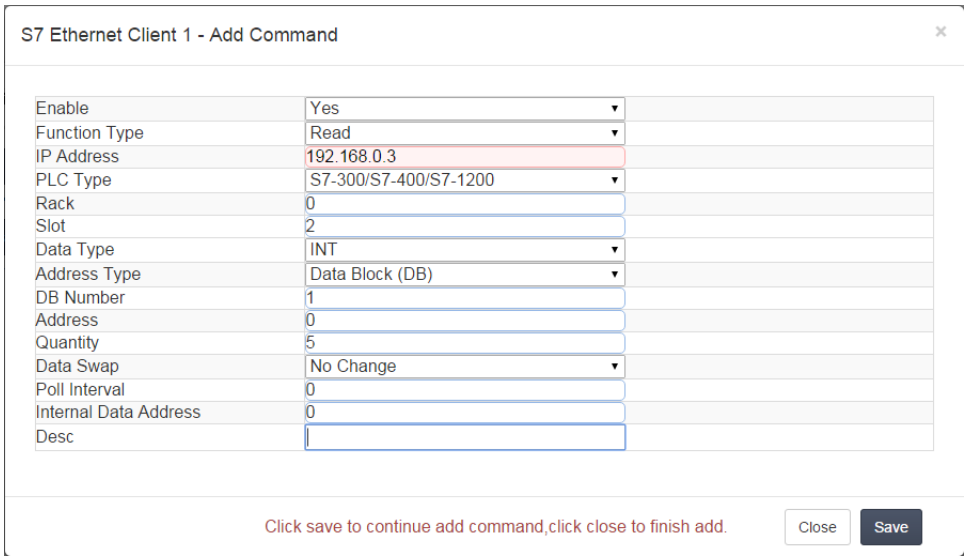
注意：为了避免读写地址冲突，请先将前面案例中，PLC 内的程序，软件内的数据和模块内的配置和地址区的数据全部删除。

在西门子 PLC 一侧建立 DB 块



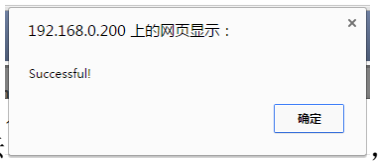


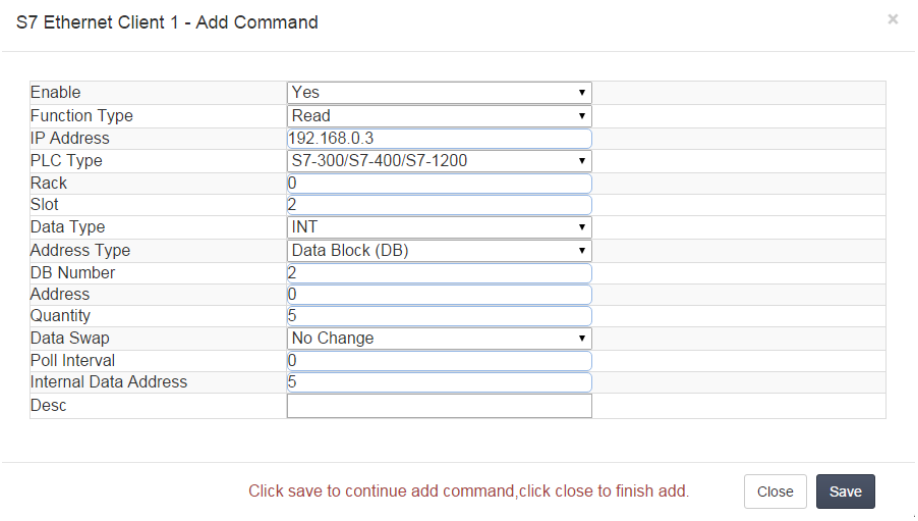
配置 S7-Eethernet Client 主站指令，点击 S7-Eethernet Client----Commands 建立两条指令



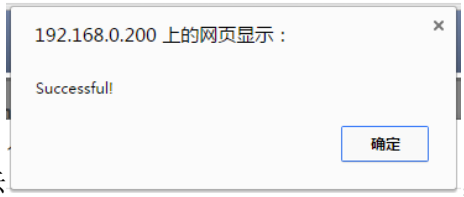
第一条命令中，需要注意的地方，Slot 是指西门子 CPU 的槽位，Address 是指 DB 数据的起始地址，Quantity 是指要传输几个数据，Data Swap 是指传输的数据是否进行高低位交换，Internal Data Address 是指要从西门子 PLC 读过来的数据存放到模块内部寄存器的起始地址。

第一条命令的含义是读 IP 地址为 192.168.0.3 的西门子 PLC 的 DB1 的 5 个字寄存器，放到模块内部寄存器 0-4 总共 5 个寄存器里面。

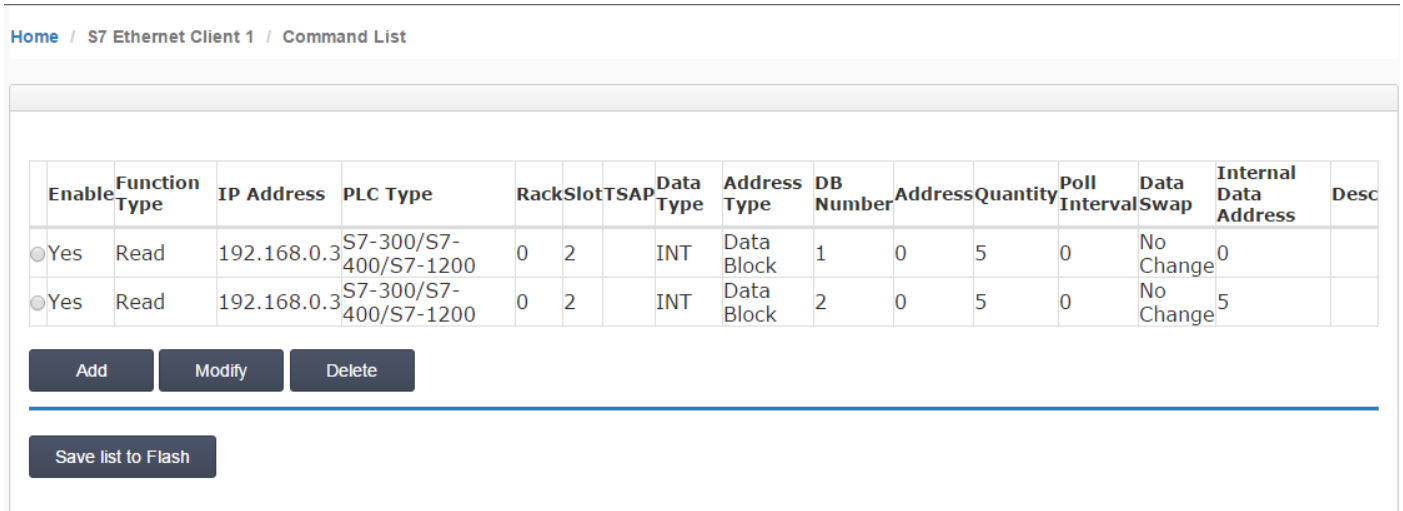
点击 Save 保存，提示  ，接着写第二条指令，

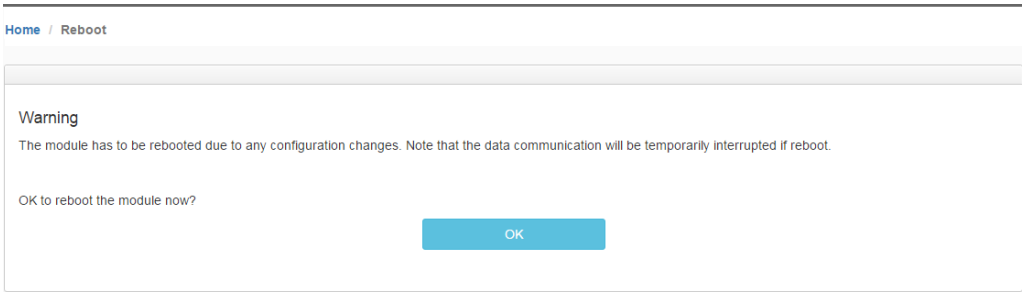


第二条命令的含义是读 IP 地址为 192.168.0.3 的西门子 PLC 的 DB2 的 5 个字，放到模块内部寄存器 5-9 总共 5 个寄存器里面。

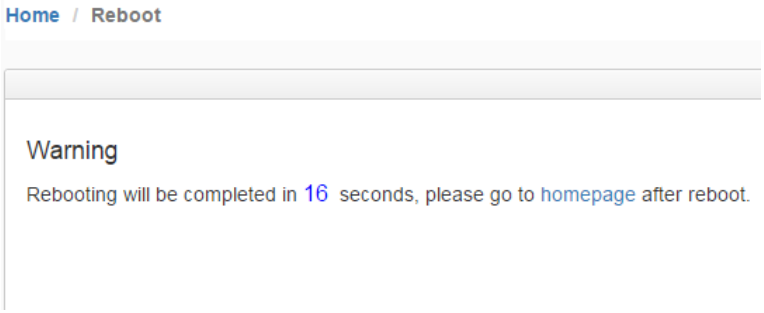


点击 Save 保存，提示，然后点击 Close 关闭这个命令。接着点击 Save list to Flash 把这个命令保存到模块里面。

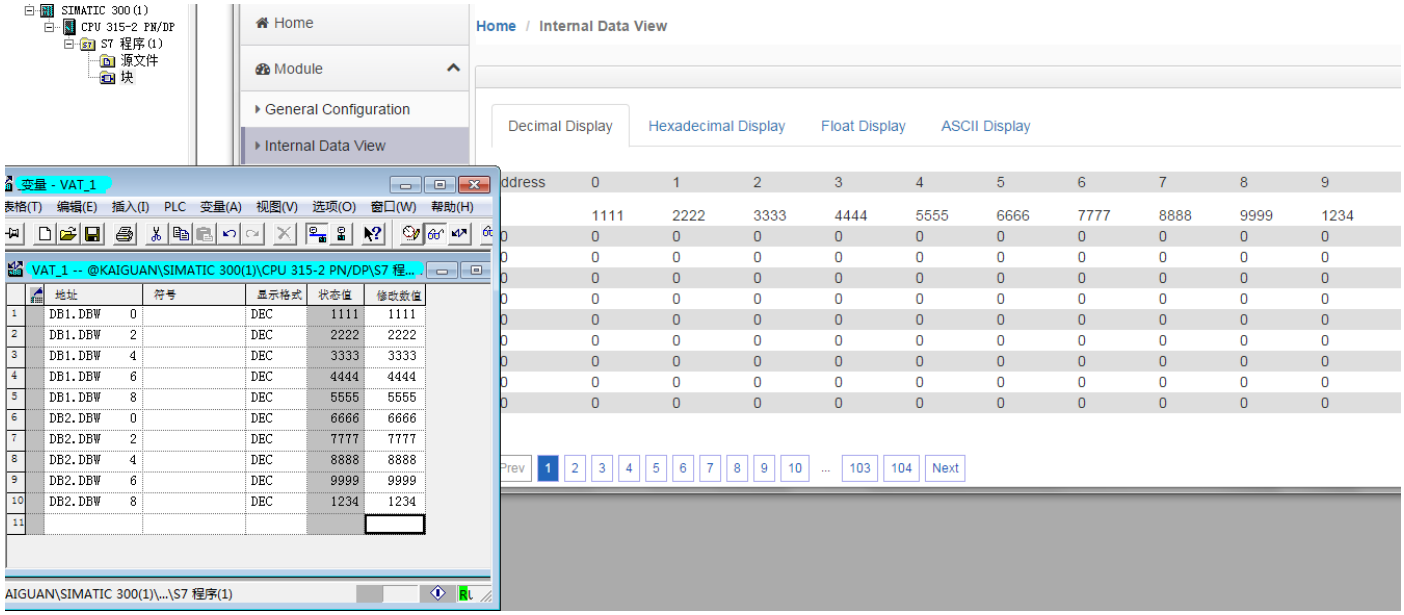




提示重启模块，点击 OK 完成重启。



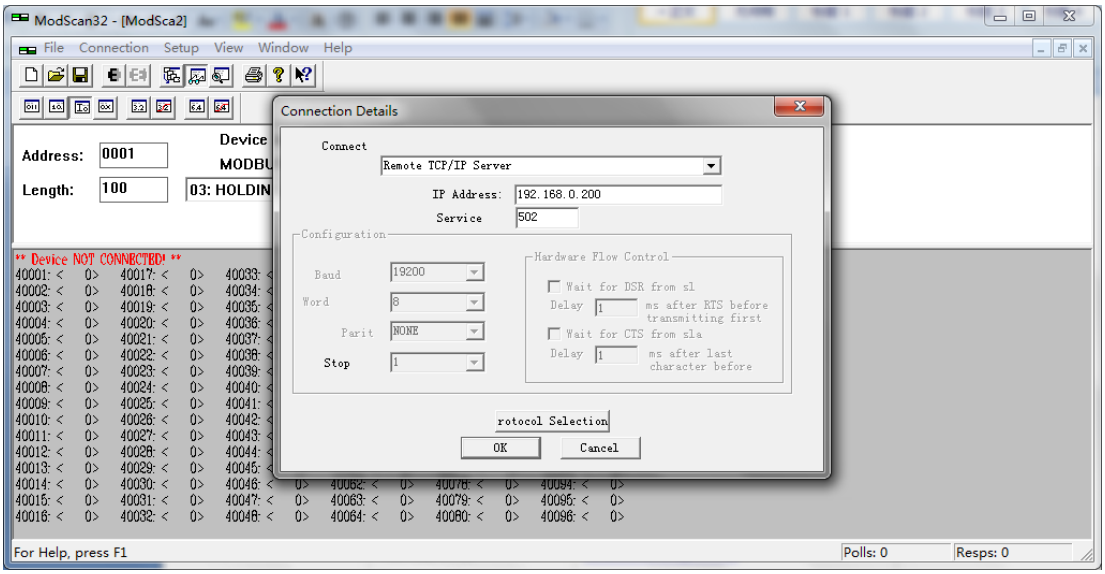
在西门子 PLC 变量表输入数据（左下图），可看到模块内部寄存器 0-9 总共 10 个寄存器显示收到数据。



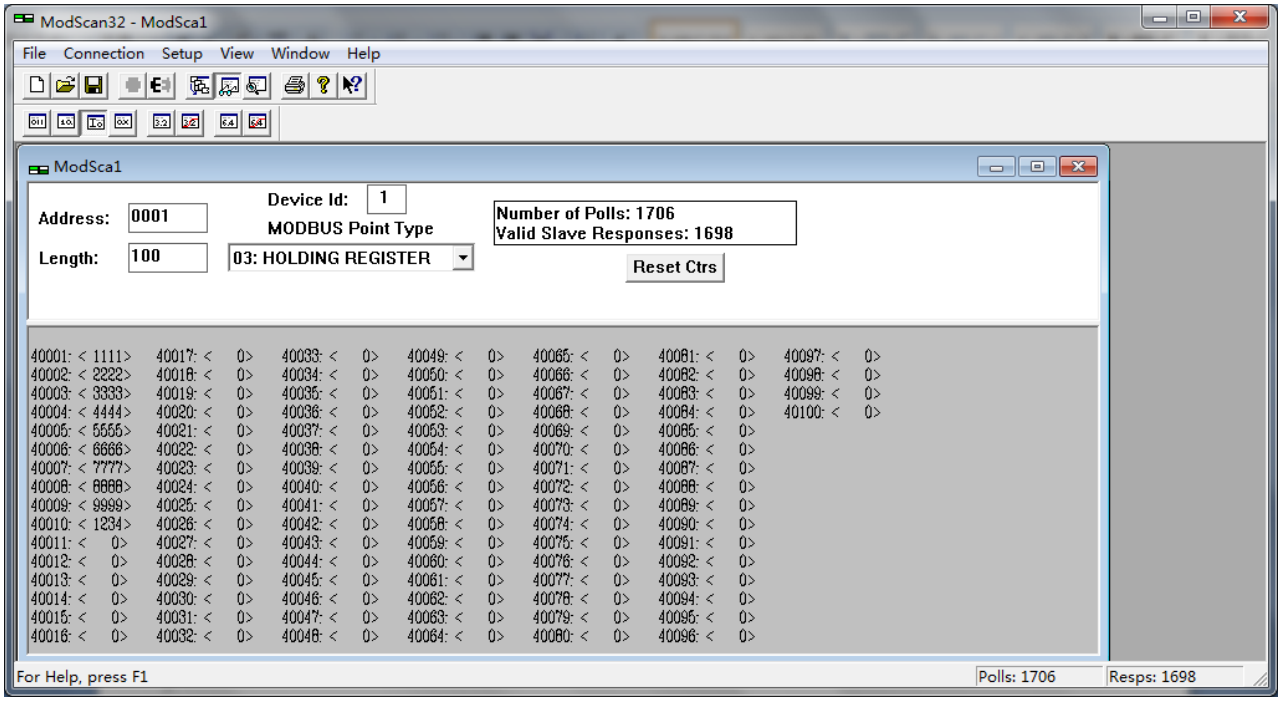
模块和 Modbus TCP 一侧设备交换数据可以采用两种方法。

第一种通过 Modscan32 仿真作为 Modbus TCP 主站，连接模块作为 Modbus TCP Server。

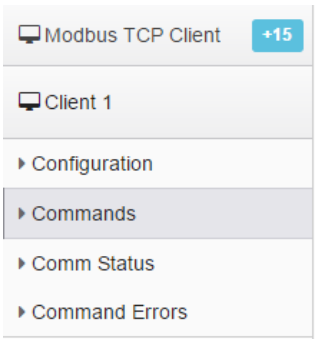
模块默认 Modbus TCP Server，不做任何配置。在仿真软件中选择功能码 FC3，连续读取 100 个模块的内部寄存器数据，存放到 40001 点击-40100.点击连接，选择 Remote TCP/IP Server.192.168.0.200 是模块的 IP 地址。



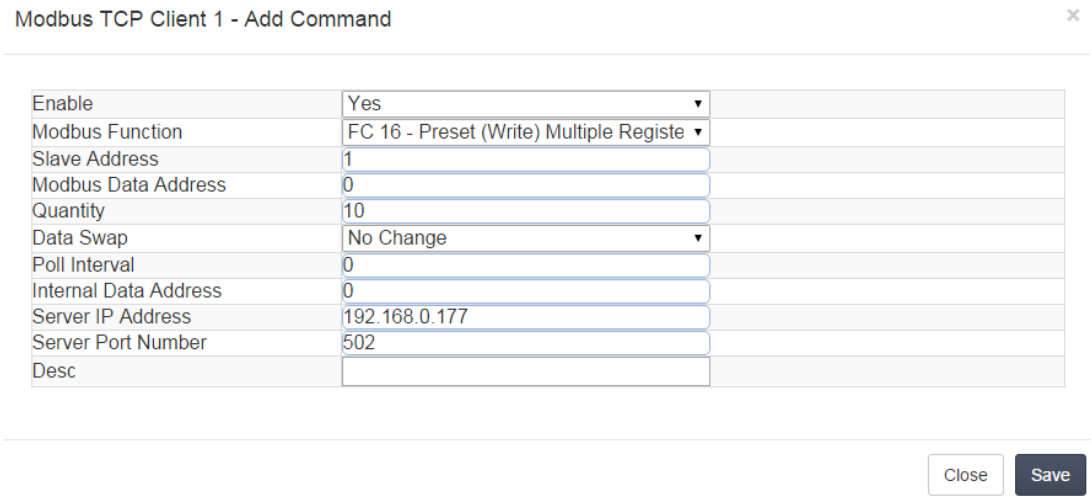
前文中已经介绍：DCS 使用功能码 FC3 时，读取作为从站的模块内部寄存器数据起始地址是 0.数量是 100，读到的数据将会放置到仿真软件地址 40001-40100 的范围内 。下图我们看到之前从西门子 PLC 读取到的数据，存放在模块内部寄存器 0-9 当中，现在这些数据被读取到 ModScan 地址 40001-40010 里面。



第二种通过 Modsim32 仿真作为 Modbus TCP server，模块作为 Modbus TCP Client。

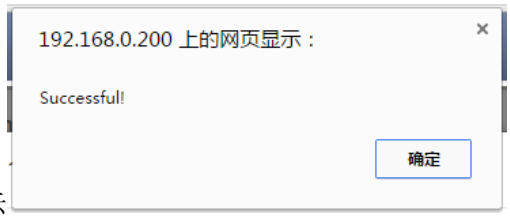


需要在模块 Modbus TCP Client --Client 1—Commands 配置命令。



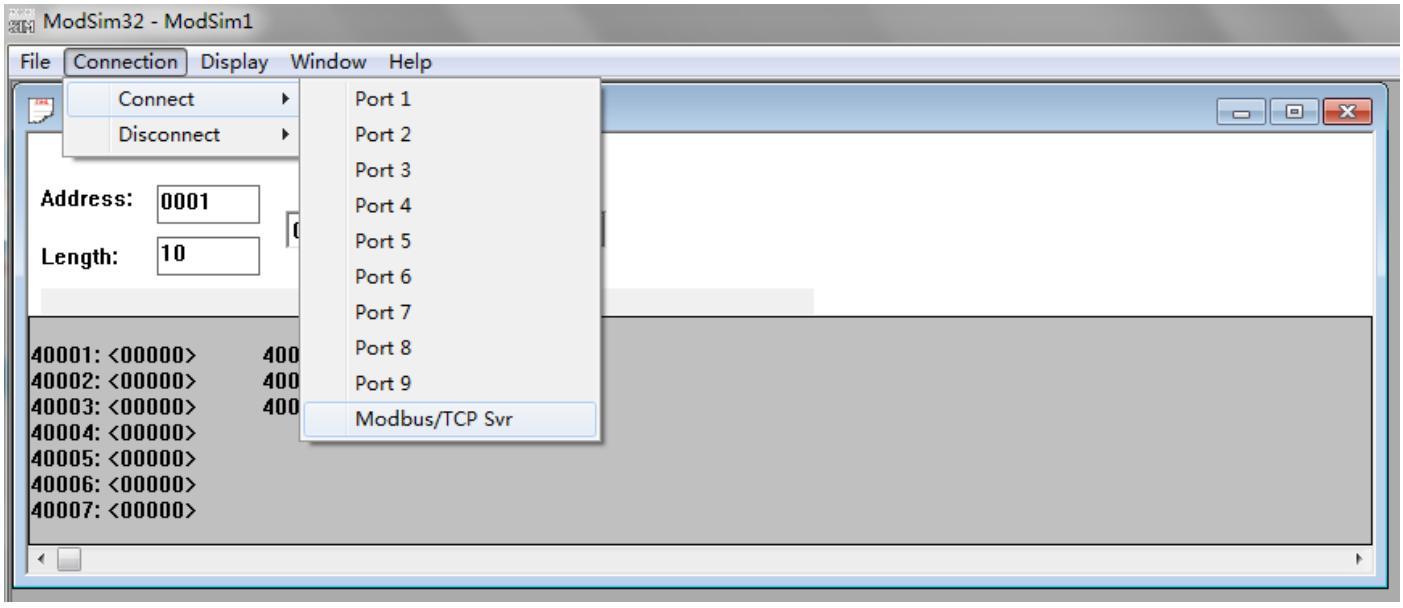
命令含义，将模块内部寄存器起始地址为 0，连续 10 个寄存器中的数据（即内部寄存器 0-9），写给 IP 是

192.168.0.177 的 Modsim32 软件，该仿真软件接收这些数据的地址为 40001-40010,连续 10 个字。

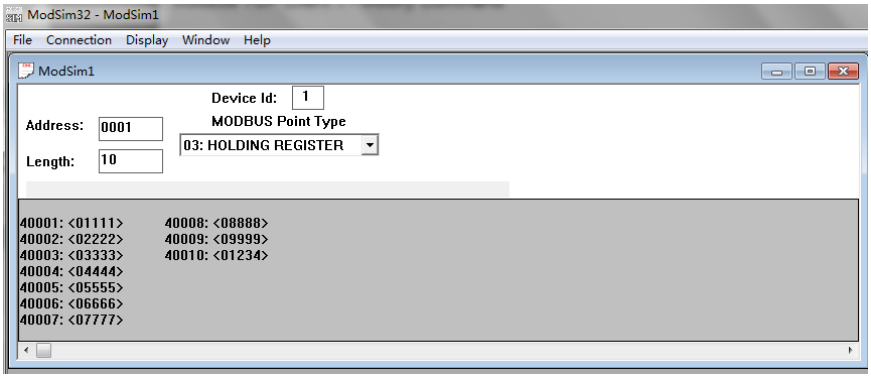


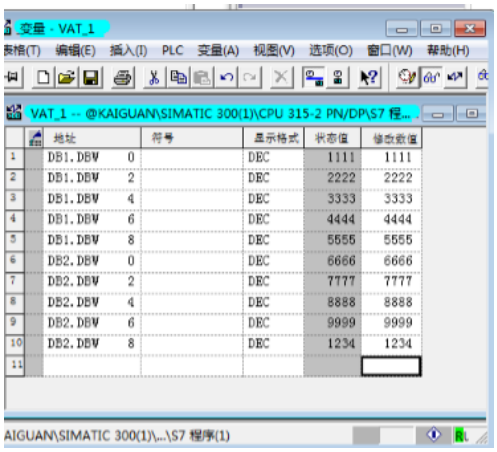
点击 Save，提示，然后点击 Close 关闭这个命令。接着点击 Save list to Flash 把这个命令保存到模块里面。

打开 Modsim32 软件,点击 Connection - Connect---Modbus/TCP Svr 来接收数据



下图中可以看到在 ModSim32 的 40001-40010 地址区里面接收到了，之前西门子 PLC 传输到模块内部寄存器 0-9 当中的数据。



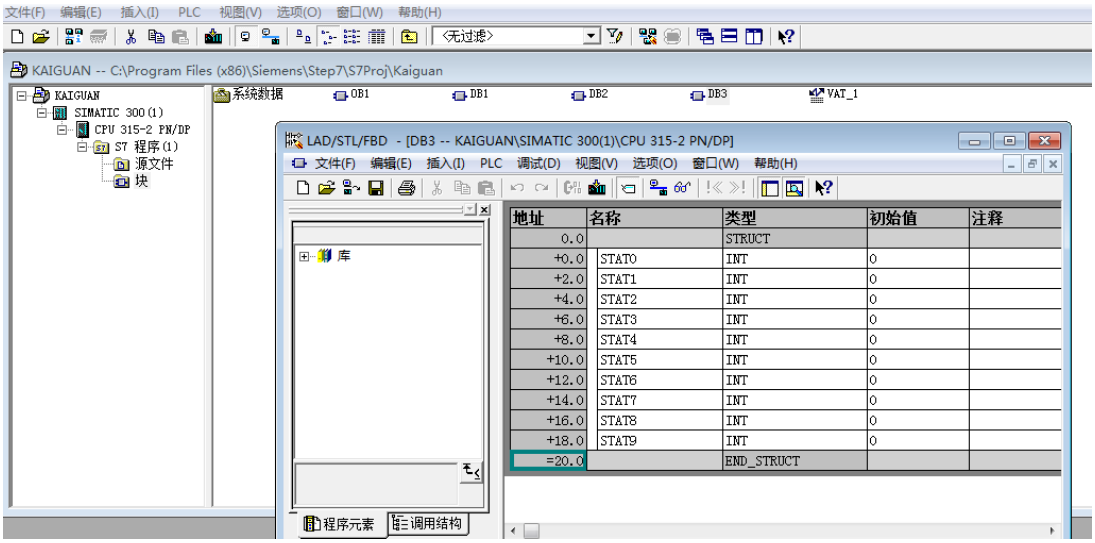


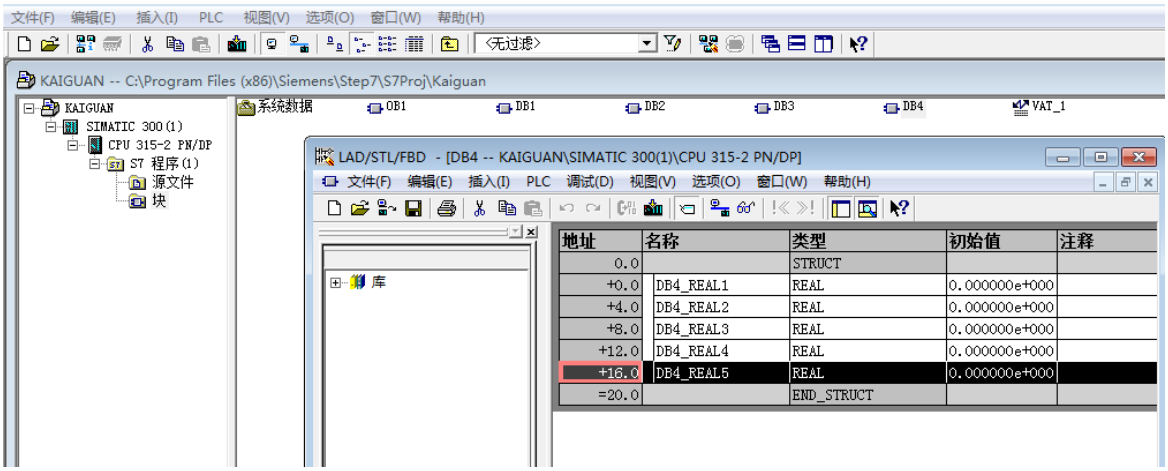
举例 6. 西门子 PLC 读取 2 个 Modbus TCP 仪表数据。

请删除之前举例的所有配置

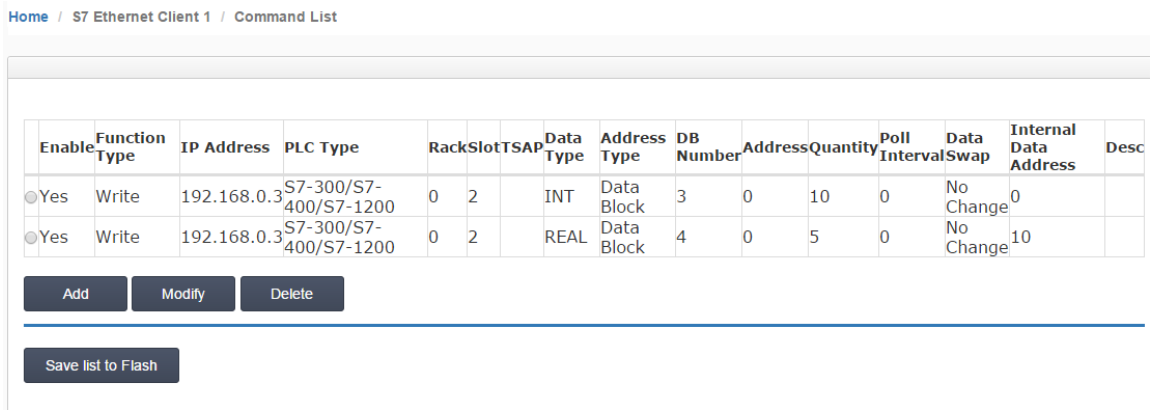
首先在西门子一侧建立 2 个新的 DB 块：DB3，包含 10 个 16 位字 ，DB4 块包含 5 个浮点数。下载到西门子 CPU 里

面，配置请见下图。





之后配置模块的 S7-Eethernet Client 主站命令，点击 S7-Eethernet Client------Commands 建立两条指令



第一条命令含义是从模块内部寄存器起始地址 0，写数据到 IP 地址 192.168.0.3（IP Address）的西门子 S7-300 PLC，CPU 在第 0 机架（Rack=0），第 2 槽(Slot=2)，DB 块 3（DB Number=3）里面的前 10 个字（Quantity=10）

第二条命令含义是从模块内部寄存器起始地址 10，写数据到 IP 地址 192.168.0.3（IP Address）的西门子 S7-300 PLC，CPU 在第 0 机架（Rack=0），第 2 槽(Slot=2)，DB 块 4（DB Number=4）里面的前 5 个浮点数（Quantity=5）

配置模块 Modbus TCP 主站命令（下图），添加两条新的指令

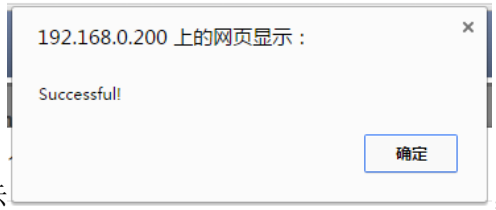
	Enable	Modbus Function	Slave Address	Modbus Data Address	Quantity	Data Swap	Poll Interval	Internal Data Address	Server IP Address	Server Port Number	Desc
○	Yes	FC 3 - Read Holding Registers(4X)	1	0	10	No Change	0	0	192.168.0.177	502	
○	Yes	FC 3 - Read Holding Registers(4X)	1	10	10	No Change	0	10	192.168.0.166	502	

Add Modify Delete

Save

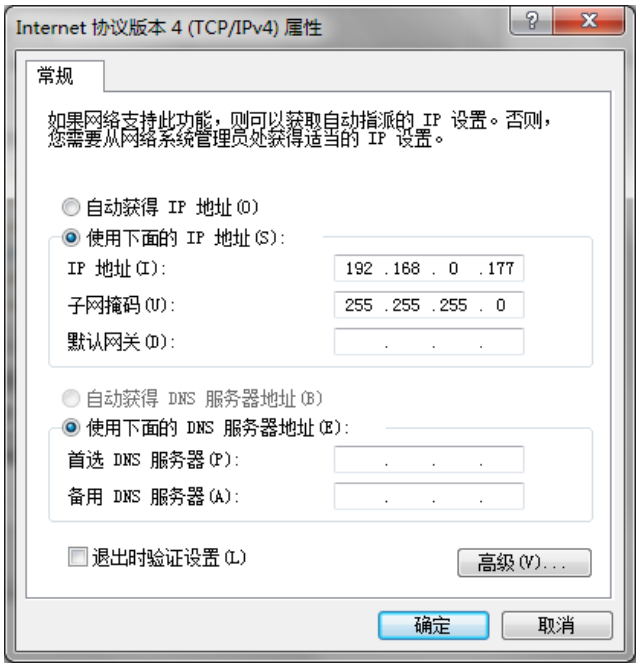
第一条命令含义是读取电脑 192.168.0.177（Server IP Address）运行的 Modsim32 仿真软件的 40001（Modbus Data Address =0）到 40010（Quantity=10）中的 10 个数据，存放放到模块内部寄存器 0-9 里面（Internal Data Address=0）

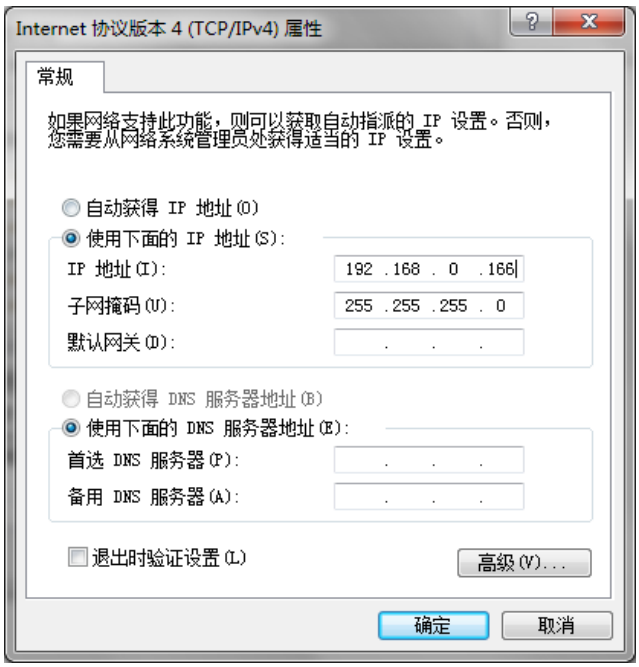
第二条命令含义是读取电脑 192.168.0.166（Server IP Address）运行的 Modsim32 仿真软件的 40011（Modbus Data Address =10）到 40020（Quantity=10）中的 10 个数据（5 个浮点数），存放到模块内部寄存器 10-19 里面（Internal Data Address=10）

点击 Save，提示 

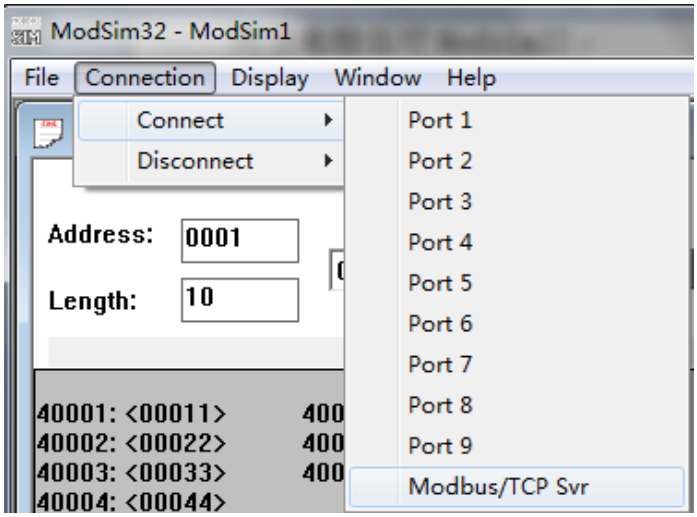
，然后点击 Close 关闭这个命令。接着点击 Save list to Flash 把这个命令保存到模块里面。

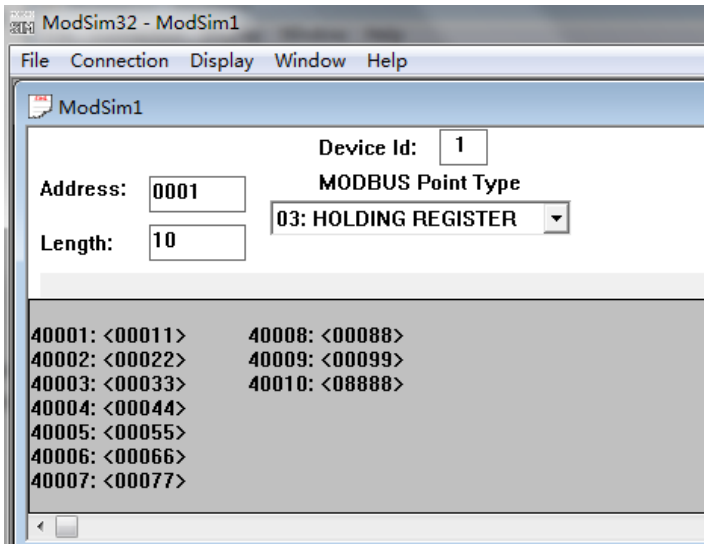
使用 Modsim32 仿真 2 个 Modbus TCP 从站。一台 IP 地址为 192.168.0.177，另外一台 IP 为 192.168.0.166

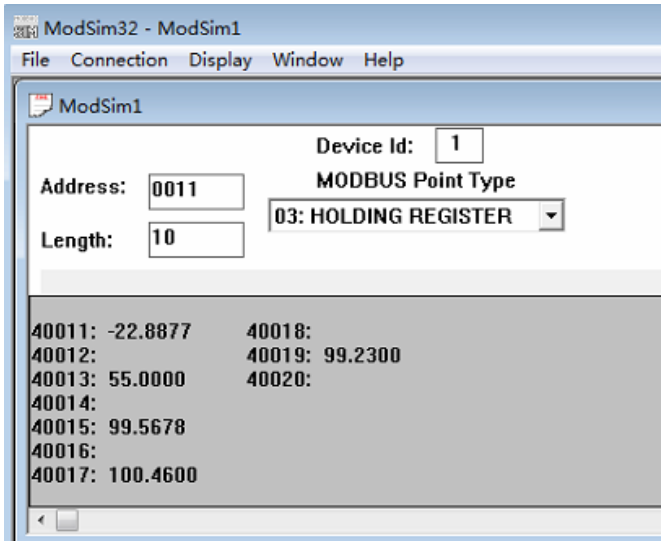




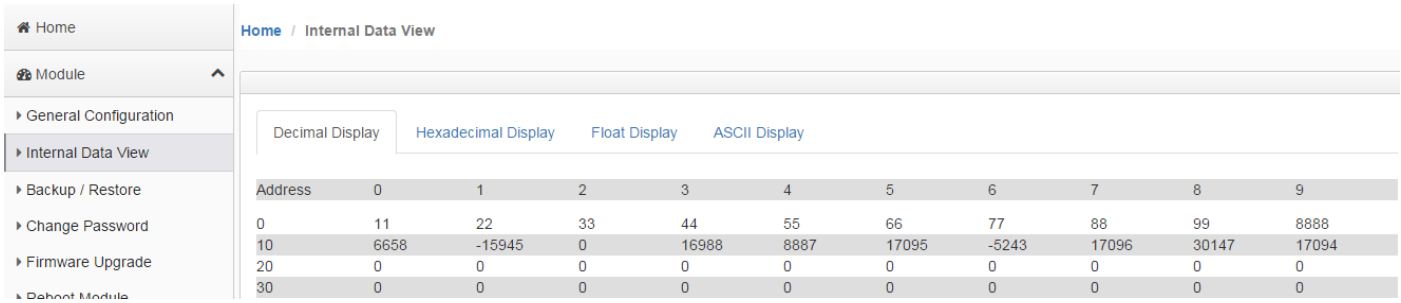
两台电脑同时运行 Modsim32 ，点击连接 Modbus TCP Svr 同时在两个 Modsim32 里面分别写一些数据。



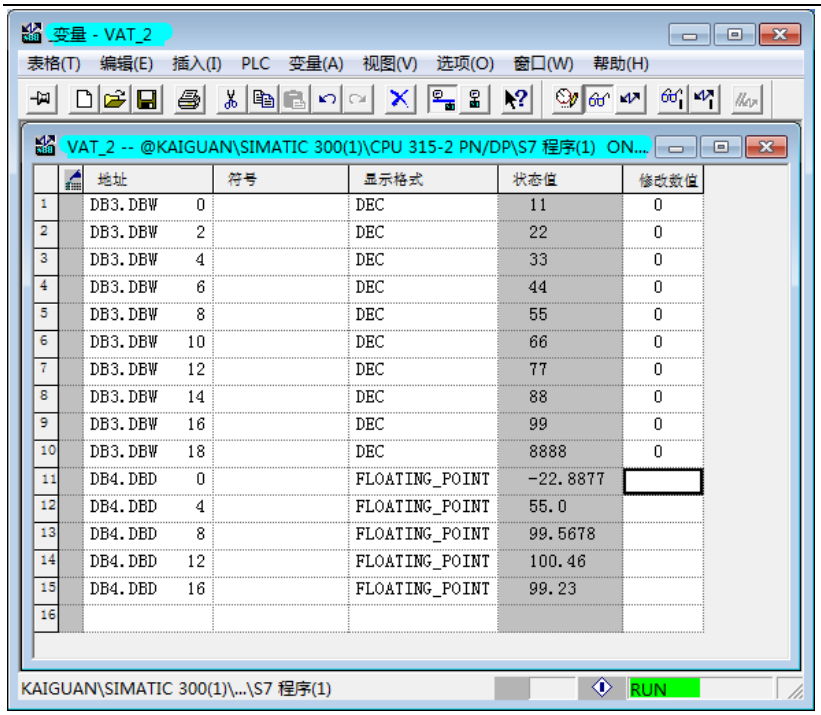




然后查看模块内部寄存器 0-9, 10-19 有数据被读取到。



再查看西门 PLC DB 块，同样 DB3 和 DB4 显示有数据从模块写入（注意两个 DB 块数据类型不同）



	地址	符号	显示格式	状态值	修改数值
1	DB3.DBW 0		DEC	11	0
2	DB3.DBW 2		DEC	22	0
3	DB3.DBW 4		DEC	33	0
4	DB3.DBW 6		DEC	44	0
5	DB3.DBW 8		DEC	55	0
6	DB3.DBW 10		DEC	66	0
7	DB3.DBW 12		DEC	77	0
8	DB3.DBW 14		DEC	88	0
9	DB3.DBW 16		DEC	99	0
10	DB3.DBW 18		DEC	8888	0
11	DB4.DBD 0		FLOATING_POINT	-22.8877	
12	DB4.DBD 4		FLOATING_POINT	55.0	
13	DB4.DBD 8		FLOATING_POINT	99.5678	
14	DB4.DBD 12		FLOATING_POINT	100.46	
15	DB4.DBD 16		FLOATING_POINT	99.23	
16					

附录 1. 模块支持读写西门子 PLC 的数据类型

S7-300/S7-400支持的数据类型

地址类型 S7-300/S7-400	功能	数据类型
DB	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Timer	READ	TIME
Counter	READ	Count
Flag	READ	BOOL

	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Input	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Output	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT

S7-200支持的数据类型

地址类型 S7-200	功能	数据类型
DB	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
Flag	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
Input	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
Output	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE

	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT

S7-1200 S7-1500支持的数据类型

地址类型 S7-1200	功能	数据类型
DB	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Flag	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Input	READ	BOOL
	Write	BOOL

	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT
Output	READ	BOOL
	Write	BOOL
	READ	BYTE
	Write	BYTE
	READ	DINT
	Write	DINT
	READ	REAL
	Write	REAL
	READ	INT
	Write	INT
	READ	TIME
	Write	TIME
	READ	COUNT
	Write	COUNT

附录 2. 模块支持读写西门子 PLC 的数据范围

S7-300/S7-400 最大支持点数

S7-300/S7-400	功能	数据类型	最大数量	最大数量
DB	READ	BOOL	16	
	Write	BOOL		8
	READ	BYTE	164	
	Write	BYTE		164
	READ	DINT	41	
	Write	DINT		41
	READ	REAL	41	

	Write	REAL		41
	READ	INT	82	
	Write	INT		82
	READ	TIME	82	
	Write	TIME		41
	READ	COUNT	82	
	Write	COUNT		82
Timer	READ	TIME	1	
Counter	READ	Count	111	
Flag	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	222	
	Write	BYTE		212
	READ	DINT	55	
	Write	DINT		53
	READ	REAL	55	
	Write	REAL		53
	READ	INT	111	
	Write	INT		106
	READ	TIME	111	
	Write	TIME		53
	READ	Count	111	
	Write	Count		106
Flag	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	222	
	Write	BYTE		212
	READ	DINT	55	
	Write	DINT		53
	READ	REAL	55	
	Write	REAL		53
	READ	INT	111	
	Write	INT		106
	READ	TIME	111	
	Write	TIME		53
	READ	Count	111	
	Write	Count		106
Input	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	128	
	Write	BYTE		128
	READ	DINT	32	

	Write	DINT		32
	READ	REAL	32	
	Write	REAL		32
	READ	INT	64	
	Write	INT		64
	READ	TIME	64	
	Write	TIME		32
	READ	Count	64	
	Write	Count		64

S7-1200 S7-1500 最大支持点数

S7-1200/S7-1500	功能	数据类型	最大数量	最大数量
DB	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	30	
	Write	BYTE		30
	READ	DINT	7	
	Write	DINT		7
	READ	REAL	7	
	Write	REAL		7
	READ	INT	15	
	Write	INT		15
	READ	TIME	15	
	Write	TIME		15
	READ	COUNT	15	
	Write	COUNT		15
Flag	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	212	
	Write	BYTE		212
	READ	DINT	53	
	Write	DINT		53
	READ	REAL	53	
	Write	REAL		53
	READ	INT	106	
	Write	INT		106
	READ	TIME	105	
	Write	TIME		105
	READ	Count	106	
	Write	Count		106
Output	READ	BOOL	1	

	Write	BOOL		1
	READ	BYTE	212	
	Write	BYTE		212
	READ	DINT	53	
	Write	DINT		53
	READ	REAL	53	
	Write	REAL		53
	READ	INT	106	
	Write	INT		106
	READ	TIME	105	
	Write	TIME		105
	READ	Count	111	
	Write	Count		106
Input	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	222	
	Write	BYTE		212
	READ	DINT	55	
	Write	DINT		53
	READ	REAL	55	
	Write	REAL		53
	READ	INT	111	
	Write	INT		111
	READ	TIME	111	
	Write	TIME		106
	READ	Count	111	
	Write	Count		106

S7-200 最大支持点数

S7-200	功能	数据类型	最大数量	最大数量
DB	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	222	
	Write	BYTE		212
	READ	DINT	55	
	Write	DINT		53
	READ	REAL	55	
	Write	REAL		53
	READ	INT	111	
	Write	INT		106
Flag	READ	BOOL	1	
	Write	BOOL		1

	READ	BYTE	32	
	Write	BYTE		32
	READ	DINT	8	
	Write	DINT		8
	READ	REAL	8	
	Write	REAL		8
	READ	INT	16	
	Write	INT		16
Output	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	16	
	Write	BYTE		16
	READ	DINT	4	
	Write	DINT		4
	READ	REAL	4	
	Write	REAL		4
	READ	INT	8	
	Write	INT		8
Input	READ	BOOL	1	
	Write	BOOL		1
	READ	BYTE	16	
	Write	BYTE		16
	READ	DINT	4	
	Write	DINT		4
	READ	REAL	4	
	Write	REAL		4
	READ	INT	8	
	Write	INT		8

联系我们

如果在使用过程中有更多的问题，可以通过以下方式联系我们获得支持。

客户服务热线 （中国大陆）	4008-710-598
技术支持	support@beacongt.com
亚太区销售	asia@beacongt.com
北美区销售	usa@beacongt.com
微信公众平台	
网址	http://www.beaconglobaltech.com