

BT-EN-MB2-B

快速启动手册

BEACON GLOBAL TECHNOLOGY

目 录

BT-EN-MB2 简介	2
模块初始配置	2
配置模块做 EtherNet/IP Server:	3
配置模块做 EtherNet/IP Client	9
配置模块做 Modbus RTU Master (主站)	15
Modbus 命令使能控制介绍	22
配置模块做 Modbus RTU Slave (从站)	24
Modbus RTU 诊断方式	27
举例 1. Modbus 从站设备和罗克韦尔 PLC 交换整型数数据	28
举例 2. Modbus 从站设备和罗克韦尔 PLC 交换布尔量数据	32
举例 3. Modbus 主站和罗克韦尔 PLC 交换数据	34
其他版本简介	39
联系我们	40

BT-EN-MB2 简介

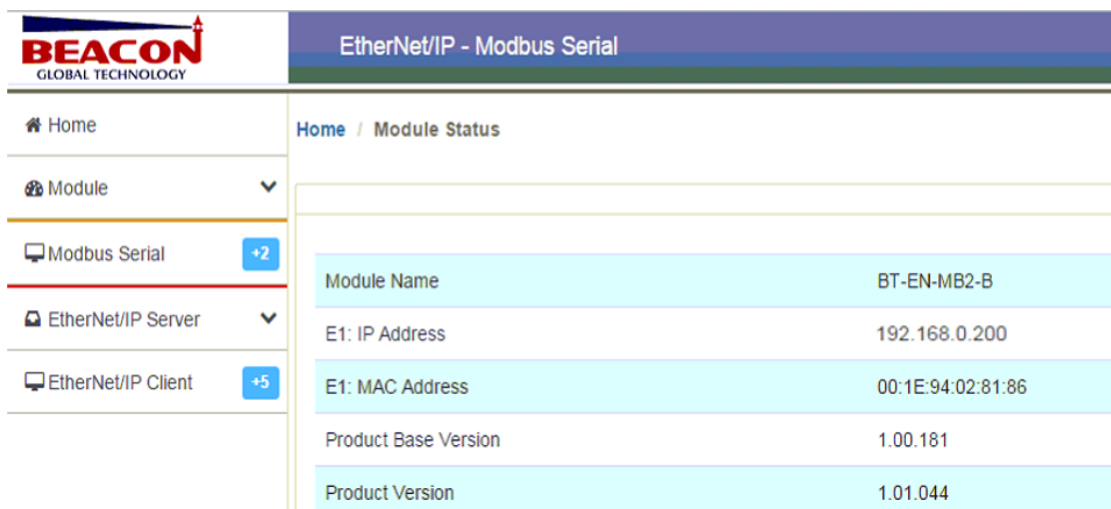
BT-EN-MB2系列分为基础型（-B）和领先型（-P），本手册中以基础型BT-EN-MB2-B进行举例。简介：该模块具有1个100M/10M的以太网端口（E1），E1可以用于作为5个EtherNet/IP协议的Client和Server，具有两个串行通讯接口S1和S2（RS-232/485/422），这两个串行接口都可以用于作为Modbus协议的Master或者Slave。

模块初始配置

模块上电后，OLED显示屏上会滚动显示IP地址，方便查找模块不同接口的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。

把本地电脑的IP地址与所连接的模块E1端口配置成相同的IP网段，例如本案例中本地电脑配置成和E1在同一网段下的，然后在GOOGLE Chrome浏览器的地址框里面输入E端口IP地址，点击回车键后，进入到BT-EN-MB2-B模块的配置页，如下图：



1. 在配置页面的右上角，点击 ，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。

2. 在配置页面的左侧导航条内，点击Module, 将打开如图所示的菜单。点击Backup/Restore。



3. 登录后看到导出配置文件 **Export Config** 和恢复配置文件

Ethernet Port 1	
IP Address	192.168.0.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1

Ethernet Port 2	
IP Address	192.168.1.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

Save

4. 查看模块IP地址，点击 **General Configuration**，修改模块的IP地址。

Home / Change Password

User Name: admin

Current Password:

New Password:

Confirm Password:

Save

5. 点击 **Change Password**，可以修改模块的登录密码。

6. 点击 **Set Date & Time** 可以设置模块的日期和时间。

Warning
Proceed with caution. It's important to set the correct date and time for the modules Time Date functions. Please refer to the user manual for additional information.

DateTime

Set Date and Time

7. 点击 **Reboot Module** 表示重启模块。

Home / Reboot

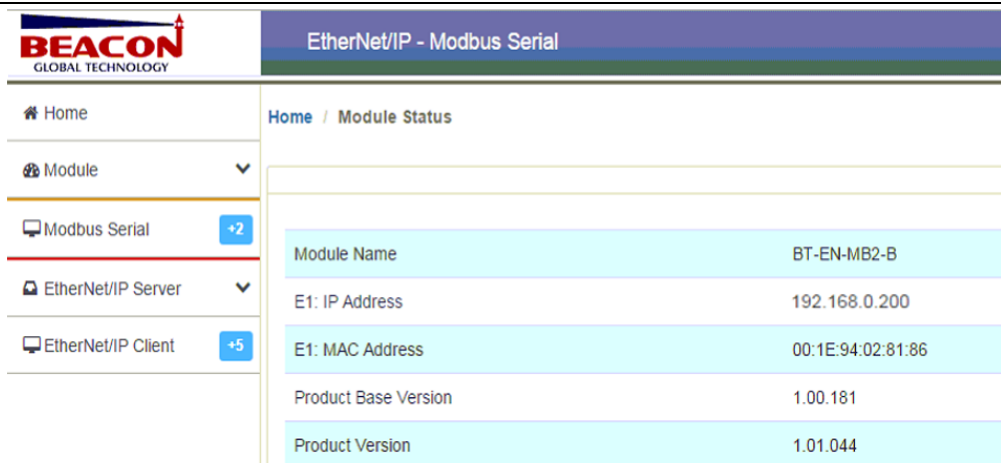
Warning
The module has to be rebooted due to any configuration changes. Note that the data communication will be temporarily interrupted if reboot.

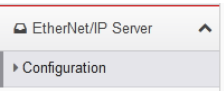
OK to reboot the module now?

OK

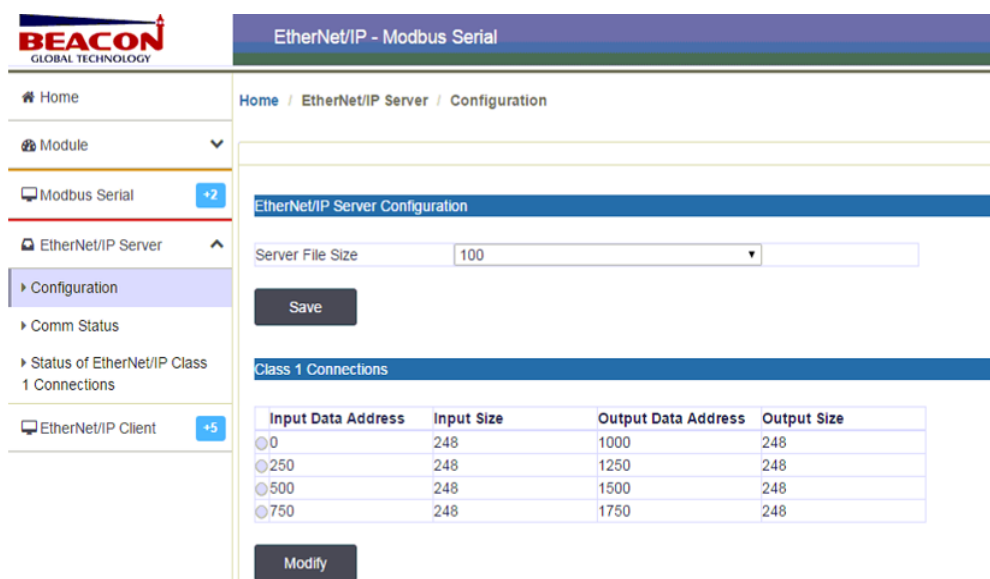
配置模块做 EtherNet/IP Server:

通过浏览器，登录模块主页面



在左侧菜单中，点击 ，查看 EtherNet/IP Server Configuration 的链接数，如下图。

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4组Class 1 Connections的链接，这4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。



上图可以看到，当前模块总共有2000个16位字的内部寄存器，模块做为EtherNet/IP Server时候，可以被多个罗克韦尔PLC同时访问。

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。

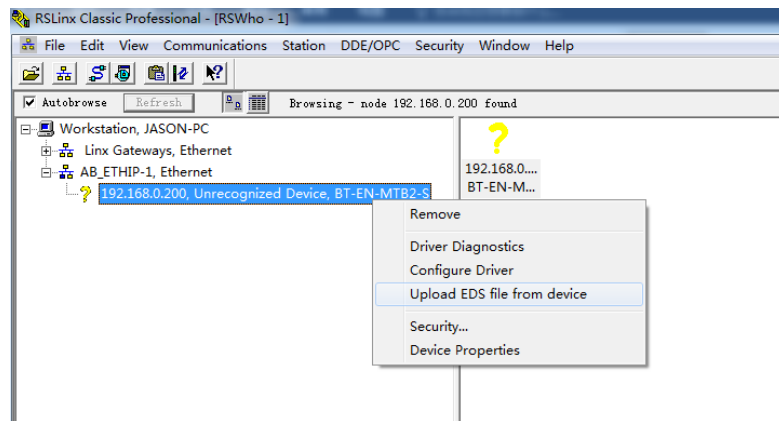
Output Data Address 表示罗克韦尔PLC写给模块数据（对PLC一侧为输出）的内部寄存器地址范围，1000是指模块内部第1000个寄存器，输出起始地址为1000,数量 248，表示PLC对模块的第一组输出数据，所占用的模块内部寄存器地址范围。

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。

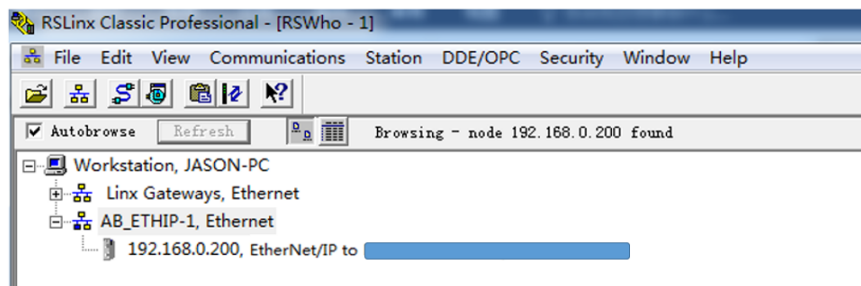
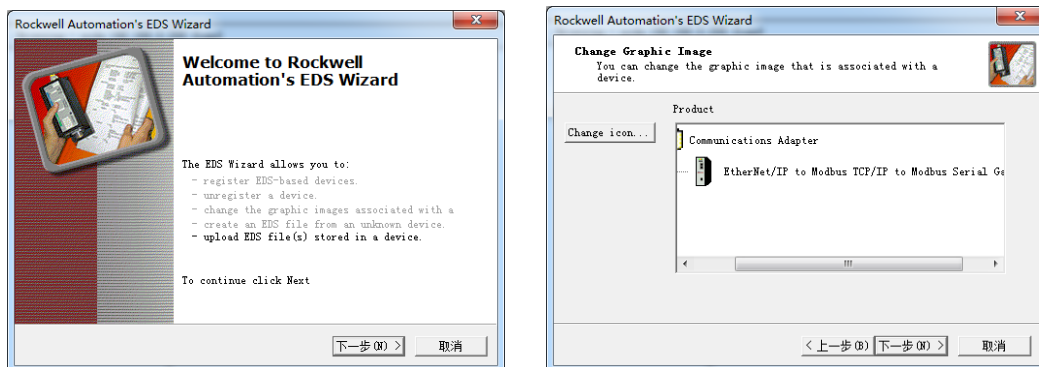
注：模块默认做EtherNet/IP从站，不需要任何设置。

如下步骤为在Logix5000配置软件中添加模块。

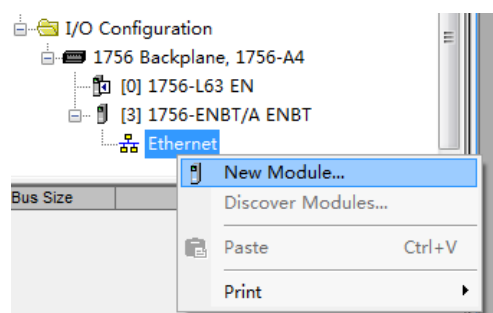
将网关E1端口和电脑，以及Logix PLC以太网接口相连接。在电脑中使用RSLinx扫描模块，然后在RSLogix5000中添加该模块的EDS文件，如下图：

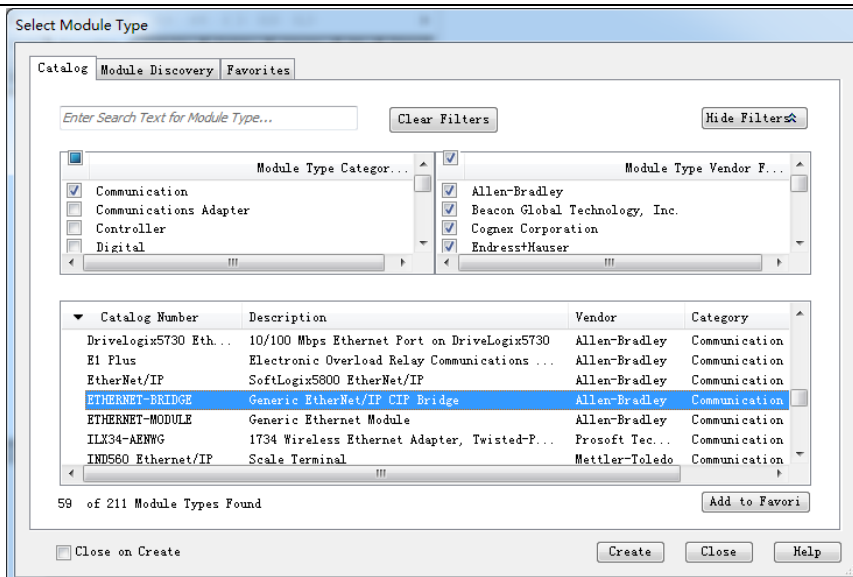


选择从设备上传 EDS 文件，如下图

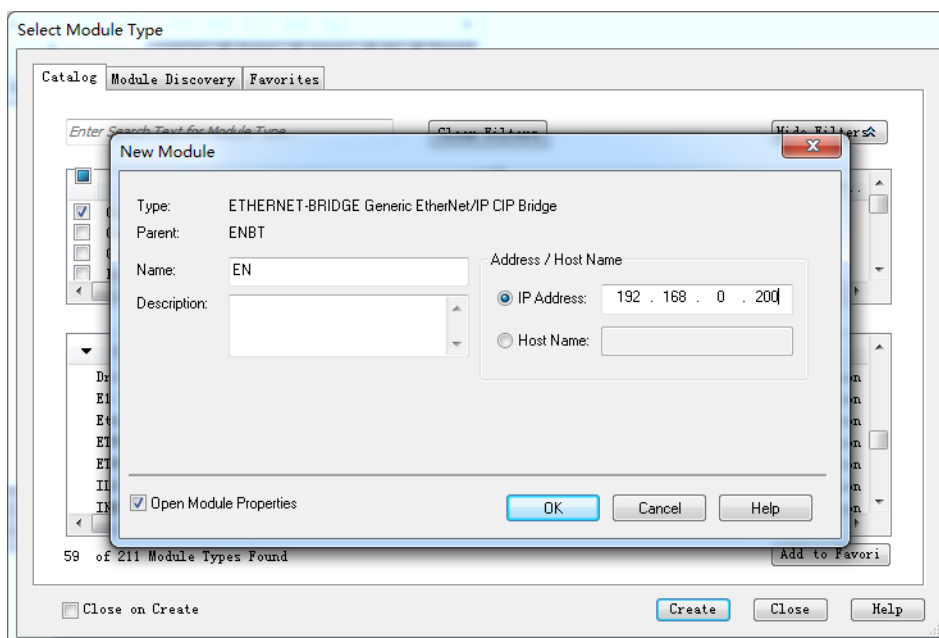


下一步通过添加“Generic EtherNet Bridge”完成 PLC 和模块的通讯，如下图：

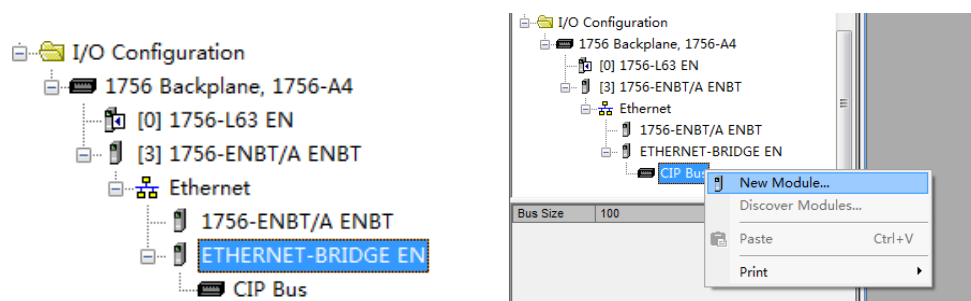


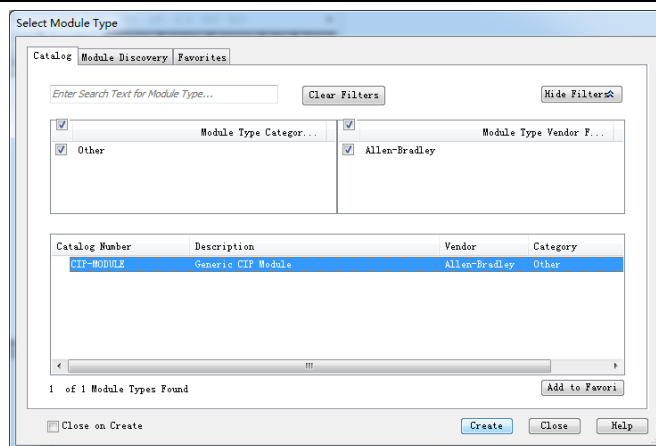


设定模块的 IP 地址，该地址为 E1 端口地址



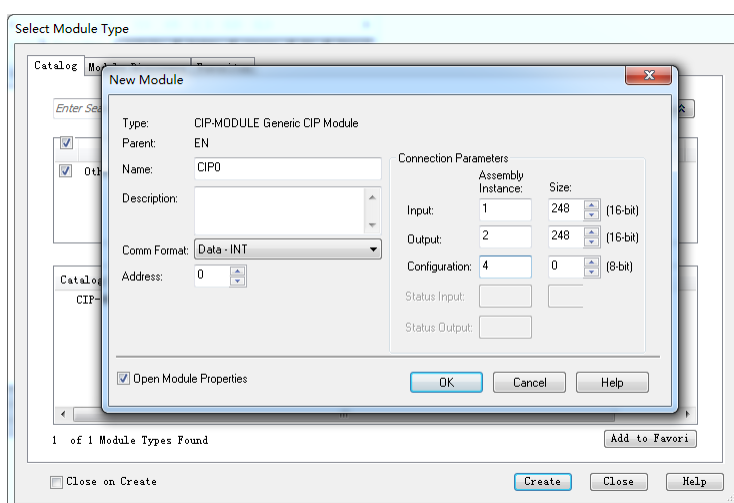
在 Generic EtherNet Bridge 下添加一个新模块，再添加一个新的 CIP-Connection.





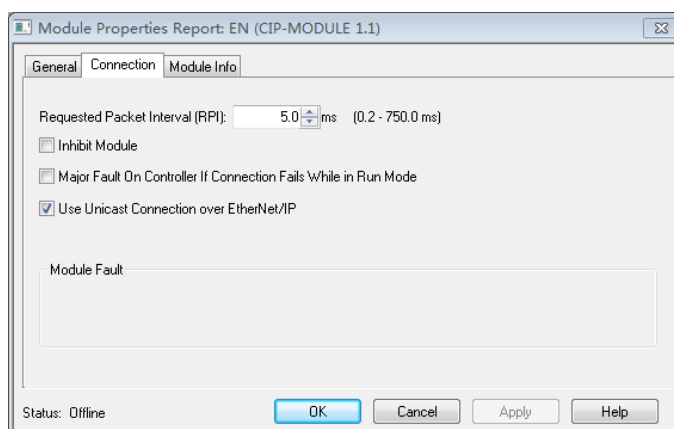
之后开始设定 PLC I/O connection 的参数，如下图：

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：



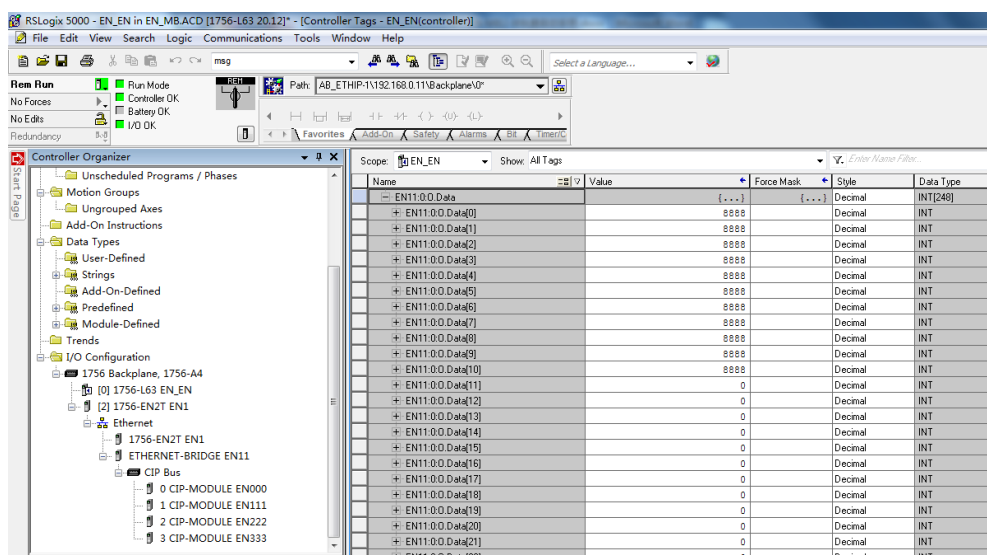
前文已经提到过，数据对应关系如下，从 AB 的 PLC 对模块 internal data base 进行读写。

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

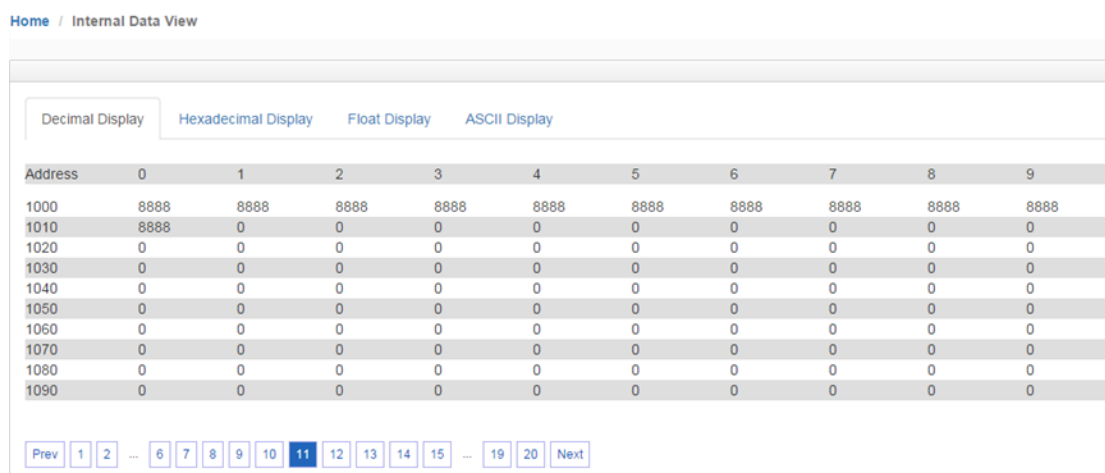
EN:1:I.Data[0]- EN:1:I.Data[247]对应模块内部寄存器 250-497 的地址 输入

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

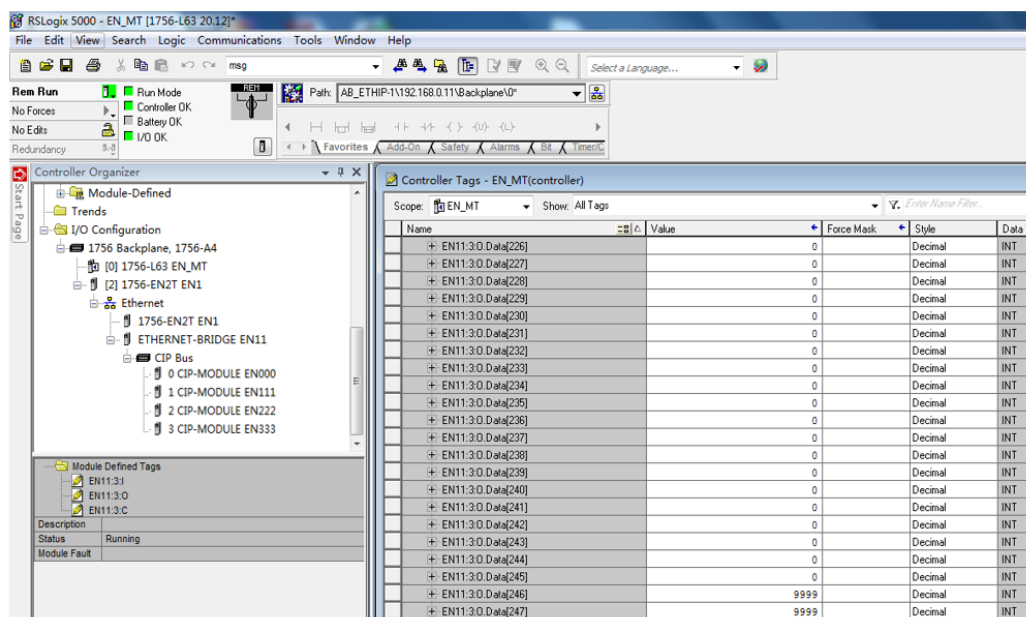


以此类推。如下图，在 RSLogix5000 第一个 CIP I/O 链接的输出标签的开头写一些数据。

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:

Home / Internal Data View

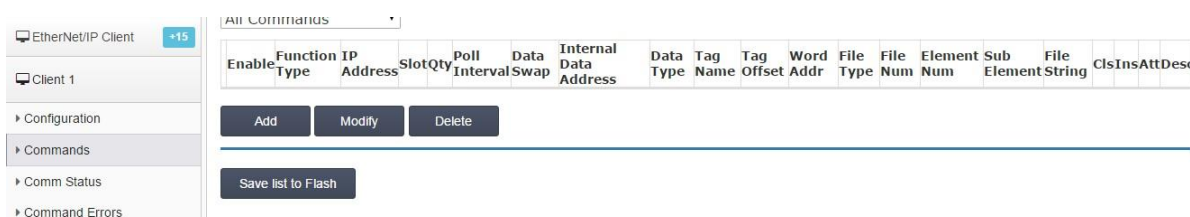
Decimal Display Hexadecimal Display Float Display ASCII Display

Address	0	1	2	3	4	5	6	7	8	9
1900	0	0	0	0	0	0	0	0	0	0
1910	0	0	0	0	0	0	0	0	0	0
1920	0	0	0	0	0	0	0	0	0	0
1930	0	0	0	0	0	0	0	0	0	0
1940	0	0	0	0	0	0	0	0	0	0
1950	0	0	0	0	0	0	0	0	0	0
1960	0	0	0	0	0	0	0	0	0	0
1970	0	0	0	0	0	0	0	0	0	0
1980	0	0	0	0	0	0	0	0	0	0
1990	0	0	0	0	0	0	9999	9999	0	0

Prev 1 2 ... 11 12 13 14 15 16 17 18 19 20 Next

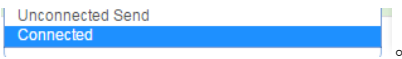
配置模块做 EtherNet/IP Client

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。

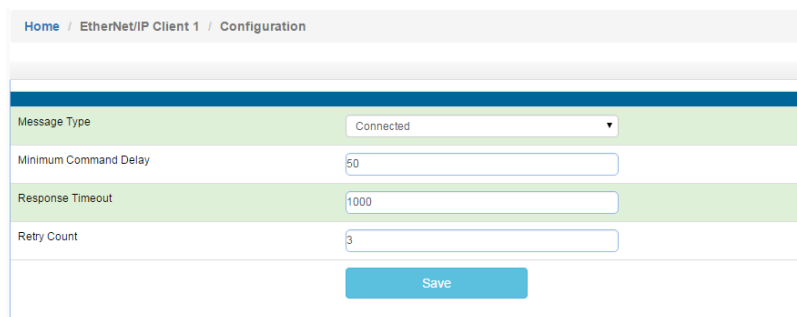


如上图，点击 EtherNet/IP Client ---Client1---Commands。

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 1756PLC, 因此选择 Connected。

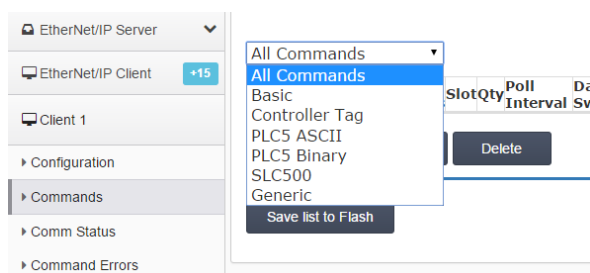
Minimum Command Delay: 每个 Client 执行指令的轮询时间, 单位 ms, 范围 0-65535

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。

EtherNet/IP Client 1 - Add Command

Controller Tag

Enable	Yes	使能，禁止，内部寄存器有变化后写
Function Type	CIP Data Table Write	功能码读或写
IP Address	1.1.1.1	要连接设备的IP地址
Slot	0	Micro800填-1,其他PLC根据RSLINX读取CPU实际位置填写
Quantity	1	读或者写的数据的数量
Poll Interval	0	指令轮询时间
Data Swap	No Change	数据高低位交换，字交换，字节交换，字和字节交换
Internal Data Address	0	模块内部寄存器，存放数据的起始地址。
Data Type	INT	数据类型，读命令INT无效，命令会跟随读取标签的类型
Tag Name	SampleTag	标签名，可以是单个标签或数组标签直接填写数组总名字
Tag Offset	0	数组标签偏移地址
Cmd Errors Mapping Enabled	No	命令错误状态位反馈开启
Cmd Errors Mapping Address	0	命令错误状态位反馈地址，填写模块内部寄存器任意位置
Desc		命令描述

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

Close Save

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。

EtherNet/IP Client 1 - Add Command

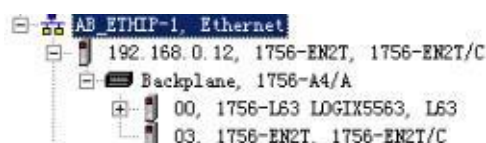
Controller Tag

Enable	Yes
Function Type	CIP Data Table Read
IP Address	192.168.0.12
Slot	0
Quantity	100
Poll Interval	0
Data Swap	No Change
Internal Data Address	1000
Data Type	INT
Tag Name	AA
Tag Offset	0
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	1200
Desc	

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

Close Save

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）



AA		INT[100]	Read/Write	☐	Decimal
----	--	----------	------------	--------------------------	---------

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。

Enable	Yes
Function Type	CIP Data Table Read
IP Address	192.168.0.12
Slot	0
Quantity	50
Poll Interval	0
Data Swap	No Change
Internal Data Address	1100
Data Type	REAL
Tag Name	BB
Tag Offset	0
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	1201
Desc	

Close Save

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。

Parameter Name	Value
Command Count	2
TNS	6354
Last Error Code	0
Number of Command Errors	0
Number of Requests Sent	1001
Number of Responses Received	1001
Number of Errors Received	0
Number of Errors Sent	0

Reset Counter
Auto Refresh 2 Second(s)

在 AA 和 BB 输入些数据:

Controller Tags - L63(controller)						
Scope: L63		Show: All Tags		Y. Enter Name Filter...		
Name	Value	Force Mask	Style	Data Type	Description	
AA	{...}	{...}	Decimal	INT[100]		
AA[0]	11		Decimal	INT		
AA[1]	11		Decimal	INT		
AA[2]	123		Decimal	INT		
AA[3]	123		Decimal	INT		

Controller Tags - L63(controller)						
Scope: L63		Show: All Tags		Y. Enter Name Filter...		
Name	Value	Force Mask	Style	Data Type	Description	
BB	{...}	{...}	Float	REAL[50]		
BB[0]	-888.99		Float	REAL		
BB[1]	0.0		Float	REAL		
BB[2]	0.0		Float	REAL		
BB[3]	77.22		Float	REAL		
BB[4]	0.0		Float	REAL		

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。

Home / Internal Data View

	0	1	2	3	4	5	6
1000	11	11	123	123	0	0	0
1010	0	0	0	0	0	0	0
1020	0	0	0	0	0	0	0
1030	0	0	0	0	0	0	0
1040	0	0	0	0	0	0	0
1050	0	0	0	0	0	0	0
1060	0	0	0	0	0	0	0
1070	0	0	0	0	0	0	0
1080	0	0	0	0	0	0	0
1090	0	0	0	0	0	0	0

Prev 1 2 ... 6 7 8 9 10 11 12 13 14 15 ... 32 33 Next

Home / Internal Data View

	0	1	2	3	4	5	6	7	8
1100	16220	-15266	0	0	0	0	28836	17050	0
1110	0	0	0	0	0	0	0	0	0
1120	0	0	0	0	0	0	0	0	0
1130	0	0	0	0	0	0	0	0	0
1140	0	0	0	0	0	0	0	0	0
1150	0	0	0	0	0	0	0	0	0
1160	0	0	0	0	0	0	0	0	0
1170	0	0	0	0	0	0	0	0	0
1180	0	0	0	0	0	0	0	0	0
1190	0	0	0	0	0	0	0	0	0

Prev 1 2 ... 7 8 9 10 11 12 13 14 15 16 ... 32 33 Next

可以看到内部寄存器 1200 和 1201 没有错误反馈：

Home / Internal Data View

	0	1	2	3	4	5
1200	0	0	0	0	0	0
1210	0	0	0	0	0	0
1220	0	0	0	0	0	0
1230	0	0	0	0	0	0
1240	0	0	0	0	0	0
1250	0	0	0	0	0	0
1260	0	0	0	0	0	0
1270	0	0	0	0	0	0
1280	0	0	0	0	0	0
1290	0	0	0	0	0	0

Prev 1 2 ... 8 9 10 11 12 13 14 15 16 17 ... 32 33 Next

如果我们在 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。

Home / EtherNet/IP Client 1 / Status

Parameter Name	Value
Command Count	2
TNS	15697
Last Error Code	4
Number of Command Errors	936
Number of Requests Sent	10344
Number of Responses Received	9408
Number of Errors Received	0
Number of Errors Sent	0

Reset Counter

☒ Auto Refresh [2] Second(s)

Home / Internal Data View

	Decimal Display	Hexadecimal Display	Float Display	ASCII Display
Address	0	1	2	3
1200	4	4	0	0
1210	0	0	0	0
1220	0	0	0	0
1230	0	0	0	0
1240	0	0	0	0
1250	0	0	0	0
1260	0	0	0	0
1270	0	0	0	0
1280	0	0	0	0
1290	0	0	0	0

Prev 1 2 ... 8 9 10 11 12 13 14 15 16 17 ... 32 33 Next

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.

Home / EtherNet/IP Client 1 / Command List

Generic

	Enable	Function Type	IP Address	Slot	Qty	Poll Interval	Data Swap	Internal Data Address	Cls Ins Att	Cmd Errors Mapping Enabled	Cmd Errors Mapping Address	Desc
1	Yes	Write Attribute Single	192.168.0.8	-1	1	0	No Change	1300	9 1 3	Yes	1400	
2	Yes	Write Attribute Single	192.168.0.8	-1	1	0	No Change	1301	9 2 3	Yes	1401	
3	Yes	Write Attribute Single	192.168.0.8	-1	1	0	No Change	1302	9 3 3	Yes	1402	

Add Modify Delete

Save list to Flash

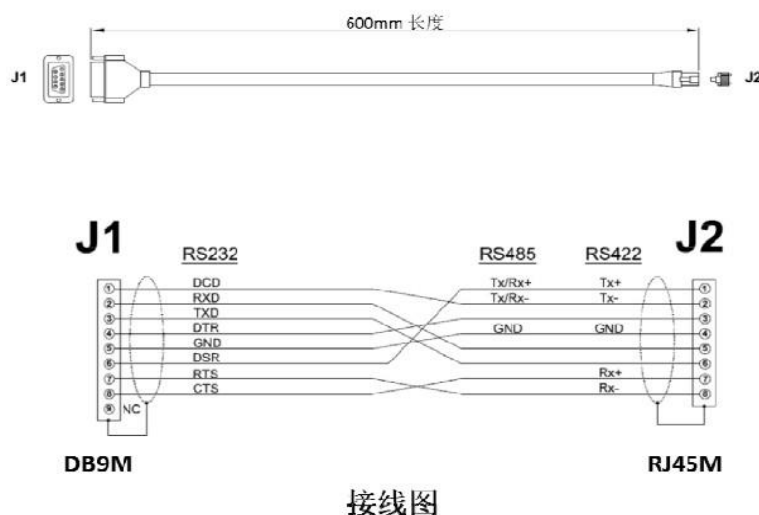
如上建立的3条指令，表示对IP地址为192.168.0.8的E300马达保护器3个输出继电器进行输出操作，如果内部寄存器1300，1301，1302值为1的时候，3个输出继电器会进行闭合动作，如果内部寄存器1300，1301，1302值为0的时候，3个输出继电器会进行分开动作，如果3条命令没有正确执行，内部寄存器1400，1401，1402会报一个非零值。注：模块作为EtherNet/IP Client可以支持的内容非常多，根据需要连接的设备的不同(Logix控制器，PowerFlex变频器，E300马达保护器，PowerMonitor电力仪表)，可以和我们联系，获取进一步的详细技术支持。联系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

配置模块做 Modbus RTU Master(主站)

MB指的通讯协议是MODBUS RTU，接线方式提供RS232/422/485三种可以选择。MB2代表2个MODBUS RTU接口，S1，S2 MODBUS RTU接口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，两个串口S1和S2可以连接62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。



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，如下图所示：

Port	On	端口使能
Mode	RS485	接线方式
Type	Master	端口主站/从站
Protocol	RTU	端口协议
Baud Rate	19200	端口波特率
Parity	None	奇偶效验位
Data Bits	8	数据位
Stop Bits	1	停止位
Response Timeout	1000	从站的响应时间
Retry Count	3	重试次数
Minimum Command Delay	0	最小命令延时
Command Trigger Address	-1	命令触发地址

None

Odd

Even

无效验
奇效验

Save

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。

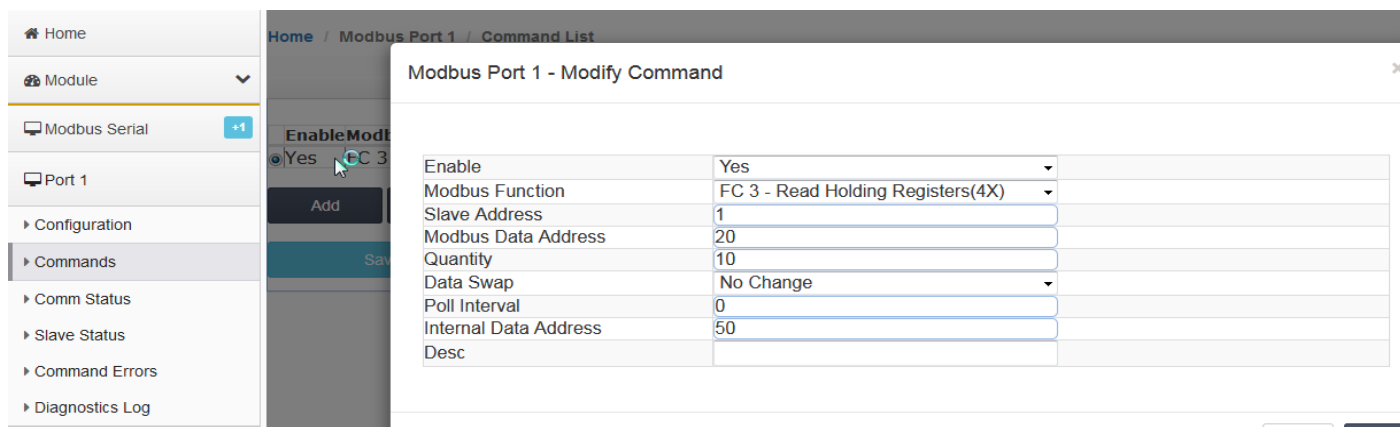
Enable	Yes
Modbus Function	FC 16 - Preset (Write) Multiple Register
Slave Address	1
Modbus Data Address	50
Quantity	20
Data Swap	No Change
Poll Interval	0
Internal Data Address	2000
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2051
Desc	

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，

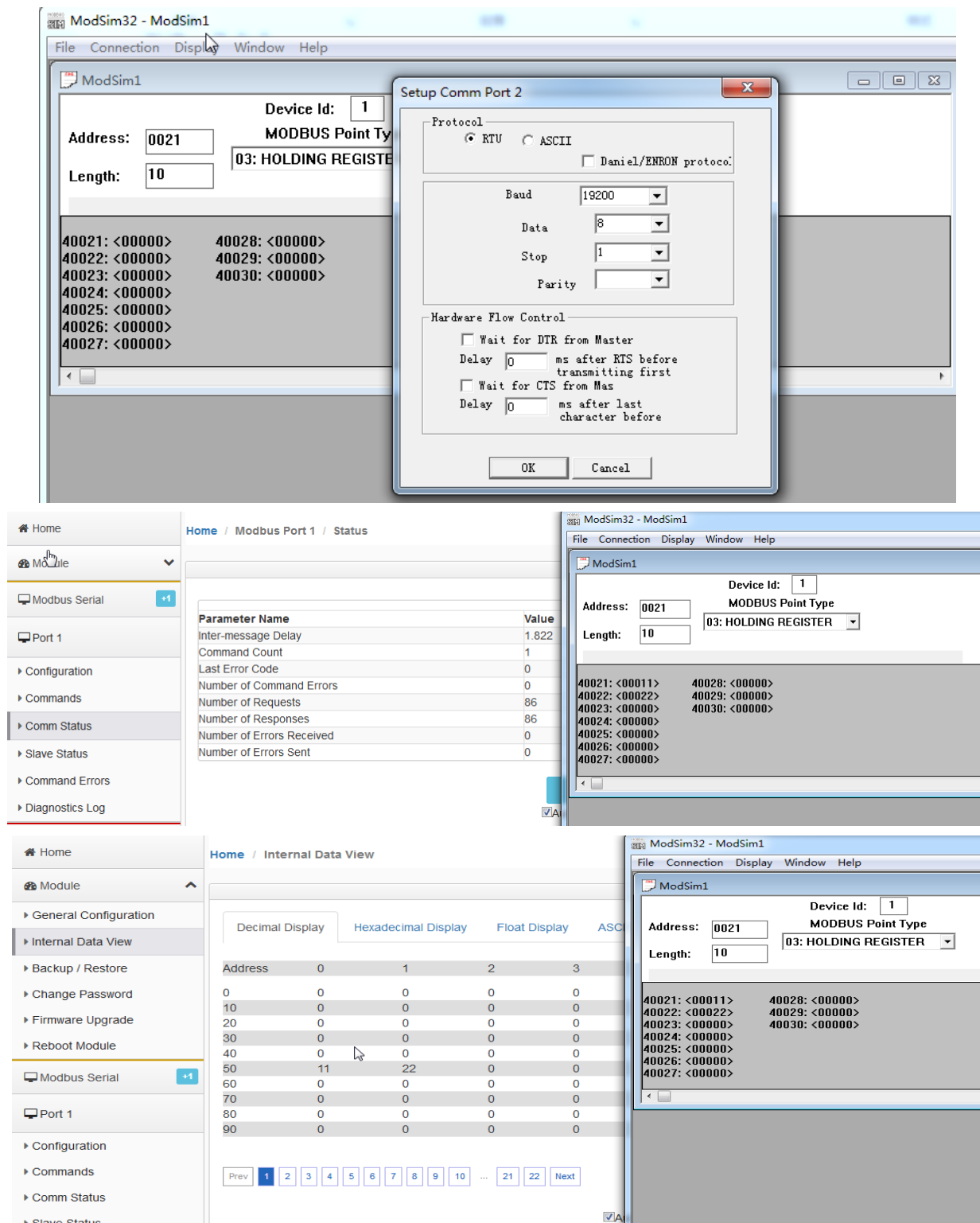


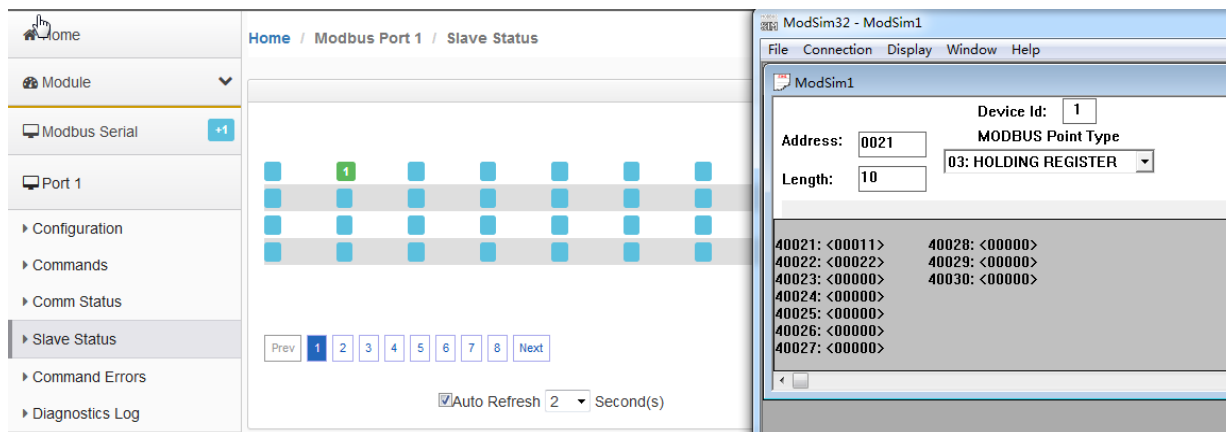
命令含义：把 MODBUS RTU 从站的 40021-40030 这 10 个 16 位的数值读到内部数据库 50-59 里面。

配置完，点 SAVE，然后关闭这个命令，再点击 SAVE，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。





Modbus Port 1 - Modify Command

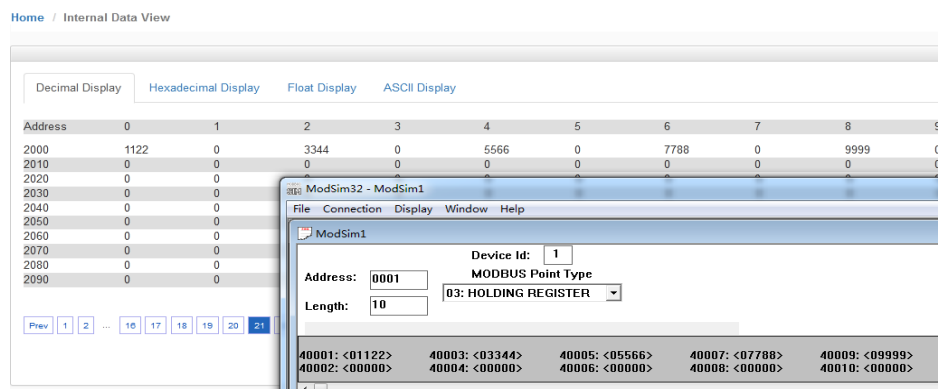
Enable	Yes	使能，禁止，内部寄存器有变化后写
Modbus Function	FC 3 - Read Holding Registers(4X)	Modbus 功能码FC1,FC2,FC3,FC4,FC5,FC6,FC15,FC16
Slave Address	1	从站地址
Modbus Data Address	0	从站读写数据Modbus起始位
Quantity	10	读或者写的数据的数量
Data Swap	No Change	数据高低位交换，字交换，字节交换，字和字节交换
Poll Interval	0	命令轮询时间
Internal Data Address	2000	模块内部寄存器，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

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

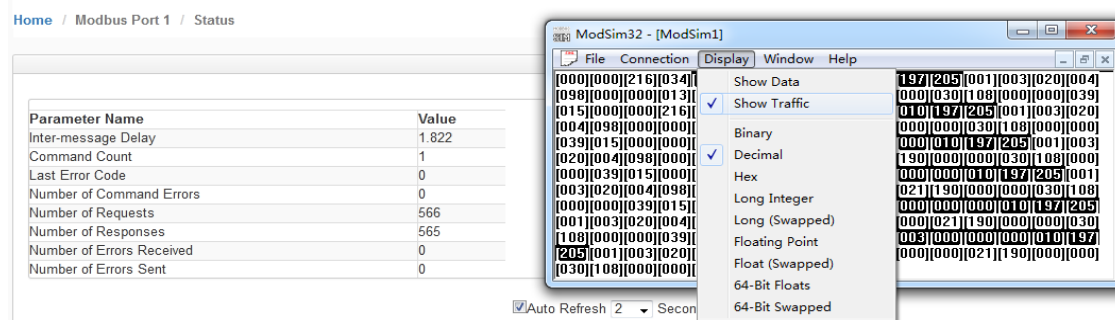
Cmd Errors Mapping Enabled表示命令错误是否映射，选择YES表示使用，选择NO，表示不使用；

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。

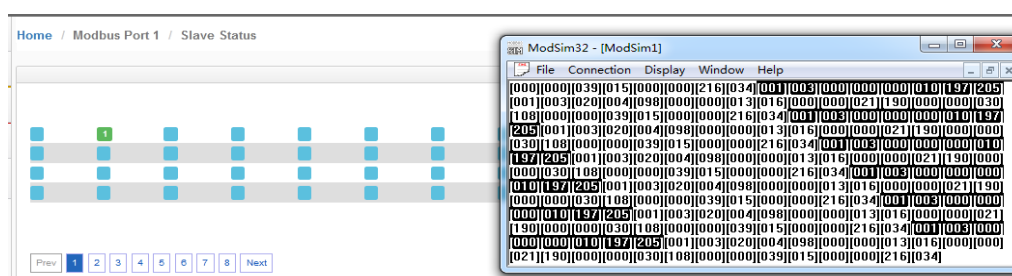


通过查看从站状态可以直接看到从站的状态，1-31路都可以直观看到：

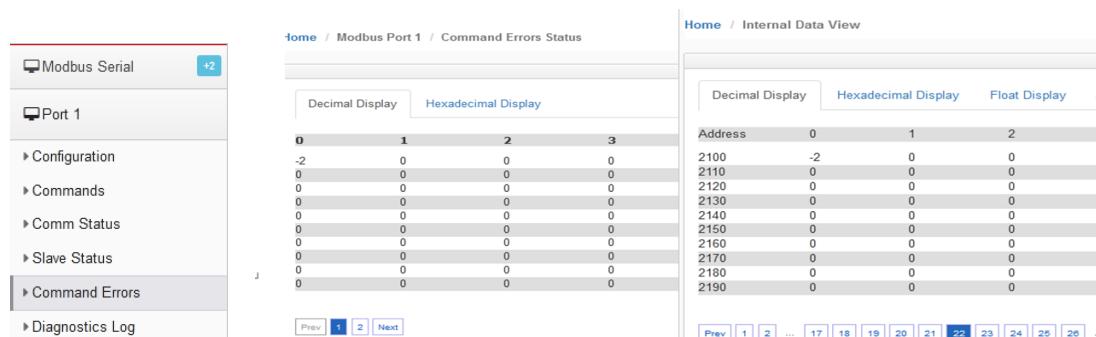
绿色表示线路数据通讯报文都正常；

红色表示线路数据通讯报文都不对；

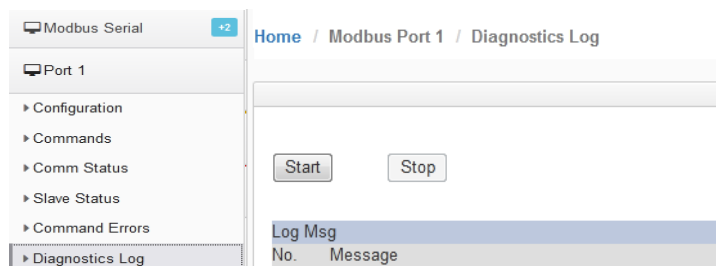
绿色和红色闪烁表示线路正常，数据通讯报文不正常。



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。

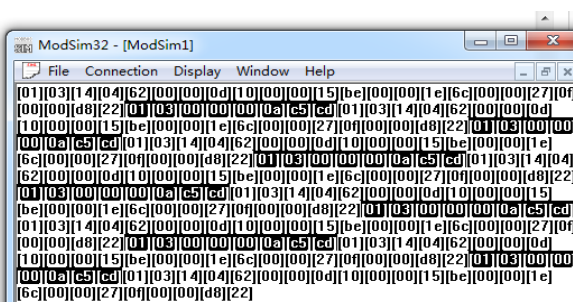


下图为主站发送和接收的报文以十六进制格式显示，Modsim32也可以从十进制报文切换到十六进制报文显示：


```

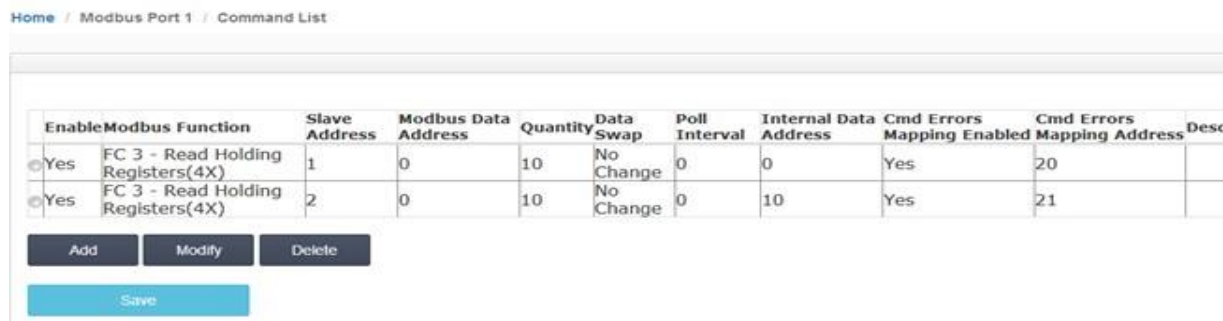
693 00:02:14.003 >> 01 03 00 00 00 0A C5 CD
694 00:02:14.105 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
695 00:02:14.309 >> 01 03 00 00 00 0A C5 CD
696 00:02:14.432 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
697 00:02:14.637 >> 01 03 00 00 00 0A C5 CD
698 00:02:14.739 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
699 00:02:15.944 >> 01 03 00 00 00 0A C5 CD
700 00:02:15.046 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
701 00:02:15.250 >> 01 03 00 00 00 0A C5 CD
702 00:02:15.353 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
703 00:02:15.557 >> 01 03 00 00 00 0A C5 CD
704 00:02:15.680 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
705 00:02:15.885 >> 01 03 00 00 00 0A C5 CD
706 00:02:16.007 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22
707 00:02:16.212 >> 01 03 00 00 00 0A C5 CD
708 00:02:16.315 << 01 03 14 04 62 00 00 0D 10 00 00 15 BE 00 00 1E 6C 00 00 27 0F 00 00 D8 22

```



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。

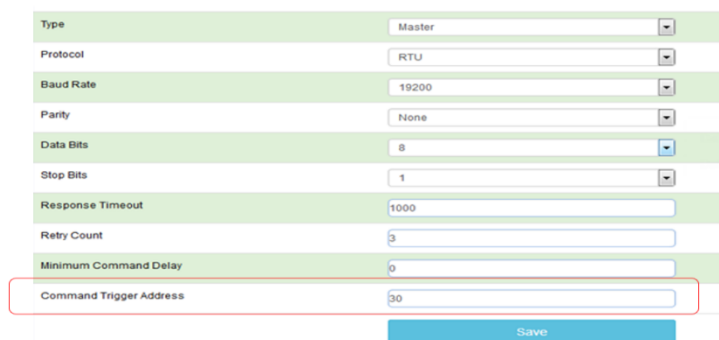


上图中建立两条指令：

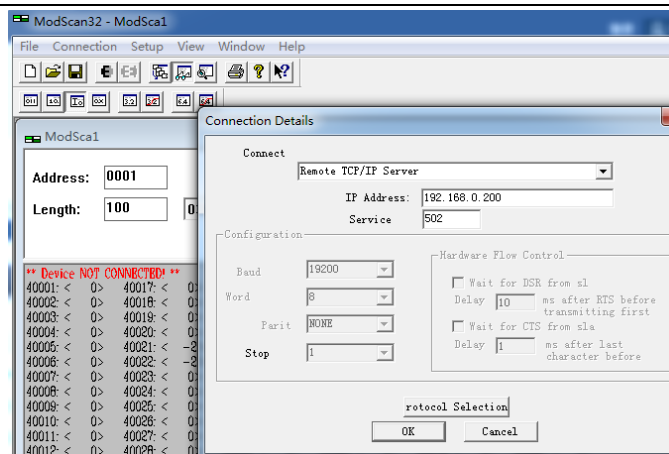
1- 读1号从站的40001-40010到内部寄存器0-9，错误状态放在了内部寄存器20。

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。

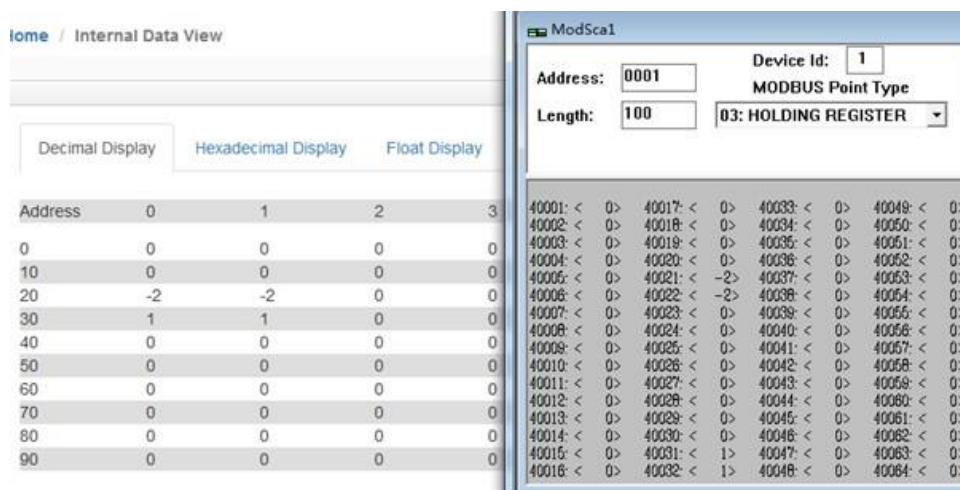
3- 使能命令触发地址，在模块Modbus主站端口配置页面中，Command Trigger Address设置成30，如下图，表示使用模块内部起始地址为30的寄存器作为触发条件。然后保存，重启生效。



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。

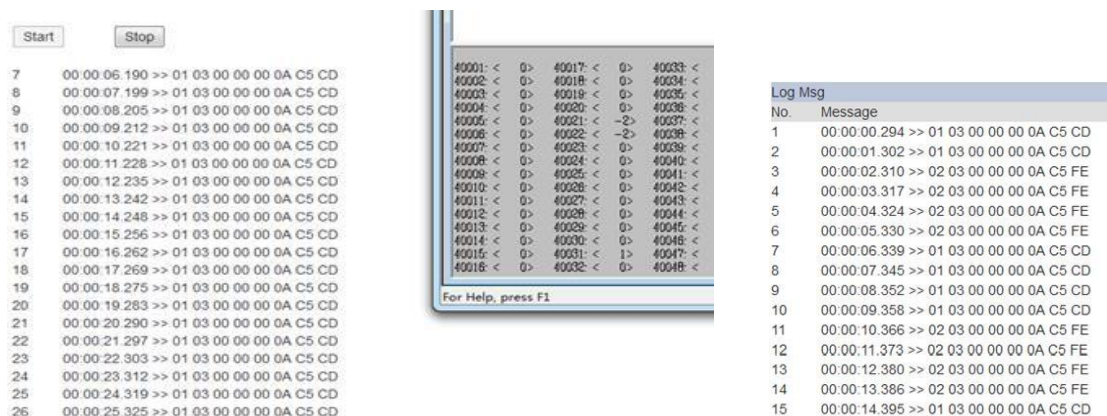
重发次数，可以在端口配置中进行修改（如下图）：

Retry Count

3

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，当其中一个命令反馈回来出现非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 Slave（从站）

点击Port1 里面的 Configuration 显示S1端口配置的页面：

Home / Modbus Port 1 / Configuration	
Port	On
Mode	RS485
Type	Slave
Protocol	RTU
Baud Rate	19200
Parity	None
Data Bits	8
Stop Bits	1
Slave ID	1
Minimum Response Delay	1
Holding Register Offset	0

点击Port1里面的Configuration显示S1端口配置的页面：

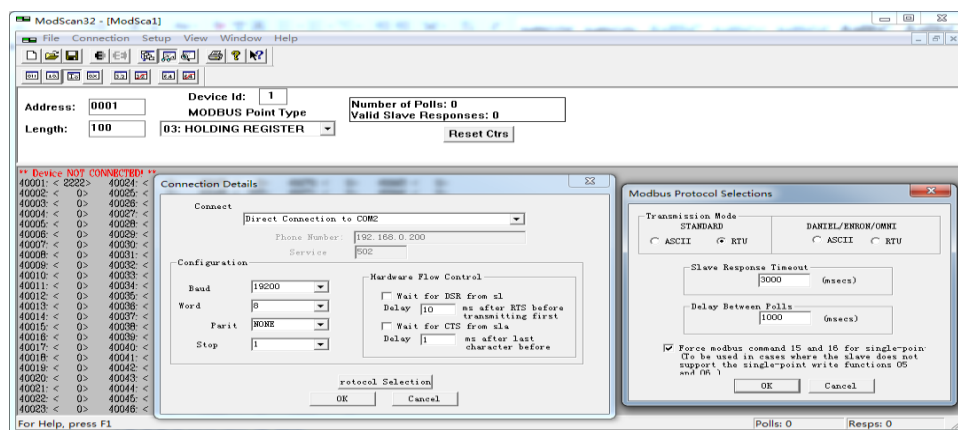
注意事项：S1或者S2作为Modbus从站，只需要配置端口参数，无需配置端口命令。S1和S2共用模块内部数据区。

如下图为设置模块的Modbus从站端口参数：

Port	On	端口使能
Mode	RS485	接线方式
Type	Slave	端口主站/从站
Protocol	RTU	端口协议
Baud Rate	19200	端口波特率
Parity	None	奇偶效验位
Data Bits	8	数据位
Stop Bits	1	停止位
Slave ID	1	从站地址
Minimum Response Delay	1	最小响应延时
Holding Register Offset	0	数据偏移
Word Input Offset	0	字输入偏移
Bit Input Offset	0	位输入偏移
Bit Output Offset	0	位输出偏移

Save

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

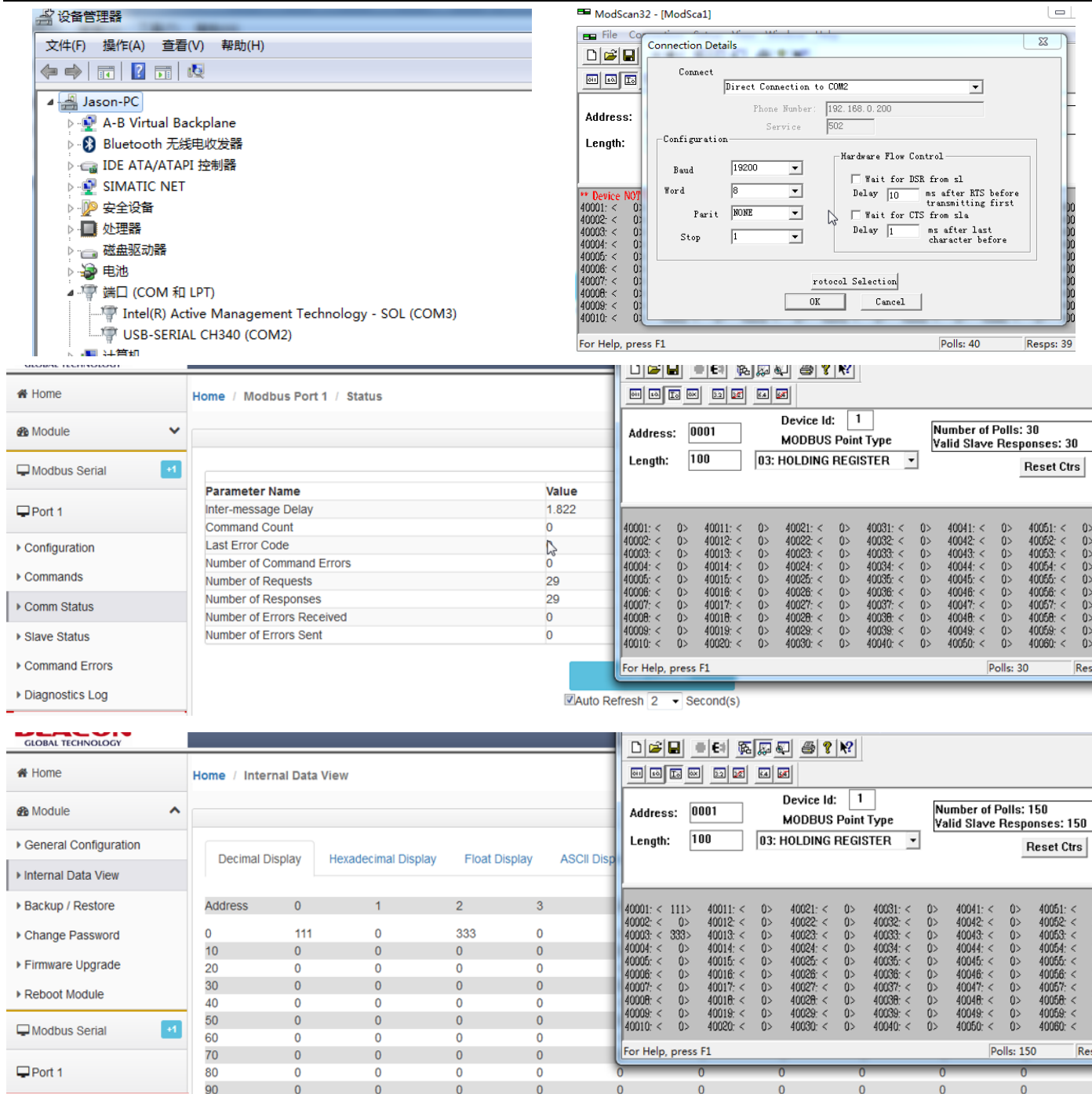


内部寄存器与Modbus数据对应关系：

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。

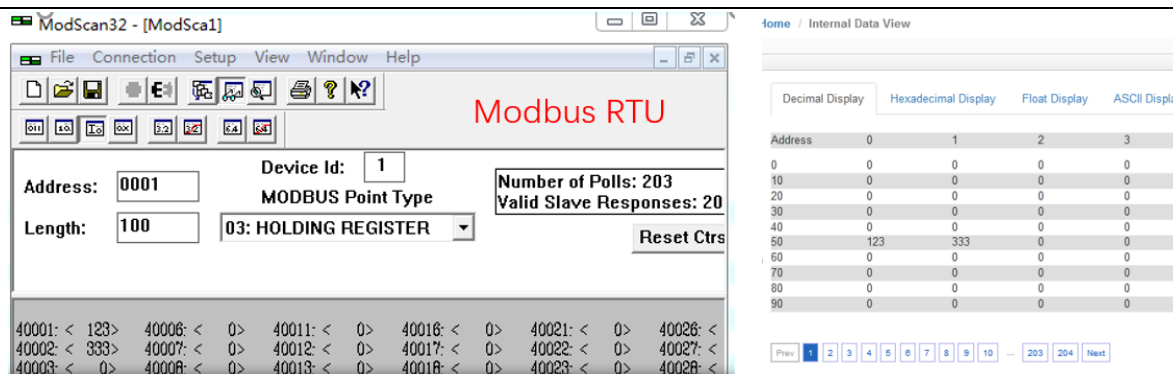


备注：40001 对应着内部寄存器 0，40100 对应着内部寄存器 99，以此类推。

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。

Minimum Response Delay	1000
Holding Register Offset	50
Word Input Offset	0

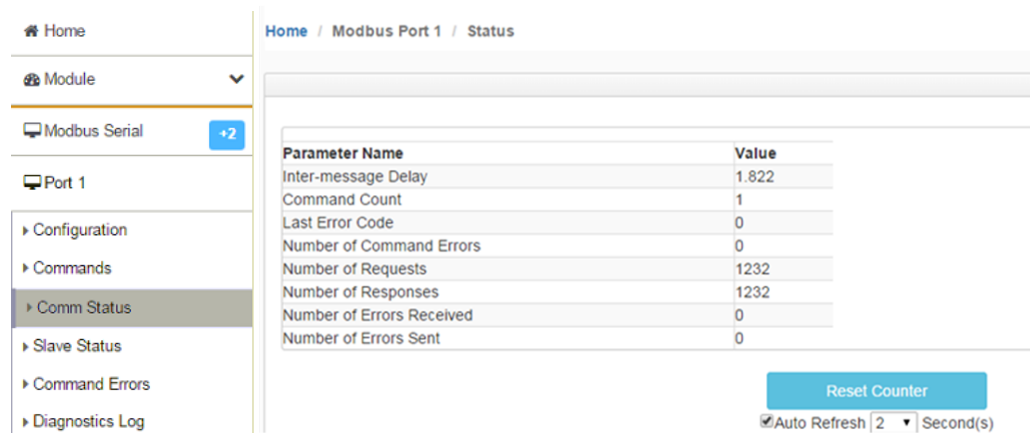


Word Input Offset使用方法：如果此处偏移量设置成50(如下图)，Modbus RTU主站一侧在3区对30001和30002输入两个数据，数据会直接向后偏移放到模块内部寄存器50-51里面，ModScan32仿真软件不能载入3区的数值，请以现场设备实际数据区域来填写。

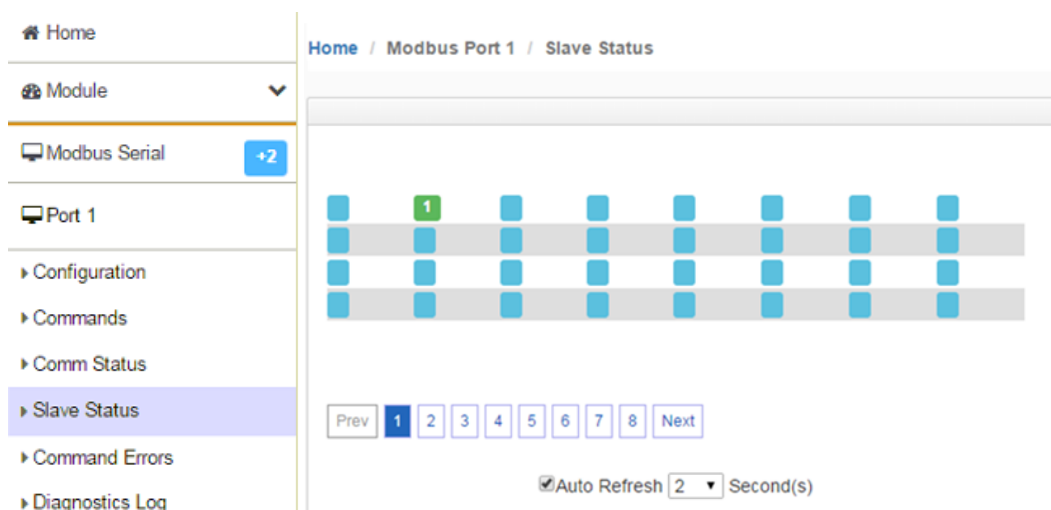
Minimum Response Delay	1000
Holding Register Offset	0
Word Input Offset	50

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。

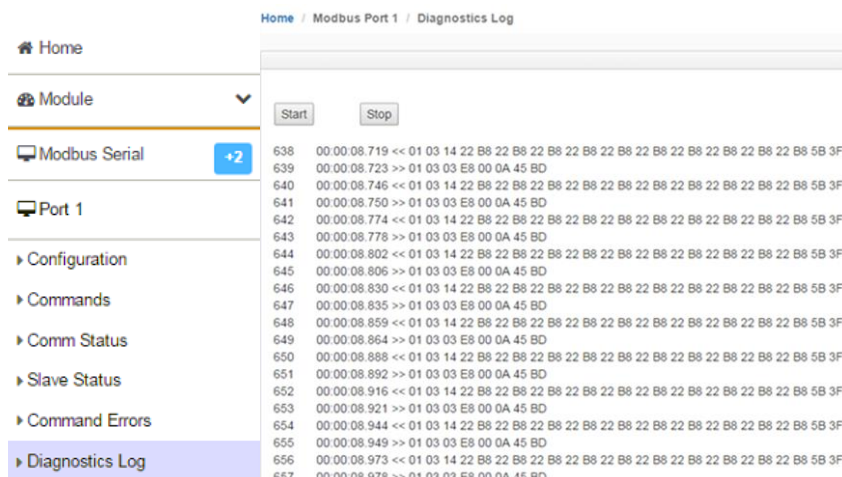


查看命令行是否有错误产生点击： ▶ Command Errors。

Decimal Display		Hexadecimal Display							
0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0

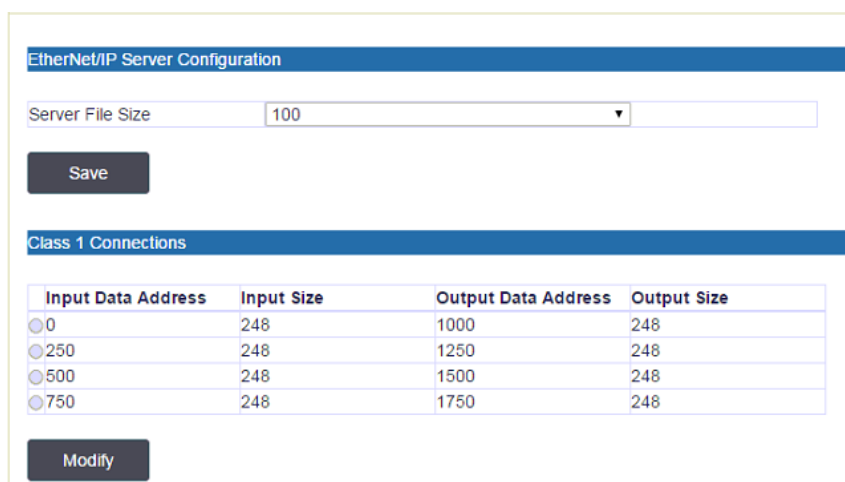
报文诊断功能：点击Diagnostics Log，再点击Start端口发送和接收报文的情况。

>>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. Modbus 从站设备和罗克韦尔 PLC 交换整型数数据

本案例中，模块配置作为Modbus RTU的master，同时配置作为EtherNet/IP的server



Logix 5000的输入输出标签和模块内部寄存器地址对应关系如下

PLC输入CIP标签组，EN:0:I.Data[0]– EN:0:I.Data[247]对应模块内部寄存器 0–247 的地址。

PLC输出CIP标签组，EN:0:O.Data[0]– EN:0:O.Data[247] 对应模块内部寄存器1500–1747 的地址。

以此类对，共计4组输入输出标签组：

如下图，我们在模块Modbus驱动一侧，使用功能码FC3读1号从站数据，从1号从站的40001至40010一共读10个字（INT类型），放入模块内部数据寄存器0–9，修改成以下配置。功点击Save，保存该指令的修改。

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	0	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	500	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

192.168.0.250/index.asp#

Home / Modbus Port 1 / Command List

Enable	Modbus Function	Slave Address	Modbus Data Address	Quantity	Data Swap	Poll Interval	Internal Data Address	Desc
☒ Yes	FC 3 - Read Holding Registers(4X)	1	0	10	No Change	0	0	

Add Modify Delete

Save

配置界面弹出成功（Successful），然后点击Close（关闭）。

点击下面的蓝色的Save保存命令写入模块缓存，点击OK。重启模块。模块倒计时19秒之后，新命令生效。

Modbus Serial ~2

Port 1

Configuration

Commands

Comm Status

Slave Status

Warning

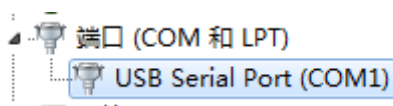
The module has to be rebooted due to any configuration changes. Note that the data communication will be temporarily interrupted if reboot.

OK to reboot the module now?

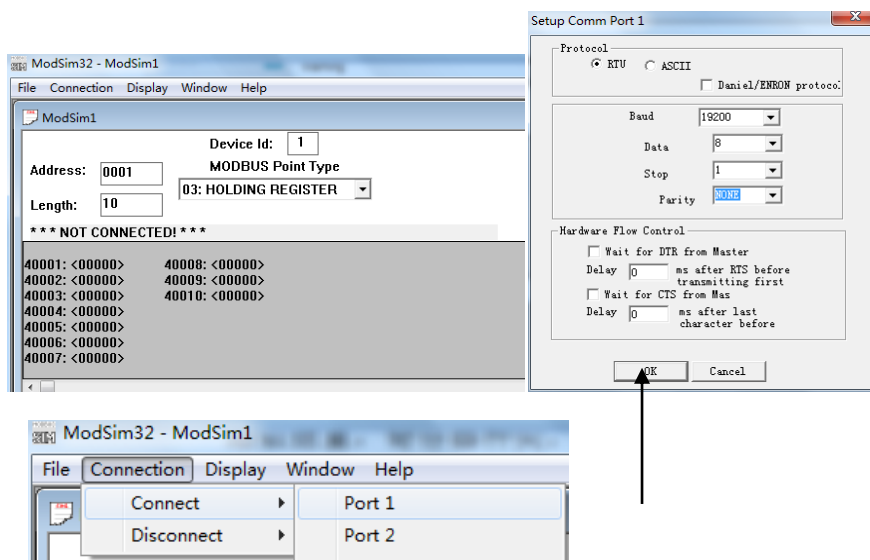
OK

仿真：

硬件连接：把USB转RS232电缆插到电脑上（如果现场电脑没有串行接口），中间经过RS232交叉转换头，再通过一根橙色的9针公头转RJ45水晶头，这三种接在一起，进行RS232接线方式的仿真工作。电脑会弹出装USB转232电缆的驱动，装好后，在电脑里面可以看到如下图，本文以及COM1说明：（注：此端口可以修改）

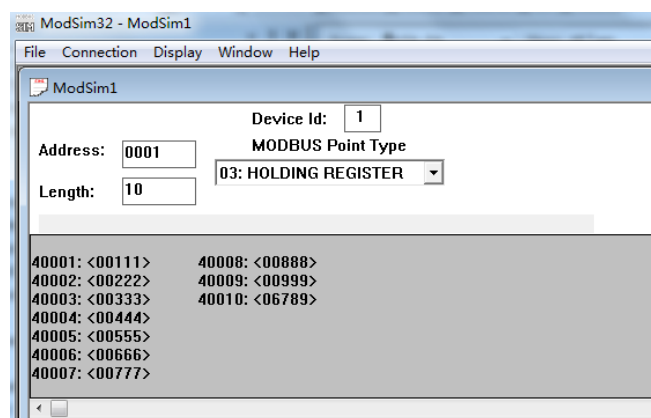


软件连接：打开ModSim32,可以仿真Modbus RTU 从站。设置从站地址，从站数据量，寄存器种类。如下图：选择连接Port 1 (USB转232串口在电脑里的配置)，然后把波特率，数据位，停止位，奇偶效验位，设置成与主站相同的参数。



点击上面的OK, 完成串口仿真连接。

在ModSim32仿真的从站里面输入数据

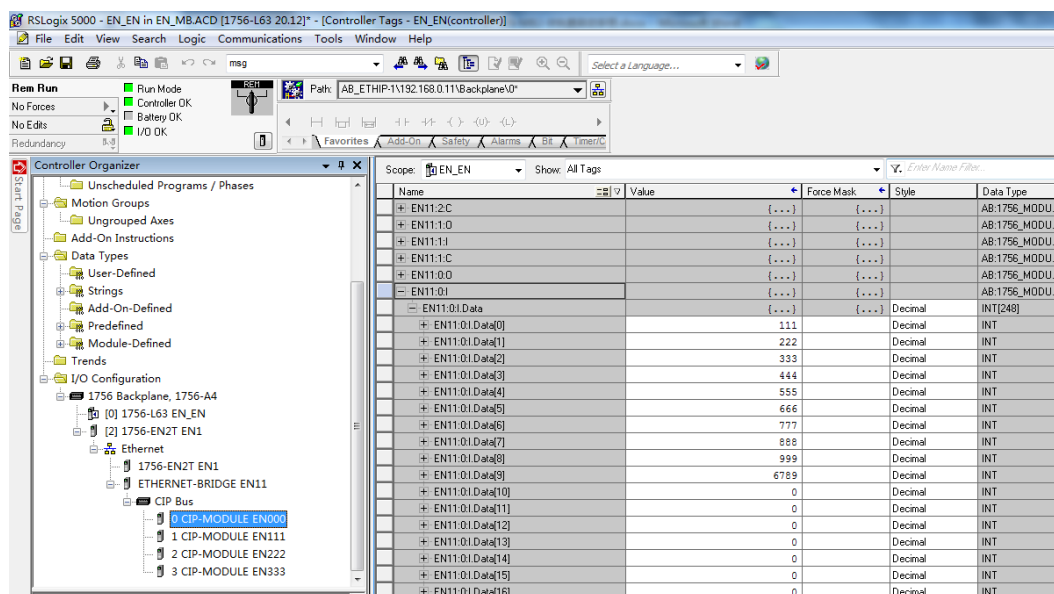


因为之前我们在模块内保存的命令（如下图）。

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	0	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	500	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

所以数据先被模块的Modbus主站驱动协议, 读到模块内部数据区寄存器0-9里面。

Home / Internal Data View											
		Decimal Display Hexadecimal Display Float Display ASCII Display									
Address	0	1	2	3	4	5	6	7	8	9	
0	111	222	333	444	555	666	777	888	999	6789	
10	0	0	0	0	0	0	0	0	0	0	
20	0	0	0	0	0	0	0	0	0	0	



同时被Logix PLC读取到EN:0:I.Data[0]– EN:0:I.Data[9]，如下图。

模块作为Modbus主站写一组数据到仿真软件（从站）里，先明确模块内部数据区的划分，1000以后是PLC输出的数据地址。所以RSLogix5000内输出的CIP标签组EN11:0:0.Data[0]– EN11:0:0.Data[9]对应模块内部寄存器地址1000–1009。

EN11:0:0	{...}
EN11:0:0.Data	{...}
EN11:0:0.Data[0]	8888
EN11:0:0.Data[1]	8888
EN11:0:0.Data[2]	8888
EN11:0:0.Data[3]	8888
EN11:0:0.Data[4]	8888
EN11:0:0.Data[5]	8888
EN11:0:0.Data[6]	8888
EN11:0:0.Data[7]	8888
EN11:0:0.Data[8]	8888
EN11:0:0.Data[9]	8888

增加一个Modbus主站的写命令，功能码使用16, 将模块内部数据区地址从1000开始的10个字写入到1号Modbus从站的40101–40110中，也就是把RSLogix5000内输出的CIP标签组EN11:0:0.Data[0]– EN11:0:0.Data[9]这10个数据写到Modbus RTU的1号从站，数据地址为40101–40110里面。

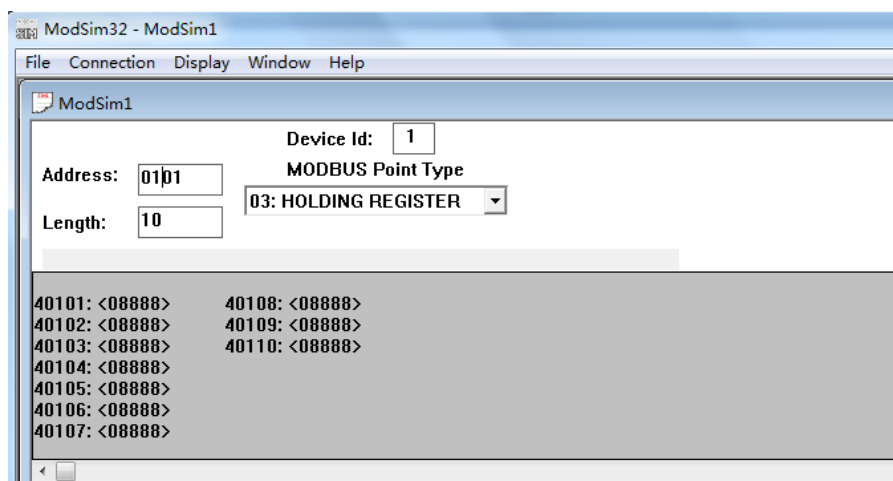
Enable	Yes
Modbus Function	FC 16 - Preset (Write) Multiple Register
Slave Address	1
Modbus Data Address	100
Quantity	10
Data Swap	No Change
Poll Interval	0
Internal Data Address	1000
Cmd Errors Mapping Enabled	
Cmd Errors Mapping Address	
Desc	

Close
Save

先看一下模块内部寄存器1000开始的地址，有数据从Logix5000写入到模块：

Address	0	1	2	3	4	5	6	7	8	9
1000	8888	8888	8888	8888	8888	8888	8888	8888	8888	8888
1010	0	0	0	0	0	0	0	0	0	0
1020	0	0	0	0	0	0	0	0	0	0
1030	0	0	0	0	0	0	0	0	0	0
1040	0	0	0	0	0	0	0	0	0	0
1050	0	0	0	0	0	0	0	0	0	0

再看一下Modsim32模拟的1号从站，40101-40110地址的数据。



至此，通过EtherNet/IP对于Modbus从站读和写字（WORD/INT）都已完成。

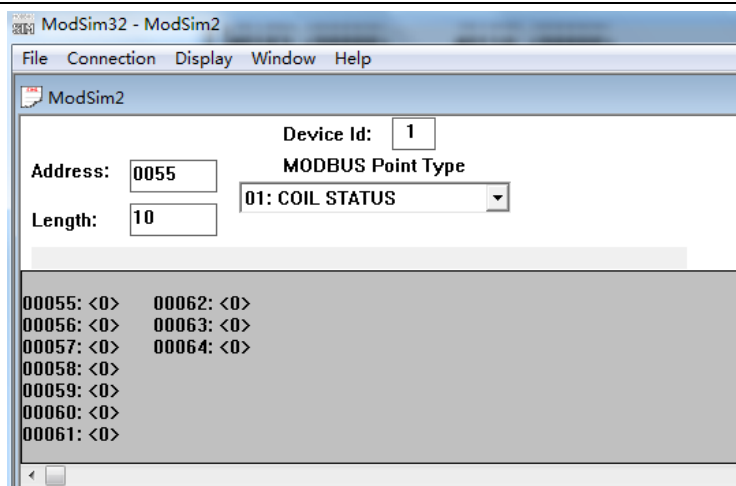
举例 2. Modbus 从站设备和罗克韦尔 PLC 交换布尔量数据

本案例中，模块配置作为Modbus RTU的master，同时配置作为EtherNet/IP的server。

特殊说明一下位（bit/bool）的操作，一般常见的应用是针对位寄存器，举一个例子来说明：

EN11:2:0	{...}
EN11:2:0.Data	{...}
EN11:2:0.Data[0]	22
EN11:2:0.Data[0].0	0
EN11:2:0.Data[0].1	1
EN11:2:0.Data[0].2	1
EN11:2:0.Data[0].3	0
EN11:2:0.Data[0].4	1
EN11:2:0.Data[0].5	0
EN11:2:0.Data[0].6	0
EN11:2:0.Data[0].7	0

想把PLC中输出CIP标签中EN11:2:0.Data[0].0- EN11:2:0.Data[0].7，这8个布尔量（如上图）写入到1号Modbus从站线圈00055-00062这8个位里面（如下图）。PLC中输出CIP标签中EN11:2:0.Data[0] EN11:2:0.Data[247]对应模块内部寄存器地址1500-1747，因为内部寄存器是16位的字，所以其中EN11:2:0.Data[0].0- EN11:2:0.Data[0].7对应于模块内部寄存器地址1500的前8位。



特别注意模块的内部寄存器是16位的字表示，如果要对位地址进行读写，指令中使用的模块的内部寄存器的起始地址要乘以16才能对应上。

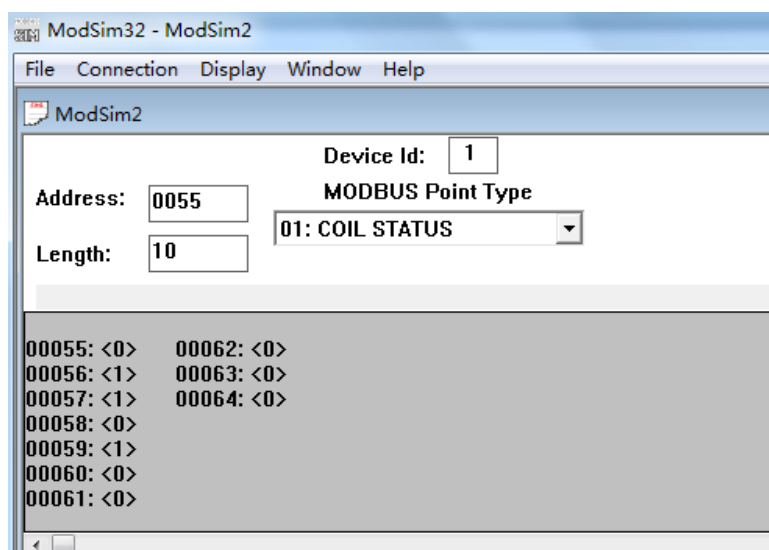
再看一遍对应关系。PLC输入标签组EN11:2:0.Data，对应模块内部寄存器起始地址为1500。

1个模块内部寄存器=16个位，想对从站的位线圈进行读写，要用 $1500 \times 16 = 24000$ 来作为起始地址。在模块Modbus主站一侧配置命令（如下图），可以选用功能码15 写多个线圈，从模块内部寄存器1500开始，连续调用8个布尔量，写入到1号Modbus从站， 00055-00062这8个位里面。

Modbus Port 1 - Add Command

Enable	Yes
Modbus Function	FC 15 - Force (Write) Multiple Coils (0)
Slave Address	1
Modbus Data Address	54
Quantity	8
Data Swap	No Change
Poll Interval	0
Internal Data Address	24000

指令配置完成生效后，Modsim32模拟的从站才能正确接收到位（bit/bool）的数据，如下图：



同理，如果是模块读取Modbus从站数据的时候，要保存数据到模块的内部寄存器时，指令中填写的内部数据

地址，需要使用模块实际内部地址*16的方式。如下图：

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

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Modbus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。

举例 3. Modbus 主站和罗克韦尔 PLC 交换数据

本案例中，模块配置作为Modbus RTU的slave，同时配置作为EtherNet/IP的server

BT-EN-MB系列模块有多个串口的型号可选，每个串口都可以做Modbus从站，是共用一个数据区的。

如下从站测试使用两种方式举例，

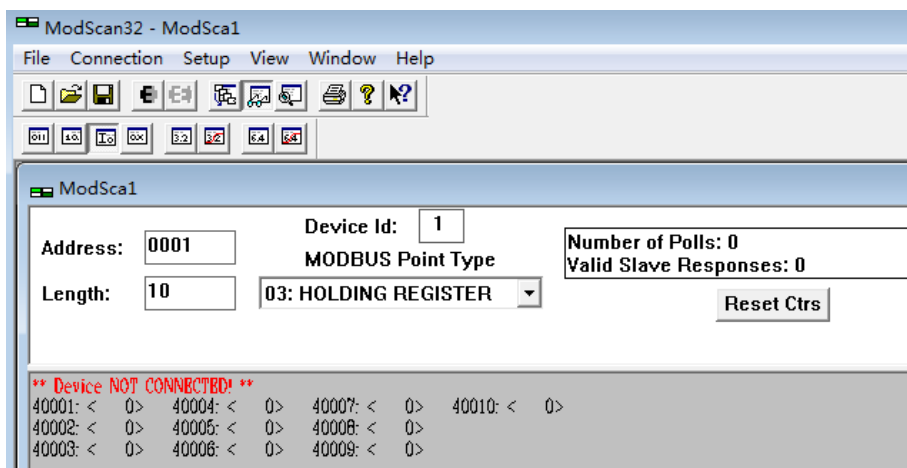
第一种使用ModScan32模拟Modbus主站，模块Port1作为Modbus从站。

第二种使用Port1做Modbus主站，Port2做Modbus从站来进行数据交换。

测试方法1，如下图，把模块Port1 改成从站,从站站号Slave ID设置为 1，点击保存。从站不需要配置命令：

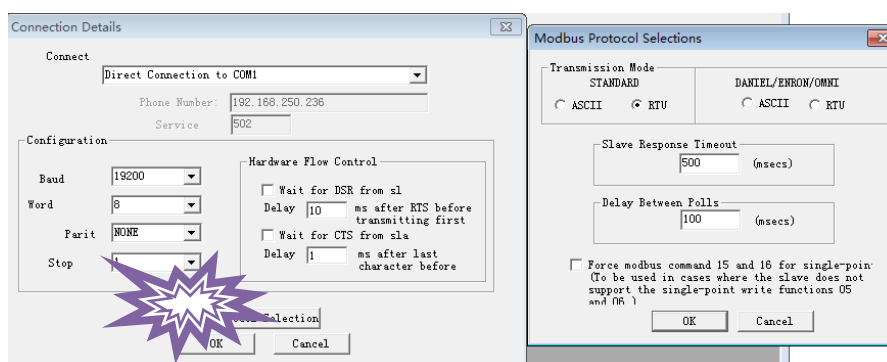
Port	On	端口使能
Mode	RS485	接线方式
Type	Slave	端口主站/从站
Protocol	RTU	端口协议
Baud Rate	19200	端口波特率
Parity	None	奇偶效验位
Data Bits	8	数据位
Stop Bits	1	停止位
Slave ID	1	从站地址
Minimum Response Delay	1	最小响应延时
Holding Register Offset	0	数据偏移
Word Input Offset	0	字输入偏移
Bit Input Offset	0	位输入偏移
Bit Output Offset	0	位输出偏移
Save		

打开ModScan32，按照下面的配置设置。

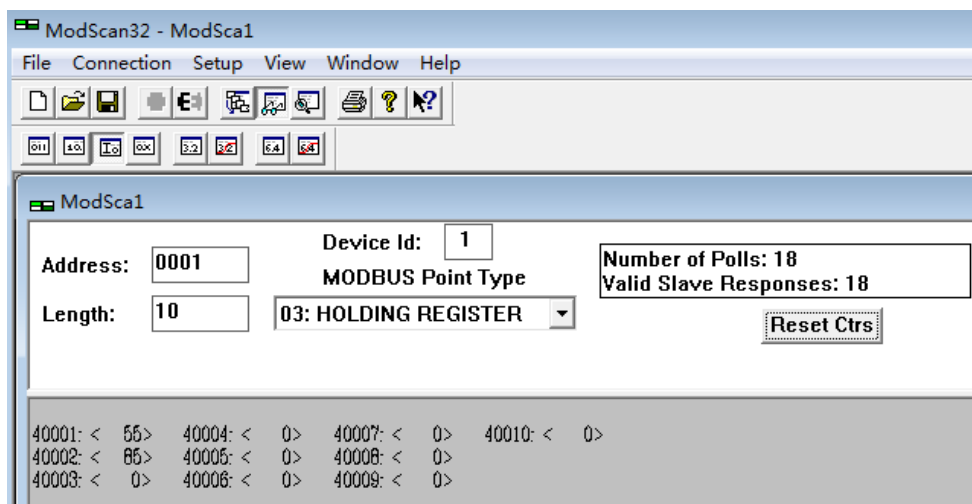


修改ModScan32配置参数，修改 Delay 1 ms after last character before 默认10，改成1。

在协议选择里面修改延时改成如下图所示。点击OK。



连接后在40001写入55，40002写入85。

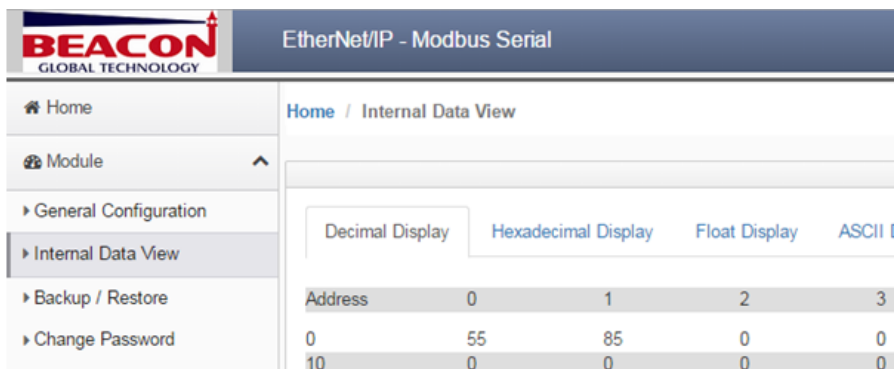


前文中我们提到Modbus主站和模块内部数据区的对应关系如下：

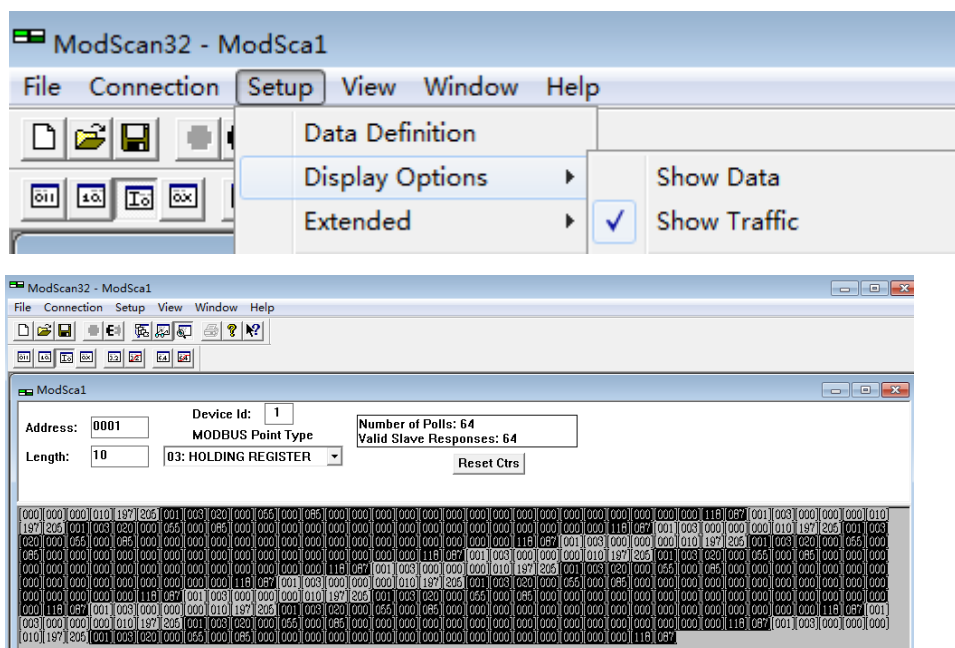
模块内部寄存器地址	等于	Modbus4区地址	等于	Modbus3区地址	等于	Modbus1区地址	等于	Modbus1区地址	等于	Modbus0区地址	等于	Modbus0区地址
0	=	40001	=	30001	=	10001	至	10016	=	00001	至	00016
1	=	40002	=	30002	=	10017	至	10032	=	00017	至	00032

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

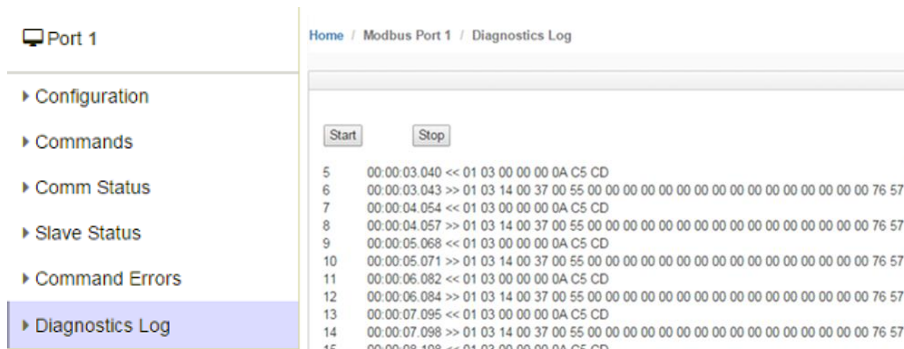
查看模块内部数据区，可以看到40001对应的是内部寄存器0，40002对应的是内部寄存器1。



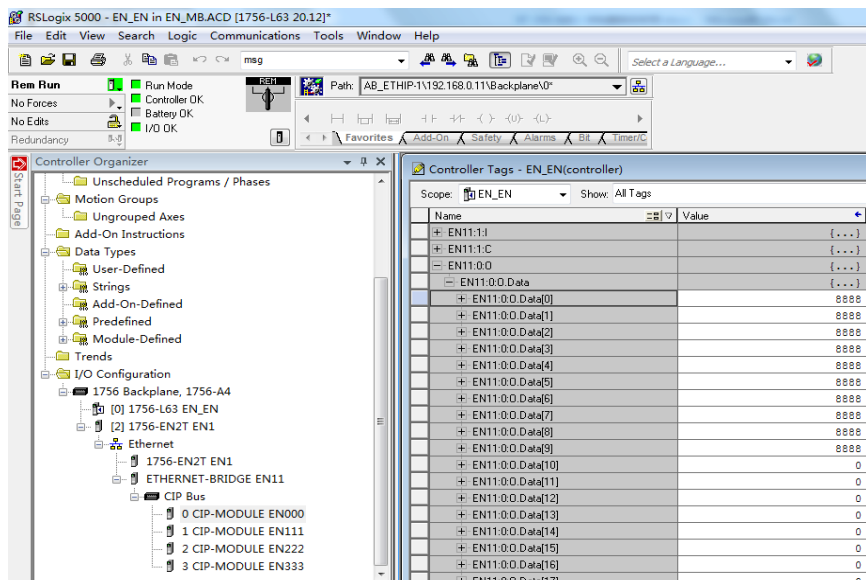
ModScan32的报文如下，看报文点击Show Traffic:



对应模块里面的报文:



测试方法2，先在RSlogix5000的CIP输出数组EN11:0:0.Data[0]–EN11:0:0.Data[9]中录入一些数据，如下图。



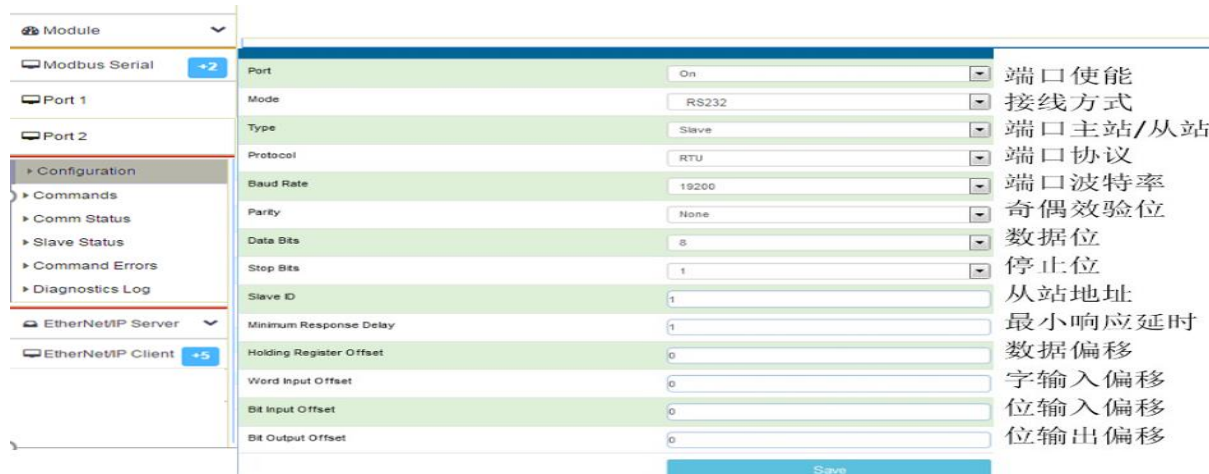
前文提到了EN11:0:0.Data[0]–EN11:0:0.Data[247]对应了模块内部寄存器 1000–1247 的地址，所以在模块内部寄存器中1000–1009中可以看到这写数据。

Home / Internal Data View

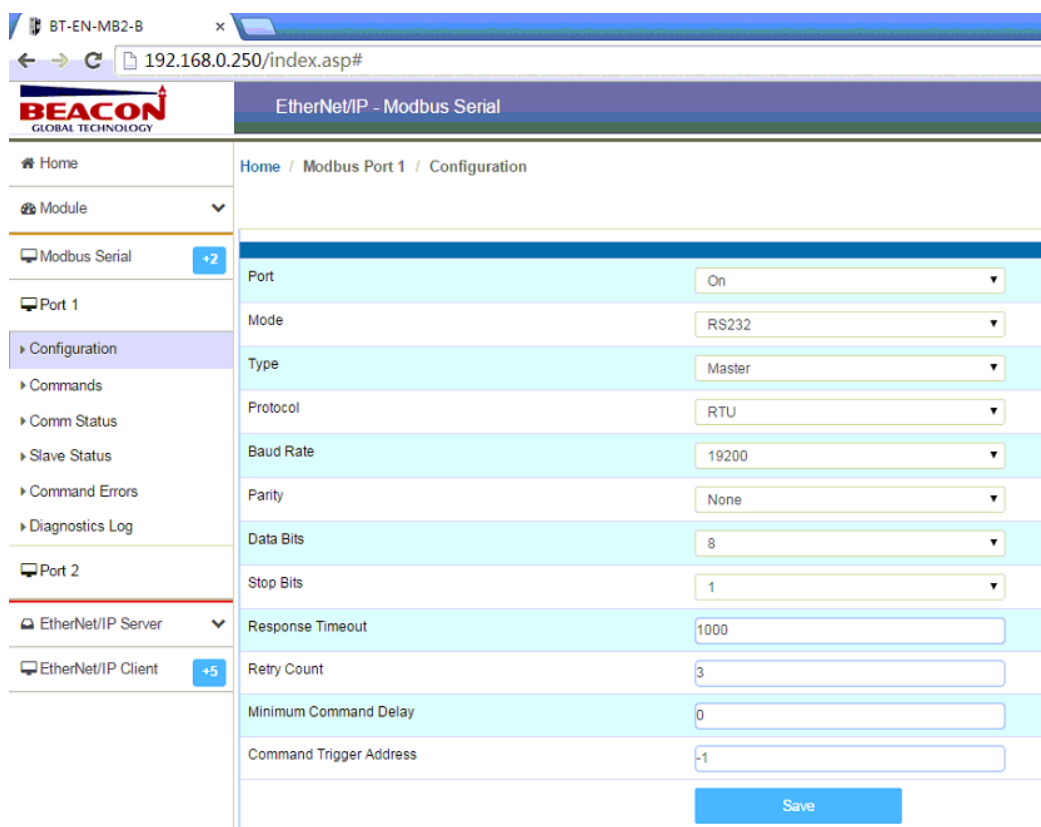
Decimal Display Hexadecimal Display Float Display ASCII Display

Address	0	1	2	3	4	5	6	7	8	9
1000	8888	8888	8888	8888	8888	8888	8888	8888	8888	8888
1010	0	0	0	0	0	0	0	0	0	0
1020	0	0	0	0	0	0	0	0	0	0

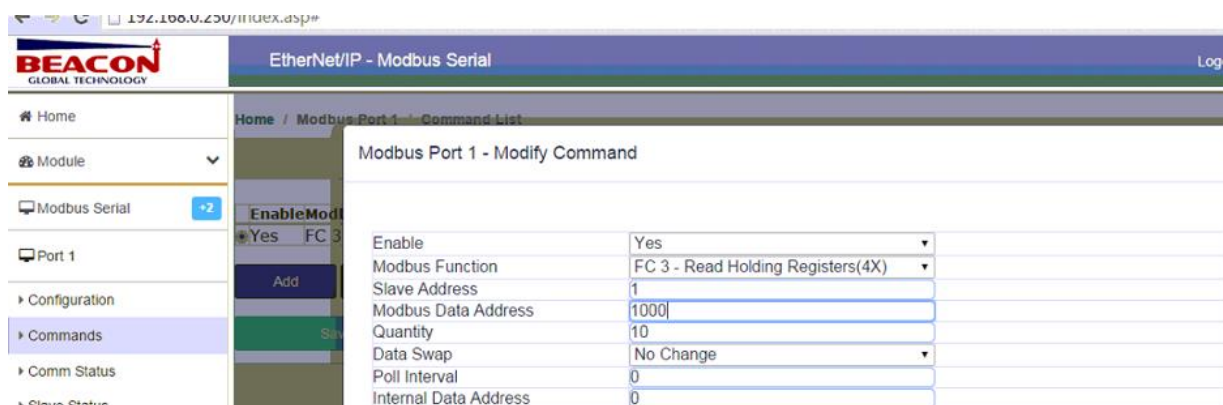
接着把模块Port2设置为Modbus从站（如下图），站号为1号从站，具体设置方法参考测试方法1中内容。



之后把模块的Port1 改成主站（如下图）。同时完成硬件配置：要把两个串口S1和S2用橙色的RJ45水晶头连接，中间经过一个2/3交叉的线接在一起（RS232模式）：



之后点击Port1 Commands, 配置一条命令用模块Port1端口作为Modbus主站，读取1号从站（Port2端口）的41001-41010这10个数据（对应模块内部寄存器地址为1000-1009），放到模块内部寄存器地址0-9里面，模块这段内部地址区对应着RSLogix5000输入CIP数组 EN11:0:I. Data[0]-EN11:0:I. Data[9]，配置如下：



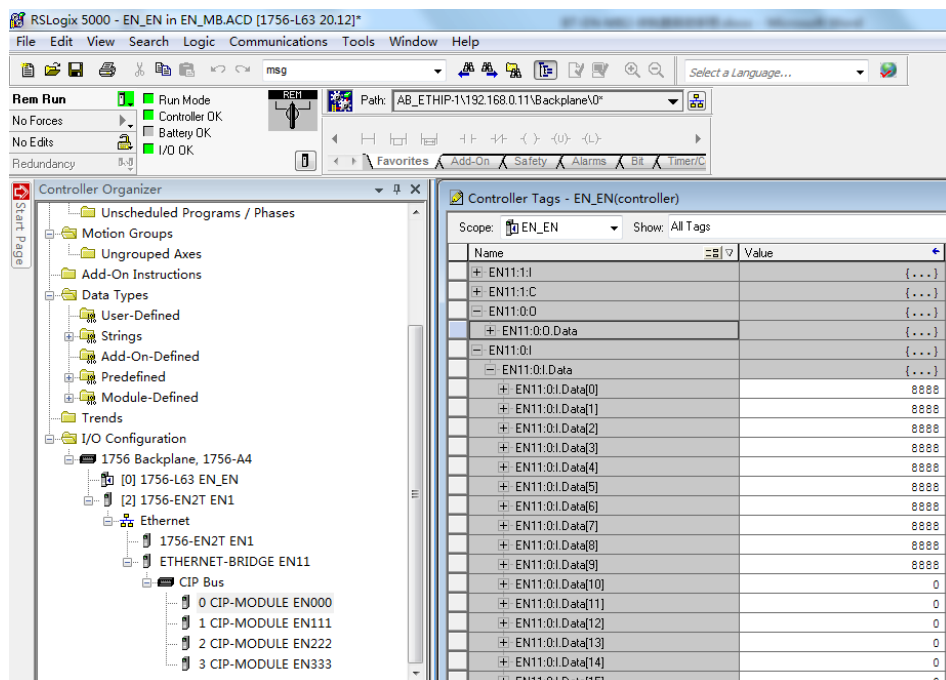
逻辑关系如下：

- 1) Logix 5000的输入标签组EN11:0:I. Data[0]-EN11:0:I. Data[9]，读取模块内部数据区 0-9 的数据；
- 2) 模块内部数据区 0-9 的数据，来自于模块端口1作为Modbus主站，读取端口2（Modbus从站）的数据；
- 3) 端口2作为Modbus从站时，其41001-41010的地址区实际上对应了模块内部数据区1000-1009的数据；
- 4) 模块内部数据区1000-1009的数据，来自于Logix 5000的输出标签组EN11:0:O. Data[0]-EN11:0:O. Data[9]的数据；
- 5) 所以等于Logix 5000的输入标签组EN11:0:I. Data[0]-EN11:0:I. Data[9] 读取输出标签组EN11:0:O. Data[0]

- EN11:0:0.Data[9]的数据。

点击保存，重启模块。

查看RS1goix5000里面的标签，可以看到PLC的输入CIP数据区，读取到了刚才输出CIP数据区中录入的数据。



其他版本简介

本案例分别介绍了最为常见的模块作为EtherNet/IP从站和1756系统（做主站）通讯，同时模块作为Modbus主站读取/写入现场Modbus从站数据的应用，以及模块作为Modbus从站将主站数据传回给1756 PLC的应用。

BT-EN-MB2-B（基础版）可以支持4个EtherNet/IP Class1 I/O链接，数据交换区2000个字，支持作为最多5个EtherNet/IP Client和5个EtherNet/IP Server，2个串口可以作为Modbus RTU的主站或者从站使用，做主站时每个端口可以支持64条Modbus指令。

BT-EN-MB2-P（领先版）可以支持10个EtherNet/IP Class1 I/O链接，数据交换区5000个字，支持作为最多15个EtherNet/IP Client和15个EtherNet/IP Server，2个串口可以作为Modbus RTU的主站或者从站使用，做主站时每个端口可以支持128条Modbus指令。

BT-EN-MB2-B/P模块除了可以支持EtherNet/IP Class1 I/O链接以外，还可以支持EtherNet/IP Class3采用MSG命令完成数据交换，此种方式数据交换的速度会大大低于Class 1的方式，配置命令也比较繁琐，本手册中不再一一举例。

BT-EN-MB系列型号众多，有单个、两个，四个Modbus RTU端口的产品可供选择，各种模块配置方式均可参考本手册中内容。

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)	13910136425
技术支持	support@beacongt.com
亚太区销售	asia@beacongt.com
北美区销售	usa@beacongt.com