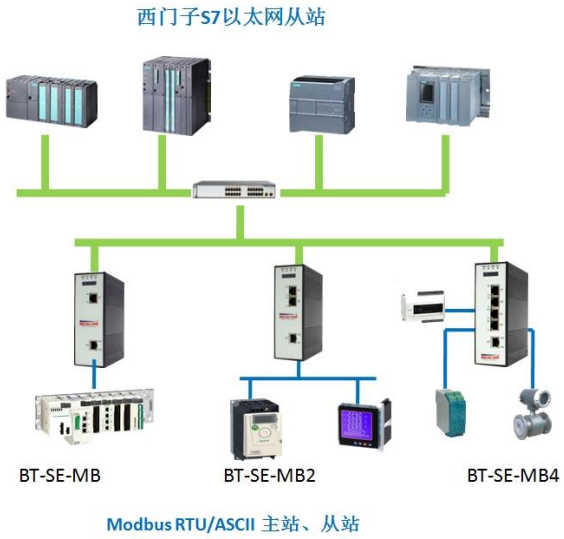
BT-SE-MB4-S
快速启动手册

BEACON GLOBAL TECHNOLOGY

目录

BT-SE-MB-S 简介：

- 模块支持S7以太网协议和Modbus RTU协议通讯。
- 模块最大支持10000个字数据交换区。
- 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 RTU协议可支持通讯的设备包括各种数显仪表，电动阀门，传感器等。
- 模块有1个以太网口，1-4个串口（不同订货号），可以任意使用。



E1 端口 ==配置端口，支持 Siemens S7 Industrial Ethernet。
S1-S4 端口 ==可配置为 Modbus RTU 主站/从站,(RS232/422/485)。
注意：不同型号的串口数量不同,本手册按照 4 个串行端口举例。

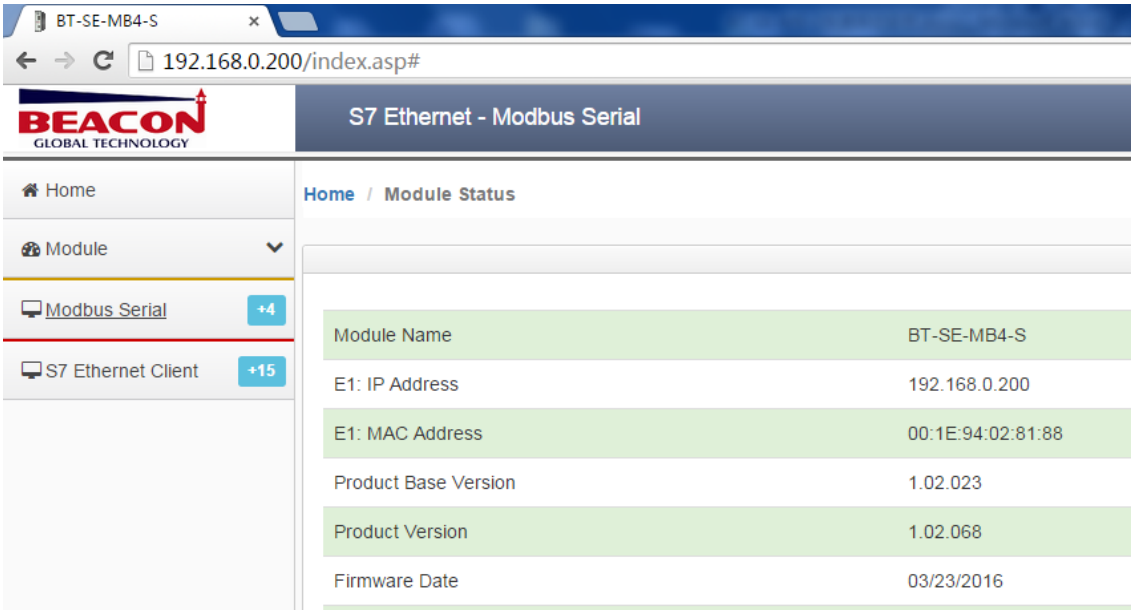
模块初始配置

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。

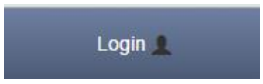
BT系列模块全部采用网页配置形式组态，无需安装其他多余的组态软件，推荐采用如下浏览器及以上版本（更好的支持HTML5的功能）对于模块进行配置：IE10，GOOGLE Chrome 35，FIREFOX 35，Safari 7 及以上的版本。

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。



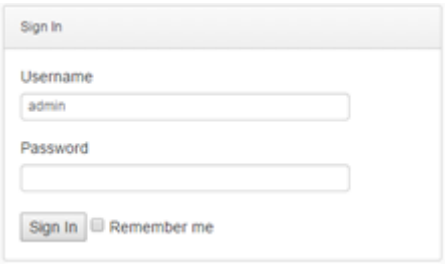
3. 按照界面提示，输入用户名和密码进入模块配置。

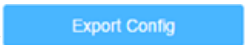
用户名(Username):admin

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。

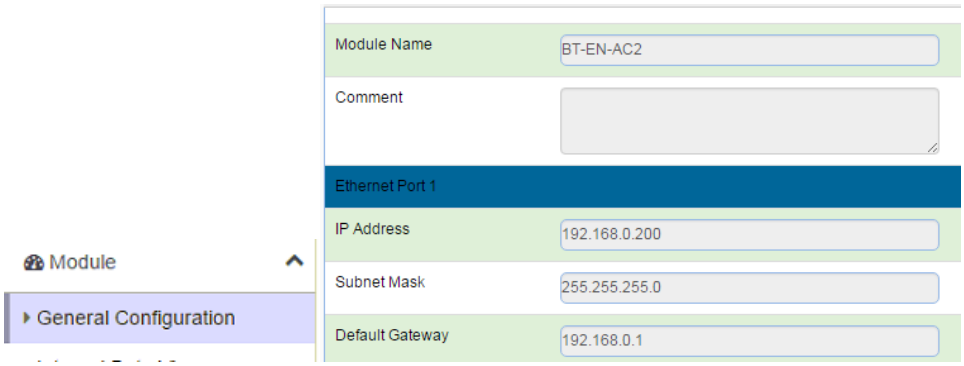


4. 登录后看到导出配置文件 

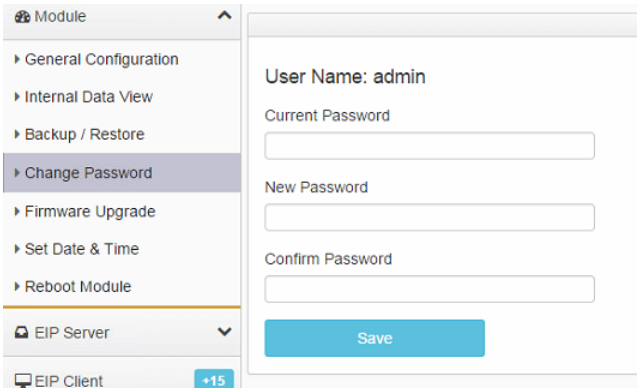
和恢复配置文件 

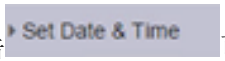
5. 查看模块 IP 地址，点击 

，修改模块的 IP 地址。

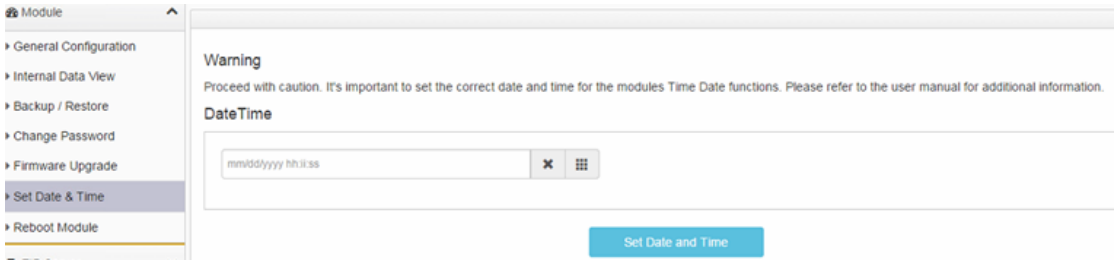


6. 点击修改密码，可以修改模块的登录密码。 

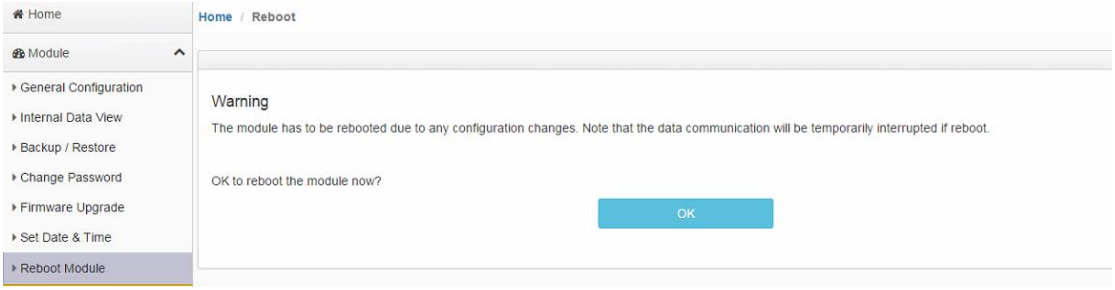


7. 点击 

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）

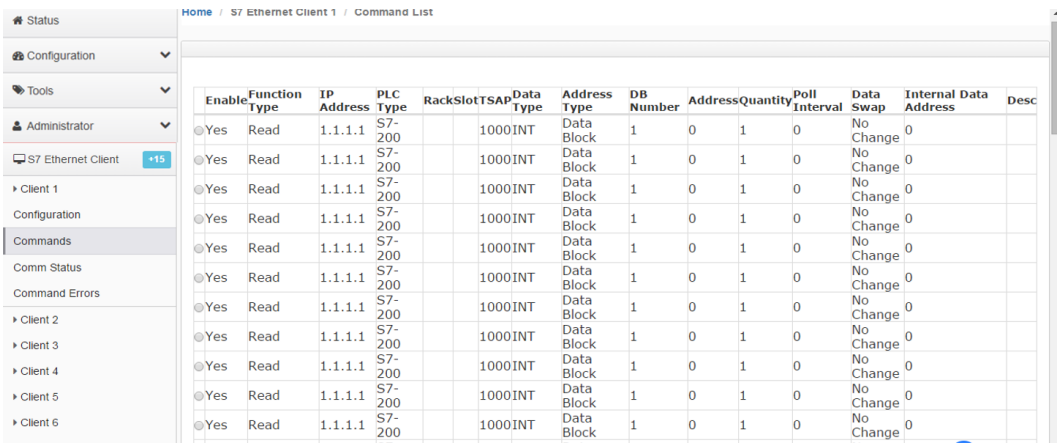


配置模块做 Siemens S7 以太网主站

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，Commands 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。



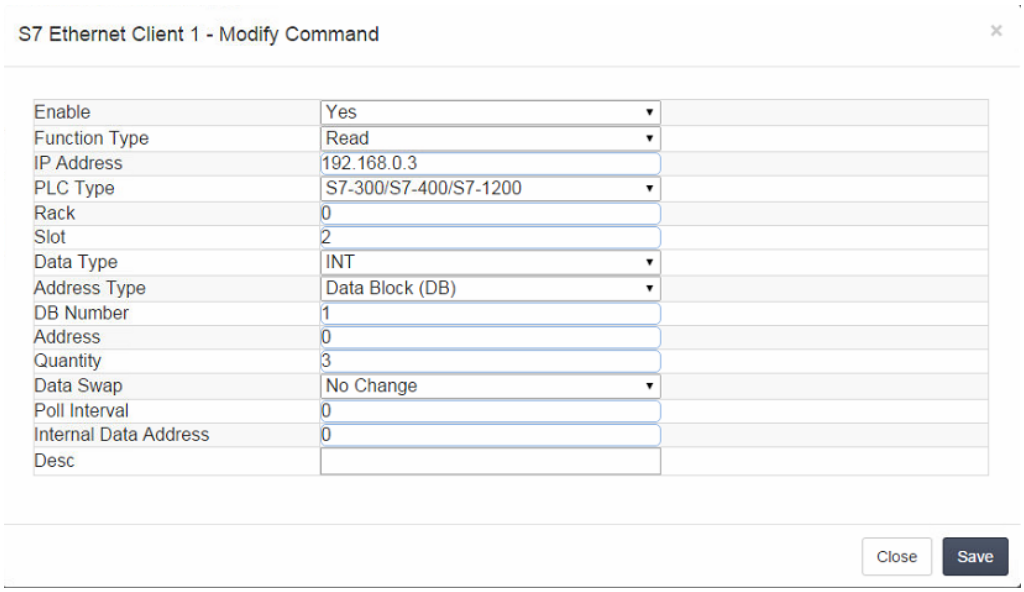
点击 Add ，可以增加新的命令，如下为针对不同种类西门子 PLC 添加指令的配置界面：

注意：不同型号的模块，内部数据区大小范围不同，本手册按照 10000 个字数据寄存器进行举例。在配置模块时，请务必先确认模块的数据寄存器实际范围，再进行配置。

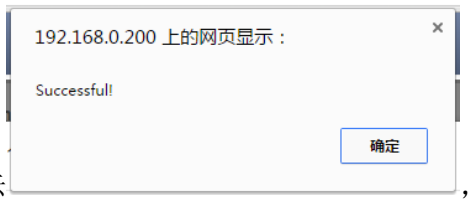
举例读写西门子 PLC 整型数据

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。

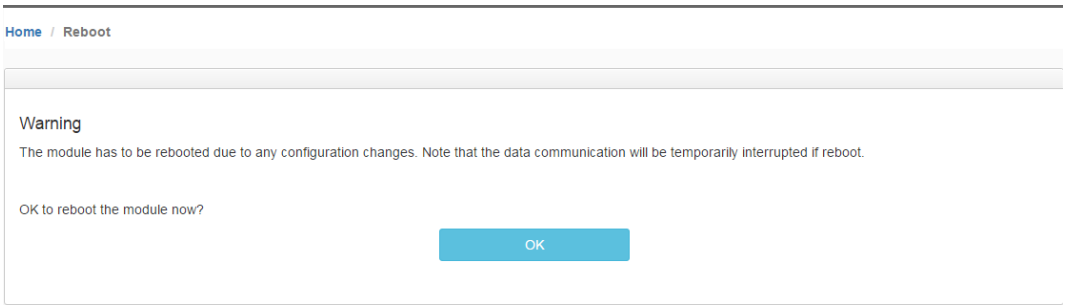
读指令解释如下，读取 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器，把其中的 DB1 数据块里面的 3 个 INT（字节地址 0-5）读到模块内部数据寄存器地址 0-2 中.



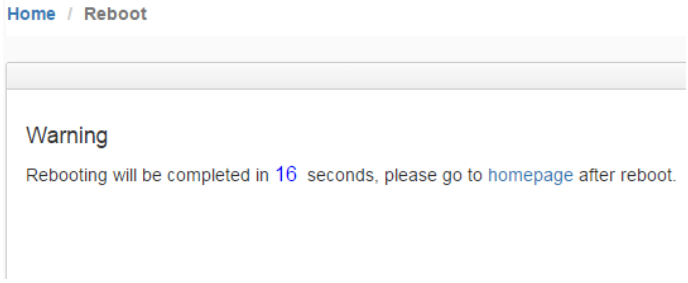
命令的要注意的地方，Slot 是指西门子 CPU 的槽位，Address 是指 DB 数据的起始地址，Quantity 是指要传输几个数据，Data Swap 是指传输的数据是否进行高低位交换，Internal Data Address 是指模块内部寄存器的起始地址。



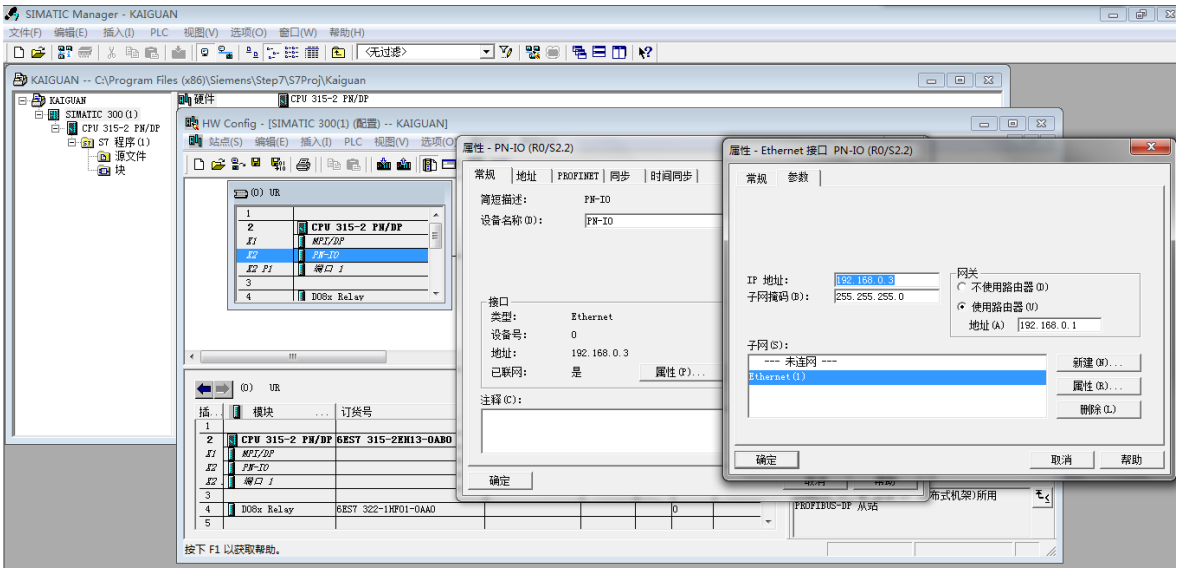
点击 Save 保存，提示，然后点击 Close 关闭这个命令。接着点击 Save list to Flash 把这个命令保存到模块里面。

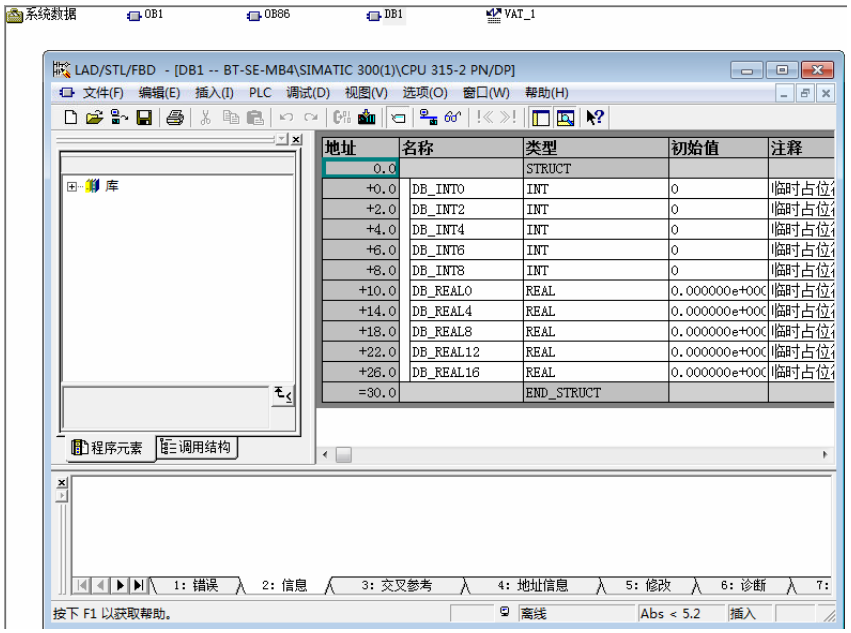


提示重启模块，点击 OK 完成重启。

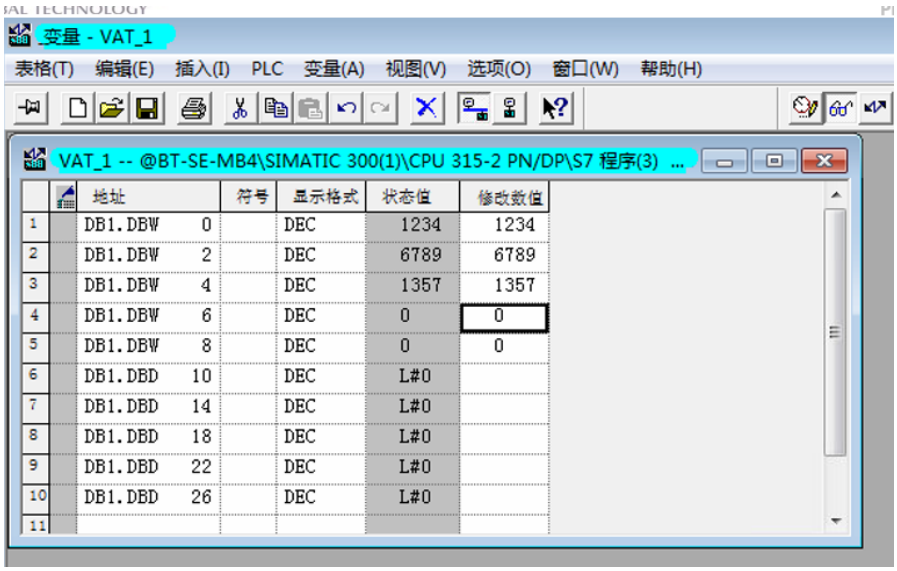


配置西门子 PLC 一侧，建立 DB 块



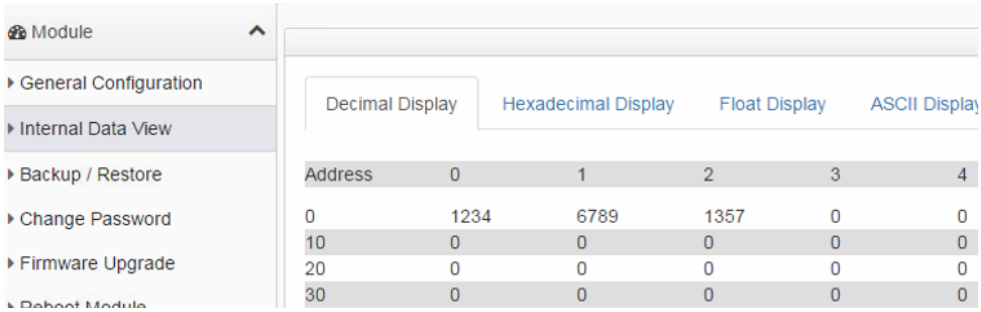


在 DB1.DBW0，DB1.DBW2，DB1.DBW4 里面写点数据。点击  赋值。



	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					

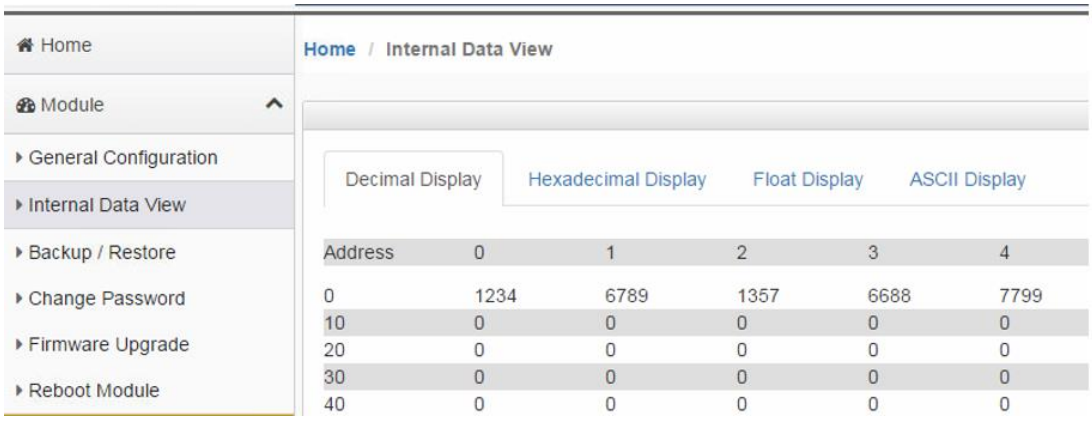
返回模块网页查看内部数据寄存器地址 0-2 中读入了相同的数据。



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

S7 Ethernet Client 1 - Modify Command

Enable	Yes
Function Type	Write
IP Address	192.168.0.3
PLC Type	S7-300/S7-400/S7-1200
Rack	0
Slot	2
Data Type	INT
Address Type	Data Block (DB)
DB Number	1
Address	6
Quantity	2
Data Swap	No Change
Poll Interval	0
Internal Data Address	3
Desc	

Close Save

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（字节地址 6-9）DBW6 和 DBW8.保存该指令，重启模块。

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	3	0	No Change	0	
Yes	Write	192.168.0.3	S7-300/S7-400/S7-1200	0	2		INT	Data Block	1	6	2	0	No Change	3	

Add Modify Delete

Save list to Flash

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

S7 Ethernet Client 1 - Modify Command

Enable	Yes
Function Type	Read
IP Address	192.168.0.3
PLC Type	S7-300/S7-400/S7-1200
Rack	0
Slot	2
Data Type	REAL
Address Type	Data Block (DB)
DB Number	1
Address	10
Quantity	3
Data Swap	No Change
Poll Interval	0
Internal Data Address	20
Desc	

Close Save

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

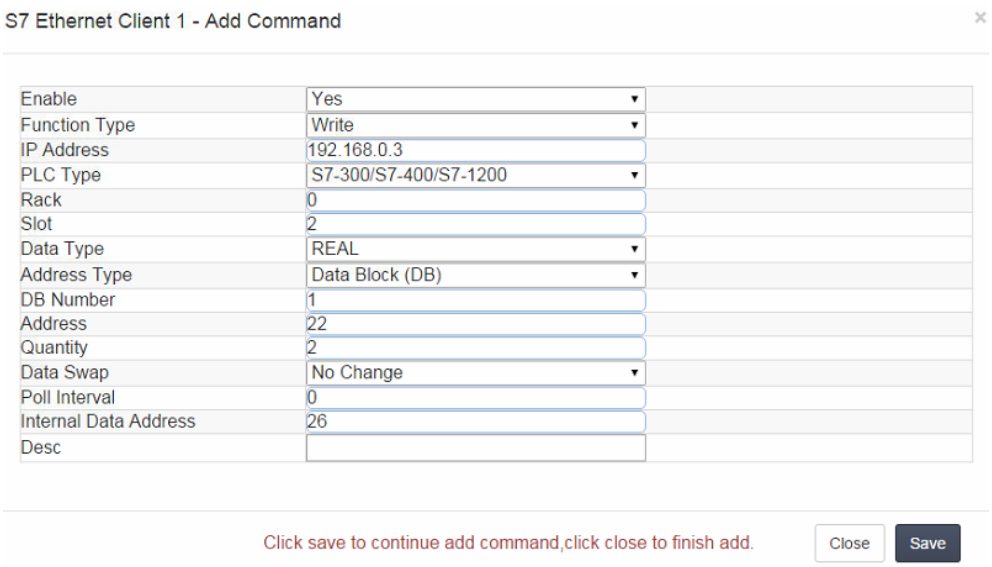
如下图，在西门子 PLC 中 DB1.DBD10/14/18 中赋值

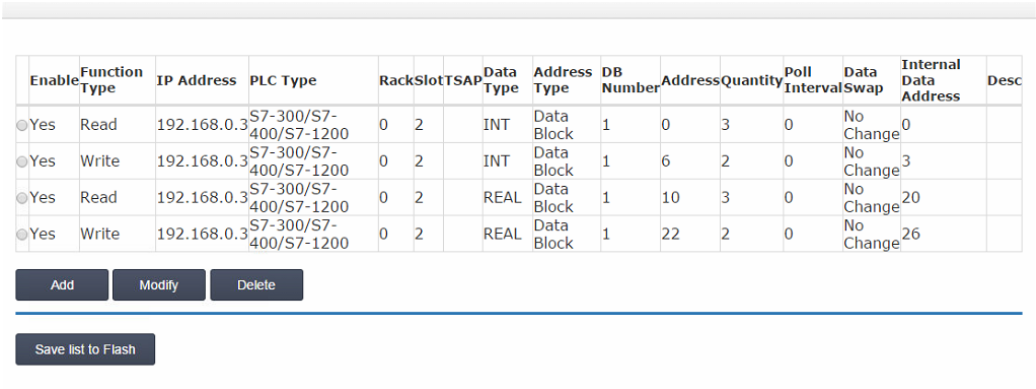
	地址	符号	显示格式	状态值	修改数值
2	DB1.DBW 2		DEC	6789	6789
3	DB1.DBW 4		DEC	1357	1357
4	DB1.DBW 6		DEC	6688	0
5	DB1.DBW 8		DEC	7799	0
6	DB1.DBD 10		FLOATING_POINT	-58.98	-58.98
7	DB1.DBD 14		FLOATING_POINT	-77.5533	-77.5533
8	DB1.DBD 18		FLOATING_POINT	69.89	69.89
9	DB1.DBD 22		FLOATING_POINT	0.0	
10	DB1.DBD 26		FLOATING_POINT	0.0	
11					
12					

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）。

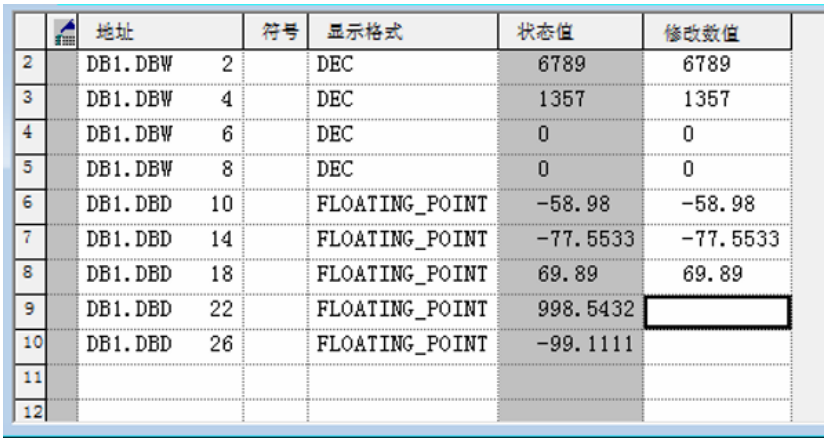
在模块 S7 以太网主站建立一条写指令含义为，从模块内部数据区起始地址 26 开始，调用 2 个 REAL 类型数据，写给 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器，写入 DB1 数据块里面的 DBD22 和 DBD26（字节地址 22-29）.保存该指令，重启模块。





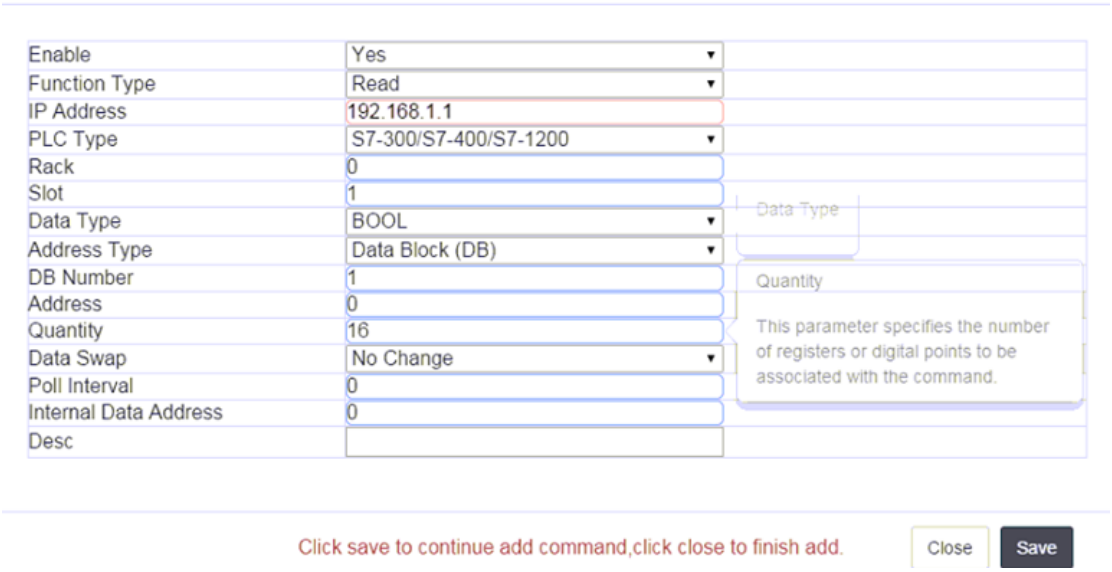
点击 Save list to Flash 重启网关，让命令生效。

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。

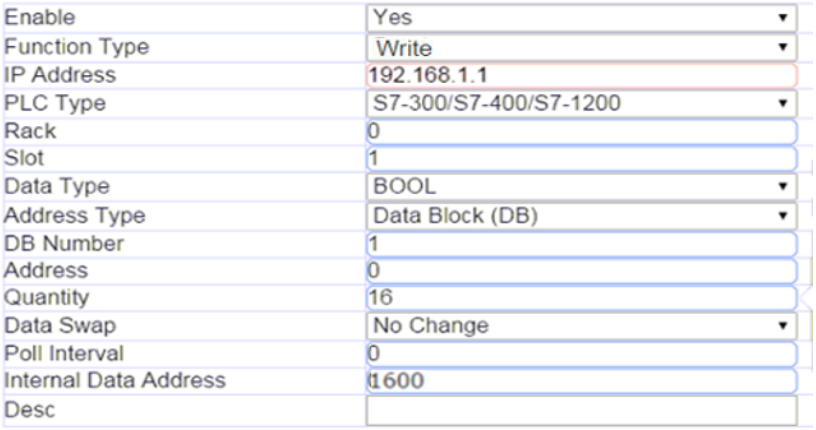


	地址	符号	显示格式	状态值	修改数值
2	DB1.DBW 2		DEC	6789	6789
3	DB1.DBW 4		DEC	1357	1357
4	DB1.DBW 6		DEC	0	0
5	DB1.DBW 8		DEC	0	0
6	DB1.DBD 10		FLOATING_POINT	-58.98	-58.98
7	DB1.DBD 14		FLOATING_POINT	-77.5533	-77.5533
8	DB1.DBD 18		FLOATING_POINT	69.89	69.89
9	DB1.DBD 22		FLOATING_POINT	998.5432	
10	DB1.DBD 26		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（字节地址 0-1）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（字节地址 0-1）。
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。

配置模块做 MODBUS RTU 主站

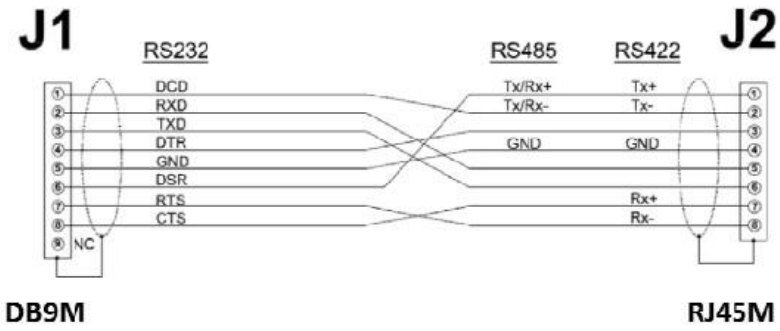
模块的MODBUS RTU接口，接线方式提供RS232/422/485三种可以选择，可以自由选择做主站或者从站。

Modbus RTU主站可以连接31个从站， RS485接线方式长度在1200米以内。工程师设计连接每个主站连接从站个数可参考如下原则：

1、遵循MODBUS RTU通讯规约。

2、主站只读取从站数据，每个RS485串口主站可以接31个从站，MODBUS RTU是令牌轮询方式，连接从站越多，或者距离越长，延时越大。

3、主站同时读写从站数据，建议每个RS485串口最多接10-15个从站，避免过长通讯延时，提升通讯响应速度。



接线图

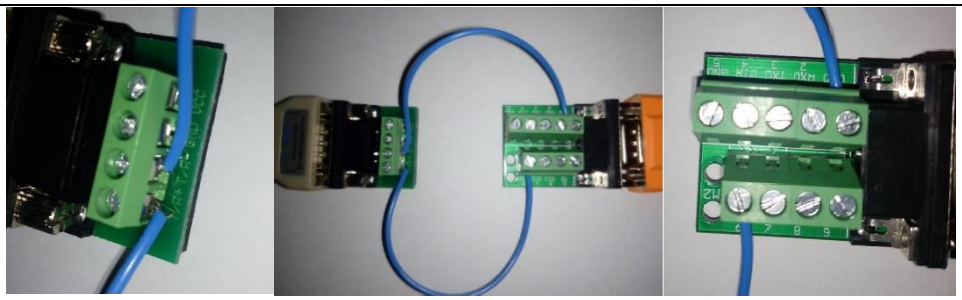
上图为S1/S2端口的接线图

举例：S1口引出来RS485接口，端子6+，1-

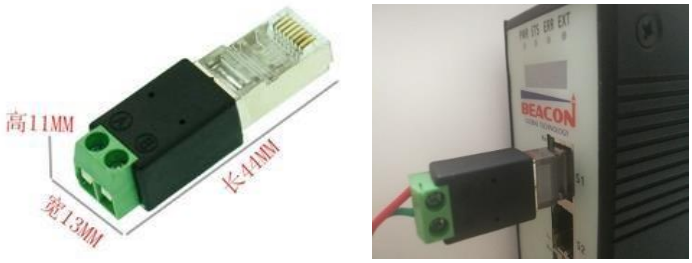
USB转RS485引出来的RS485接口，端子T/R+,T/R-

6+----------端子T/R+

1----------端子T/R-



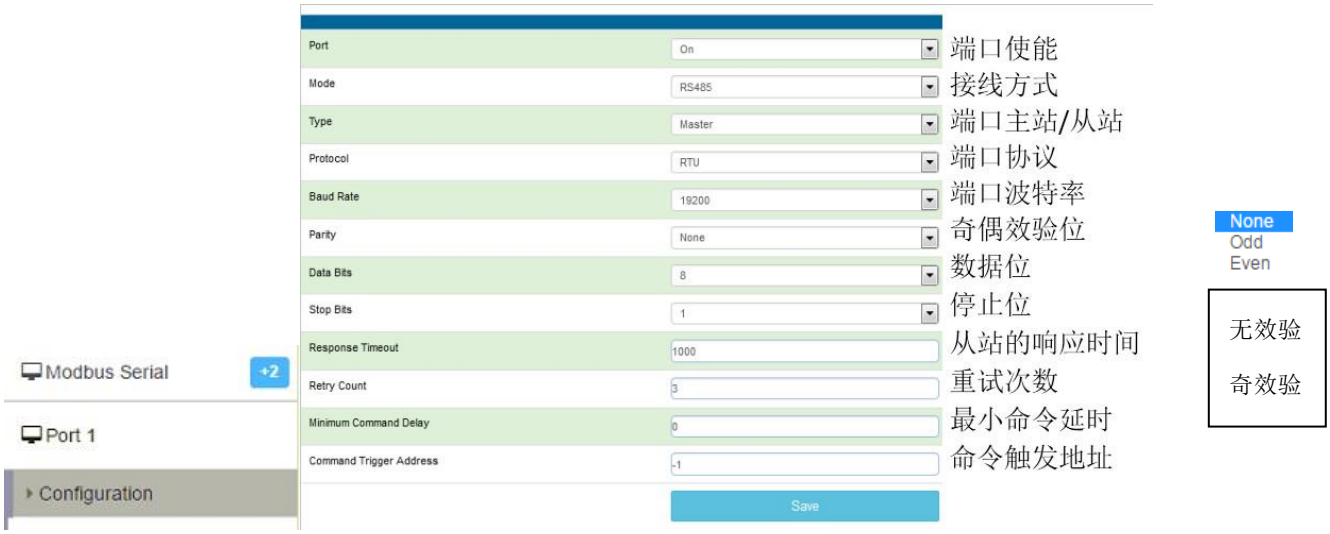
或水晶头直插网关串口。



举例：S1口引出来RS232接口，端子2RX，3TX，5GND接线。

如果选用RS232接线方式，每个串口只能连接一个从站，接线长度不能超过15米。串口注意不能热插拔，容易对串口造成不必要的损坏。

打开浏览器，在左侧导航栏点击 Modbus Serial---Port1 里面的 Configuration，显示 S1 端口配置的页面，如下图:



此处模块作为Modbus主站，请根据需要连接的Modbus从站情况，合理在此页面配置参数。之后，点击Port1里面的Commands显示S1端口命令的配置页面，点击Add。出现如下指令配置页面：

Modbus Port 1 - Modify Command

Enable	Yes	使能，禁止，内部寄存器有变化后写
Modbus Function	FC 3 - Read Holding Registers(4X)	Modbus 功能码FC1,FC2,FC3,FC4,FC5,FC6,FC15,FC16
Slave Address	1	从站地址
Modbus Data Address	0	从站读写数据Modbus起始位
Quantity	10	读或者写的数据的数量
Data Swap	No Change	数据高低位交换，字交换，字节交换，字和字节交换
Poll Interval	0	命令轮询时间
Internal Data Address	2000	模块内部寄存器，存放数据的起始地址
Cmd Errors Mapping Enabled	Yes	命令错误状态位反馈开启
Cmd Errors Mapping Address	2100	命令错误状态位反馈地址，模块内部寄存器任意位置
Desc		命令描述

Modbus 主站命令解释，采用功能码控制读写区域，**注意一定要先确定模块内部数据的范围。以下举例中采用的模块最多可以支持 4000 个字数据区地址范围，实际配置模块时，请按照模块真实数据区大小进行指令的使用。**

模块内部寄存器是 16 位的 INT 格式，读写布尔量的时需要注意 16 倍关系。

Enable	Yes
Modbus Function	FC 3 - Read Holding Registers(4X)
Slave Address	1
Modbus Data Address	0
Quantity	100
Data Swap	No Change
Poll Interval	0
Internal Data Address	2000
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 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 1 号从站，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 1 号从站，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。

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
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 1 号从站，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 1 号从站，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。

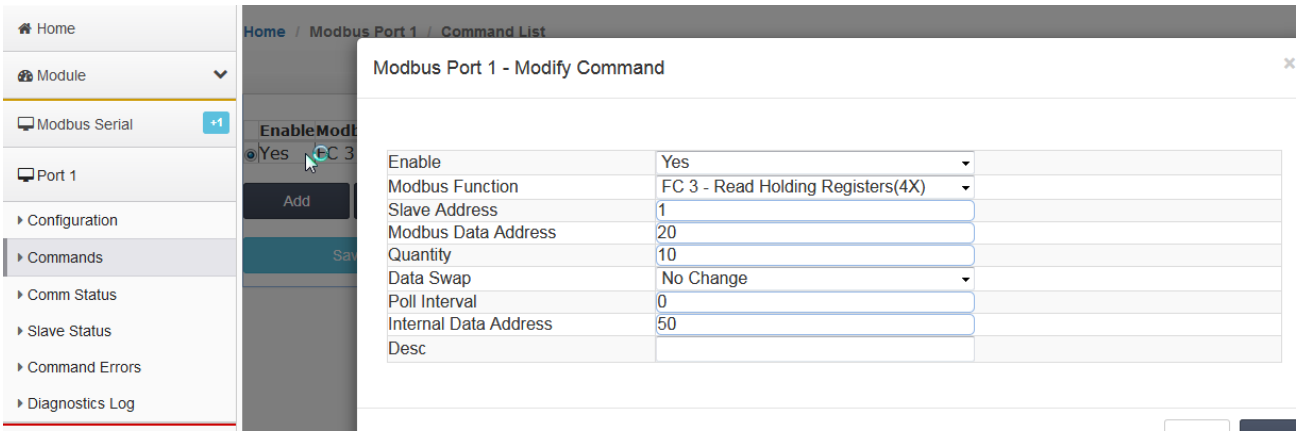
Enable	Yes
Modbus Function	FC 16 - Preset (Write) Multiple Register
Slave Address	1
Modbus Data Address	50
Quantity	20
Data Swap	No Change
Poll Interval	0
Internal Data Address	2000
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2051
Desc	

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 1 号从站，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。

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
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2501
Desc	

以上指令含义如下：模块功能码 FC6 或者 FC16 时，写出数量是 20.模块内部寄存器起始地址 2000。表示内部寄存器范围 2000-2019 的数据，一直连续的写出到 1 号从站，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。

举例：新建一条命令，

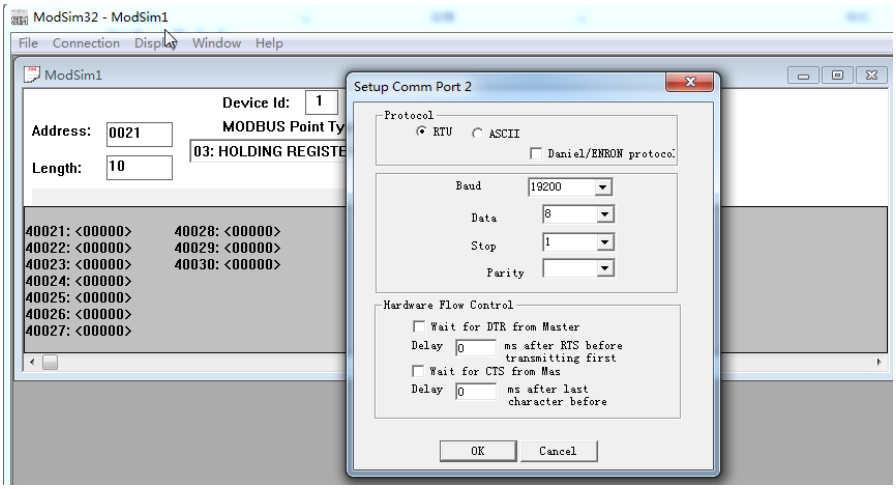


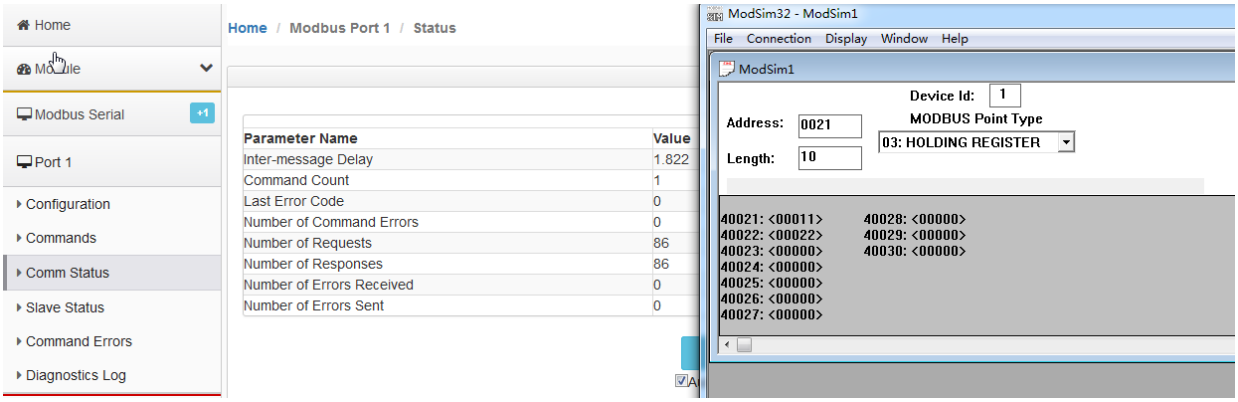
命令含义：把 MODBUS RTU 从站的 40021-40030 这 10 个 16 位的数值读到内部数据库 50-59 里面。

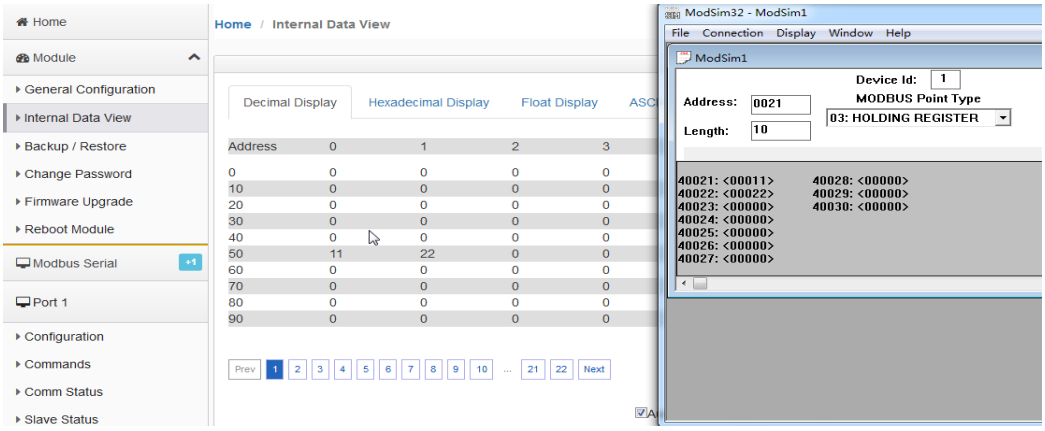
配置完，把这个命令保存到命令列表里面，然后根据提示重启模块。

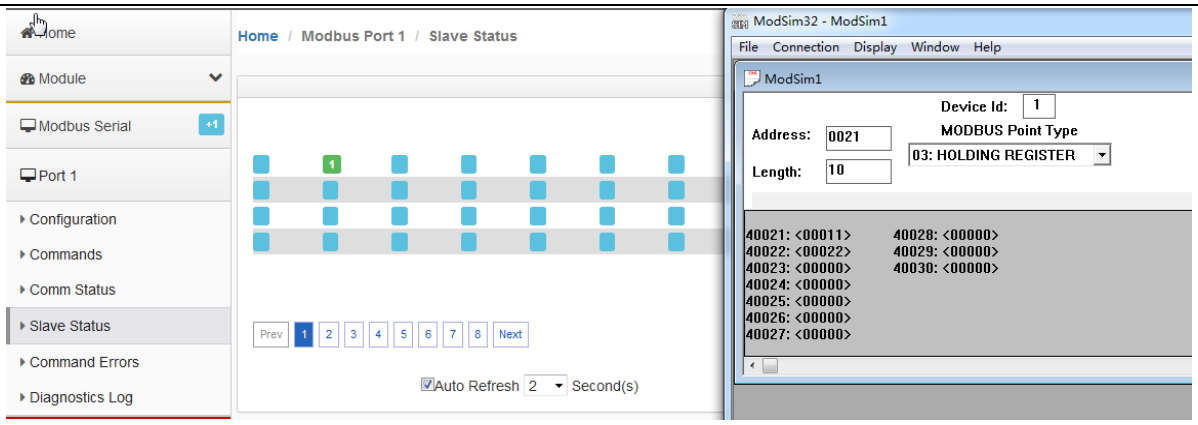
用户在配置好模块 MODBUS RTU 主站端口后，可以利用 MODBUS RTU 仿真软件 MODSIM32，作为 MODBUS RTU 从站，仿真测试与模块主站端口通讯。

打开 MODSIM 32 软件，配置端口 2 参数，从 40021-40030 写入十个数据。点击 OK。可以看到模块主站对应的内部数据区也相应的显示出从站的数值变化。


ModSim32 - ModSim1
File Connection Display Window Help
ModSim1
Device Id: 1
Address: 0021
Length: 10
MODBUS Point Ty
03: HOLDING REGISTE
40021: <00000>
40022: <00000>
40023: <00000>
40024: <00000>
40025: <00000>
40026: <00000>
40027: <00000>
40028: <00000>
40029: <00000>
40030: <00000>
Setup Comm Port 2
Protocol
RTU
ASCII
Daniel/ENRON protocol
Baud 19200
Data 8
Stop 1
Parity
Hardware Flow Control
Wait for DTR from Master
Delay 0 ms after RTS before transmitting first
Wait for CTS from Mas
Delay 0 ms after last character before
OK
Cancel


Home
Module
Modbus Serial
Port 1
Configuration
Commands
Comm Status
Slave Status
Command Errors
Diagnostics Log
Home / Modbus Port 1 / Status
Parameter Name
Value
Inter-message Delay 1.822
Command Count 1
Last Error Code 0
Number of Command Errors 0
Number of Requests 86
Number of Responses 86
Number of Errors Received 0
Number of Errors Sent 0
ModSim32 - ModSim1
File Connection Display Window Help
ModSim1
Device Id: 1
Address: 0021
Length: 10
MODBUS Point Type
03: HOLDING REGISTER
40021: <00011>
40022: <00022>
40023: <00000>
40024: <00000>
40025: <00000>
40026: <00000>
40027: <00000>
40028: <00000>
40029: <00000>
40030: <00000>


Home
Module
General Configuration
Internal Data View
Backup / Restore
Change Password
Firmware Upgrade
Reboot Module
Modbus Serial
Port 1
Configuration
Commands
Comm Status
Slave Status
Home / Internal Data View
Decimal Display
Hexadecimal Display
Float Display
Address 0 1 2 3
0 0 0 0 0
10 0 0 0 0
20 0 0 0 0
30 0 0 0 0
40 0 0 0 0
50 11 22 0 0
60 0 0 0 0
70 0 0 0 0
80 0 0 0 0
90 0 0 0 0
Prev 1 2 3 4 5 6 7 8 9 10 ... 21 22 Next
ModSim32 - ModSim1
File Connection Display Window Help
ModSim1
Device Id: 1
Address: 0021
Length: 10
MODBUS Point Type
03: HOLDING REGISTER
40021: <00011>
40022: <00022>
40023: <00000>
40024: <00000>
40025: <00000>
40026: <00000>
40027: <00000>
40028: <00000>
40029: <00000>
40030: <00000>

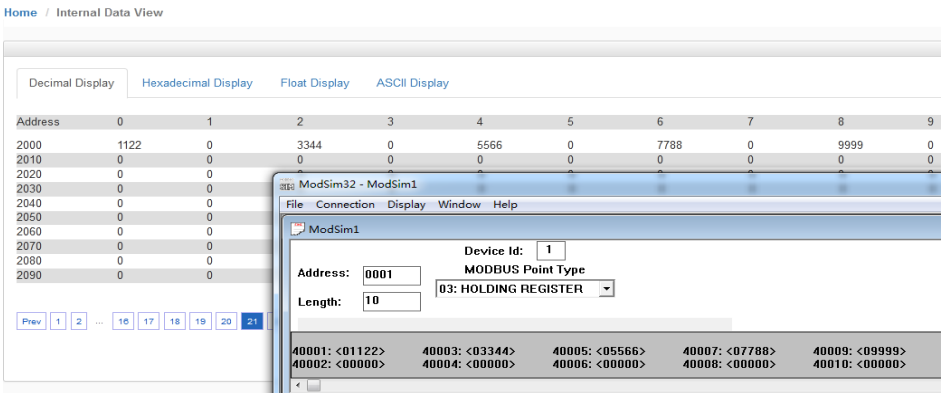


Cmd Errors Mapping Enabled和Cmd Errors Mapping Address这两个参数介绍；

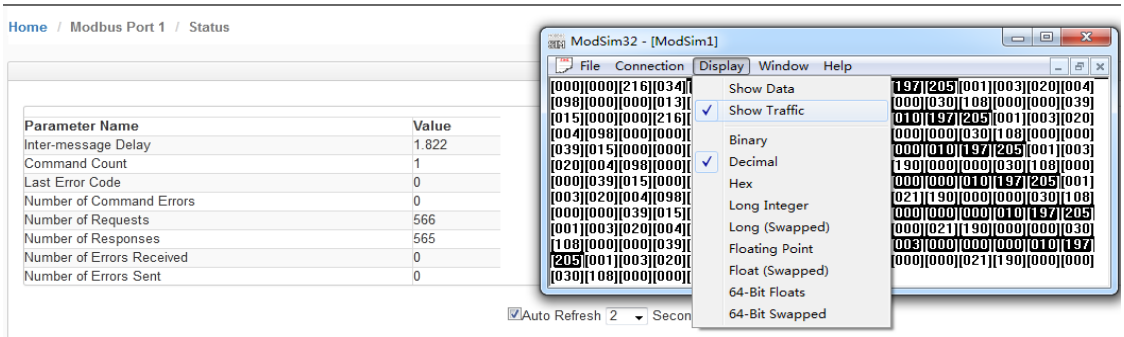
Cmd Errors Mapping Enabled表示命令错误是否映射，选择YES表示使用，选择NO，表示不使用；

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

上图命令表示：读取1号从站,从站数据地址范围40001-40010，这10个数放到内部起始地址为2000的连续10个寄存器内（2000-2009），如果发送错误，错误反馈会放到内部寄存器2100里面。指令执行效果如下图显示：



通过查看命令状态（Comm Status）可以看到命令执行情况，通过点击Mosim32菜单栏显示报文，可以查看从站与主站的发送和接收报文的情况。

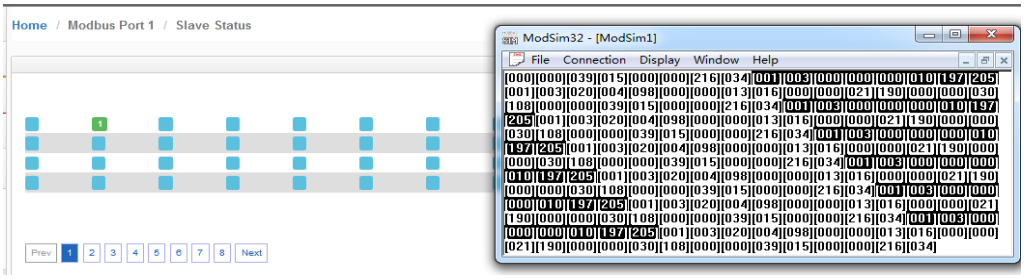


通过查看从站状态可以直接看到从站的状态，1-31路都可以直观看到：

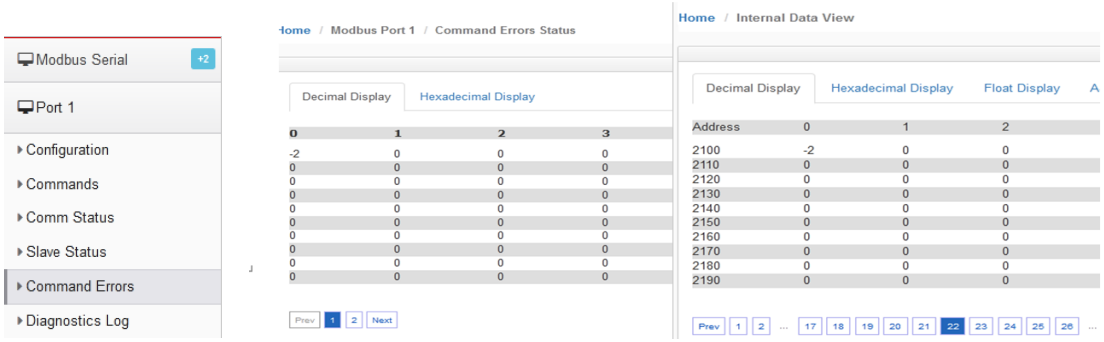
绿色表示线路数据通讯报文都正常；

红色表示线路数据通讯报文都不对；

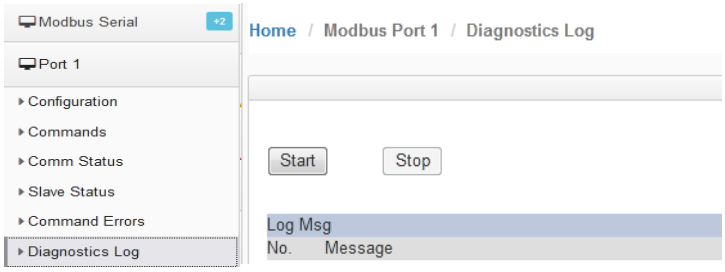
绿色和红色闪烁表示线路正常，数据通讯报文不正常。



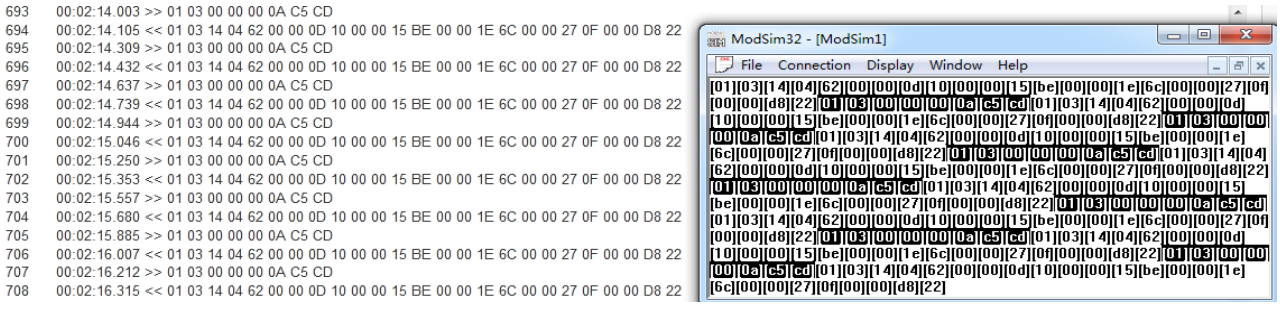
通过查看命令错误可以看到从站报的错误值，如果开启了命令反馈功能，这个值也会送到工程师填写的命令错误存放地址(内部寄存器地址2100)里面。



通过诊断报文，可以查看主站发送和接收的报文情况。点击Start，就可以看到下面报文发送和接受的情况。

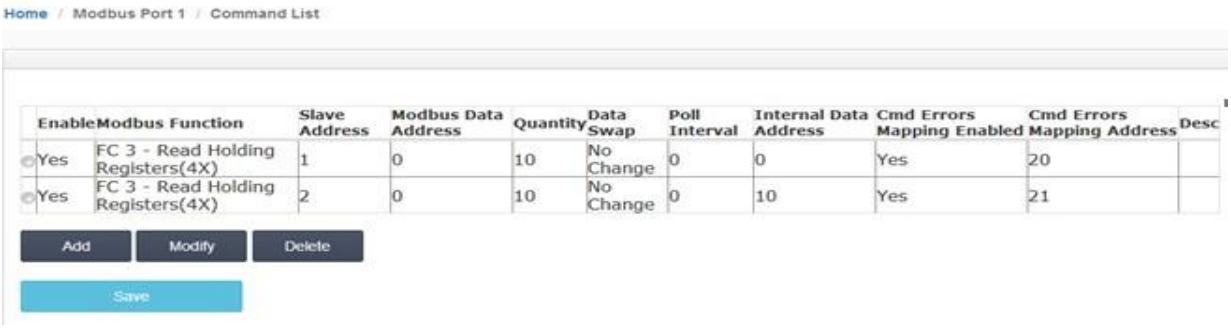


下图为主站发送和接收的报文以十六进制格式显示，Modsim32也可以从十进制报文切换到十六进制报文显示：



Modbus 命令使能控制介绍

新版本增加了Modbus RTU做主站的命令使能控制，这个作用是表示可以控制发出几个命令，比如模块连接了15个从站，如果有一个从站坏掉了，这时候Modbus RTU网络会变慢，主站每次发送命令会等待这个从站响应，解决的办法是不发送这个从站的命令，具体使用方法如下。

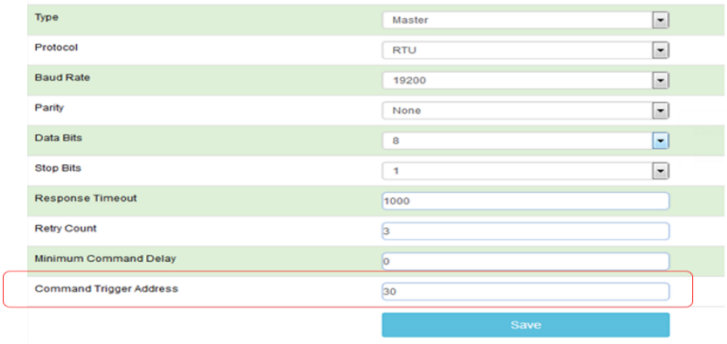


上图中建立两条指令：

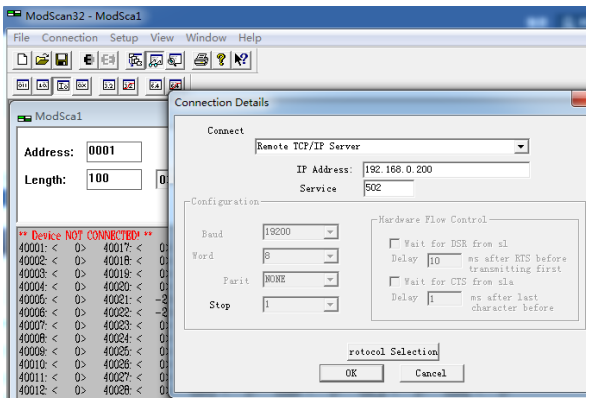
1- 读1号从站的40001-40010到内部寄存器0-9，错误状态放在了内部寄存器20。

2- 读2号从站的40001-40010到内部寄存器10-19，错误状态放在了内部寄存器21

3- 使能命令触发地址，在模块Modbus主站端口配置页面中，Command Trigger Address设置成30，如下图，表示使用模块内部起始地址为30的寄存器作为触发条件。然后保存，重启生效。

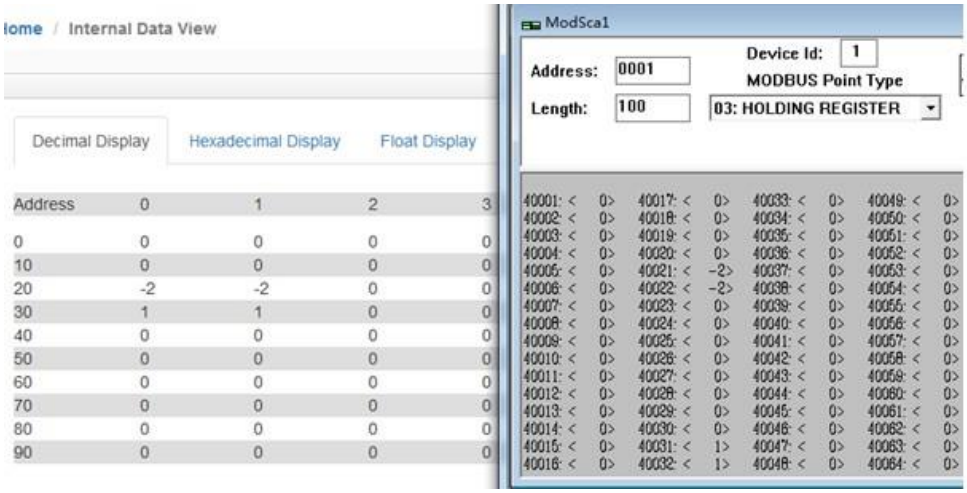


之后使用ModScan仿真作为Modbus从站，用ModScan的40031和40032可以模拟控制这两条指令的触发状态。



ModScan的40031和40032设置为1，可以看到模块内部寄存器地址30数据是1，内部寄存器地址31也是1，表示

以上两条指令处于触发情况。模块内部寄存器地址20-21数据是-2，表示有错误代码，说明以上两条指令都没有正确执行。

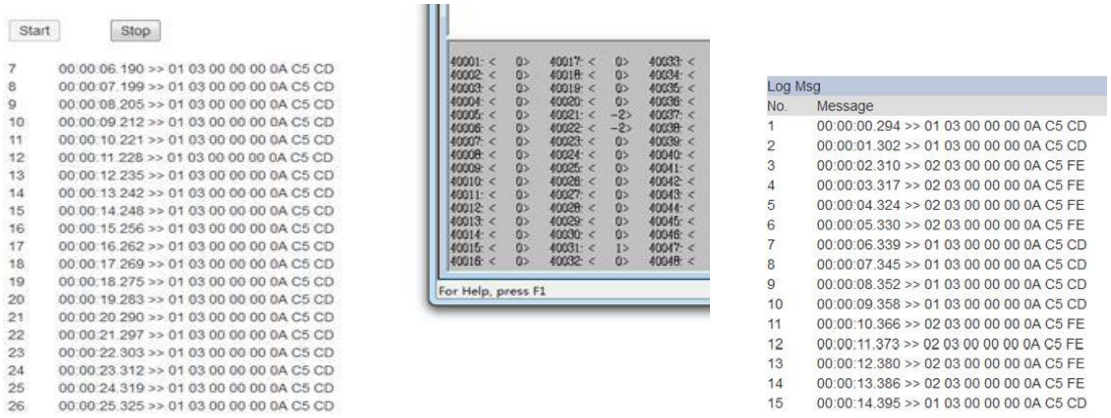


直观表现如下：检查Port1报文发送情况，显示第一条命令发送4次，第二条命令发送4次。因为命令本身发送1次，如果找不到从站设备，该命令会重新发送3次，共计4次。

重发次数，可以在端口配置中进行修改（如下图）：

以上两条指令都没有正确执行，如果是2号从站有问题，我们可以把2号从站的命令停止发送。

需要修改ModScan中40032的数值，从1改成0（如下图），这样相当于停止了触发读取2号从站的指令。



就实现了模块只读取1号从站数值的报文。避免了多个从站中有一个或两个掉线而影响整体Modbus RTU网络变慢的情况。

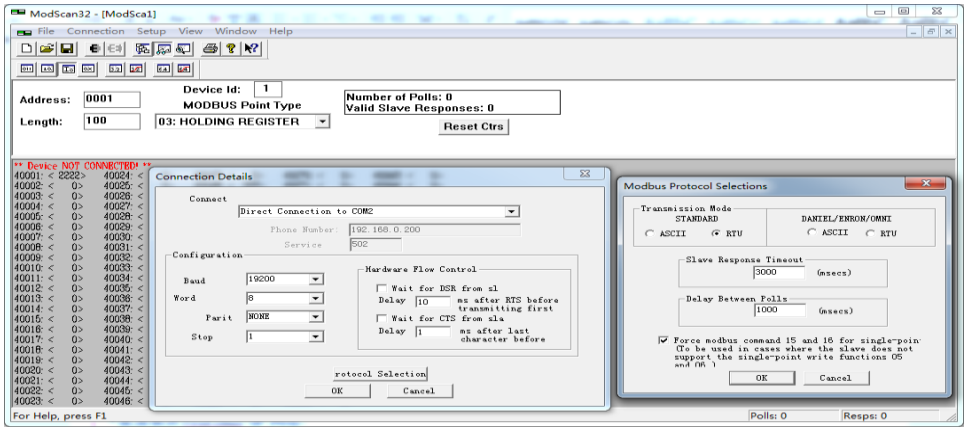
该功能建议配合前文提到的命令反馈功能一并使用，当其中一个命令返馈回来出现非 0 值，PLC 的程序可以自动关联这个触发值去停止 Modbus 指令的执行。

配置模块做 MODBUS RTU 从站

点击Port1里面的Configuration显示S1端口配置的页面：

注意事项：S1或者S2作为Modbus从站，只需要配置端口参数，无需配置端口命令。S1和S2共用模块内部数据区。如下图为设置模块的Modbus从站端口参数：

使用ModScan32仿真Modbus RTU主站，可以对模块内部寄存器读写。

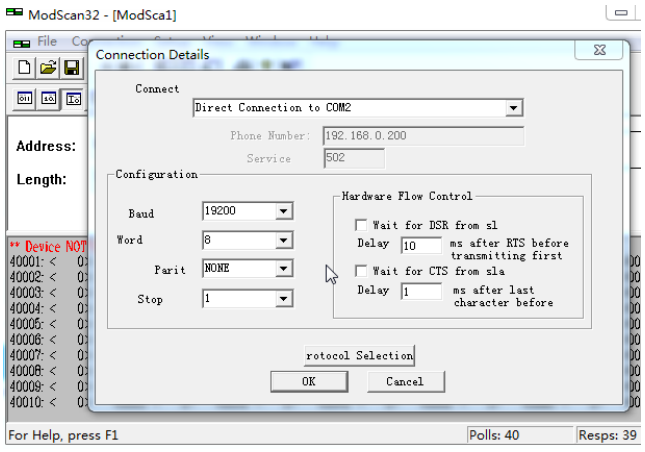


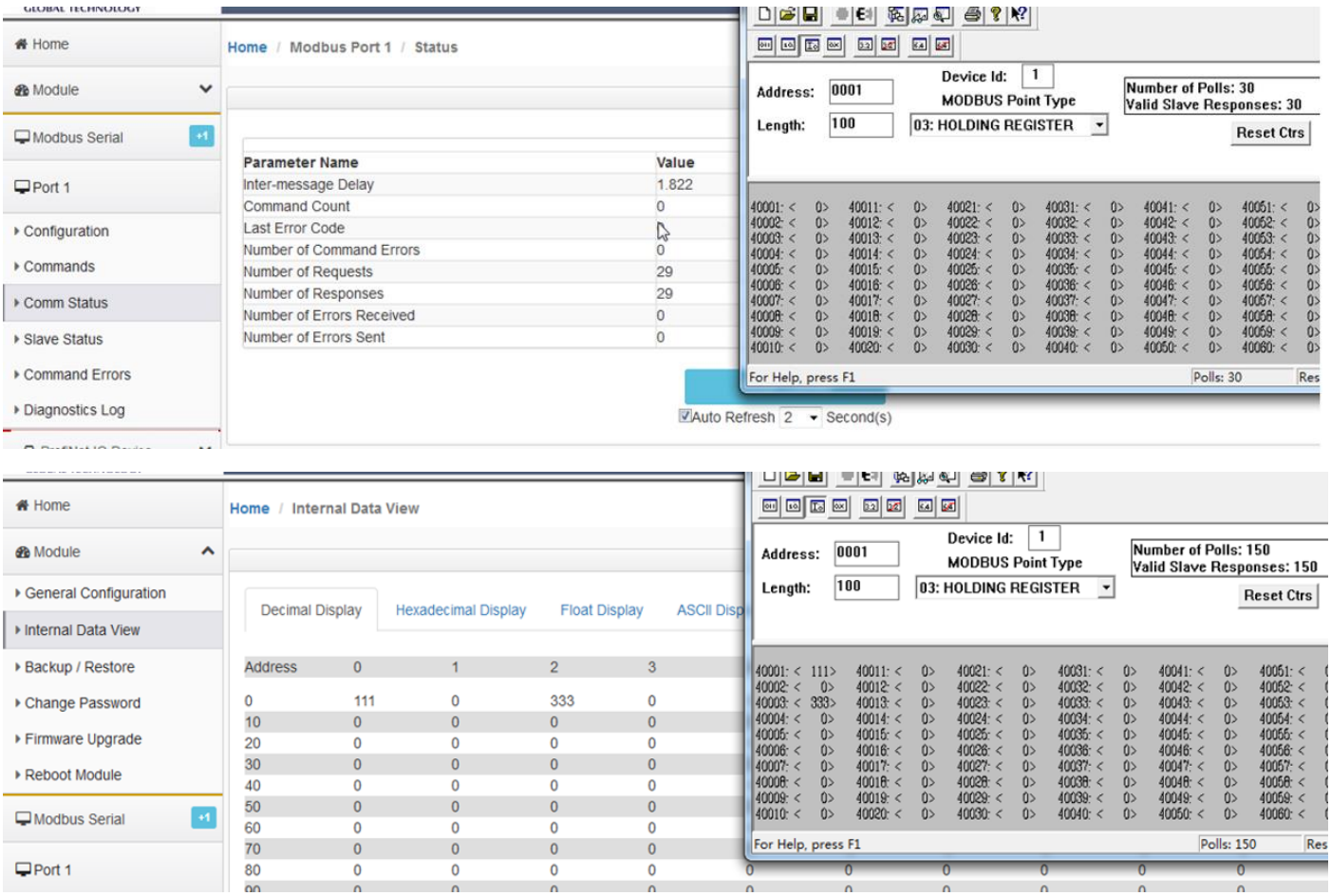
内部寄存器与Modbus数据对应关系：

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 RTU 仿真软件 MODSCAN32，其作用是仿真 MODBUS RTU 主站。软件连接作为 MODBUS RTU 从站的模块。选择 Connection，选择电脑的 USB-485 接口 COM2，修改波特率，数据位，奇偶校验位，停止位等参数与模块的端口参数一致。点击 OK，可以看到连接的发送和接收次数。在 40001 等数据区进行写数据，可以看到模块内部对应寄存器同样有数据显示。

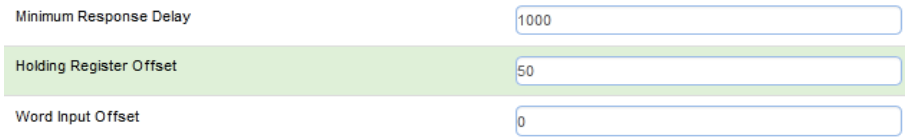


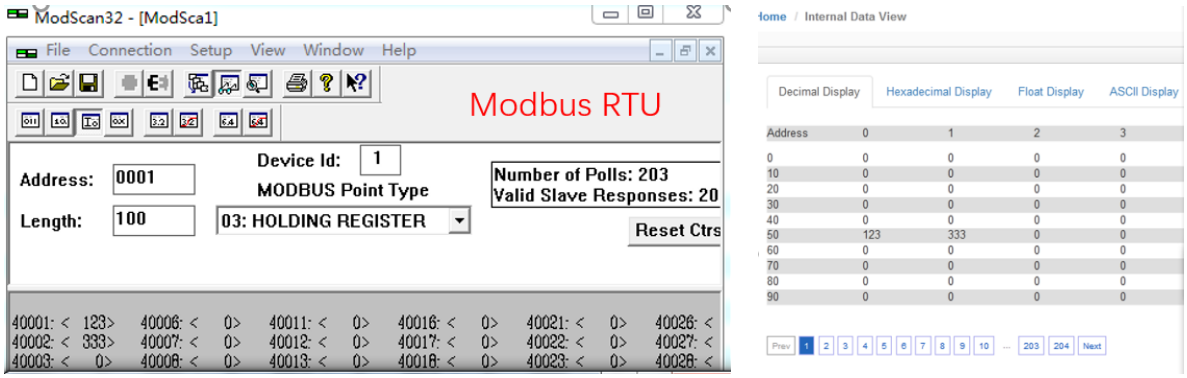


备注：40001 对应着内部寄存器 0，40100 对应着内部寄存器 99，以此类推。

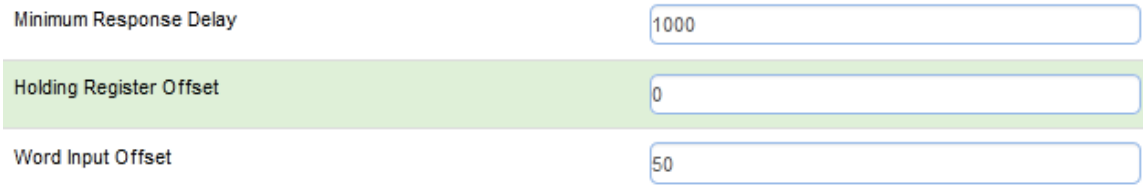
Modbus RTU 配置成从站时，在主页面可以设置接收地址偏移。

Holding Register Offset使用方法：Modbus RTU主站使用FC3功能码，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。



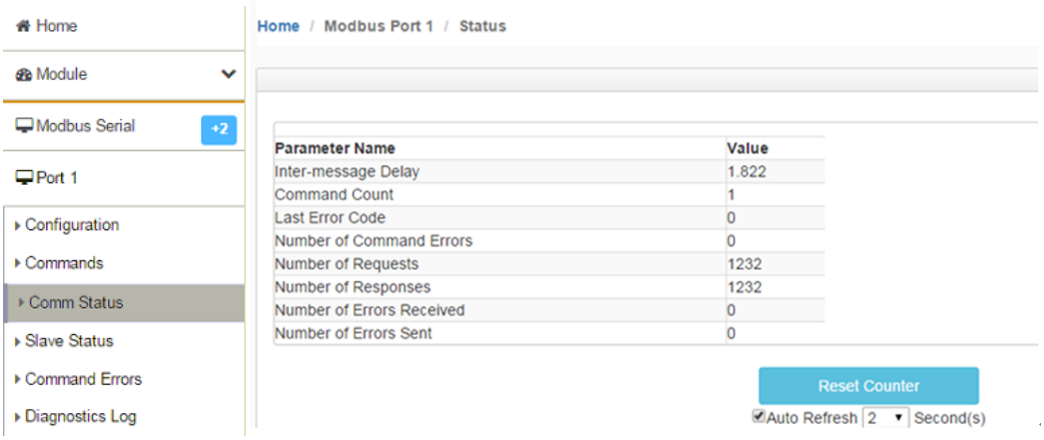


Word Input Offset使用方法：如果此处偏移量设置成50(如下图)，Modbus RTU主站一侧在3区对30001和30002输入两个数据，数据会直接向后偏移放到模块内部寄存器50-51里面，ModScan32仿真软件不能载入3区的数值，请以现场设备实际数据区域来填写。

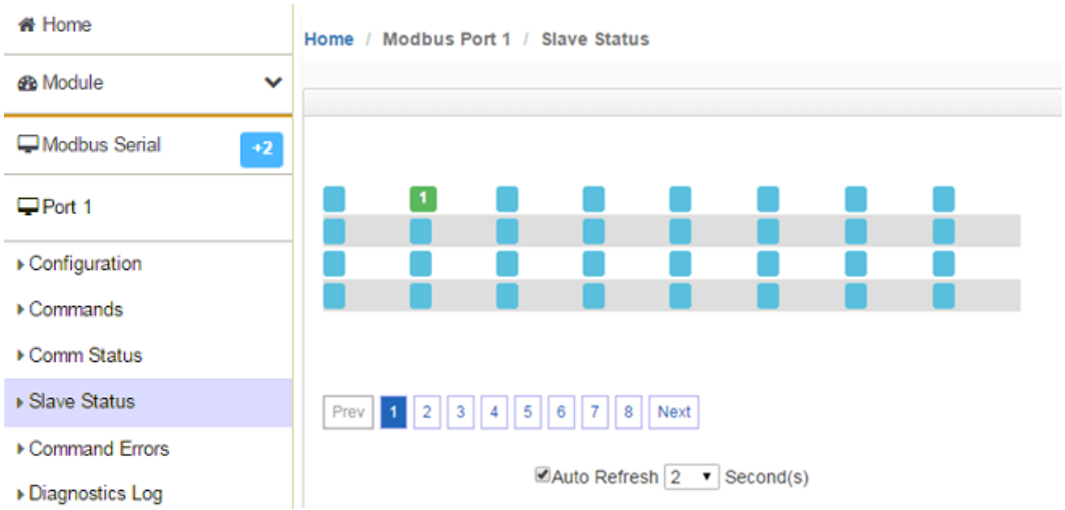


Modbus RTU 诊断方式

查看主站端口命令是否有错误，发包和收包状态:

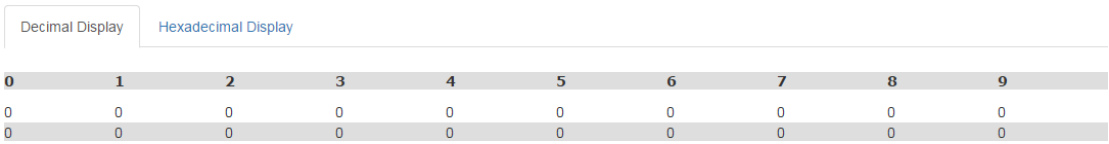


可视化查看从站状态 点击Slave Status 可以看到1号从站是绿色的。



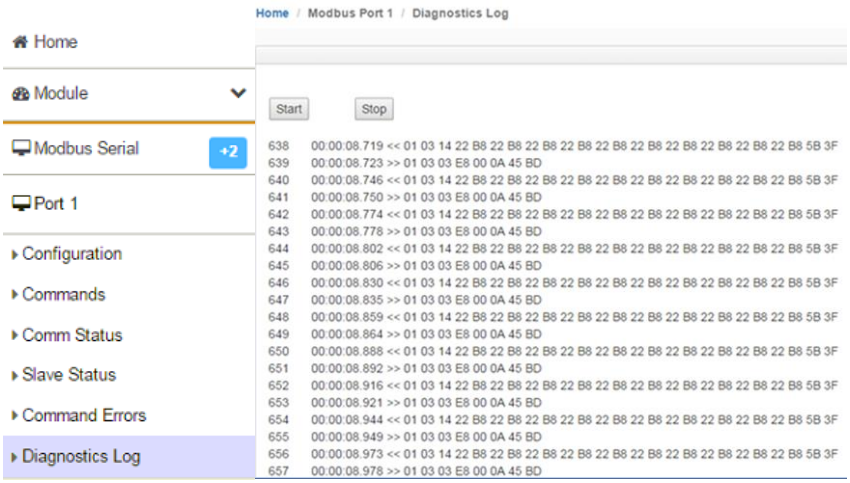
查看命令行是否有错误产生点击：

。



报文诊断功能：点击Diagnostics Log，再点击Start端口发送和接收报文的情况。

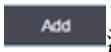
>>符号是S1端口发送的报文，<<符号是S1端口接收的报文。



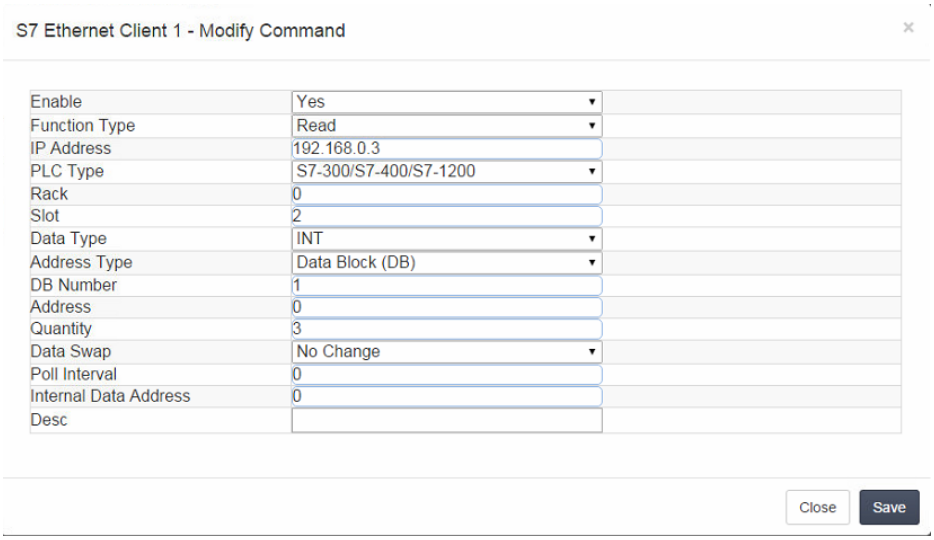
举例 1. 西门子 PLC 和 Modbus RUT 主站交换数据

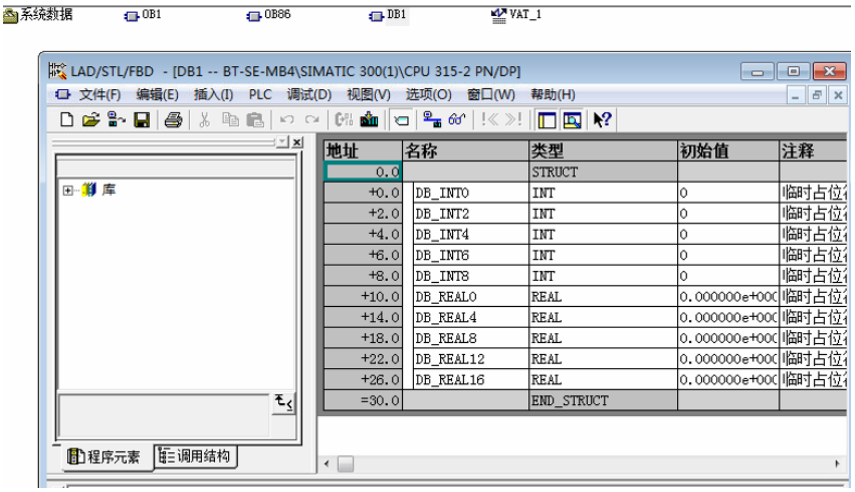
本案例中，模块Modbus RTU串口配置为slave，S7 Ethernet配置成为Client

点击 S7 Ethernet Client ---Client1 ---Commands

点击添加按钮 

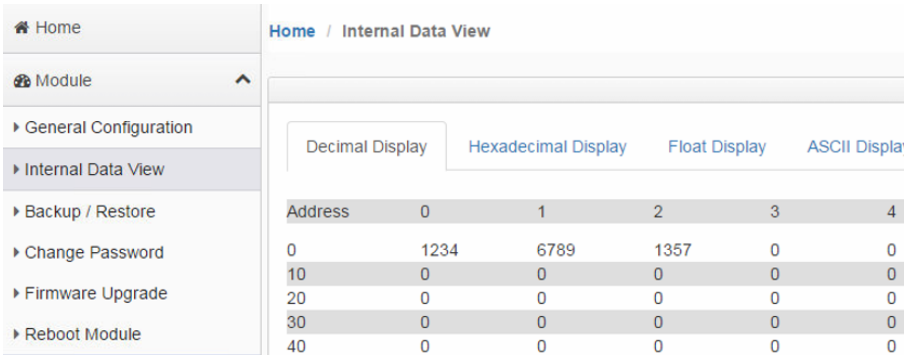
添加一条 S7 以太网指令，指令解释如下，把 IP 地址为 192.168.0.3 的西门子 S7-300 PLC 中的 DB1 数据块里面的前 3 个 INT 数据读到模块第寄存器地址 0-2 里面.



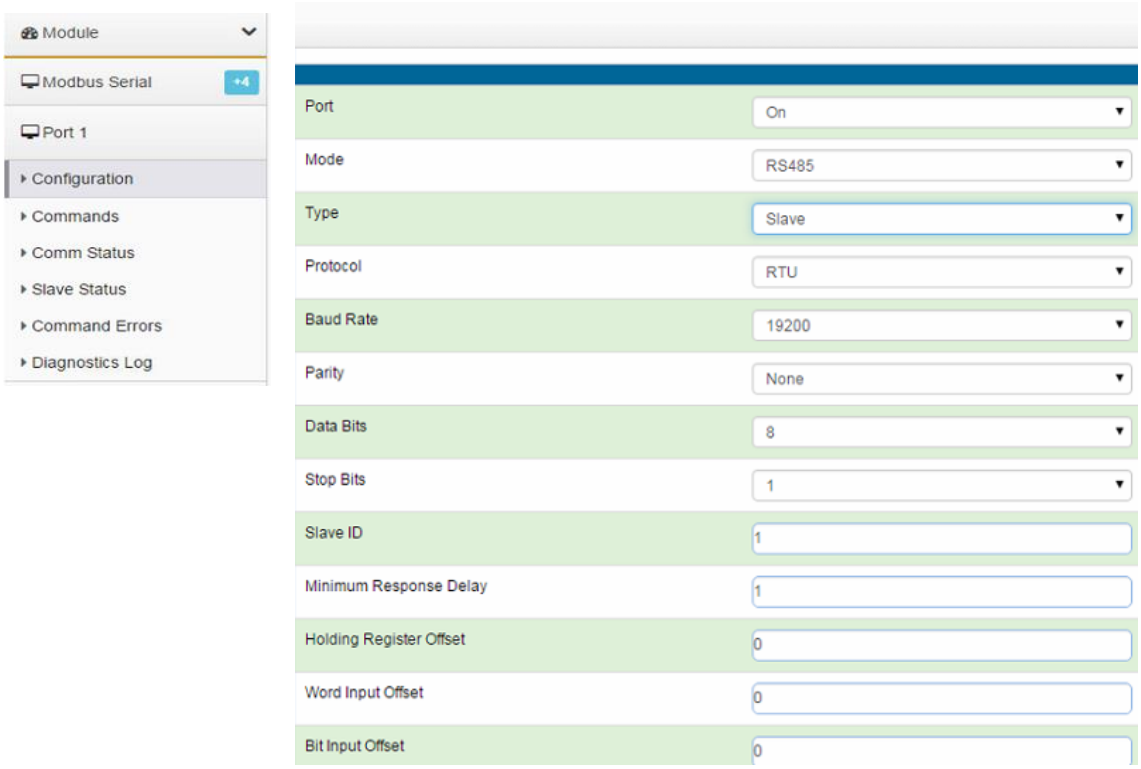


在 DB1.DBW0，DB1.DBW2，DB1.DBW4 里面写点数据。点击  写进去。

返回查看模块内部数据库寄存器 0-2



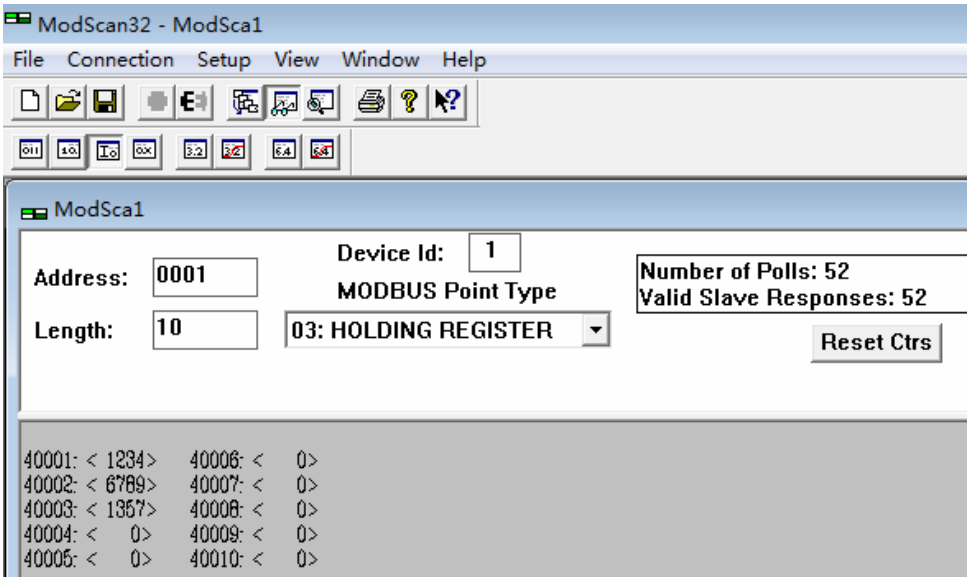
之后，配置模块的 Modbus 串口，如下点击 Modbus Serial—Port1---Configuration 将该串口配置成为 Modbus Slave



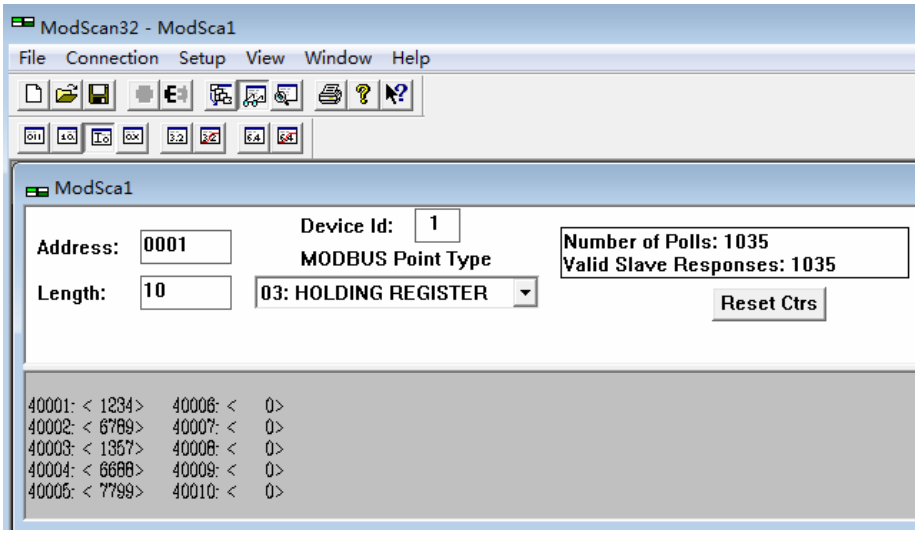
前文中已经介绍过，模块作为 Modbus 从站时内部数据区和 modbus 主站数据地址对应关系，如下

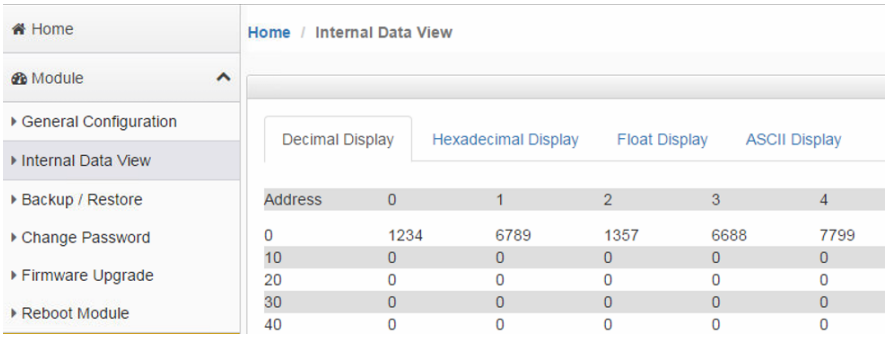
模块内部寄存器地址	对应Modbus主站的	Modbus 4 区地址
0	=	40001
1	=	40002
10	=	40011
11	=	40012
20	=	40021
30	=	40031
99	=	40100
100	=	40101
220	=	40221
1000	=	41001

采用 ModScan 模拟 Modbus RTU 主站，使用 FC3 读取模块内部地址数据，可见，模块内部寄存器 0-9 地址的数据，被读取到了 ModScan 的 40001-40010 中。



在 MODSCAN 32 仿真软件 40004-40005 地址写数据，数据将被写入到模块内部寄存器地址 3-4 里





在模块的 S7 以太网一侧，再添加命令，将模块内部寄存器地址 3 开始的 2 个 INT 数据，写给 IP 地址为 192.168.0.3 的西门子 DB1.DBW6 和 DB1.DBW8 里面。

S7 Ethernet Client 1 - Modify Command

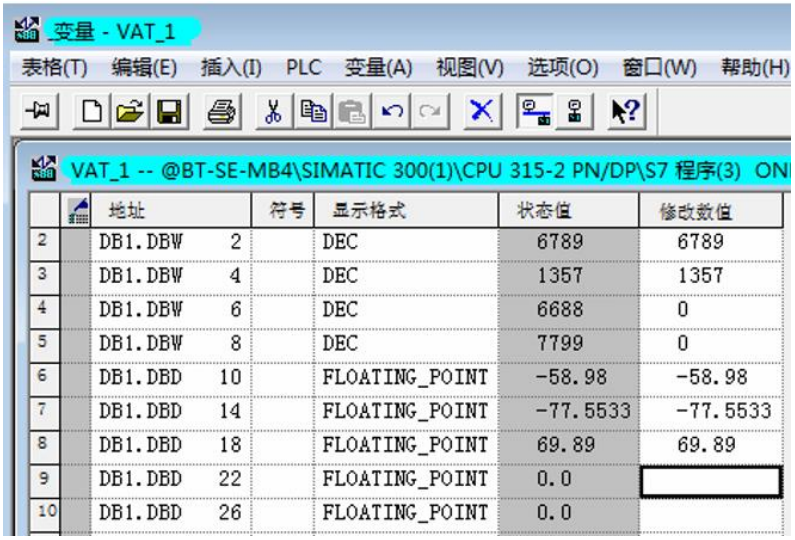
Enable	Yes
Function Type	Write
IP Address	192.168.0.3
PLC Type	S7-300/S7-400/S7-1200
Rack	0
Slot	2
Data Type	INT
Address Type	Data Block (DB)
DB Number	1
Address	6
Quantity	2
Data Swap	No Change
Poll Interval	0
Internal Data Address	3
Desc	

Close Save

保存指令，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。

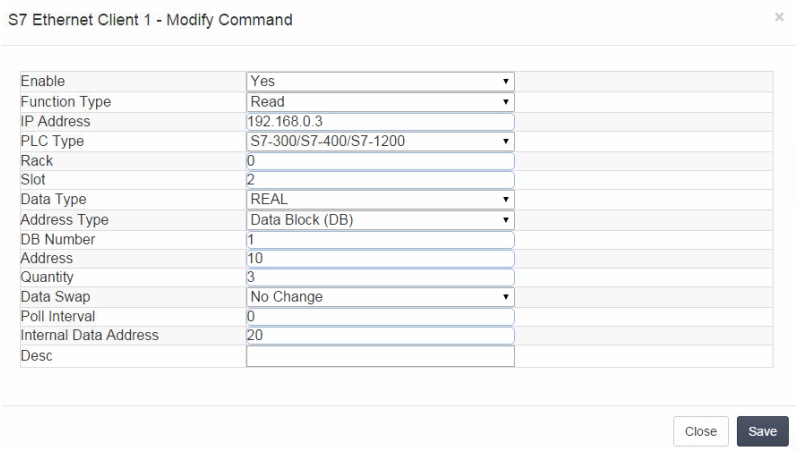
	地址	符号	显示格式	状态值	修改数值
1	DB1.DBW 0		DEC	1234	1234
2	DB1.DBW 2		DEC	6789	6789
3	DB1.DBW 4		DEC	1357	1357
4	DB1.DBW 6		DEC	6688	0
5	DB1.DBW 8		DEC	7799	0
6	DB1.DBD 10		DEC	L#0	
7	DB1.DBD 14		DEC	L#0	
8	DB1.DBD 18		DEC	L#0	
9	DB1.DBD 22		DEC	L#0	
10	DB1.DBD 26		DEC	L#0	
11					

在西门子 S7-300 PLC 的 DB1 中，对于 DBD10-DBD18 录入一些浮点数，如下图

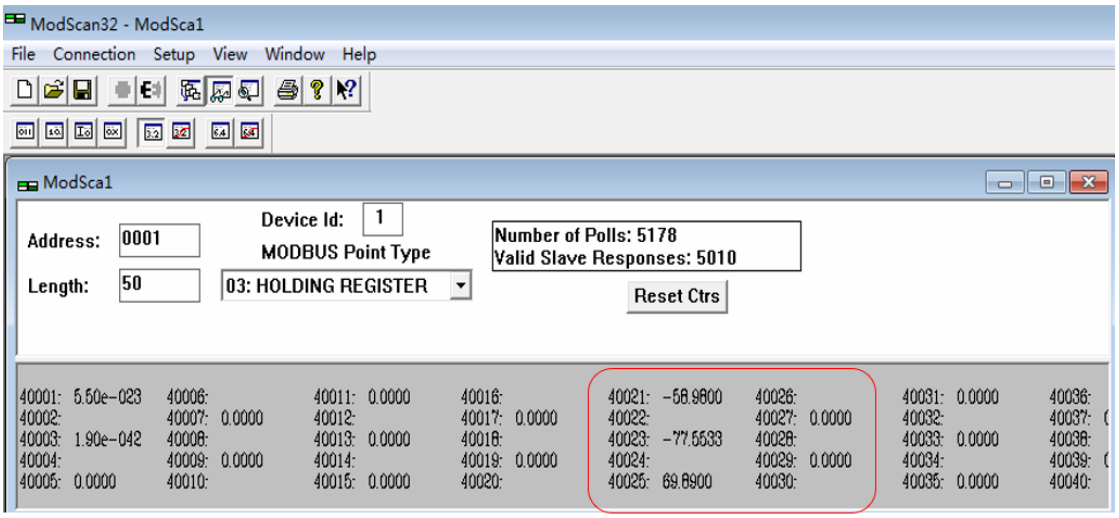


	地址	符号	显示格式	状态值	修改数值
2	DB1.DBW 2		DEC	6789	6789
3	DB1.DBW 4		DEC	1357	1357
4	DB1.DBW 6		DEC	6688	0
5	DB1.DBW 8		DEC	7799	0
6	DB1.DBD 10		FLOATING_POINT	-58.98	-58.98
7	DB1.DBD 14		FLOATING_POINT	-77.5533	-77.5533
8	DB1.DBD 18		FLOATING_POINT	69.89	69.89
9	DB1.DBD 22		FLOATING_POINT	0.0	
10	DB1.DBD 26		FLOATING_POINT	0.0	

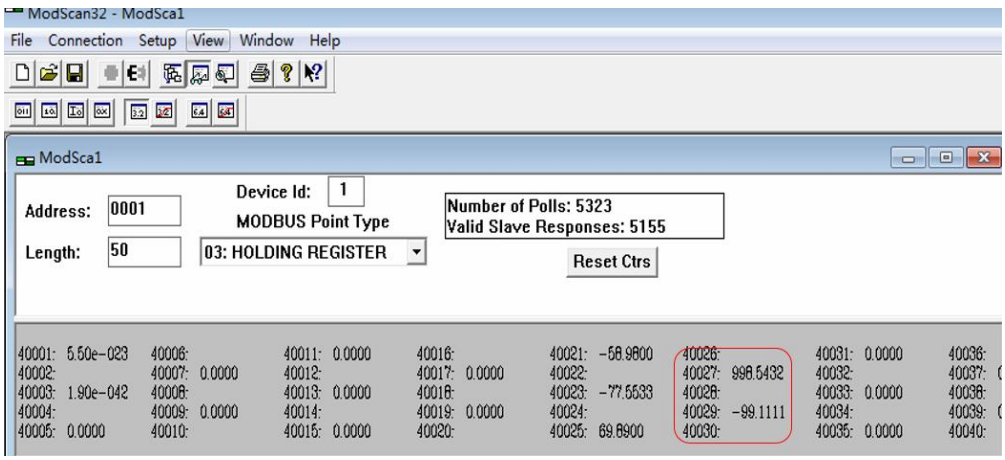
之后在模块的 S7 以太网一侧，添加一条指令。指令解释如下，读取 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器，把其中的 DB1 数据块里面，从 DBD10 开始的 3 个 REAL 类型数据，读到模块内部数据寄存器起始地址为 20 的区域中. 因为模内部数据寄存器为 16 位的字，所以 3 个浮点数会占用 6 个寄存器，也就是存放到模块内部地址 20-25 中



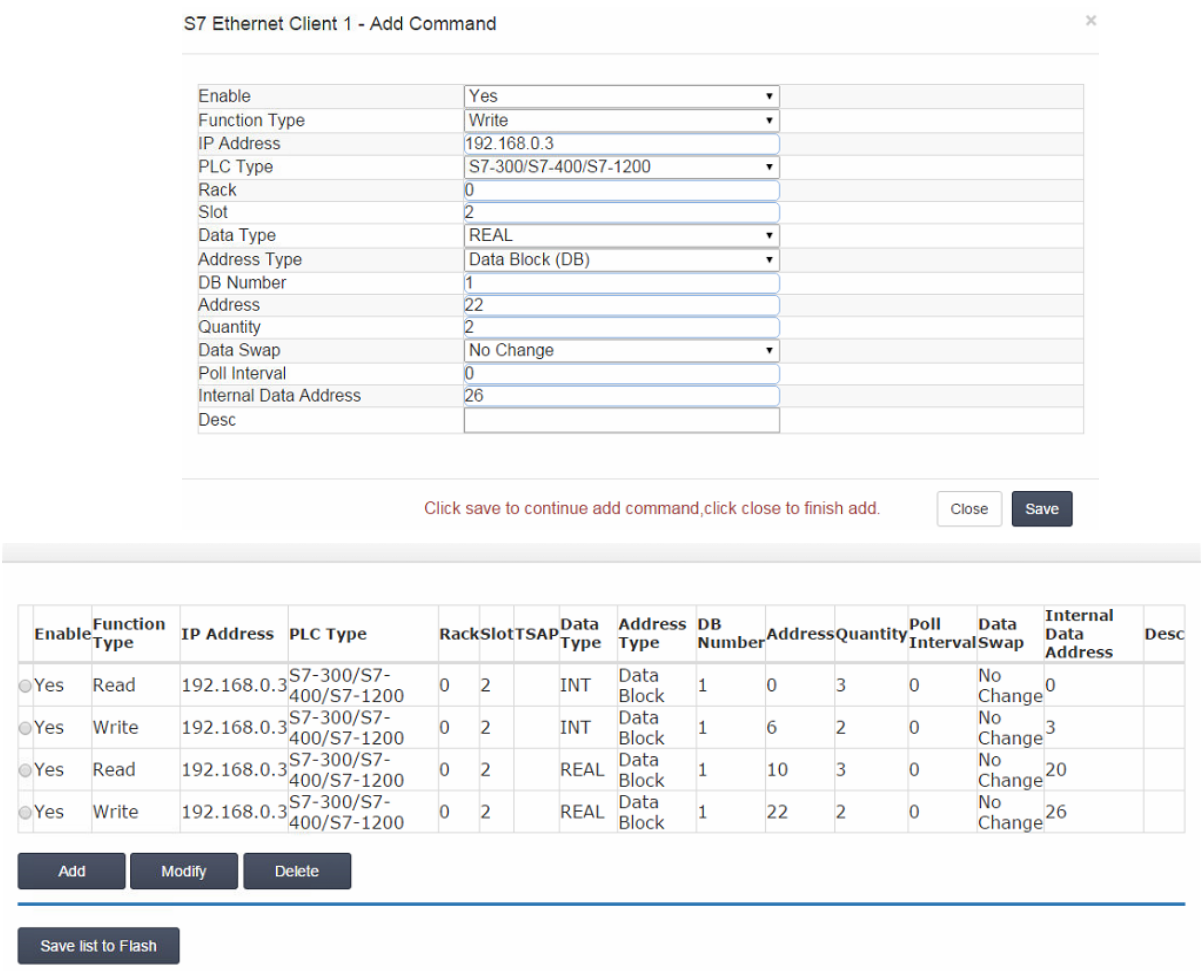
仍然采用 ModScan 模拟 Modbus RTU 主站，使用 FC3 读取模块内部地址数据，可见模块内部寄存器 20-25 地址的数据，被读取到了 ModScan 的 40021-40026 中。



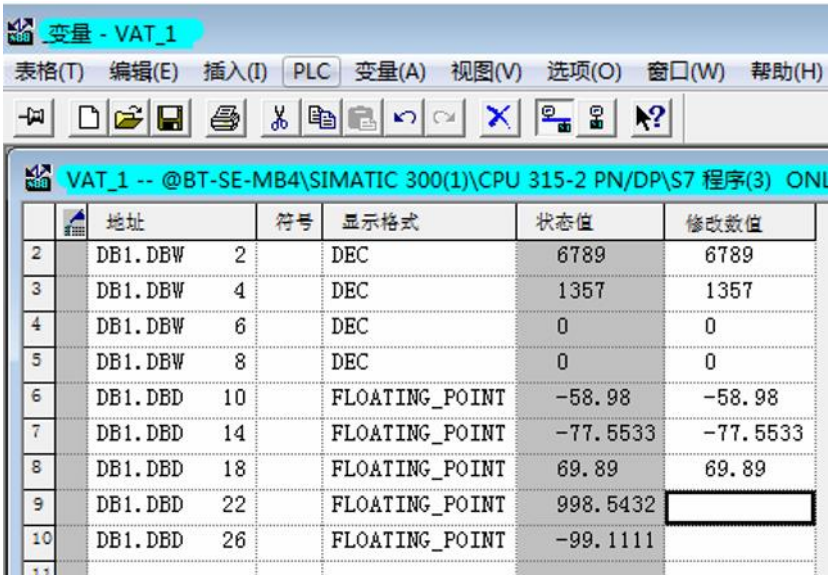
我们在 MODSCAN 的 40027-40030 位置录入 2 个浮点数，这两个浮点数将会被写入到模块的内部寄存器 26-29 的地址。



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。



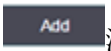
如下图查看西门子 PLC 的数据，可以看到 DB1.DBD22 和 DB1.DBD26 的数据值，和模块内部数据区一致。



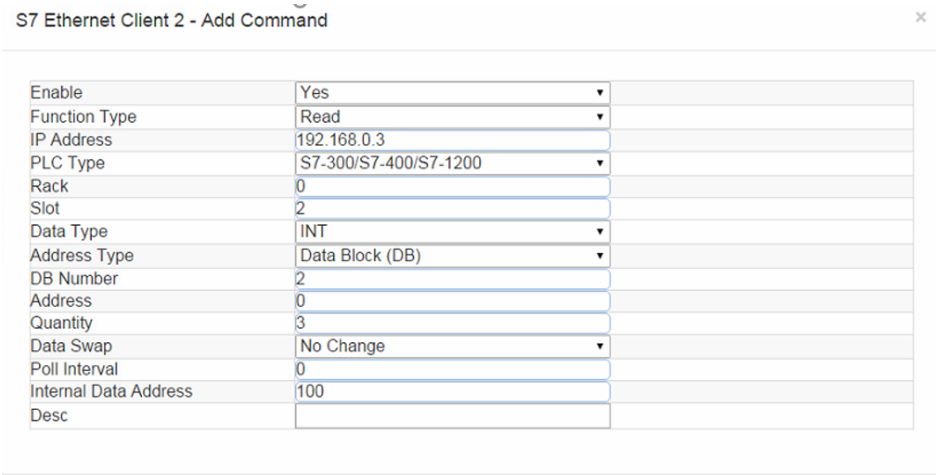
举例 2. 西门子 PLC 和 Modbus RUT 从站交换数据

本案例中，模块Modbus RTU串口配置为Master，S7 Ethernet配置成为Client

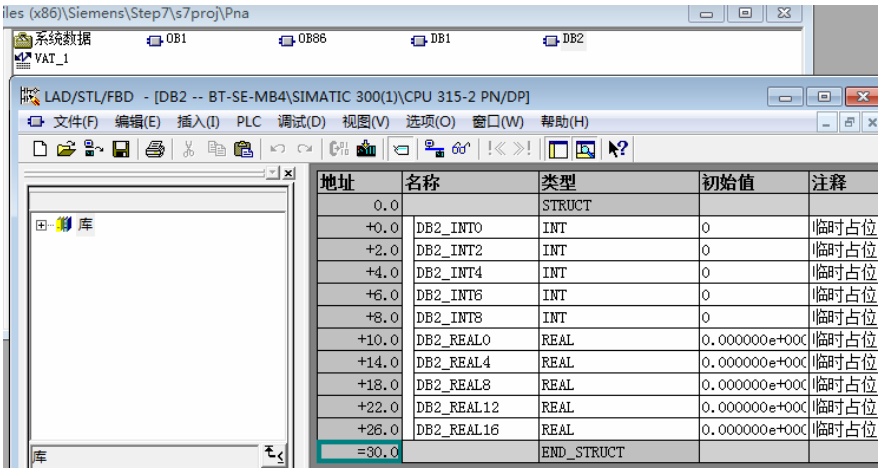
整型数的读写操作

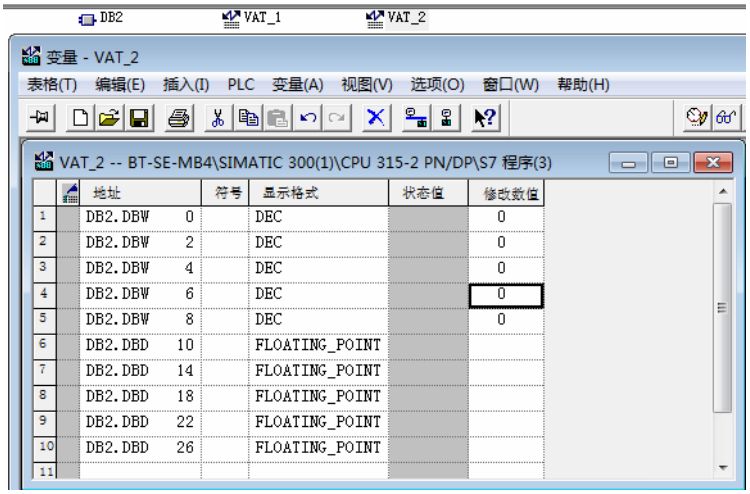
点击添加按钮 

添加一条 S7 以太网读指令，指令解释如下，把 IP 地址为 192.168.0.3 的西门子 S7-300 系列控制器中的，DB2 数据块里面的 3 个 INT 数据（地址 0-5 的字节数据）读取到模块内部寄存器地址 100-102 中.



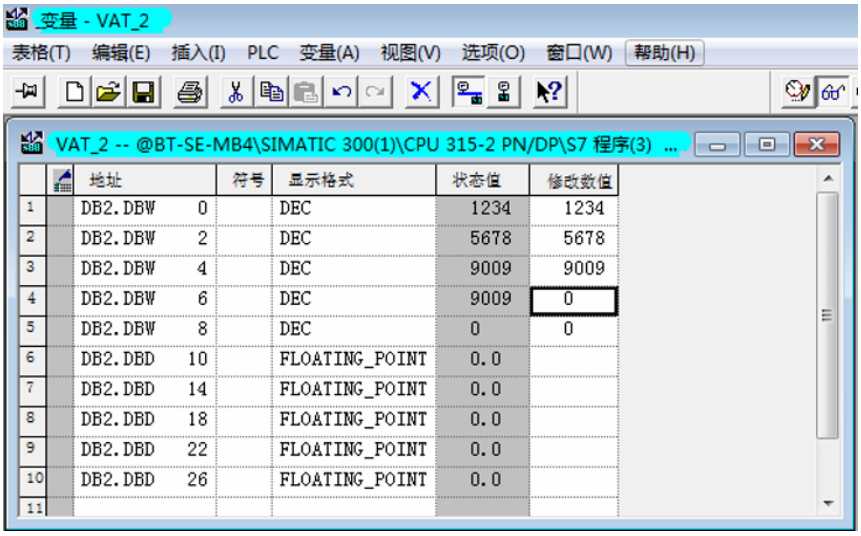
我们在西门子 PLC 程序中建立 DB2





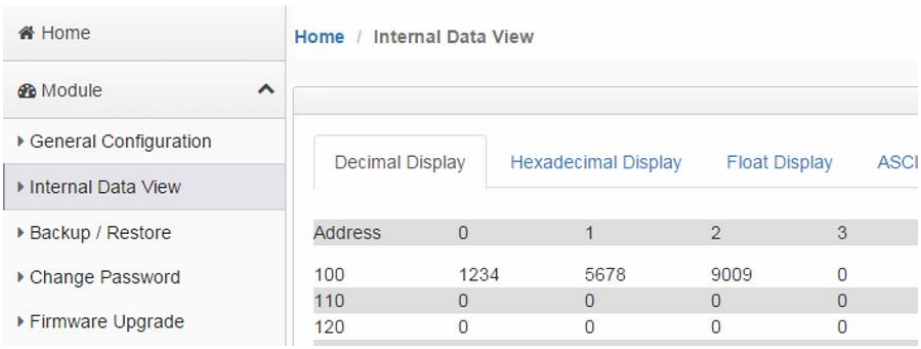
	地址	符号	显示格式	状态值	修改数值
1	DB2.DBW 0		DEC		0
2	DB2.DBW 2		DEC		0
3	DB2.DBW 4		DEC		0
4	DB2.DBW 6		DEC		0
5	DB2.DBW 8		DEC		0
6	DB2.DBD 10		FLOATING_POINT		
7	DB2.DBD 14		FLOATING_POINT		
8	DB2.DBD 18		FLOATING_POINT		
9	DB2.DBD 22		FLOATING_POINT		
10	DB2.DBD 26		FLOATING_POINT		
11					

在变量表里面写前 3 个 INT 的数值，更改数值，点击  写入。

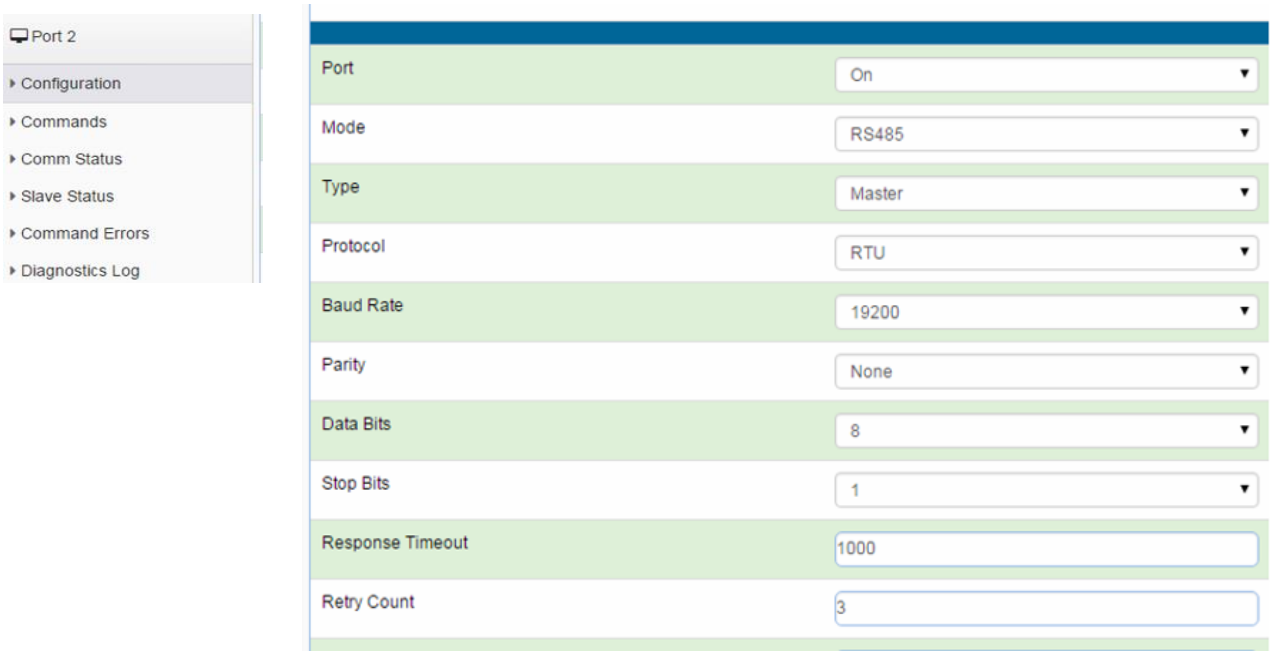


	地址	符号	显示格式	状态值	修改数值
1	DB2.DBW 0		DEC	1234	1234
2	DB2.DBW 2		DEC	5678	5678
3	DB2.DBW 4		DEC	9009	9009
4	DB2.DBW 6		DEC	9009	0
5	DB2.DBW 8		DEC	0	0
6	DB2.DBD 10		FLOATING_POINT	0.0	
7	DB2.DBD 14		FLOATING_POINT	0.0	
8	DB2.DBD 18		FLOATING_POINT	0.0	
9	DB2.DBD 22		FLOATING_POINT	0.0	
10	DB2.DBD 26		FLOATING_POINT	0.0	
11					

观察模块内部寄存器 100-102 采集到了西门子 PLC 的数据。

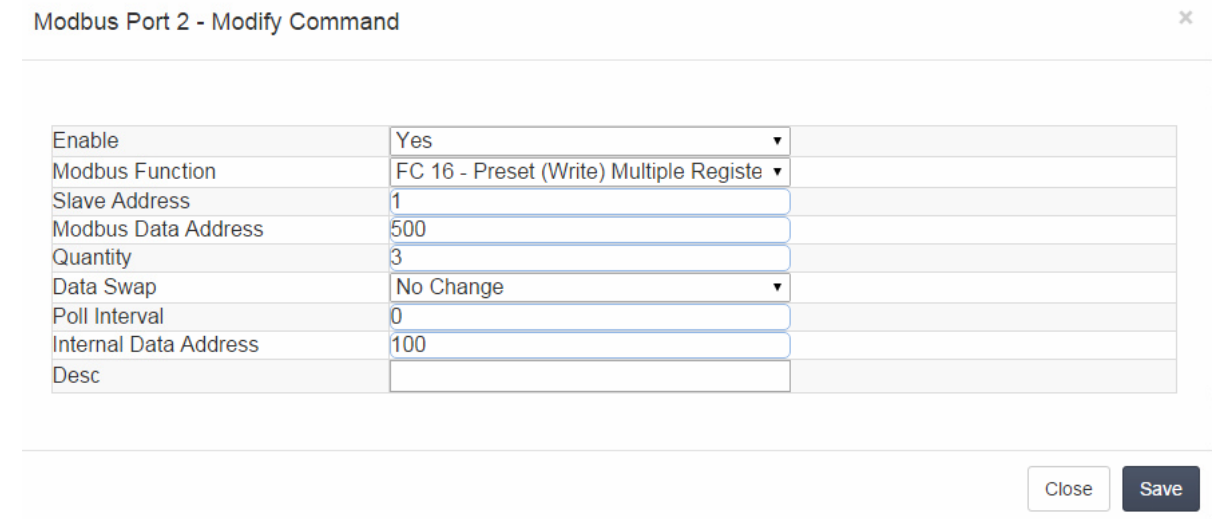


设置模块串行端口 Prot2 的配置，模块作为 MODBUS RTU 主站如下图。

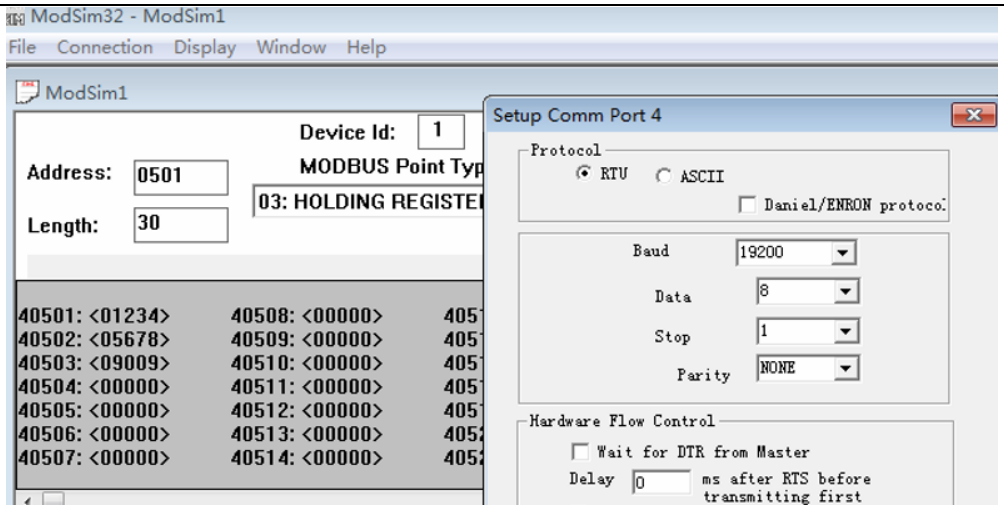


然后在 Modbus 主站命令里面配置命令 Commands.

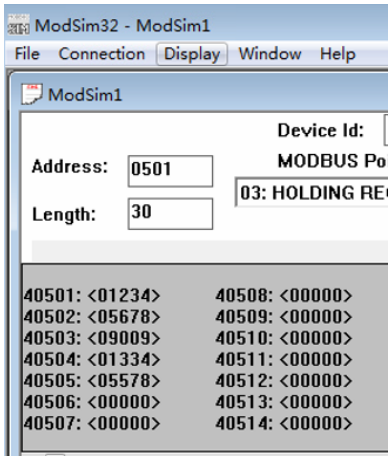
命令含义：把模块内部数据寄存器地址 100-102 的 3 个 INT 数据写入到 1 号 Modbus 从站的地址区 40501-40503 里面。



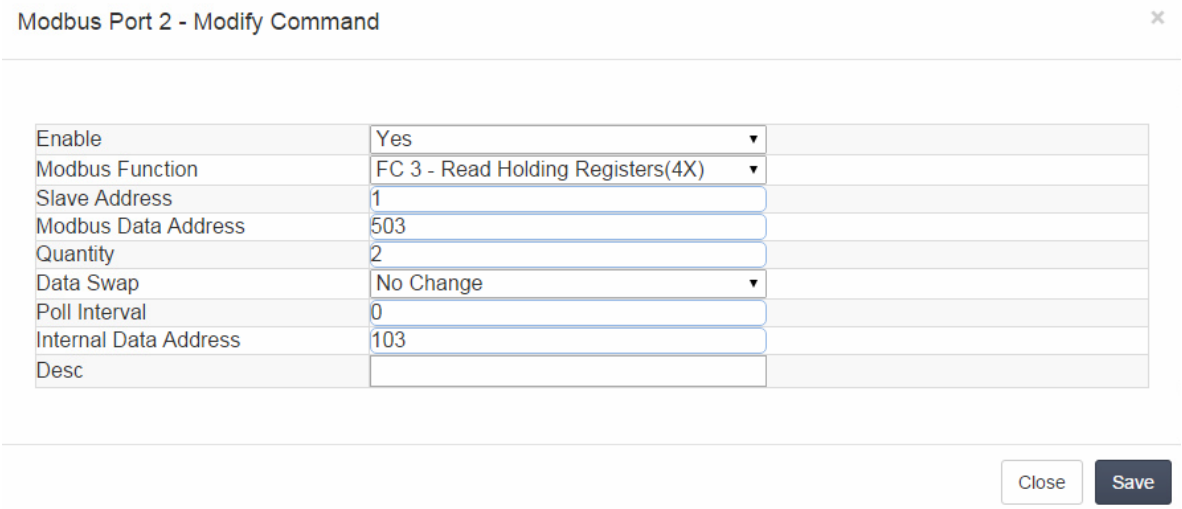
采用 MODSIM32 的 来仿真 Modbus RTU 从站，如下图可见，从站的地址区 40501-40503 里面写入了，模块读取自西门子 PLC 中 DB2 数据块里面的 3 个 INT 数据（地址 0-5 的字节数据）



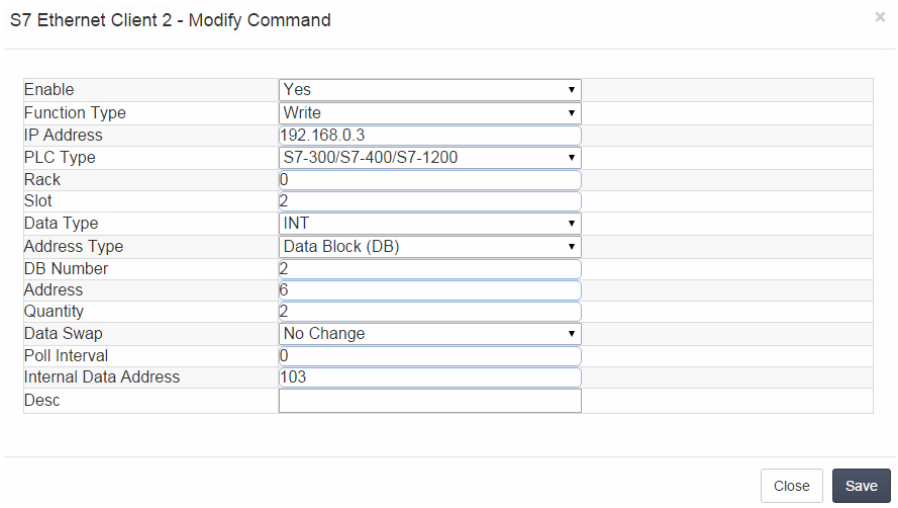
MODSIM32 软件，仿真 MODBUS RTU 从站。然后在从站地址 40504 和 40505 写一些数值如下图。



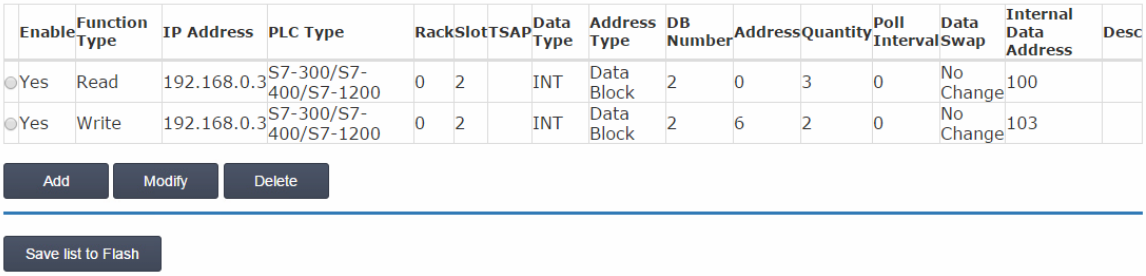
同时，我们在模块的 Modbus RUT 主站的命令区，再添加一条读指令，命令含义：把 MODSIM32 中的 40504-40505 数值读到模块内部数据库 103-104 里面。



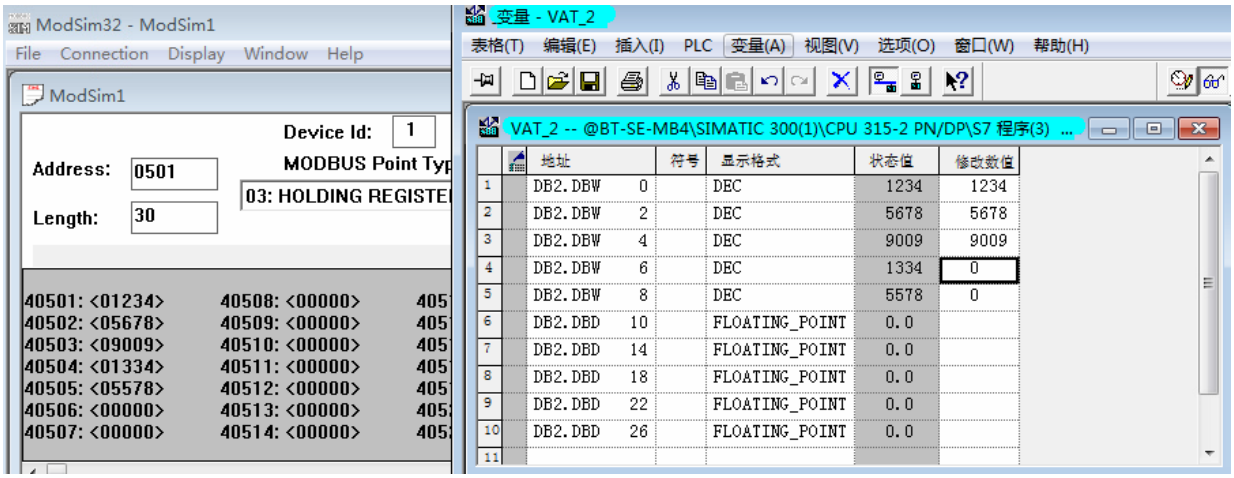
之后返回 S7 以太网主站一侧，到再添加一条 S7 以太网写指令，指令解释如下，把模块第 103-104 寄存器中的 2 个 INT 数据，写给 IP 地址为 192.168.0.3 的西门子 S7-300 系列控制器中，写入到 DB2 数据块里面的字节地址 6-9 的寄存器中.



点击 Save list to Flash 保存重启，如下为本案例中配置的读和写指令。



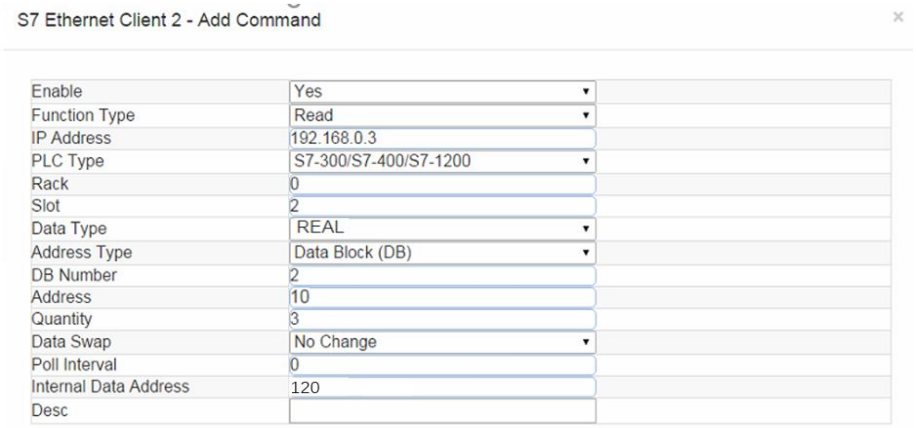
可见下图中，S7-300 PLC 相应的地址区收到了模块从 MODBUS 从站中采集到的数据。



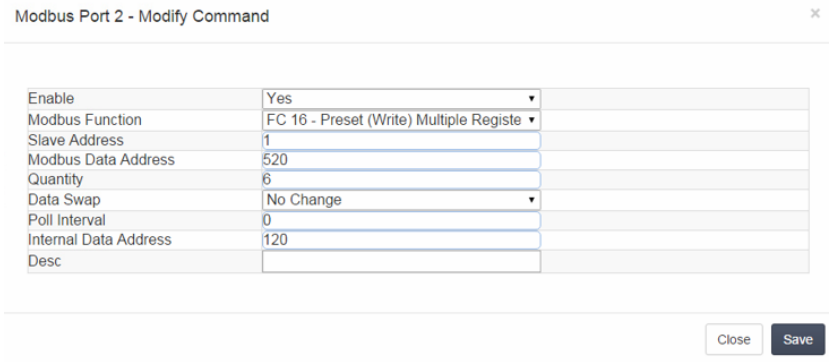
浮点数的读写操作

在西门子 PLC 的 DB2 中录入一些浮点数，注意 1 个浮点数为 4 个字节，2 个字。

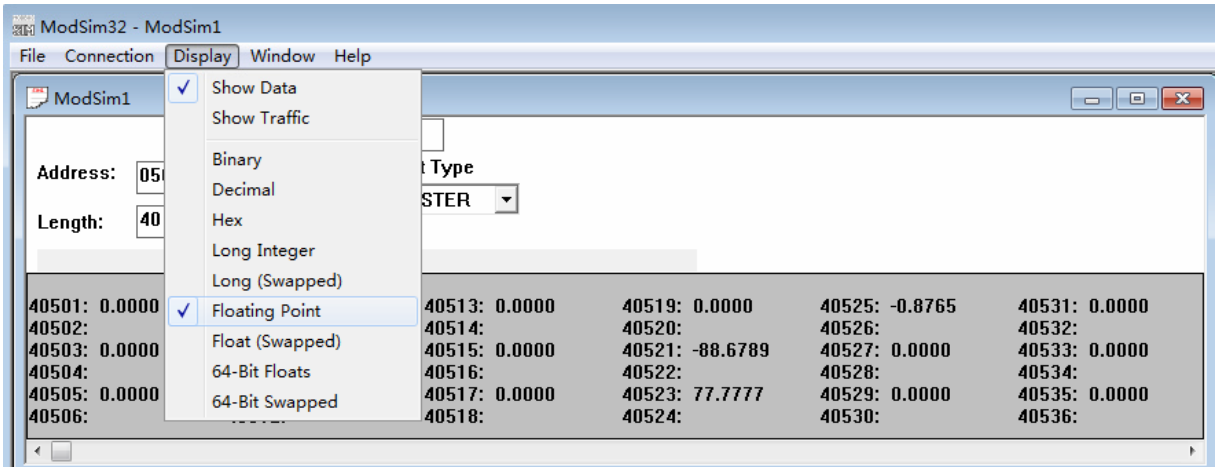
模块中配置西门子 S7 以太网一侧的读指令。指令解释如下，把 IP 地址为 192.168.0.3 的西门子 S7-300 系列的控制器中的 DB2 数据块里面的 3 个 REAL 数据（字节地址 10-21），读到模块第 120-125 寄存器里面.1 个浮点数占网模块内部 2 个寄存器。



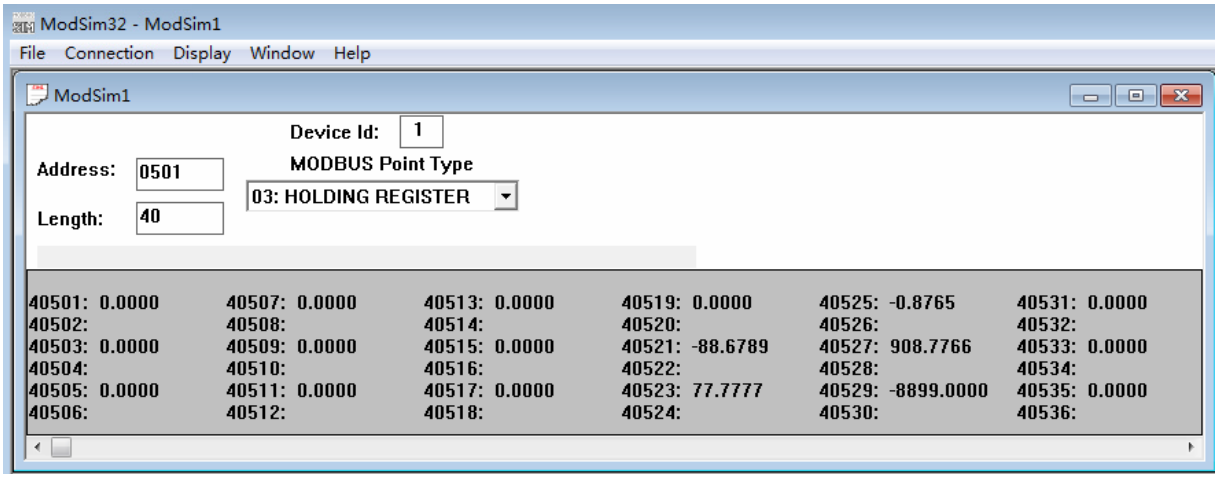
同时在模块的 Modbus 主站一侧，配置 MODBUS 写指令，将内部寄存器地址 120 开始的连续 6 个字（3 个浮点数），写入 1 号从站地址 40521-40526 中



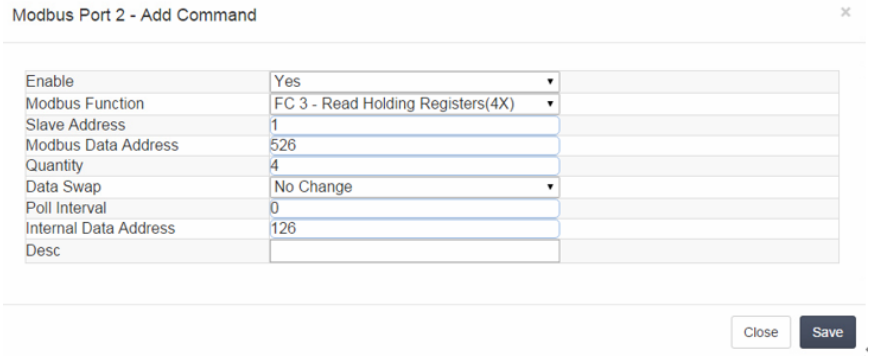
保存并重启网关。如下图，Modsim 模拟 Modbus 从站中正确地址接收到了写入的西门子 PLC 的数据。



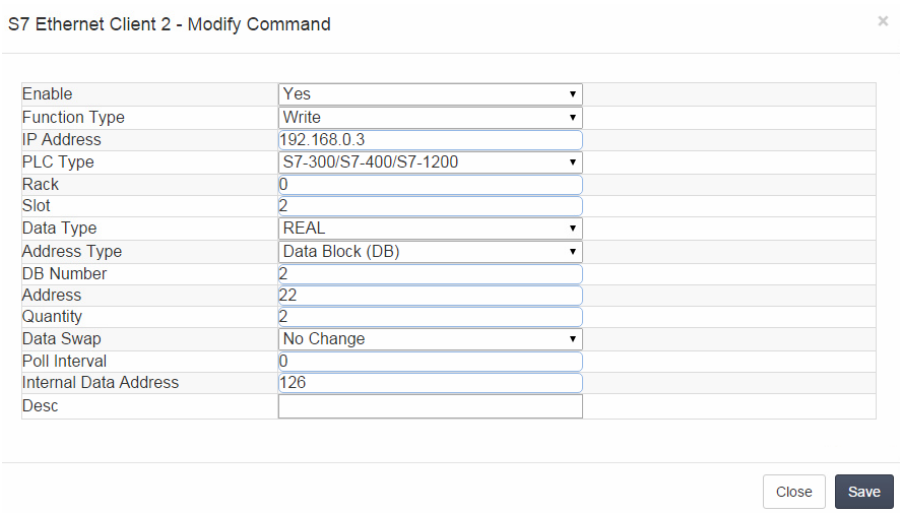
之后我们在 ModSIM 的地址区 40527-40530 中录入 2 个浮点数。



同时，回到模块的 Modbus RTU 主站一侧，增加一条读指令，含义为读取 1 号 modbus 从站的 40527-40530 的 4 个字到模块内部寄存器地址 126-129 中去。



之后在 S7 以太网一侧，添加一条写指令，将模块内部寄存器地址 126-129 中的 4 个字数据（2 个 REAL 数据），写给到 IP 地址为 192.168.0.3 的 S7-300 中，写入到 DB2 的字节地址 22-30.



返回到西门子 PLC 中，可以看到 DB2 中字节地址 22-30 接收到了，来自 Modbus 从站的两个浮点数。

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