BT-MTMB2-DM
快速启动手册

BEACON GLOBAL TECHNOLOGY

目 录

BT-MTMB2-DM 简介 2

配置 BT-MTMB2-DM 模块 2

配置模块 Profibus-DP 网络 5

组态 Profibus DP 主站驱动 6

组态 Profibus DP 从站 8

配置模块做 Modbus TCP 从站 14

配置模块做 Modbus TCP 主站 18

配置模块做 Modbus RTU 主站 21

Modbus 命令使能控制介绍 25

配置模块做 Modbus RTU 从站 27

举例 1.Modbus TCP 和西门子 PLC 之间数据交换 29

举例 2.Modbus RTU 和西门子 PLC 之间数据交换 37

举例 3.Modbus TCP 和 Modbus RTU 之间数据交换 44

特别注意 47

模块硬件前端的指示灯状态说明 48

联系我们 49

BT-MTMB2-DM 简介

Beacon Global Technology 通讯模块 BT-MTMB2-DM，支持多种设备在 Modbus TCP，Profibus-DP 以及 Modbus 串口网络中的数据交换，最大支持 20,000 个字节数据交换区。

网关提供一个 Modbus TCP 以太网端口，提供一个 Profibus-DP 串行端口，提供 2 个 Modbus 端口。

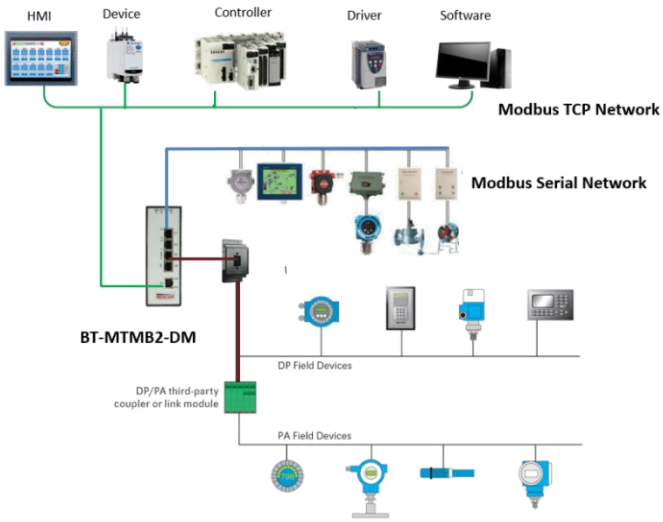
Profibus-DP 串行端口，可配置为 Profibus-DP 主站支持 V0 和 V1。

Modbus TCP 驱动做服务器时，可以支持多个主站设备进行访问。Modbus TCP 同时可以支持作为多个客户端，每个客户端最大支持 32 条指令，指令总数最多可达 480 条。

Modbus 串行端口可以支持配置成为主站或者从站，支持选择 RS232/RS422/RS485 模式，每个主站支持 128 条 Modbus 指令。

可以直接通过网页对网关进行配置和诊断，通过串行接口对 Profibus-DP 网络进行组态和配置。

BT-MTMB2-DM 网关采用独立的 DIN 导轨安装，所有网关均配置宽输入电源范围（10 - 36 VDC），和扩展级温度范围（-35° C 至 75° C）。



S1 端口==Modbus RTU 主站或从站，可以选择 RS-232/422/485 串口。

S2 端口==Modbus RTU 主站或从站，可以选择 RS-232/422/485 串口。

MASTER 端口==Profibus-DP 主站与从站数据通讯端口。

CFG 端口==Profibus-DP 主站组态配置端口。

E1 端口==模块配置端口，同时支持做为 Modbus TCP 主站/从站。

E2 端口==本型号不可用（请勿使用 E2 端口进行配置和应用）。

配置 BT-MTMB2-DM 模块

模块初始配置如下：

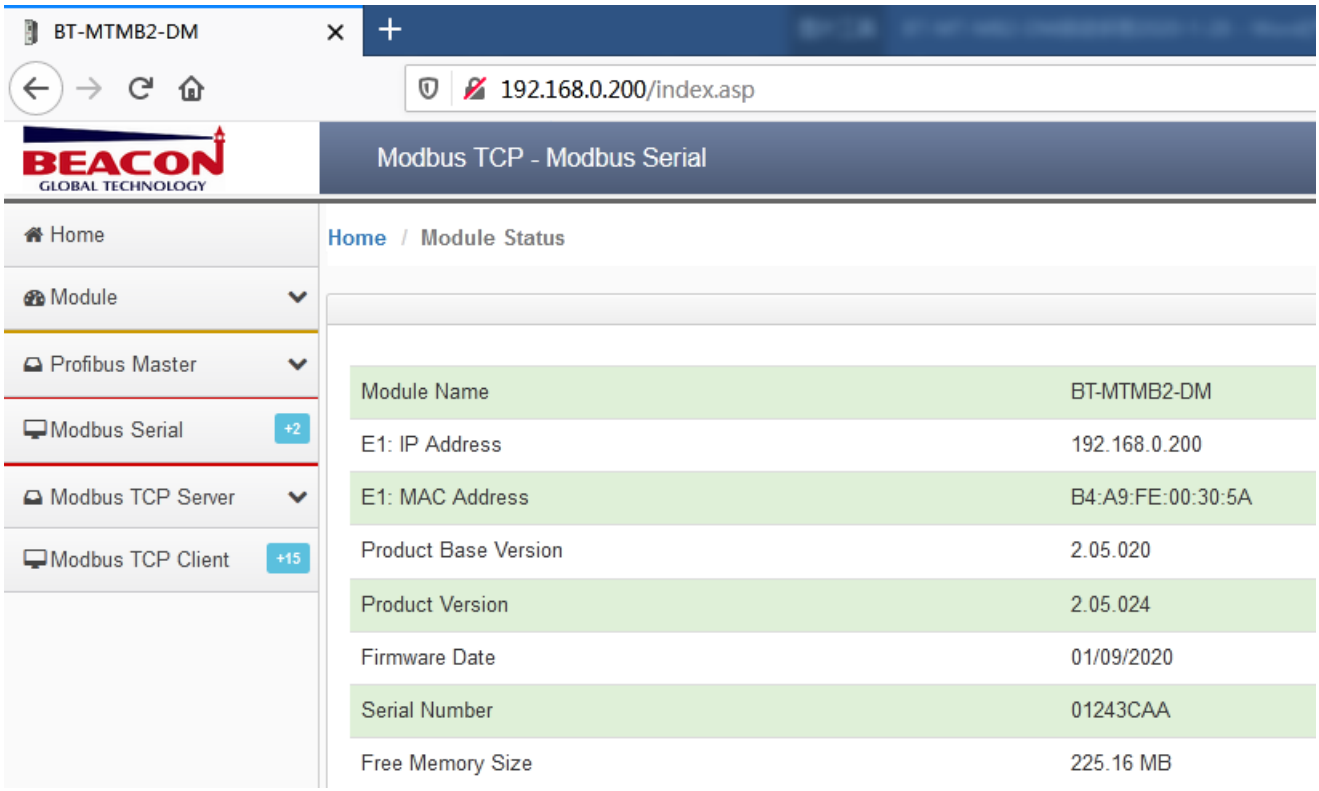
E1 以太网接口出厂 IP 地址为 192.168.0.200。如果 E1 以太网端口地址进行过修改，可以使用 BEACON 的 IP Browser 软件查找该端口的 IP 地址。软件下载地址为：

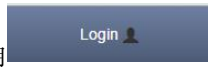
www.beaconglobaltech.com/upload/Public/Uploads/5c782dca2af1e.zip。

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 BT-MTMB2-DM 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 BT-MTMB2-DM模块的配置页面如下图。



2. 在配置页面的导航条内，点击右上角 

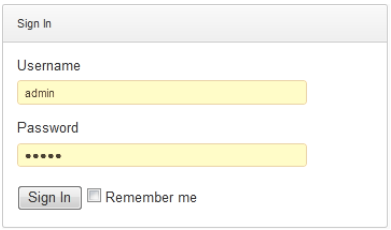
。
3. 按照界面提示，输入用户名和密码进入模块配置。

   用户名(Username):admin

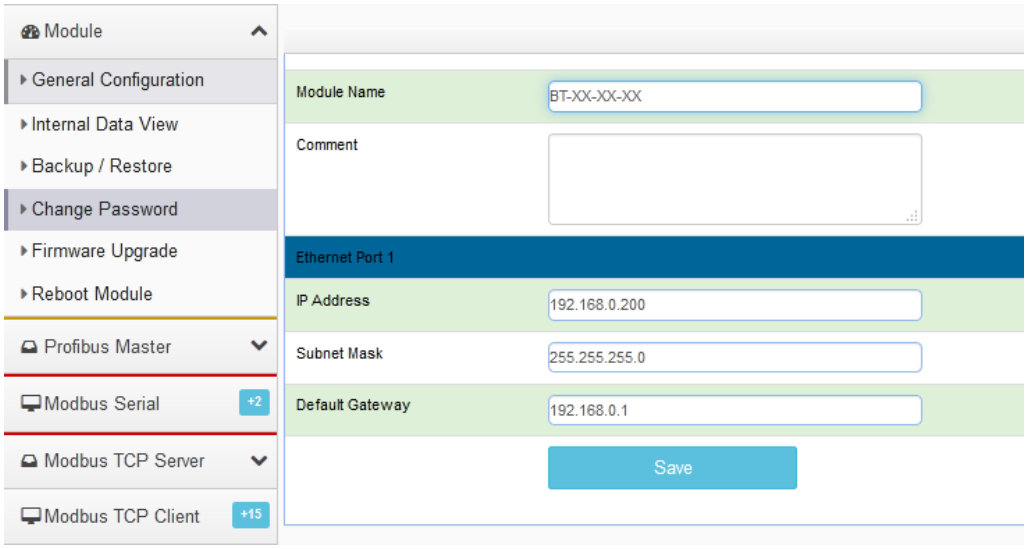
   密码(Password): admin

   点击登录(Sign In)

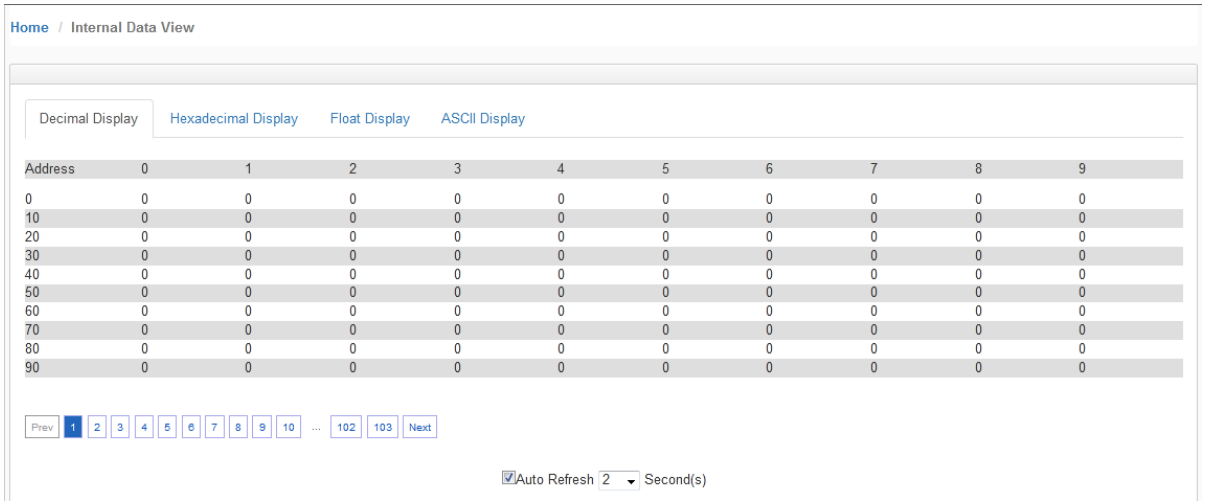
   请注意：如果不登录，只能浏览配置，无法进行配置修改。



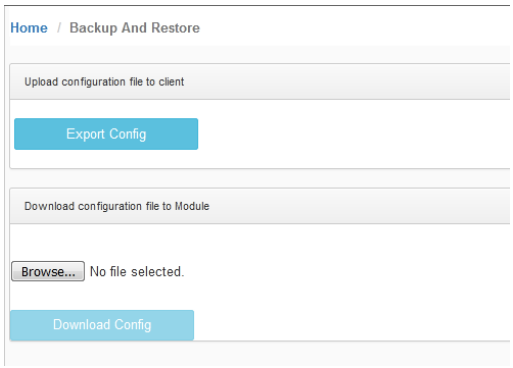
4. 查看模块 IP 地址，点击 General Configuration，修改模块的 IP 地址。



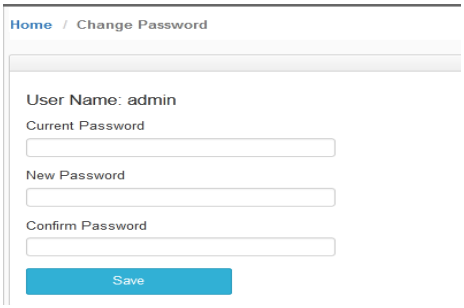
5. 点击 Internal Data View，可以查看模块内部寄存器数据动态的显示值，每个寄存器是 16 位的 WORD 格式，数据区的大小和模块具体型号有关联，不同型号模块的内部寄存器的数据区不一样。每页 100 个 16 位的寄存器。



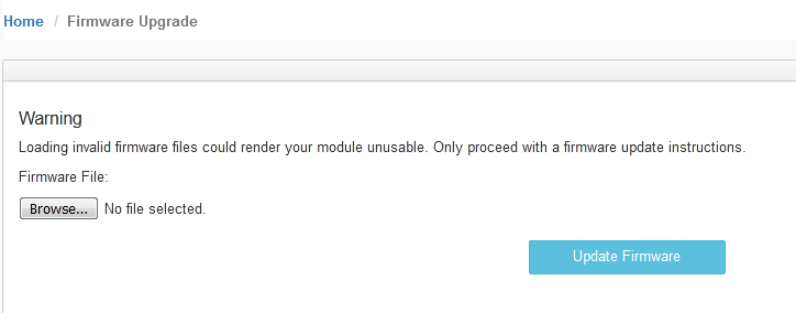
6. 点击 Backup And Restore 导出配置文件 Export Config 和恢复配置文件 Browse... No file selected. 。



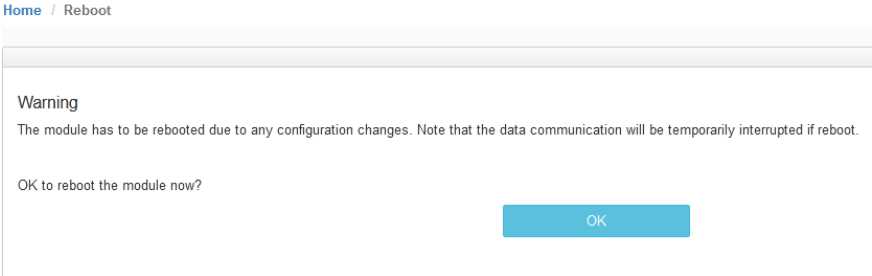
7. 点击修改密码，可以修改模块的登录密码。 Change Password 。



8. 点击 Firmware Upgrade 是模块升级的选项。



9. 点击 Reboot 是模块修改配置后，重启让配置生效的功能。（不是复位）



配置模块 Profibus-DP 网络

PROFIBUS 是过程现场总线(Process Field Bus)的缩写，于 1989 年正式成为现场总线的国际标准。在多种自动化的领域中占据主导低位，全世界的设备节点数已经超过 2000 万。它由三个兼容部分组成，即PROFIBUS-DP(Decentralized Periphery)，PROFIBUS-PA(Process Automation)，PROFIBUS-FMS (Fieldbus Message Specification)。其中PROFIBUS-DP应用于现场级，它是一种高速低成本通信，用于设备级控制系统与分散式 I/O 之间的通讯，总线周期一般小于 10ms，使用协议第 1、2 层和用户接口，确保数据传输的快速和有效进行。Profibus 主协议驱动程序作为一个单一的端口实现存在，驱动程序可以配置为 1 类和 2 类 Profibus 主协议与其他 Profibus 从设备进行接口。该单元还用于配置 Profibus 网络中的节点。它提供了对标准和扩展诊断信息的访问，以及冻结/同步功能、非循环通信(DPv1、1 类和 2 类)和报警处理(DPv1)。利用 Profibus 主端口可以通过串行通信接口(RS-485)与 Profibus 从设备连续接口。

BEACON不同型号的模块，Profibus-DP主站网络驱动，最大提供768word（1536 bytes）的输入和768word（1536

bytes）的输出，支持DP-V0\V1类1或2类 DP V1特性为非循环通信，报警处理，扩展诊断；支持最大32个从站节点（不适用中继器）；支持最大125个从站节点（4个DP网段里面使用3个中继器连接）。下图显示为 Profibus波特率与网段长度对应关系：

数据传输速率（kbit/s）	9.6	19.2	45.45	93.75	187.5	500	1500	3000	6000	12000
最大网段长度（m）	1200	1200	1200	1200	1000	400	200	100	100	100

组态 Profibus DP 主站驱动

对模块参数进行配置，点开模块 Home ->Profibus ->Master Configuration（如下图所示）：

在该窗口中可以配置 Profibus 主站的输入数据量（Input data size）和输出数据量（Output data size），此参数可根据用户的实际应用进行设置。此页面中：

DP从站对于模块的输入起始地址为0，代表模块DP主站读取DP从站数据，存储在模块内部数据区的起始地址；

模块对于 DP 从站输出起始地址为 1500，代表模块 DP 主站写给 DP 从站数据，调用模块内部数据区的起始地址。

注意：此处“Master Configuration”配置页面中的输入/输出起始地址，和后文中提到的“Slave configuration”配置页面中的输入/输出起始地址，正好相反。

DP Master的输入起始地址=DP slave 的输出起始地址，DP Master的输出起始地址=DP slave 的输入起始地址。

同时该窗口还可以对输入数据、输出数据的字节转换方式进行设置。建议选择默认参数即可，如果所连的从站设备类型为同一设备类型（例如从站都是西门子S7-300 PLC）且需要字节高8位和低8位交换，可以在该窗口设置输入和输出数据交换。如果所连接从站设备类型为不同设备类型（例如有西门子DP从站，传感器DP从站），就不用在该窗口设置数据交换，后面篇幅会介绍具体交换的方法。

由于配置Profibus网络比较复杂，因此我们为客户提供了专门的Profibus网络配置软件DP MASTER （该软件可在模块随机U盘内找到，无需安装，可直接在WINDOW环境中运行）该软件可实现以下功能：

1、建立一个Profibus网络项目；

2、对主站模块进行配置；

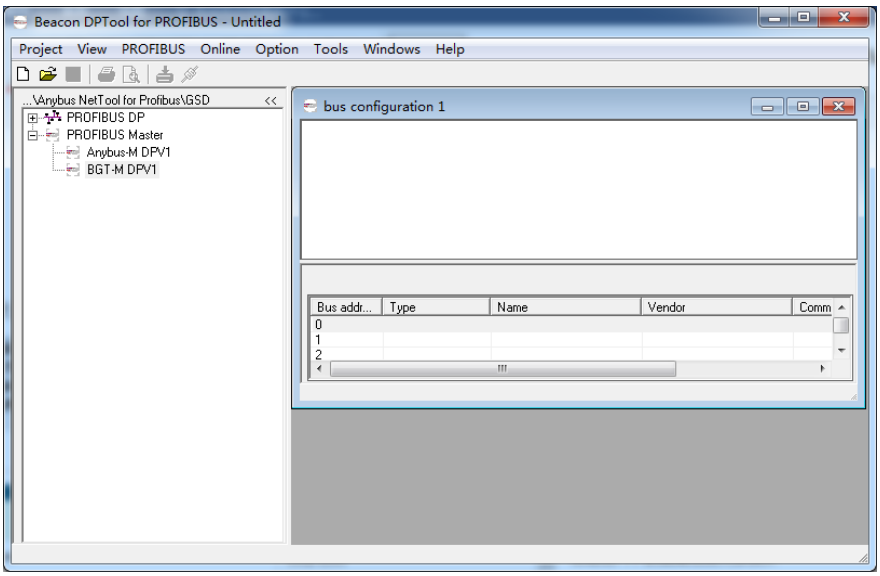
3、Profibus网络的配置（包括主站和从站的配置）；

4、将配置文件传输到模块。

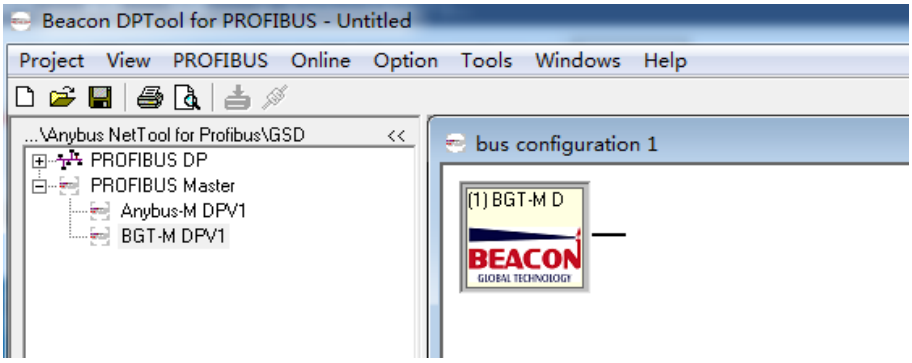
运行 DP MASTER 软件配置模块前，先找到包装内的黑色 USB to RJ45 电缆，电缆 USB 端口连接电脑 USB 端口，电缆RJ45端口连接模块CFG端口。

电脑运行

软件，进入PROFIBUS-DP组态页面，点击左上角新建项目。

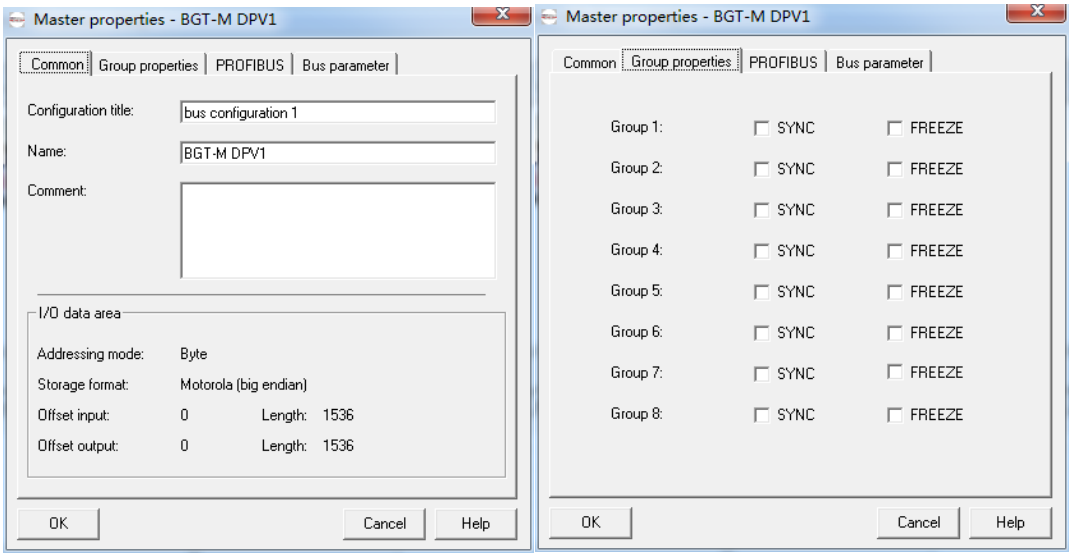


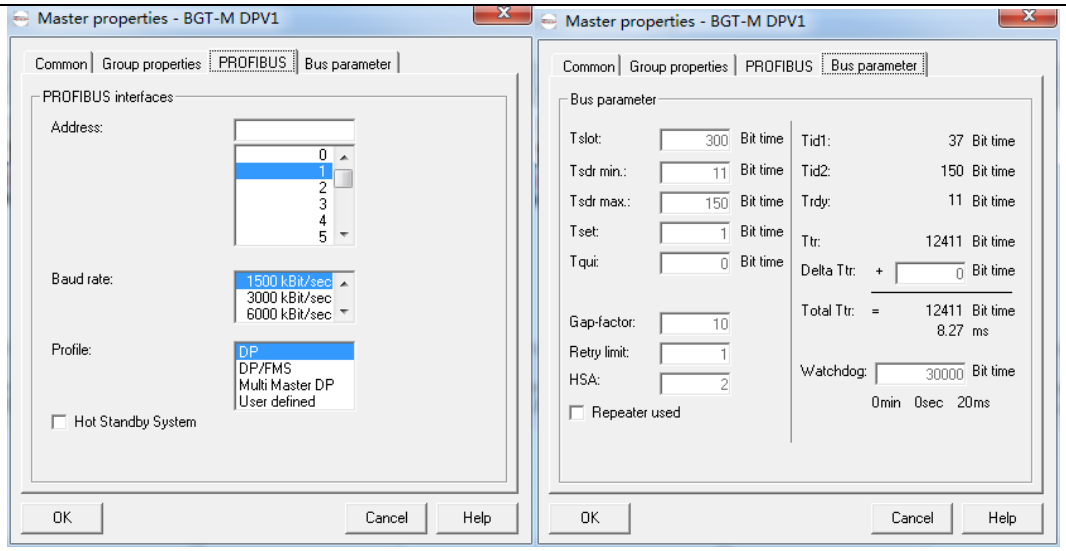
拖动BGT-M DPV1图标到右侧bus configuration 1的空白页面里面，然后开始对DP主站进行配置。



双击

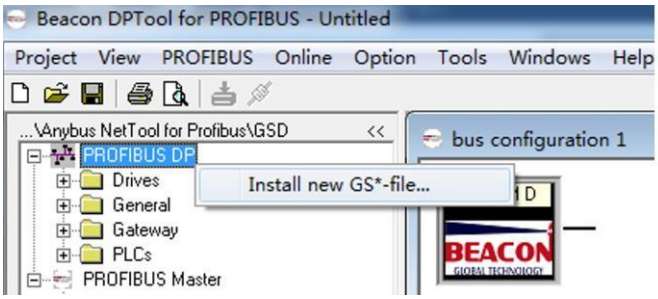
图标显示DP主站配置的界面如下4张图所示。用户只需要修改波特率即可，其余参数默认。

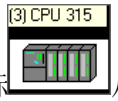




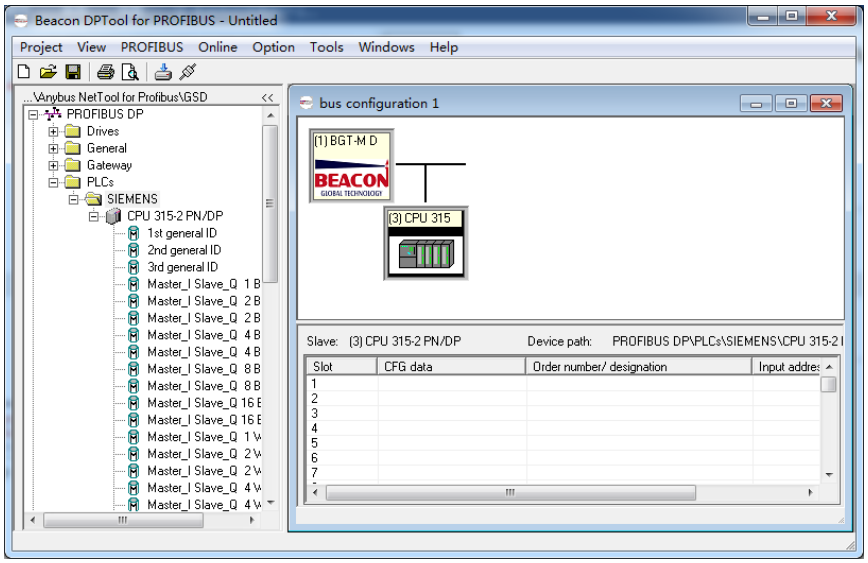
组态 Profibus DP 从站

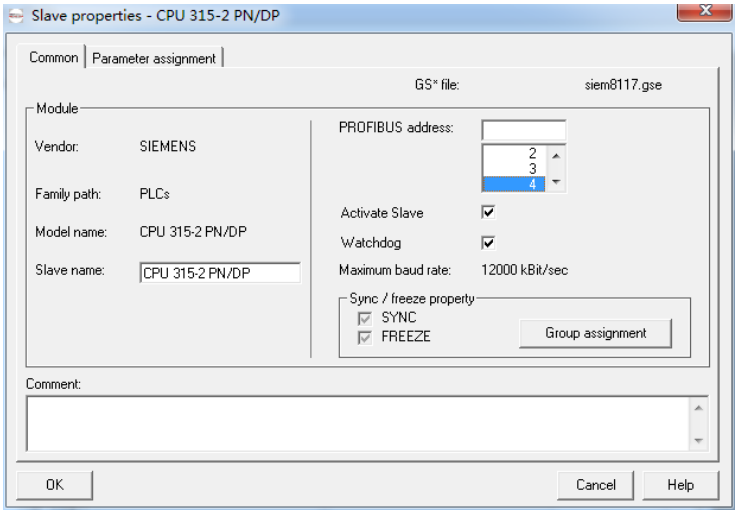
安装新的DP从站GSD文件。鼠标右键点击PROFIBUS DP,出现Install new GS*-file… ，选择导入对应的DP从站GSD文件。



拖动DP从站设备加入到DP网络中进行组态，双击图标 

从站会弹出从站属性对话框，我们在这里可以对从站设备的一些属性参数进行设置。



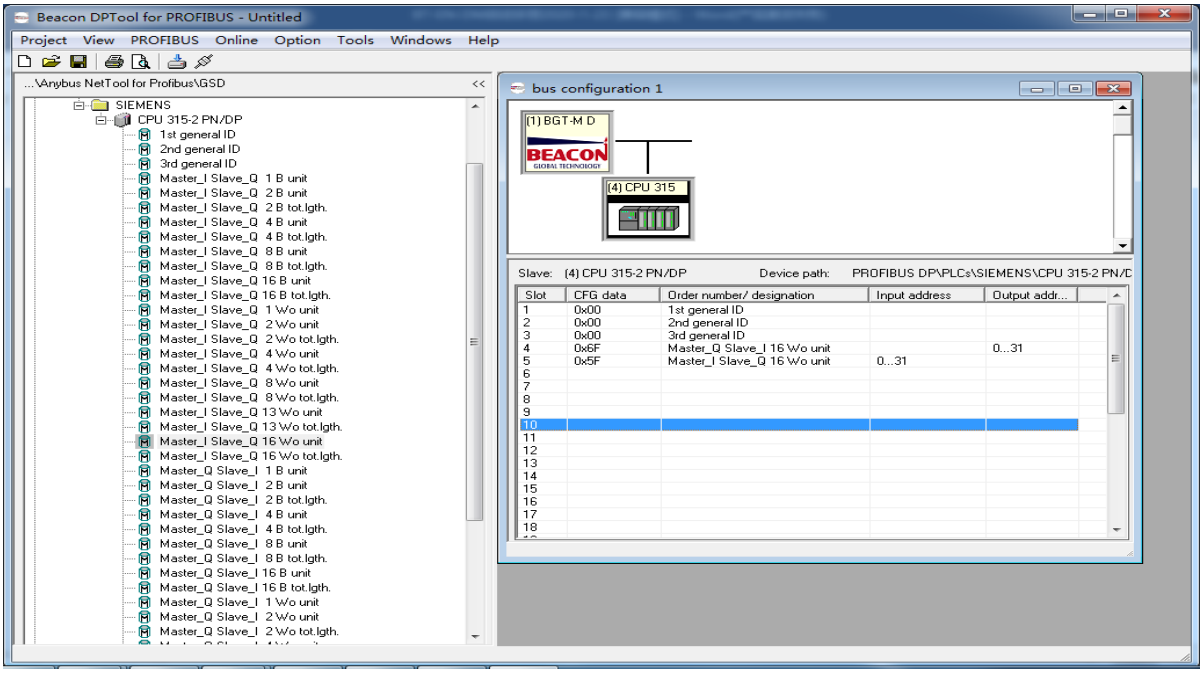


- Slave name：从站名称设置。
- Profibus address：从站站点地址设置，有效输入0 - 125。
- Activate：激活从站，如果不激活则从站停止和主站的数据交换。
- Watch Dog：是否启用看门狗，如果启用看门狗设置则意味着主站对从站的轮询一定要在定义的看门狗时间内，如果超时，则从站自动复位。
- Sync/Freeze：是否启用同步和冻结模式，最大8组，通过Group assignment可设置相关组别。

配置从站的IO数据文件：

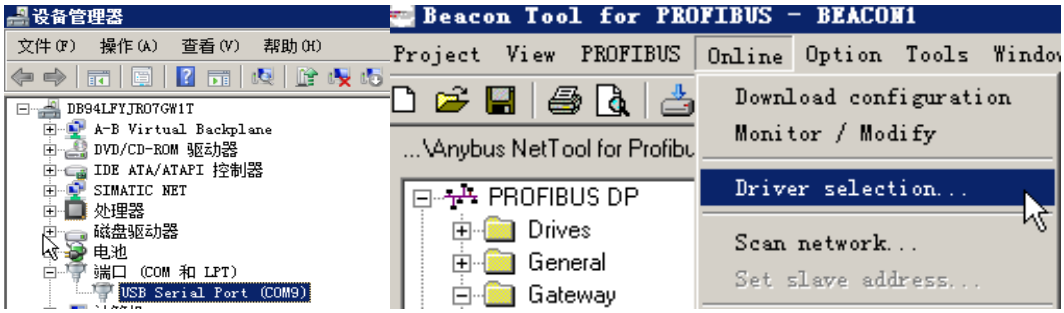
首先我们展开导入的从站设备，展开后我们可以看到一个配置数据列表，该列表根据所选从站设备的不同，GSD 文件的不同，配置列表也不同（举例，添加西门子315-2PN/DP PLC的GSD文件）。

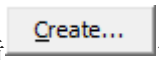
点击从站设备，会弹出从站的配置表格，从这里我们添加从站的IO模块，左键点住16 words in put拖到右下表格中，这样一个16个word的输入模块我们就添加进来了，同理我们还可以添加一个16 words out put的输出模块。



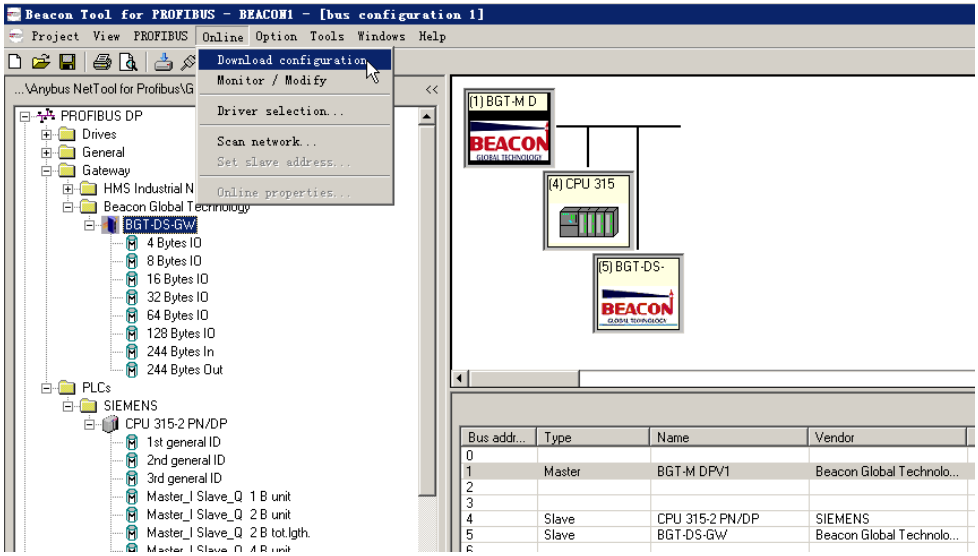
这时DP从站的IB0—IB31和QB0—QB31的数据就可以和这个Profibus-DP主站模块进行数据交换了。如果增加两个或多个输入输出模块，Input address和Output address会随着模块的增加自动分配Profibus地址。

点击保存Profibus DP网络配置并返回到主站设置窗口，将配置文件下载到模块里面。将模块包装内自带的USB 转RJ45水晶头的数据线，电缆USB端口链接到电脑USB接口。可以通过驱动精灵下载该USB设备的驱动，下载并安装好该驱动后，查看电脑设备管理器会出现COM号,然后把RJ45接口连接模块的CFG端口上，下载网络配置文件。

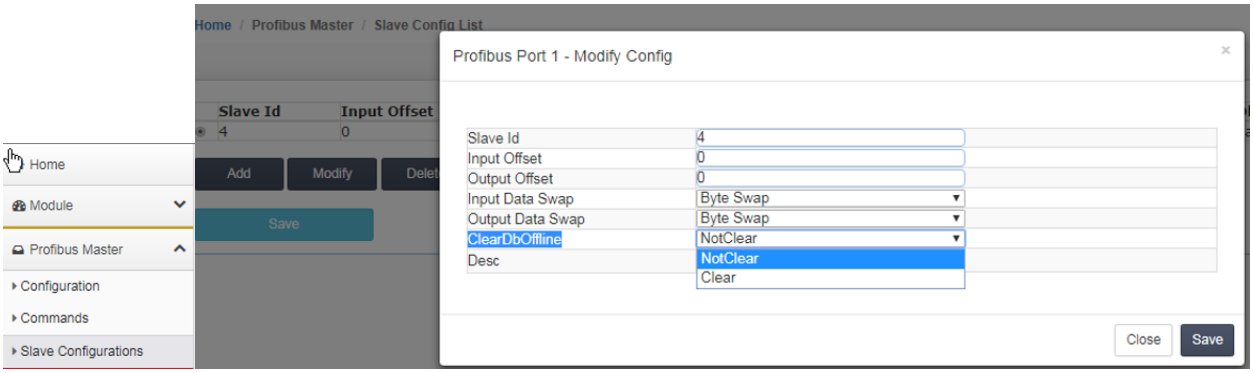


点击 

创建一个新的串口下载路径，然后点右侧图形的OK按钮，弹出选择对应的串口COM号，点击OK ,这样下载路径就建立完毕。然后点击菜单栏下载配置文件到模块里面。

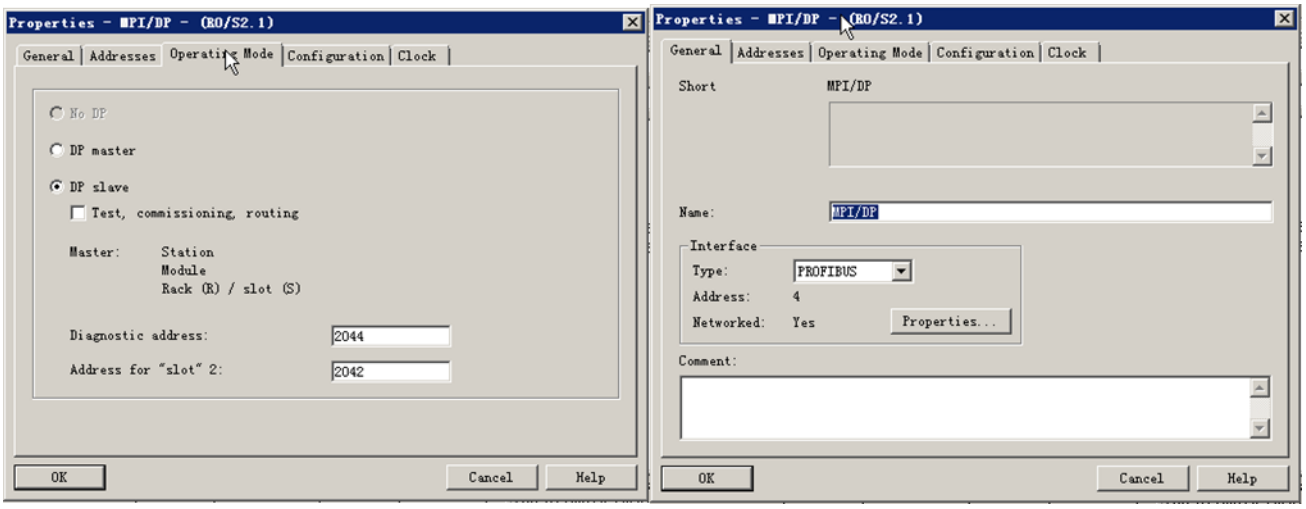


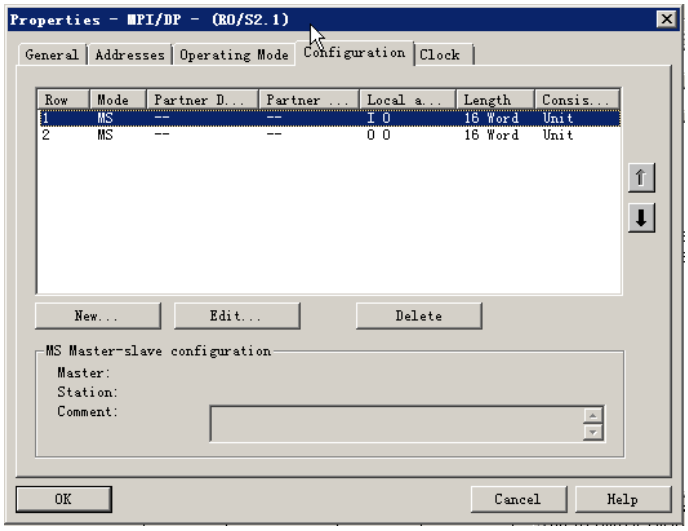
回到模块的网页配置界面（登录后操作），点击Slave Config List，点 Add按钮可以增加配置4号从站输入输出字节的高位和低位交换。



注意：如果涉及到 EtherNet/IP 的产品型号，由于罗克韦尔和西门子数据字的高 8 位和低 8 位是反向的，所以这里需要选择 Byte Swap 字节交换。“ClearDbOffline”表示 DP 从站离线或者发生断线情况下，是否保留断线之前的数据，这里可以选择不清零或者清零。配置完成后，点击 Save，提示 Success 成功。再点击配置列表里面的 Save 保存所有的配置。

以上步骤便完成了DP主站模块和一个设备从站的配置。同时西门子315-2PN/DP PLC作为DP从站的硬件设置如下：





配置好硬件后，下载到西门子CPU，之后点击PLC变量表查看输入输出关系，如下图：

4	0x6F	Master_Q Slave_I 16 Wo unit		0...31
5	0x5F	Master_I Slave_Q 16 Wo unit	0...31	

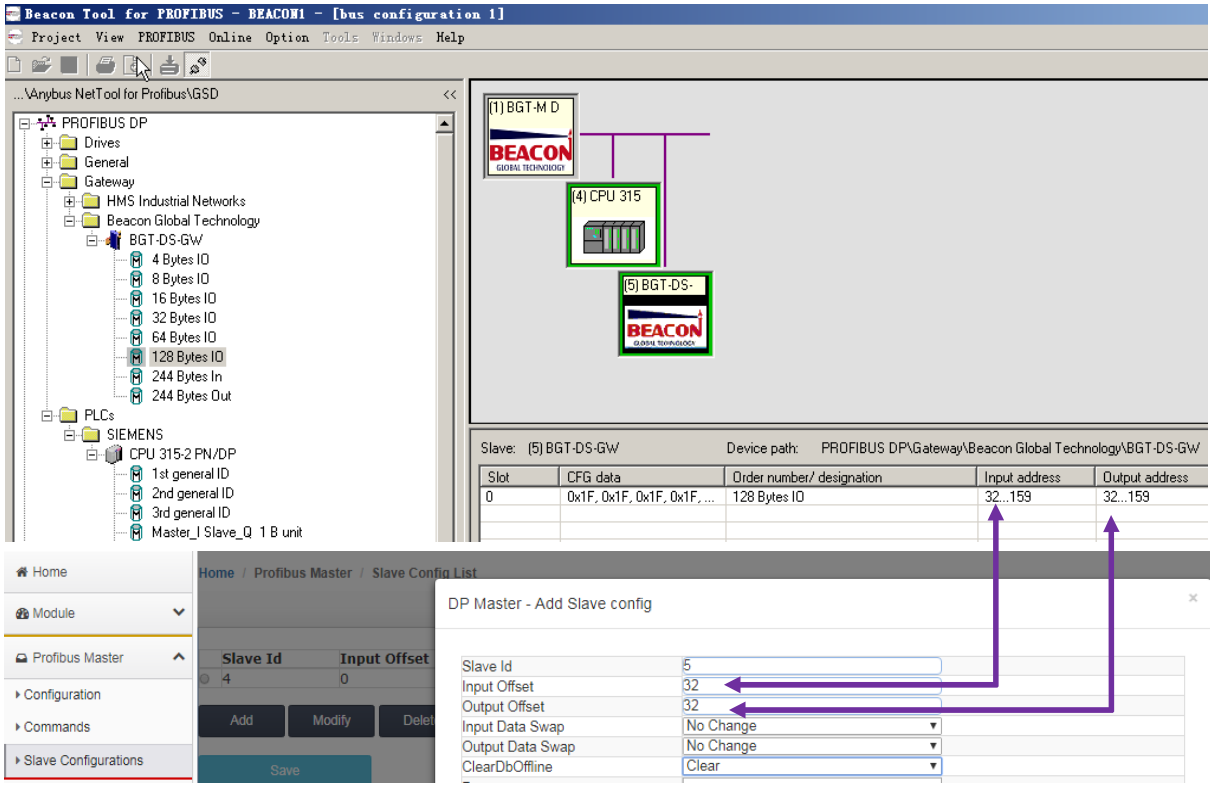
第一行是DP从站输入的16个字（32个字节），对应模块（DP主站）输出区域，模块内部寄存器地址1500-1515。

第二行是DP从站输出的16个字（32 个字节），对应模块（DP主站）输入区域，模块内部寄存器地址0-15。

下图为模块内部寄存器地址区域分配的配置：

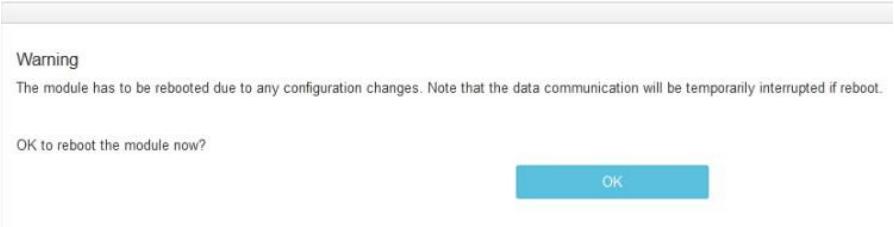
接下来我们继续介绍添加第二个DP从站的方法及配置。

举例：配置第二个DP从站（BEACON系列DP从站模块，5号站），方法与前面介绍相同。从下图可以看到，5号从站自动分配的地址输入和输出范围都是 32-159，这里的范围是字节显示方式，而模块内部寄存器是字的显示方式。所以模块内部寄存器实际对应的输入、输出范围是128字节等于64个字。同样也可以在模块网页中配置5号从站的数据交换模式和清零模式。由于5号从站为非西门子设备，所以字节高低位并不需要交换，另外用户也可以选择DP从站离线后，模块内部寄存器是否清零。如下图显示，添加第二个DP从站的配置。由于前文配置的第一个DP从站设备，已经占据了模块内部寄存器输入和输出的前32个字节（0-31字节=0-15个字寄存器）的地址，所以第二个DP从站所使用的模块内部数据区的起始地址，需要向后偏移32个字节。所以在输入偏移和输出偏移的地址需要填写32。

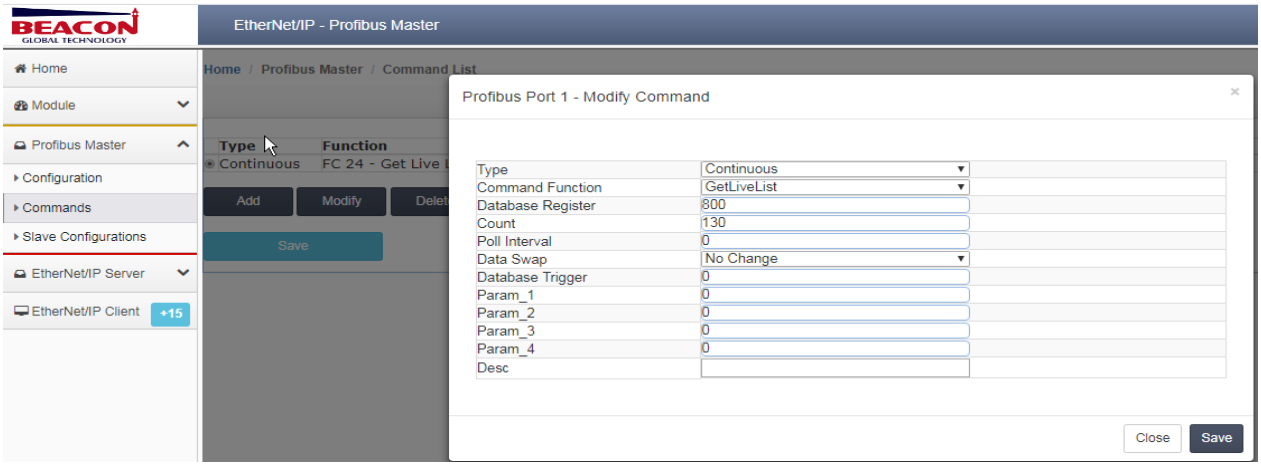


此处需要注意，“Slave configuration”配置页面中的 input 地址区域是该 DP 从站的输入数据区域，对应 DP Master的output地址区域；同理，DP从站设备对模块（DP主站）的output数据区域，对应于DP Master数据的input地址区域；所以此处的配置代表如下含义：模块（DP 主站）写给该DP从站的数据，将来自于模块内部寄存器地址1516到1579的区域，同时模块（DP主站）读取该DP从站的数据，将被保存在模块内部寄存器地址16到79的区域。模块对该DP从站输入和输出数据出高低位字节不交换，该DP从站离线后，内部寄存器清零。

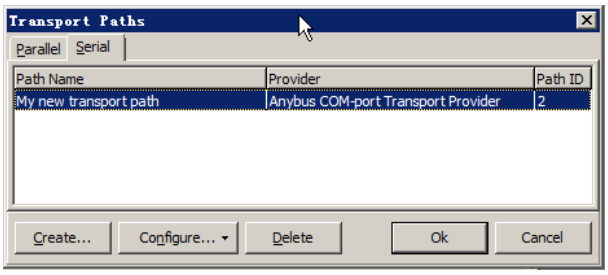
点击保存，然后点击重启模块，使配置生效。后面要接入更多的DP从站均可按照这个规则进行配置。

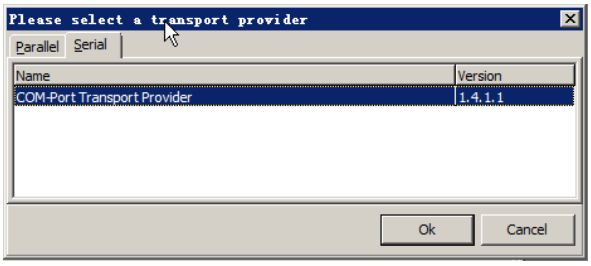


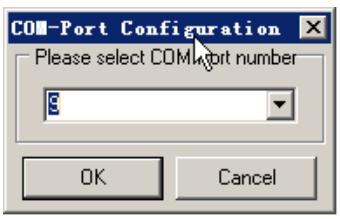
举例：配置3个从站，获取从站在线和离线状态到模块内部寄存器，查看模块内部寄存器地址800开始再次点击网页配置模块的部分（需登录后操作），点击Profibus Master---Command，点击Add按钮增加从站状态反馈（如下图），可获取127个从站的状态，Count填写规则要大于127，800表示状态值从内部寄存器800开始放置。

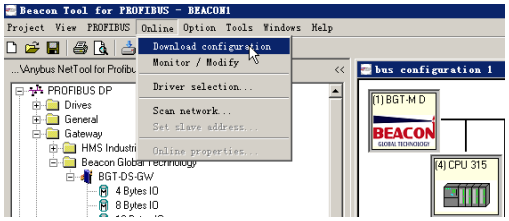


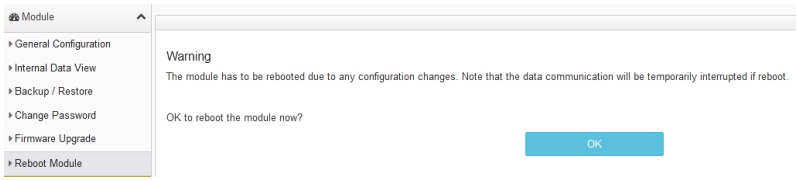
配置完成后，点击Save，提示Success成功。再点击配置列表里面的Save保存所有的配置再次重新启动模块后，使整体配置生效。



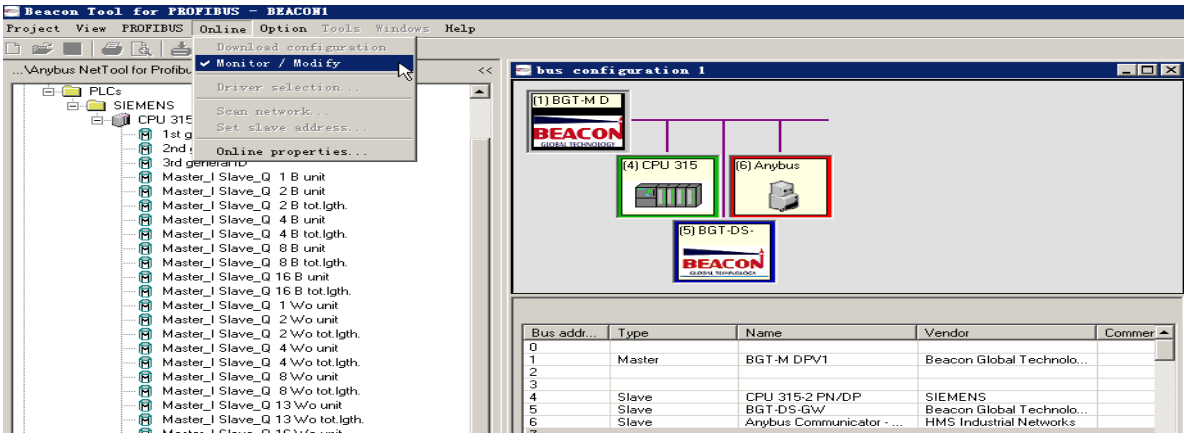








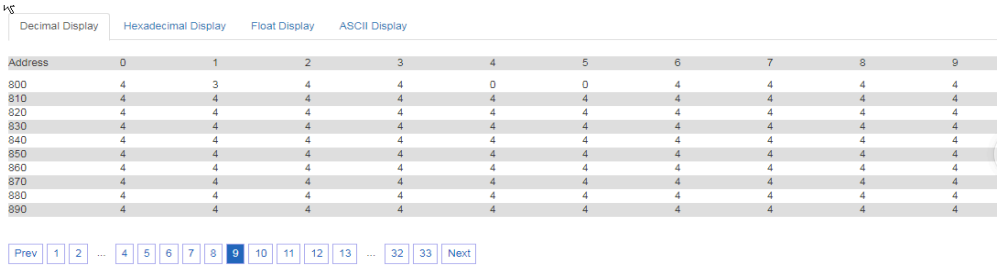
获取从站在线和离线状态到模块内部寄存器，查看模块内部寄存器地址800开始。



在配置软件中，从站绿色外框表示从站 GSD 文件正确，输入输出字节数与从站输出输入字节数一致，DP 终端电阻和DP线路正确。

从站蓝色外框（红色外框偶尔闪烁）表示从站 GSD 文件不正确，或者 GSD 文件配置的输入和输出与从站的输出和输入字节数不相符DP线路正确。

从站红色外框表示从站线路不正确，有可能是 DP 中断电阻拨码不对或者是线路没有按照 Profibus-DP 标准来接线。



在模块的内部寄存器页面中，如上图：

800 数据为 4，表示 Profibus-DP 0 号站地址没有使用设备；

801 数据为 3，表示 1 号站地址是主站，主站正常运行状态；

802 数据为 4，表示 Profibus-DP 2号站地址没有使用设备；

803 数据为 4，表示 Profibus-DP 3号站地址没有使用设备；

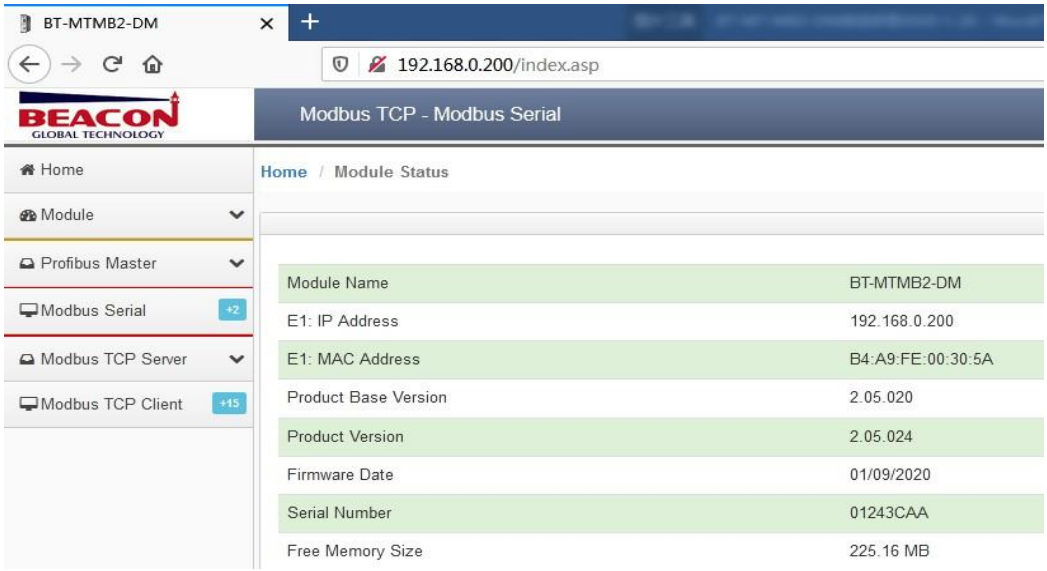
804 数据为 0，表示 Profibus-DP 4号站地址设备正常运行；

805 数据为 0，表示 Profibus-DP 5号站地址设备正常运行；

806 及以后的地址，数据均为 4，表示 Profibus-DP 6 号站地址（及以后站号）没有设备。

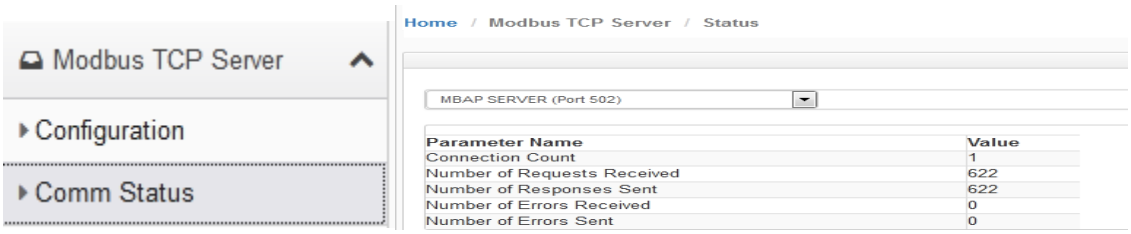
配置模块做 Modbus TCP 从站

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



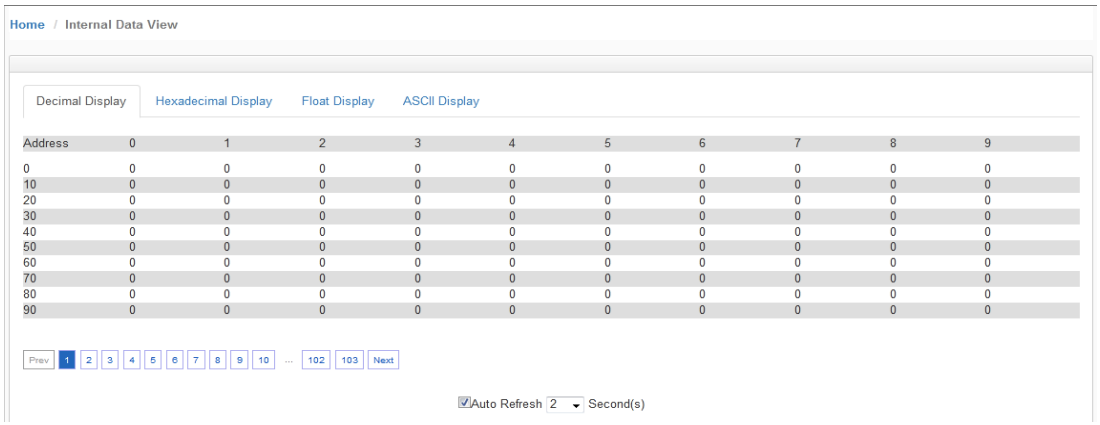
在左侧导航栏点击 Modbus TCP Server ---Comm Status 如下图：

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



模块内部寄存器对应着MODBUS TCP地址如下：Internal Data模块内部寄存器同时提供MODBUS 4区，3 区，1区，0区的访问。模块内部寄存器0对应着40001，同时对应着30001，同时对应着10001-10016，同时对应着00001-00016。

注意先要确认模块的内部寄存器数据区大小，点击 Internal Data View，可以查看模块内部寄存器数据动态的显示值，每个寄存器是 16 位的 WORD 格式，数据区的大小和模块具体型号有关联，不同型号模块的内部寄存器的数据区不一样。每页可显示100个 16 位的寄存器。

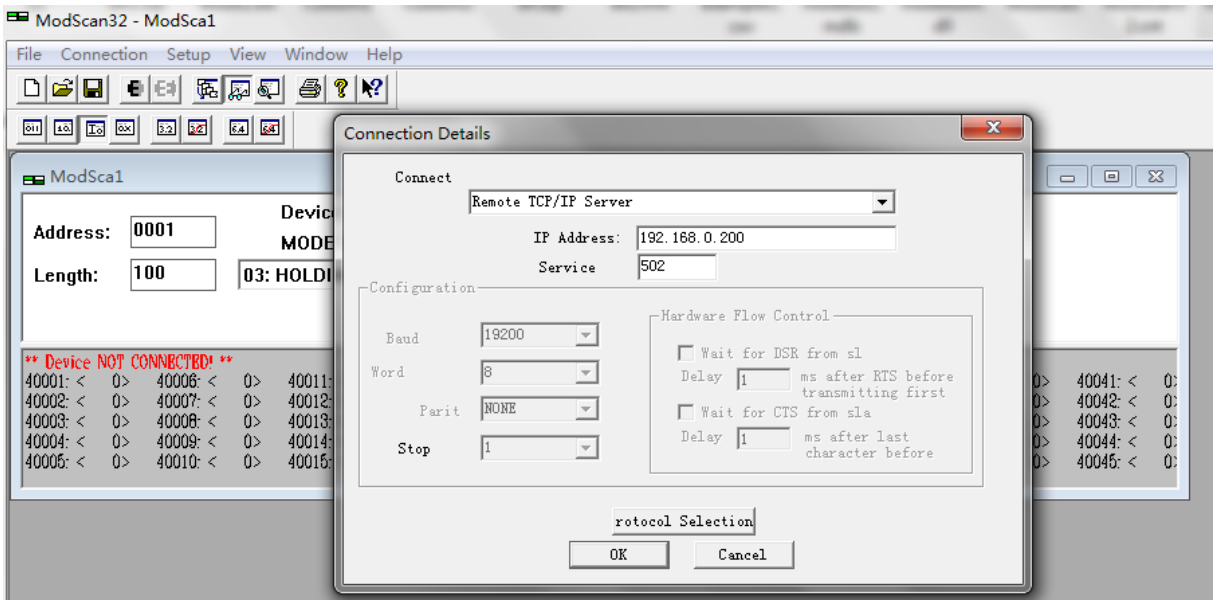


模块内部寄存器和 Modbus 读取区域的对应关系如下：

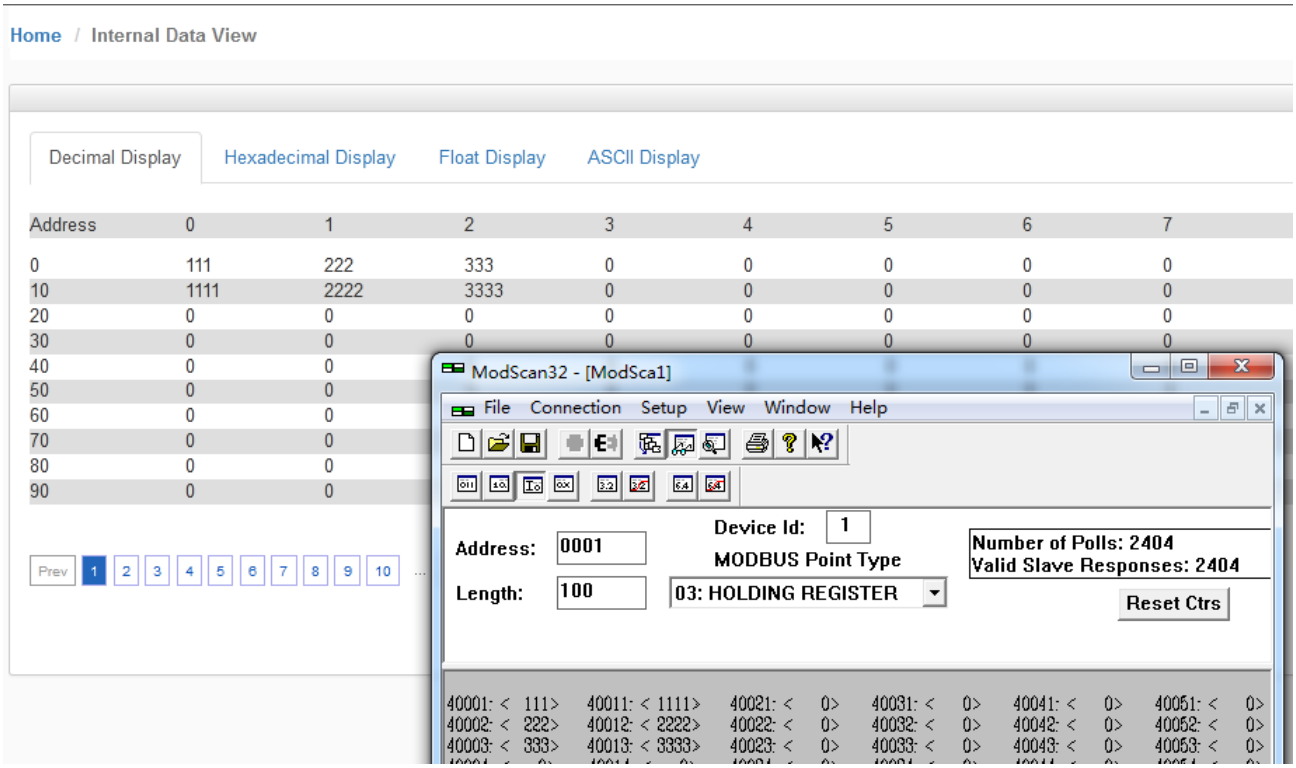
模块内部寄存器地址	等于	Modbus4区地址	等于	Modbus3区地址	等于	Modbus1区地址	等于	Modbus1区地址	等于	Modbus0区地址	等于	Modbus0区地址

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

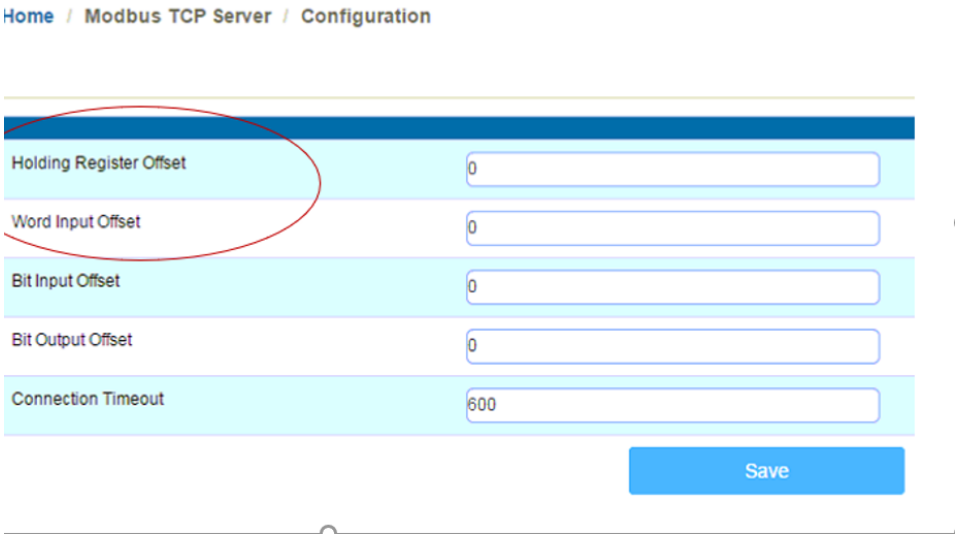
打开MODBUS TCP仿真软件MODSCAN32,作用是仿真MODBUS TCP主站。使用功能码FC03，读写模块内部数据区0-99 的连续 100 个字的数据，40001 对应着内部寄存器 0 ,40100 对应着内部寄存器 99 ,以此类推。选择 Connection，选择 Remote TCP/IP Server ，填写模块 E1 口的 IP 地址 192.168.0.200，端口号默认 502。 然后点击OK。



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

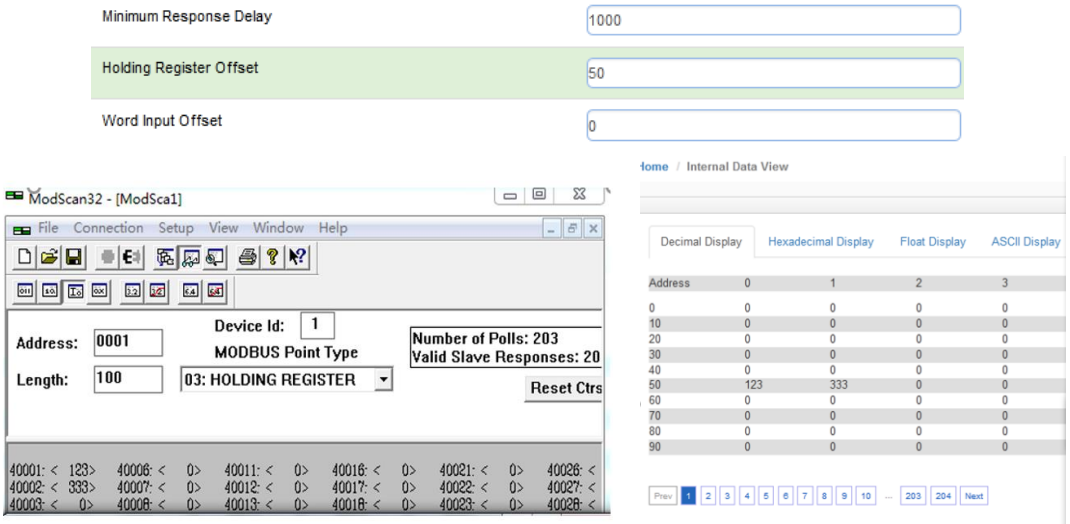


模块设置成为Modbus TCP从站的时候，在configuration界面中，可以看到下图两个选项。

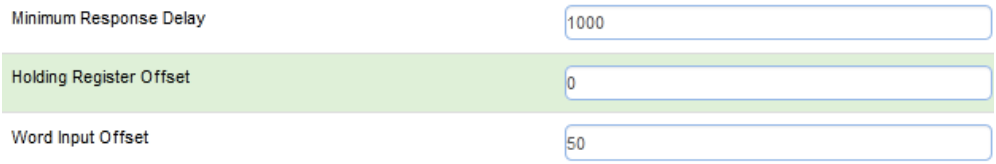


Holding Register Offset使用方法：

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



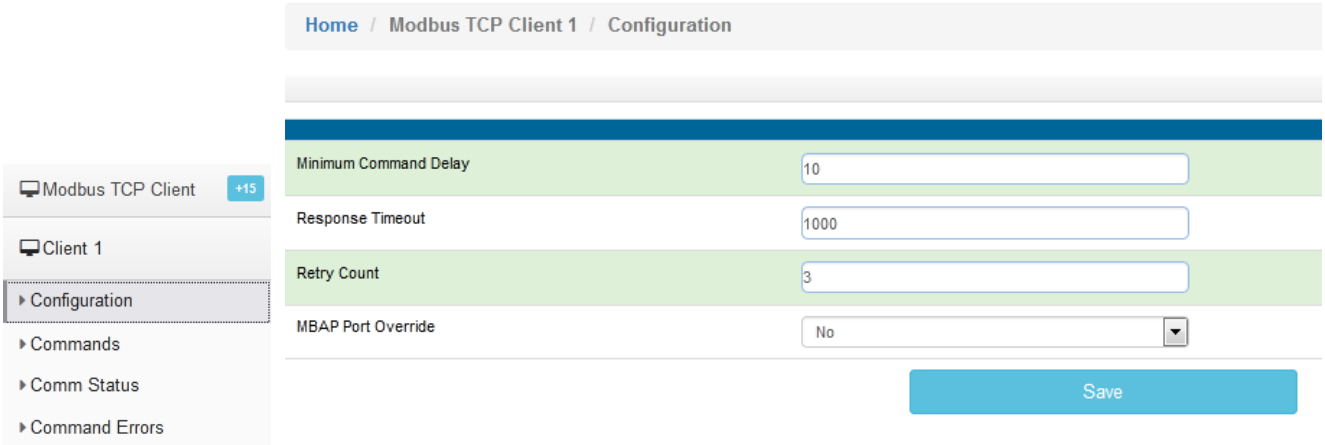
Word Input Offset使用方法：如果此处偏移量设置成50(如下图)，Modbus TCP主站一侧在3区对30001和30002输入两个数据，数据会直接向后偏移放到模块内部寄存器50-51里面，ModScan32仿真软件不能载入3区的数值，请以现场设备实际数据区域来填写。



配置模块做 Modbus TCP 主站

注：模块的 Modbus TCP 端口可以同时支持作为主站和从站，由于 Profibus-DP 主站可连接的从站设备类型和数量较多，故在使用该模块和支持Modbus TCP 协议的PLC或DCS通讯的时候，建议采用配置模块作为 Modbus TCP 从站。如果采用配置模块作为 Modbus TCP 主站，请谨慎使用，该功能如果使用在需要传输的 Profibus-DP 从站设备数量较多的情况下，则需要添加多条 Modbus TCP 主站指令，会增加配置工作量和模块 CPU 的负荷。做主站功能适用于连接另外的Modbus TCP的从站设备。

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



点开Configuration.查看默认的配置，此配置默认就可以使用。

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

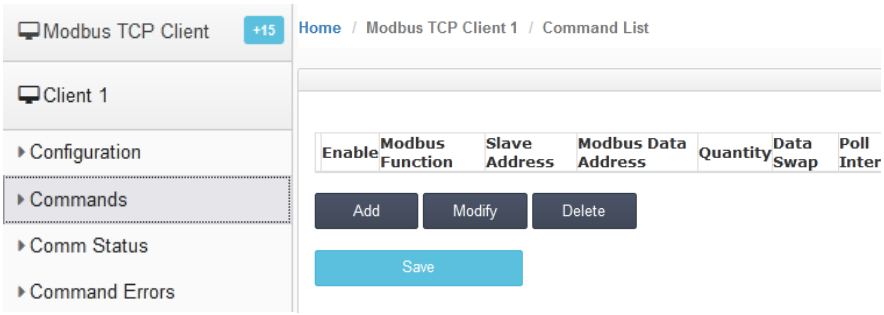
注：该时间越小，发送命令越快，但并非越小越好，需要先查看从站设备的说明书，确定从站响应时间是否能及时接受和反馈，主站发送命令的间隔。

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

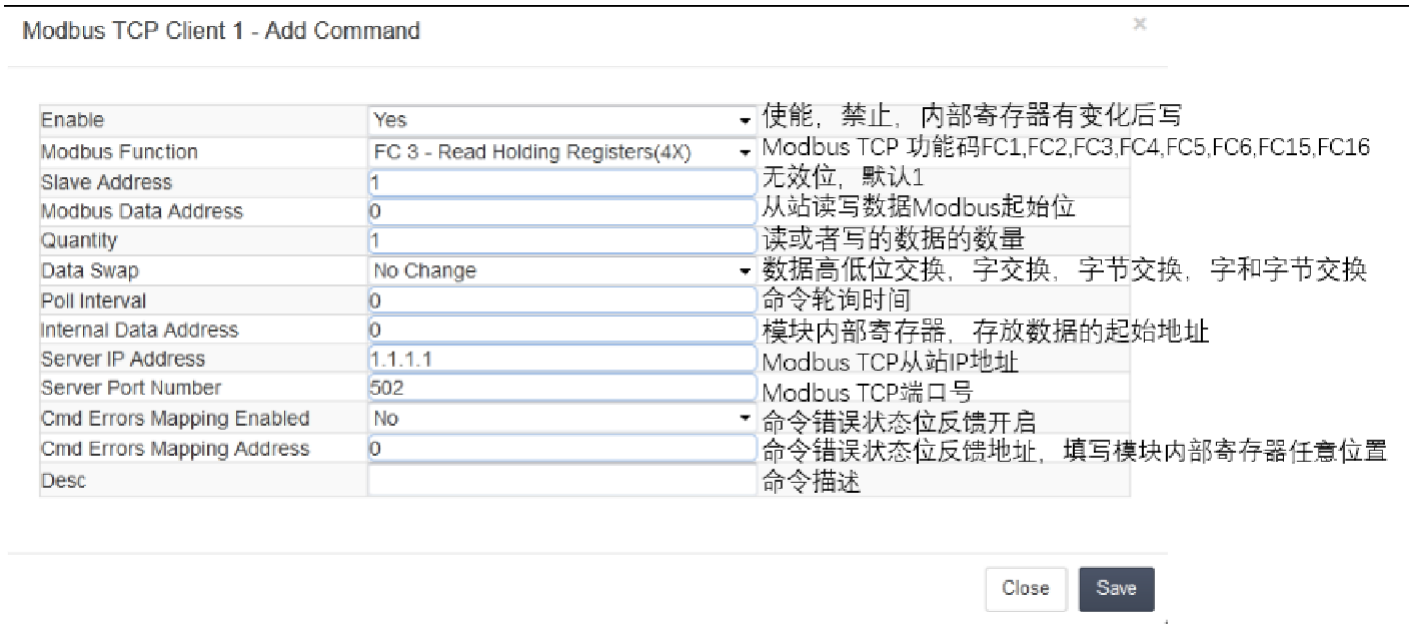
Retry Count：重新尝试连接次数　　0-65535

MBAP Port Override 端口 502 覆盖　　NO/YES

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



点击 Add,可以增加一条命令，命令如下：



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

注意，先要确认模块的内部寄存器数据区大小，以下指令均按照 4000 个字的数据区举例，实际配置模块时，请严格参照模内部数据区的范围。

Modbus TCP Client 1 - Add Command

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
Server IP Address	192.168.0.177
Server Port Number	502
Cmd Errors Mapping Enabled	Yes
Cmd Errors Mapping Address	2501
Desc	

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

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

Modbus TCP Client 1 - Add Command

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

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

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

Modbus TCP Client 1 - Add Command

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

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

Modbus TCP Client 1 - Add Command

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

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

配置模块做 Modbus RTU 主站

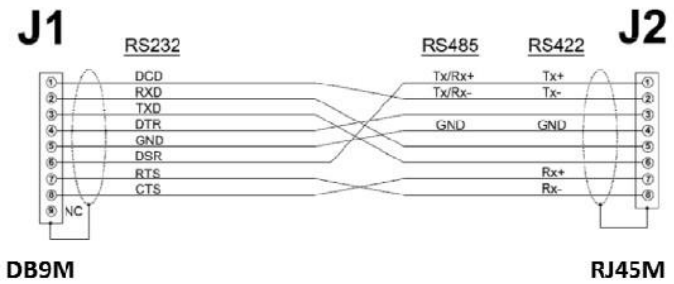
MB指的通讯协议是MODBUS RTU，接线方式提供RS232/422/485三种可以选择。MB2代表2个MODBUS RTU接口，S1，S2 MODBUS RTU接口可以自由选择做主站或者从站。

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，MODBUSRTU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

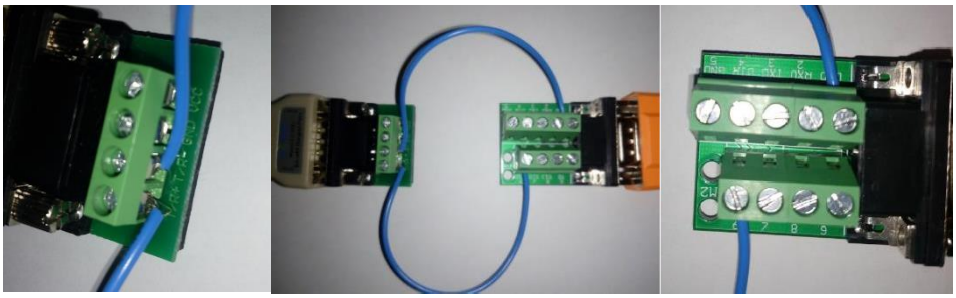
上图为S1/S2端口的接线图

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-



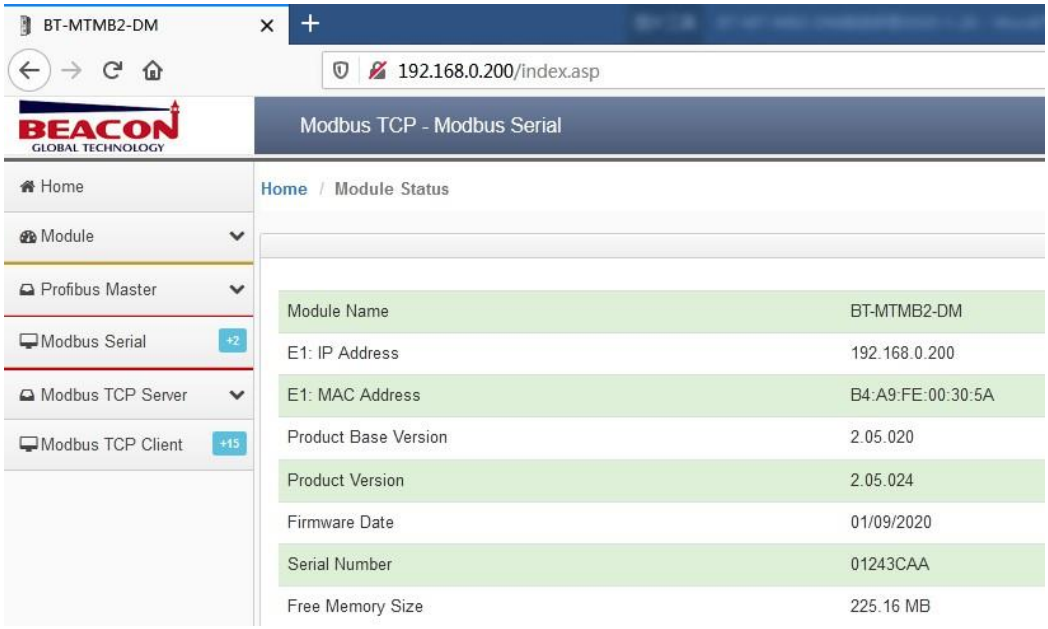
或水晶头直插网关串口。

举例：S1口引出来RS232接口，端子2RX，3TX，5GND接线。

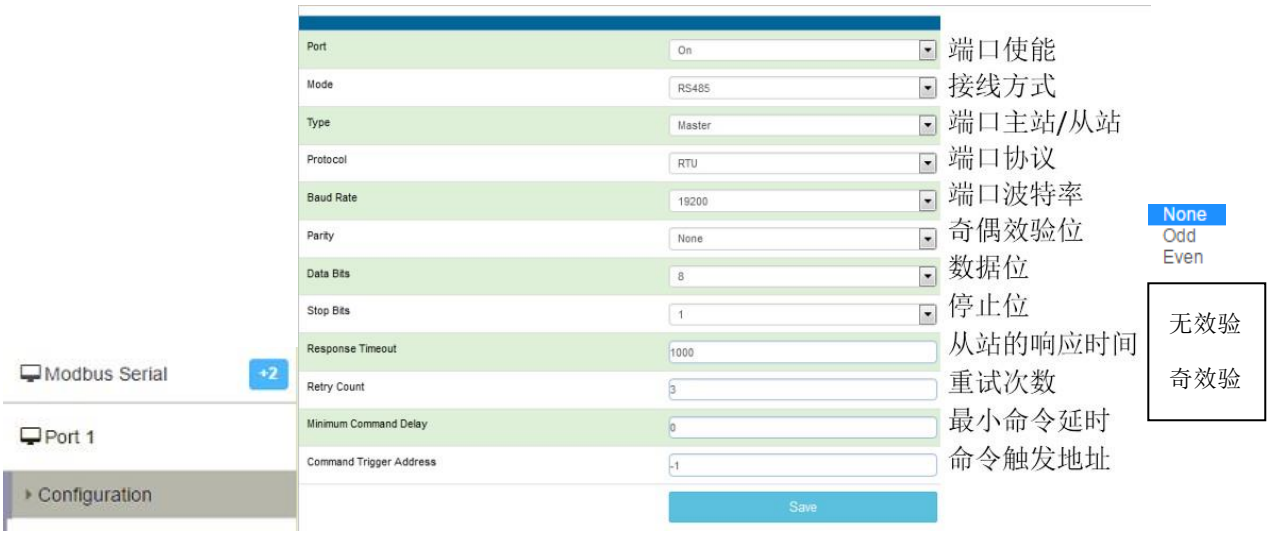
如果选用RS232接线方式，每个串口只能连接一个从站，接线长度不能超过15米。注意不能热插拔串口，容易

对串口造成不必要的损坏。

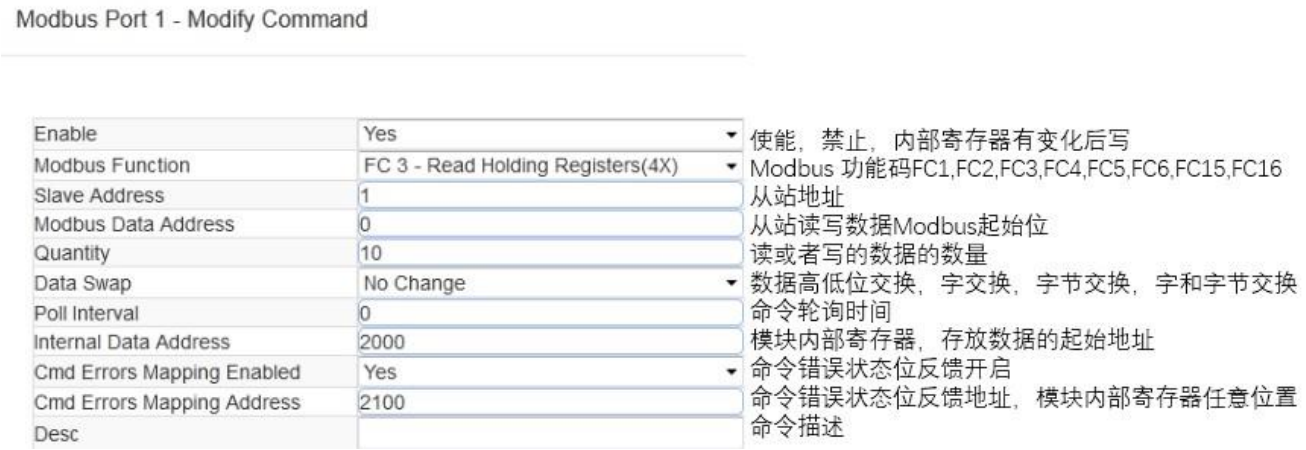
打开浏览器，进入模块主配置页面，如下图：



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：

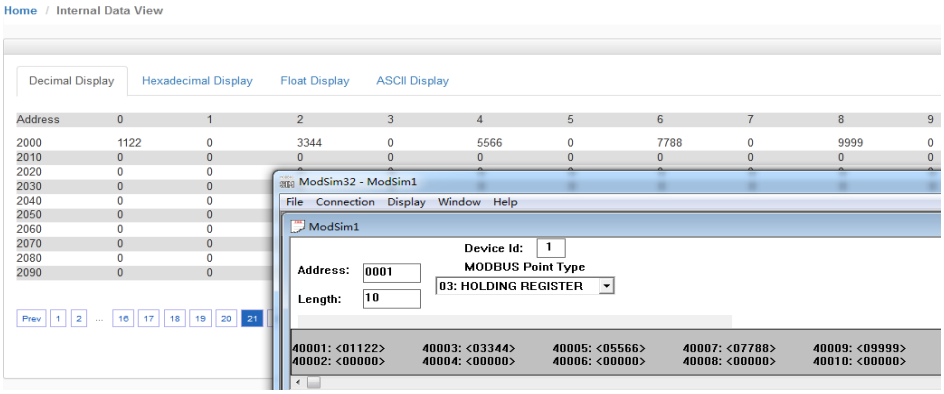


Cmd Errors Mapping Enabled和Cmd Errors Mapping Address这两个参数；

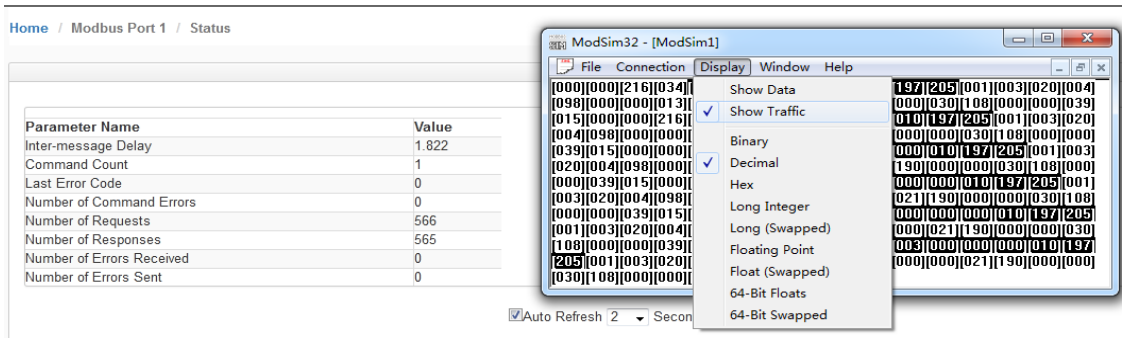
Cmd Errors Mapping Enabled表示命令错误是否映射，选择YES表示使用，选择NO，表示不使用；

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。Modbus功能码和指令的使用方式和上文中Modbus TCP一致，此章节省略。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。

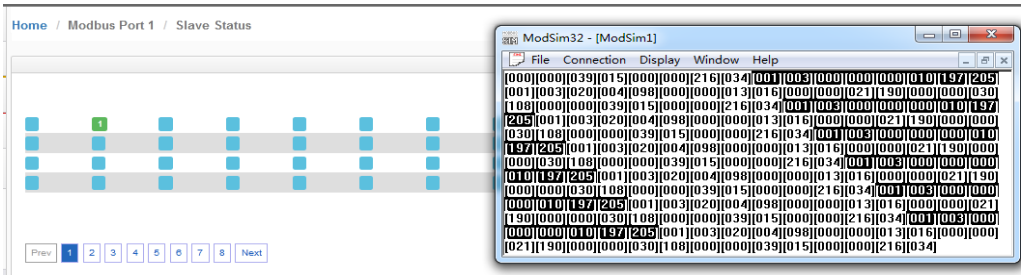


通过查看从站状态可以直接看到从站的状态，1-31路都可以直观看到：

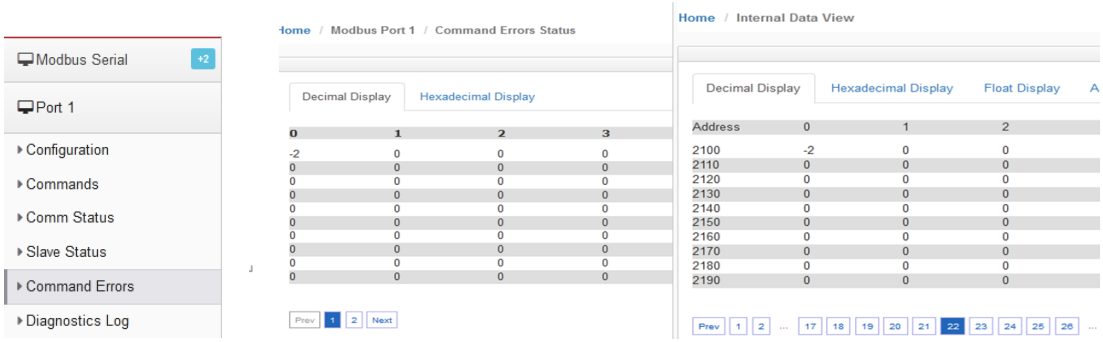
绿色表示线路数据通讯报文都正常；

红色表示线路数据通讯报文都不对；

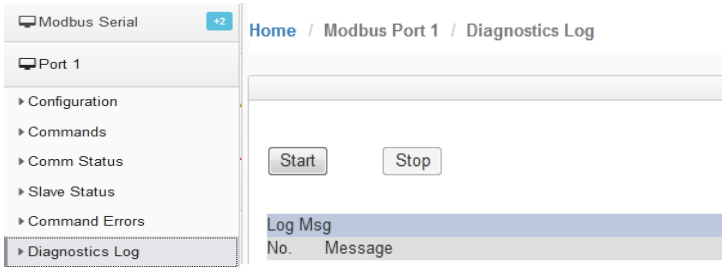
绿色和红色闪烁表示线路正常，数据通讯报文不正常。



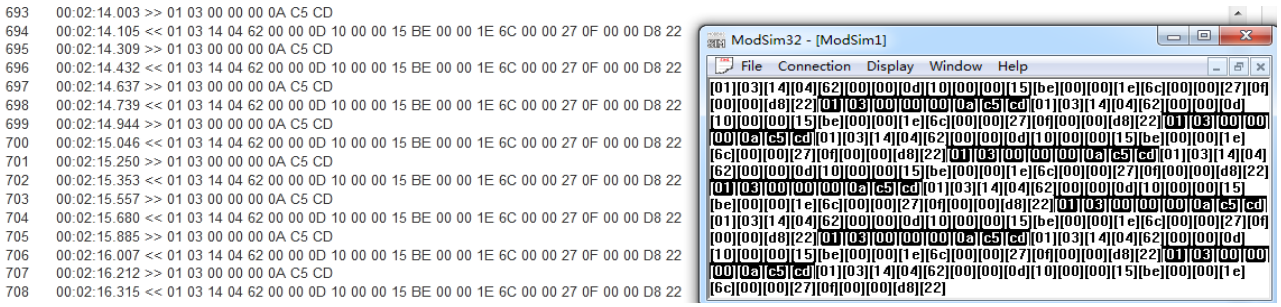
通过查看命令错误可以看到从站报的错误值，如果开启了命令反馈功能，这个值也会送到工程师填写的命令错误存放地址(寄存器地址2100)里面。



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。

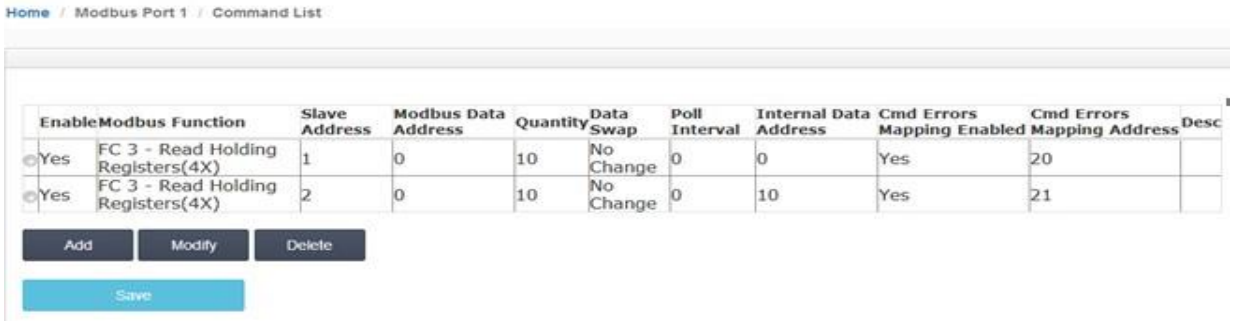


下图为主站发送和接收的报文以十六进制格式显示，Modsim32也可以从十进制报文切换到十六进制报文显示：



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。

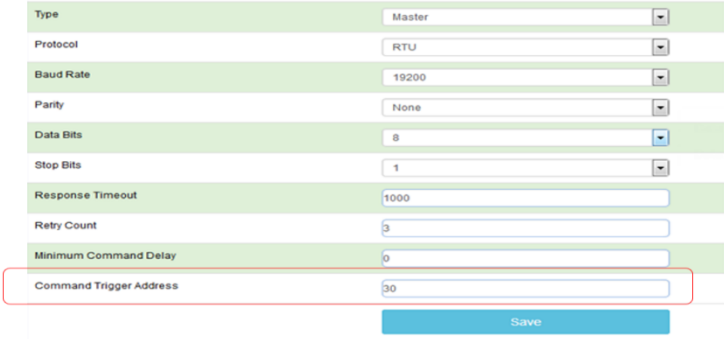


上图中建立两条指令：

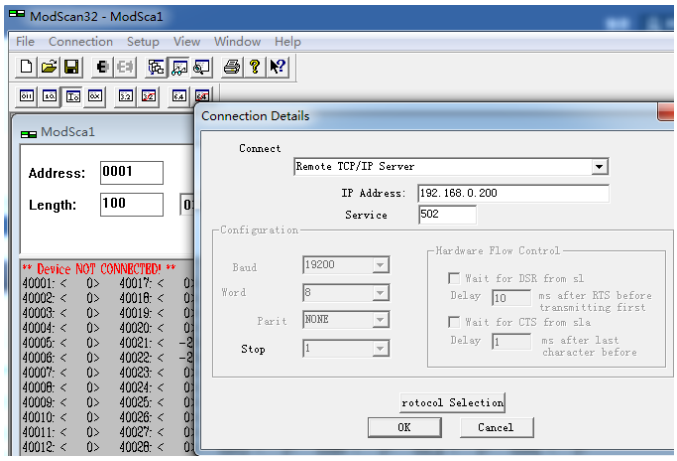
1- 读1号从站的40001-40010到内部寄存器0-9，错误状态放在了内部寄存器20。

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

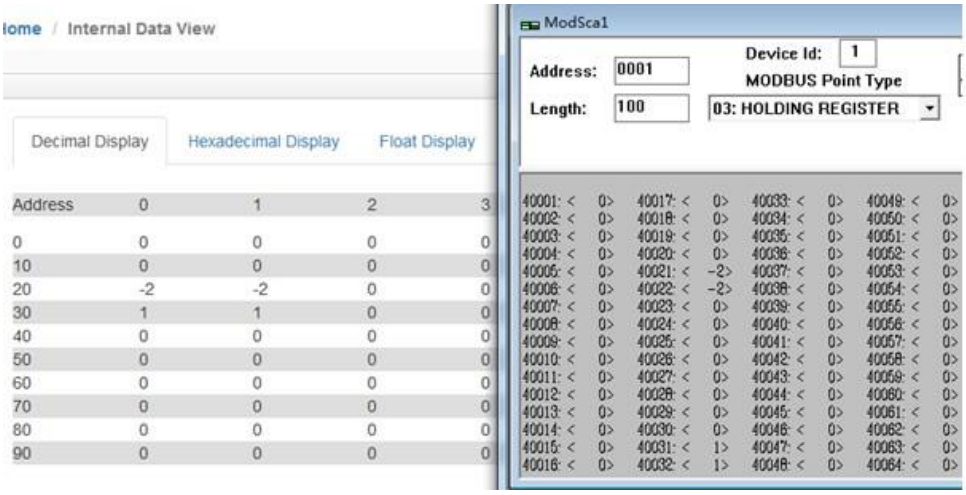
3- 使能命令触发地址，在模块Modbus主站端口配置页面中，Command Trigger Address设置成30，如下图，表示使用模块内部起始地址为30的寄存器作为触发条件。然后保存，重启生效。



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。

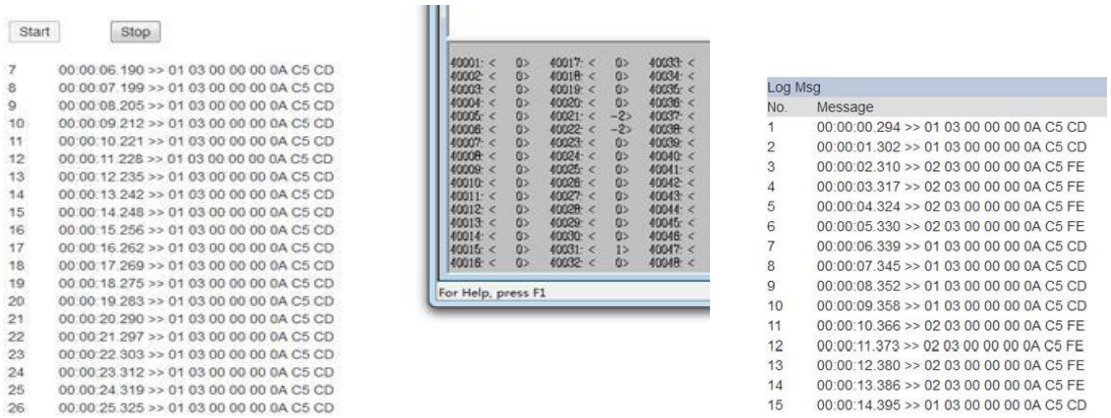


直观表现如下：检查Port1报文发送情况，显示第一条命令发送4次，第二条命令发送4次。因为命令本身发送1次，如果找不到从站设备，该命令会重新发送3次，共计4次。

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。

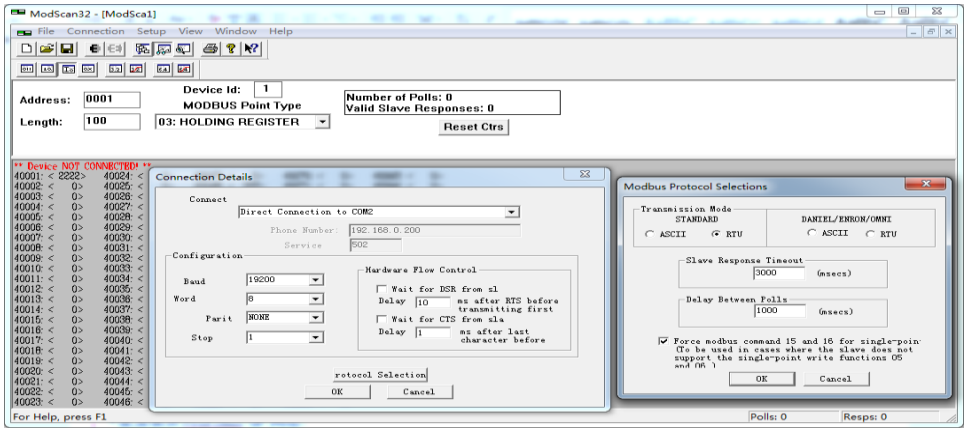
该功能建议配合前文提到的命令反馈功能一并使用，当其中一个命令返馈回来出现非 0 值，PLC 的程序可以自动关联这个触发值去停止 Modbus 指令的执行。

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：

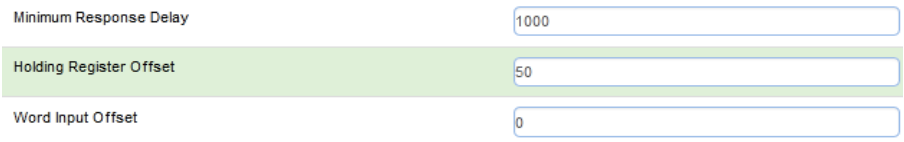
使用ModScan32仿真Modbus RTU主站，可以对模块内部寄存器读写。

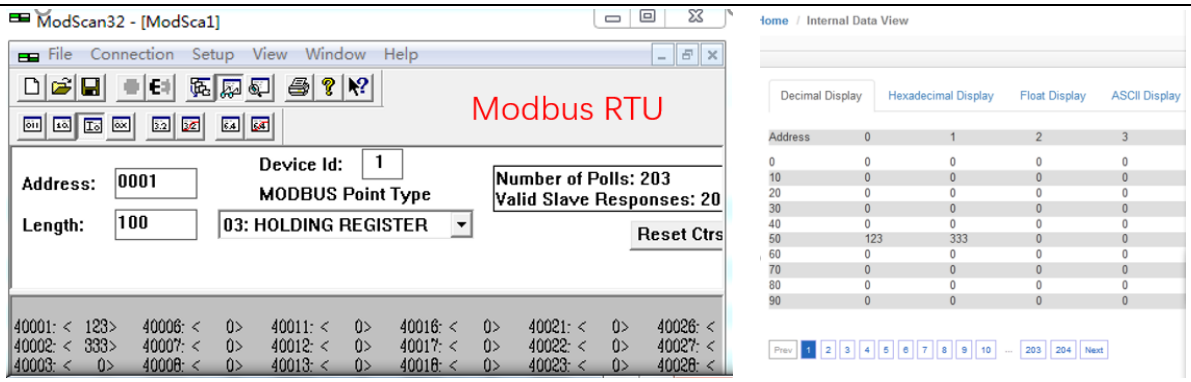


内部寄存器与Modbus数据对应关系：

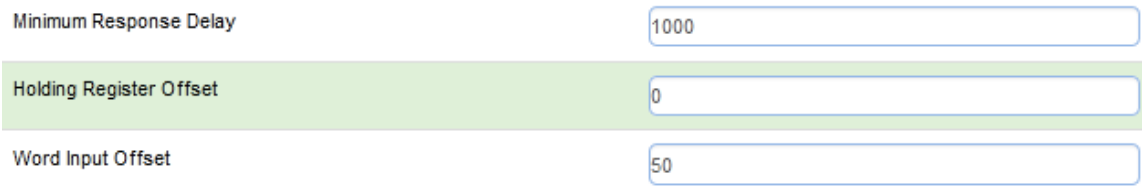
模块内部寄存器地址	等于	Modbus4区地址	等于	Modbus3区地址	等于	Modbus1区地址	等于	Modbus1区地址	等于	Modbus0区地址	等于	Modbus0区地址
0	=	40001	=	30001	=	10001	至	10016	=	00001	至	00016
1	=	40002	=	30002	=	10017	至	10032	=	00017	至	00032
10	=	40011	=	30011	=	10161	至	10176	=	00161	至	00176
11	=	40012	=	30012	=	10177	至	10192	=	00177	至	00192
20	=	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

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。





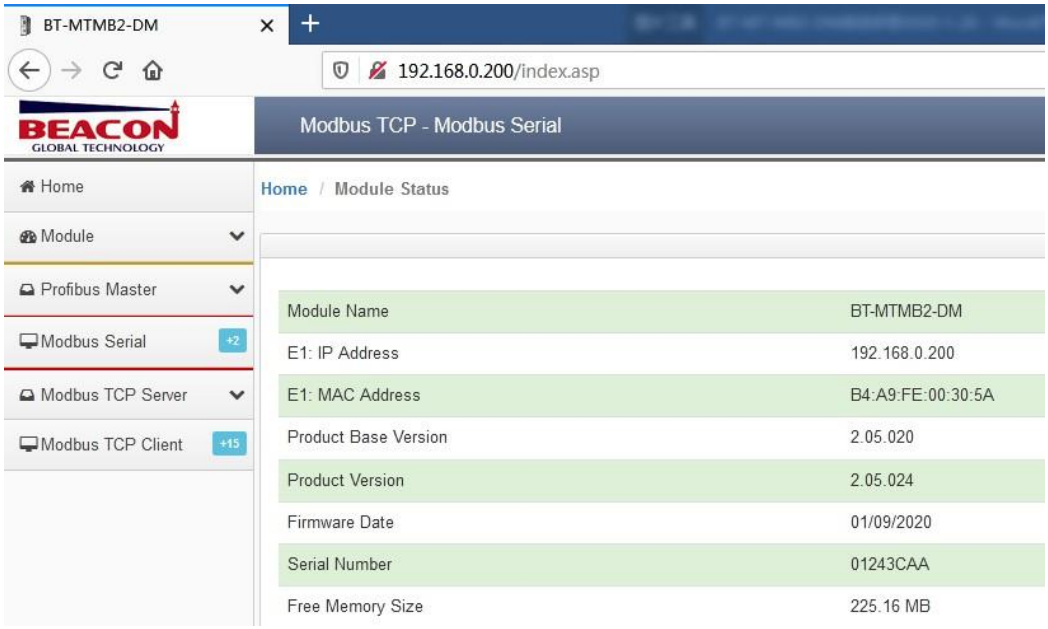
Word Input Offset使用方法：如果此处偏移量设置成50(如下图)，Modbus RTU主站一侧在3区对30001和30002输入两个数据，数据会直接向后偏移放到模块内部寄存器50-51里面，ModScan32仿真软件不能载入3区的数值，请以现场设备实际数据区域来填写。



举例 1.Modbus TCP 和西门子 PLC 之间数据交换

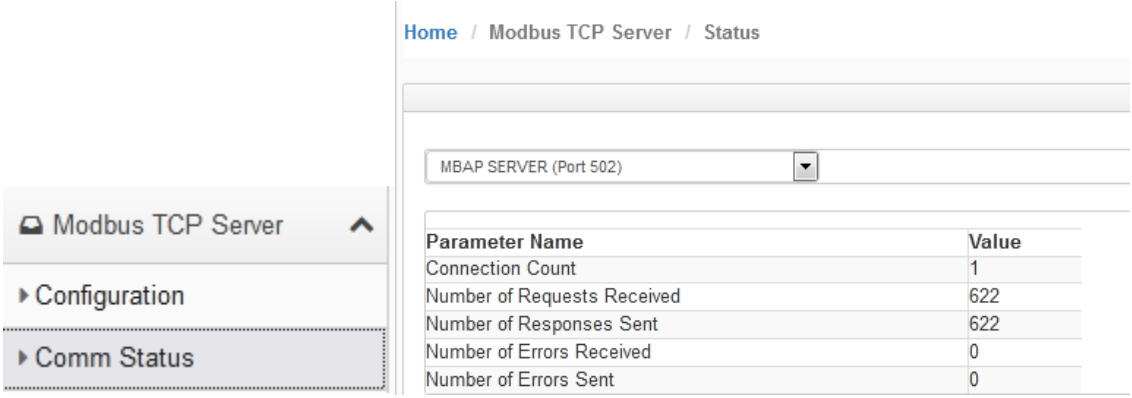
此案例中，模块的Modbus TCP驱动采用server方式。

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



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

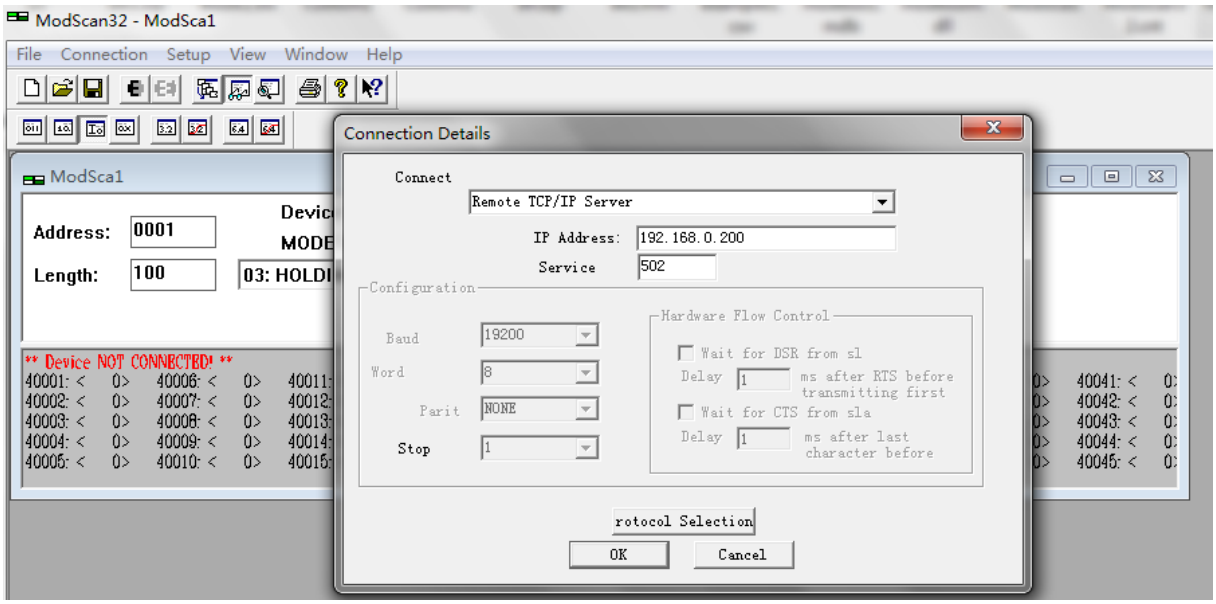
注：模块默认做MODBUS TCP从站，不需要任何设置，可同时被多个MODBUS TCP主站访问。



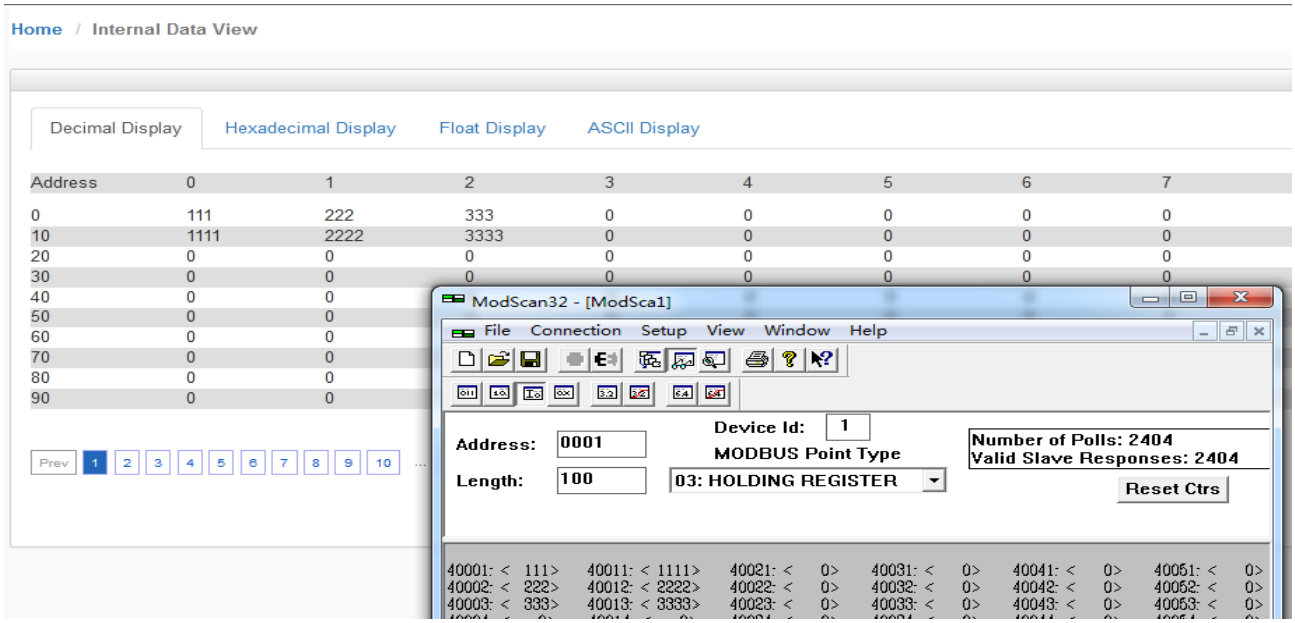
模块内部寄存器对应着MODBUS TCP地址如下：Internal Data模块内部寄存器同时提供MODBUS 4区 ，3 区，1区，0区的访问。模块内部寄存器0对应着40001，同时对应着30001，同时对应着10001-10016，同时对应着00001-00016。

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

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



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



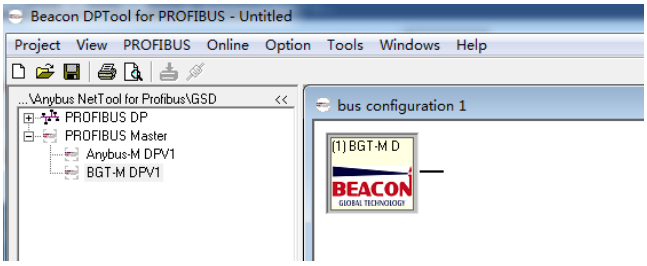
之后对模块 Profibus-DP 主站参数进行配置，具体内容请参考前文“组态 Profibus-DP 主站”。点开模块 Home ->Profibus ->Master Configuration（如下图所示）：

在该窗口中可以配置Profibus主站的输入数据量（Input data size）和输出数据量（Output data size）此参数可根据用户的实际应用进行设置。此页面中 ：

DP 从站对于模块的输入起始地址为 0，代表模块作为 DP 主站读取 DP 从站数据，存储在模块内部数据区的起始地址。

模块对于 DP 从站输出起始地址为 1500，代表模块作为 DP 主站写给 DP 从站数据，调用模块内部数据区的起始地址。

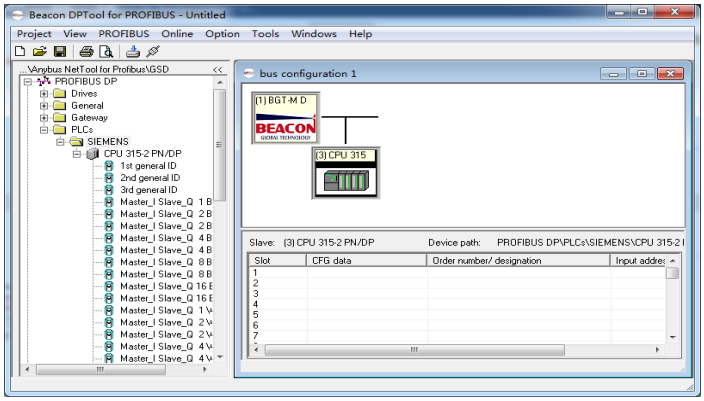
在电脑中双击 软件，进入 PROFIBUS-DP 组态页面，点击左上角新建项目。之后拖动 BGT-M DPV1图标到右侧bus configuration 1的空白页面里面。



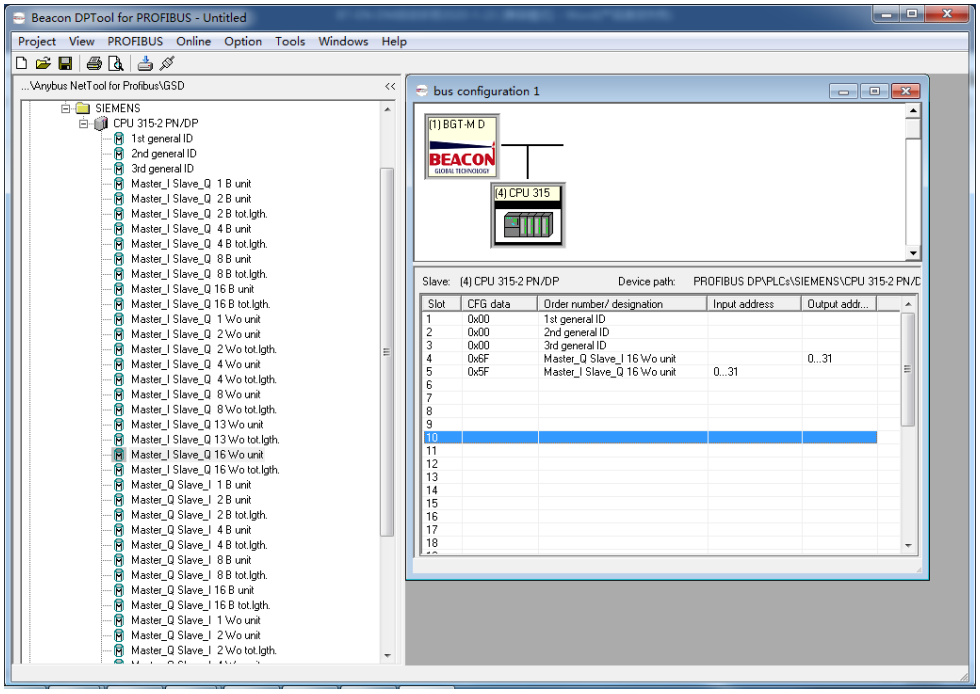
然后双击 图标显示 DP 主站配置的界面，对主站参数进行配置，具体内容请参考前文“组态 Profibus-DP 主站”。 之后安装新的 DP 从站 GSD 文件。鼠标右键点击 PROFIBUS DP，出现 Install new GS*-file… ，选择导入对应的 DP 从站 GSD 文件。

拖动DP从站设备加入到DP网络中进行组态，双击图标 ，从站会弹出从站属性对话框，我们在这里可以对从站设备的一些属性参数进行设置。具体内容请参考前文“组态 Profibus-DP 从站”。

这时 DP 从站的 IB0—IB31 和 QB0—QB31 的数据就可以和这个 Profibus-DP 主站模块进行数据交换了。如果增加两个或多个输入输出模块，Input address 和 Output address 会随着模块的增加自动分配Profibus地址。



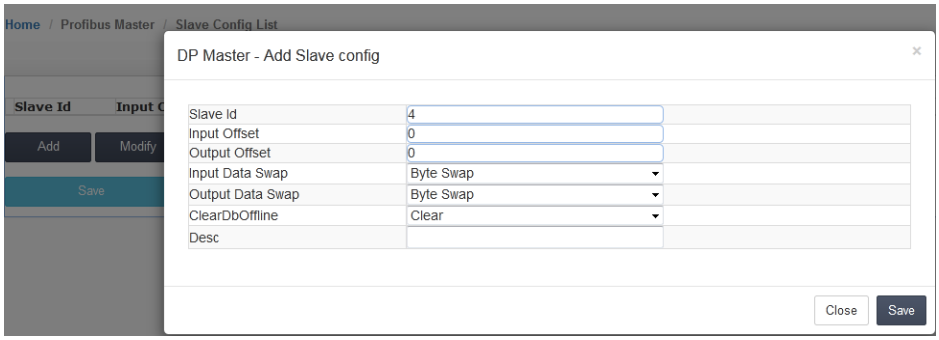
首先我们展开导入的从站设备，展开后我们可以看到一个配置数据列表，该列表根据所选从站设备的不同，GSD 文件的不同，配置列表也不同。添加西门子 315-2PN/DP PLC 的 GSD 文件，点击从站设备，会弹出从站的配置表格，从这里我们添加从站的 IO 模块，左键点住 16 words in put 拖到右下表格中，这样一个 16 个 word 的输入模块我们就添加进来了，同理我们还可以添加一个16 words out put的输出模块。



点击保存Profibus DP网络配置并返回到主站设置窗口，将配置文件下载到模块里面。

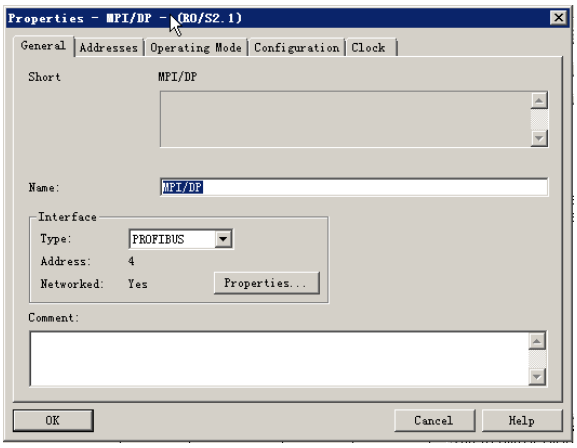
回到模块的网页配置界面（登录后操作），点击Slave Config List，点击Add按钮可以增加配置4号从站输入输出字节的高位和低位交换。 “ClearDbOffline”表示 DP 从站离线或者发生断线情况下，是否保留断线之前的数据，这里可以选择不清零或者清零。

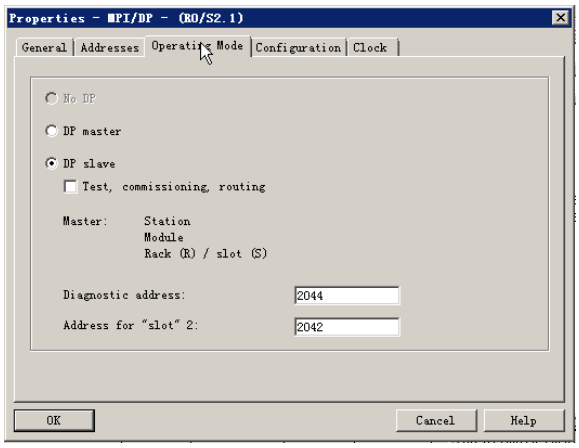
配置完成后，点击Save，提示Success成功。再点击配置列表里面的Save保存所有的配置。

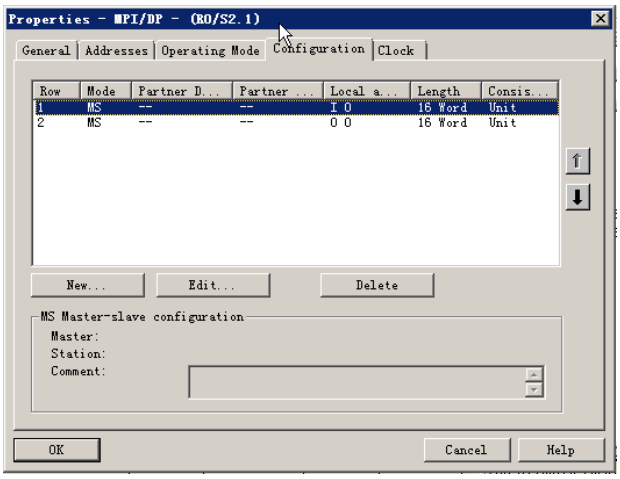


然后点击重启模块，使配置生效。

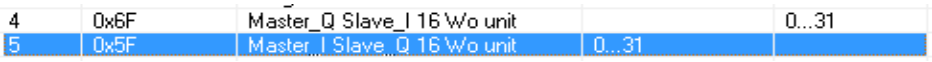
以上步骤便完成了模块作为DP主站和一个DP从站的通讯配置。同时西门子315-2PN/DP PLC作为DP从站的硬件设置如下：







配置好硬件后，下载到西门子CPU，之后点击PLC变量表查看输入输出关系，如下图：



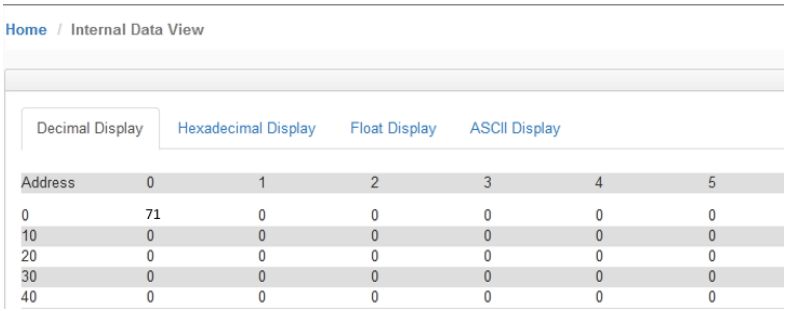
4	0x6F	Master_Q Slave_I 16 Wo unit		0...31
5	0x5F	Master_I Slave_Q 16 Wo unit	0...31	

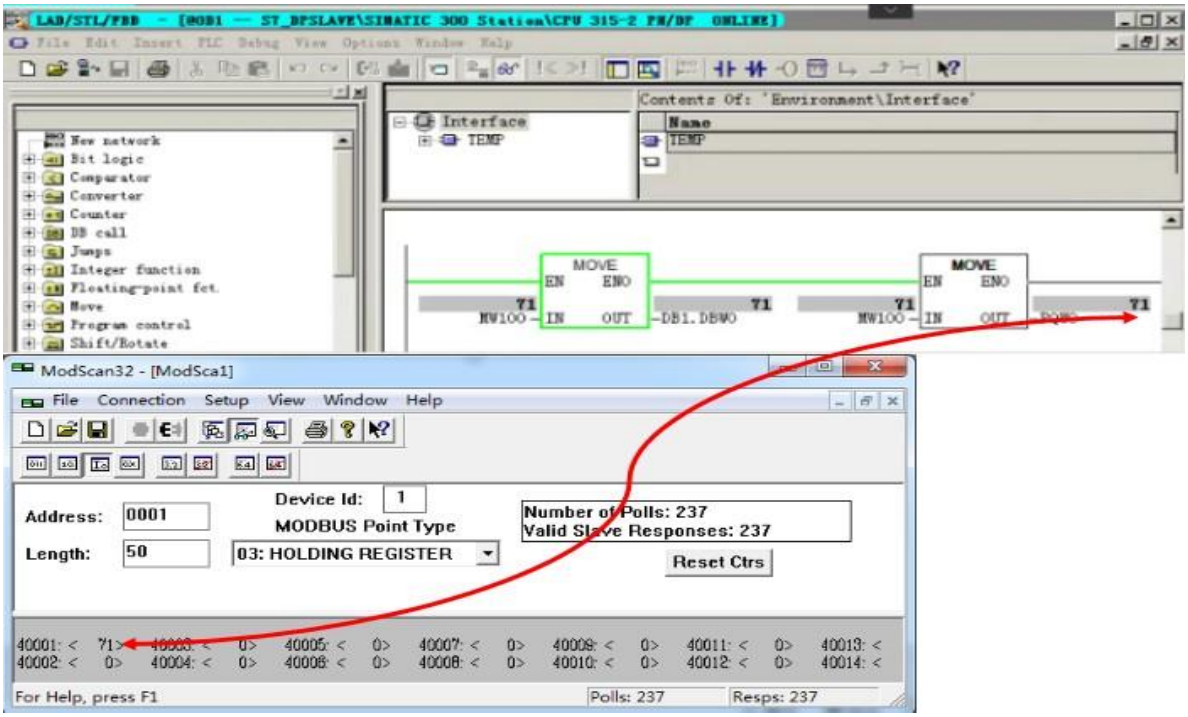
第一行是DP从站输入的16个字，对应模块（DP主站）输出区域，模块内部寄存器地址1500-1515。

第二行是DP从站输出的16个字，对应模块（DP主站）输入区域，模块内部寄存器地址0-15。

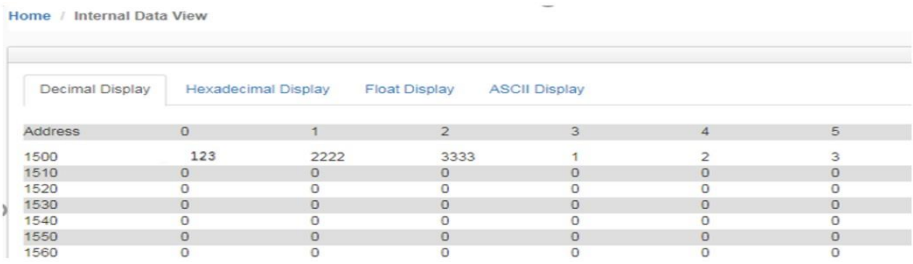
下图为模块内部寄存器地址区域分配的配置：

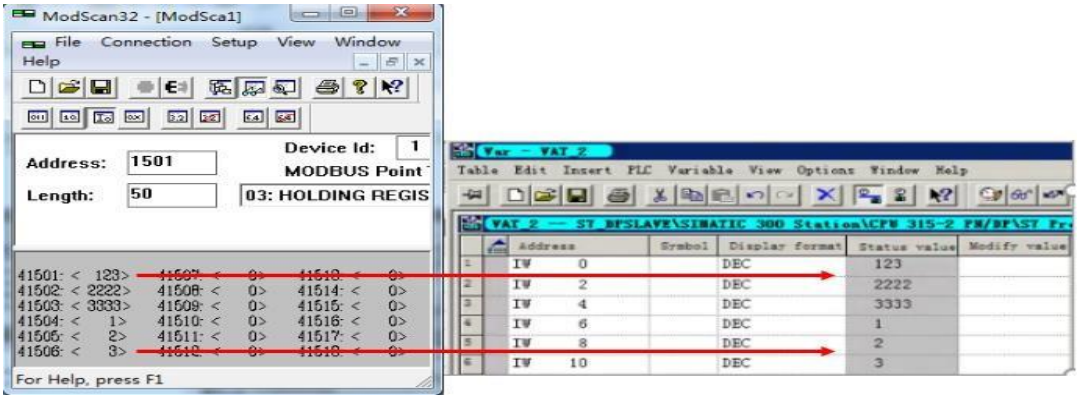
先清除掉刚才 ModScan32 软件对模块内部寄存器写入的数据。之后在西门子 PLC（DP 从站）的程序内给定 PQW0 的输出一个值，查看模块内部寄存器 0，同时查看 ModScan32 与 Modbus TCP server 连接，仿真软件里面 40001 获取到该数值。



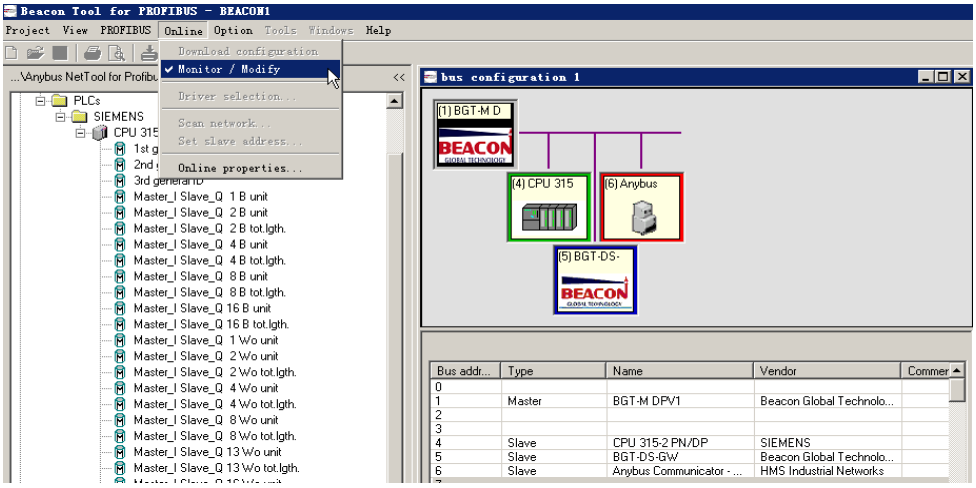


ModScan32 与 Modbus TCP server（模块以太网端口）连接，仿真软件里面 41501，41502，41503，41504，41505，41506 数值中给定一些数值，同时查看模块内部寄存器 1500-1505，并且在西门子 PLC（DP 从站）输入的值可看到 PIW0- PIW10的输入值，与ModScan32中给出的数值一致。

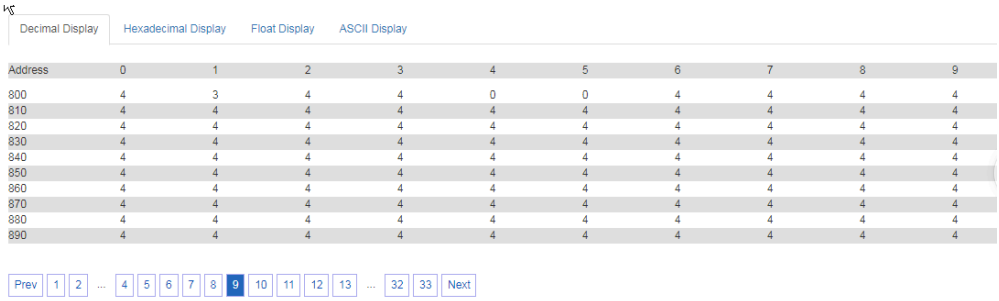




同样可以使Modbus TCP主站获取DP从站在线和离线状态。



在配置软件中，从站绿色外框表示从站 GSD 文件正确；从站蓝色外框（红色外框偶尔闪烁）表示从站 GSD 文件不正确，或者 GSD 文件配置的输入和输出与从站的输出和输入字节数不相符 DP 线路正确；从站红色外框表示从站线路不正确，有可能是DP中断电阻拨码不对或者是线路没有按照Profibus-DP 标准来接线。先查看模块内部寄存器起始地址为 800 的区域。



在模块的内部寄存器页面中，如上图：

800数据为4，表示Profibus-DP0号站地址没有使用设备；

801数据为3，表示1号站地址是主站，主站正常运行状态；

802数据为4，表示Profibus-DP2号站地址没有使用设备；

803数据为4，表示Profibus-DP3号站地址没有使用设备；

804数据为0，表示Profibus-DP4号站地址设备正常运行；

805数据为0，表示Profibus-DP5号站地址设备正常运行；

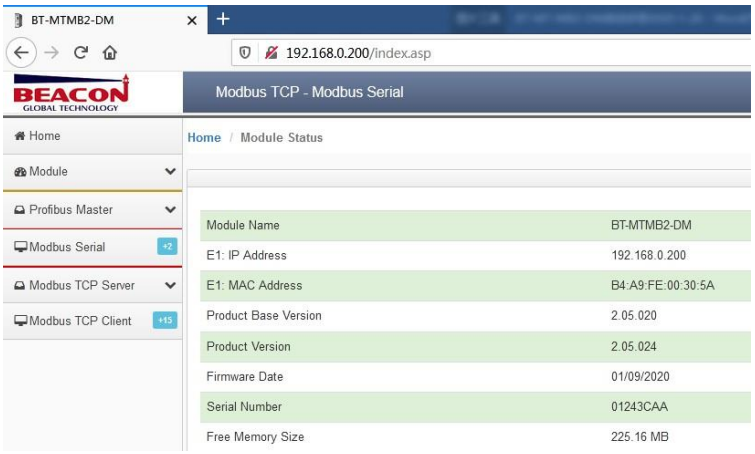
806 及以后的地址，数据均为 4，表示 Profibus-DP6 号站地址（及以后站号）没有设备。从802以后的状态值0表示从站正常运行，4表示从站离线状态，对应Modbus32地址标签组如下，

内部寄存器地址	Modbus 地址
800	40801
801	40802
**	**
926	40927

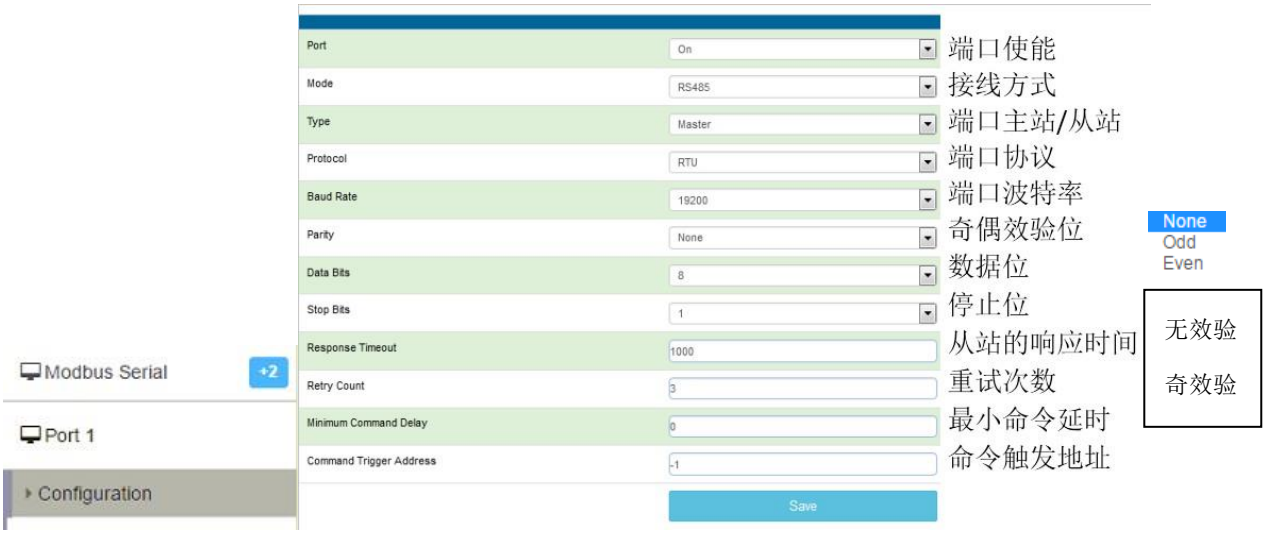
关于如何通过模块的 Modbus TCP 协议，连接各类 Modbus TCP 从站例如变频器，PLC，现场仪表等设备的内容，可以参考前文提到的“配置模块做 Modbus TCP Client”，者和BEACON办事处进行咨询。

举例 2.Modbus RTU 和西门子 PLC 之间数据交换

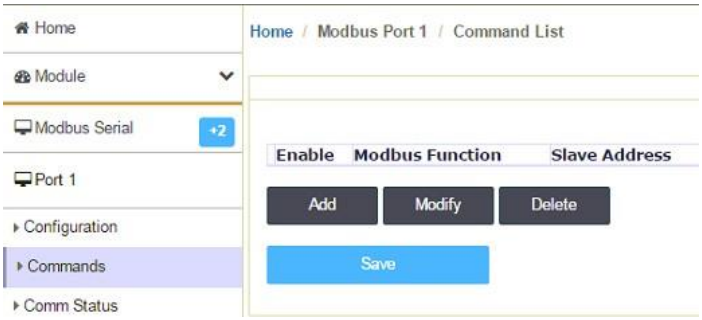
此案例中，模块的Modbus 串口驱动采用Master方式。打开浏览器，进入模块主配置页面，如下图：



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：



接着点击Port1里面的“Commands”显示S1端口命令的配置页面，点击Add。



如下图添加一条Modbus串口主站指令：

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	1500	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

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1500的连续10个寄存器内（1500-1509），如果发送错误，错误反馈会放到内部寄存器2100里面。

通过查看命令状态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，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里面。

通过诊断报文，可以查看主站发送和接收的报文情况。

以上详细内容以及Modbus功能码和指令的使用方式，可以参考前文“配置模块作为Modbus RTU主站”中的内容。之后对模块Profibus-DP主站参数进行配置，具体内容请参考前文“组态Profibus-DP主站”。点开模块Home－>Profibus－>Master Configuration（如下图所示）

Home / Profibus Master / Configuration

Input Start Reg	0	模块作为DP主站读取DP从站的数据，到模块内部寄存器的起始位置
Input Data Size	768	模块作为DP主站读取DP从站的数据，到模块内部寄存器的总数据范围（16位字）
Output Start Register	1500	模块作为DP主站写给DP从站的数据，调用模块内部寄存器的起始位置
Output Data Size	768	模块作为DP主站写给DP从站的数据，调用模块内部寄存器的总数据范围（16位字
Input Byte Swap	NO	模块作为DP主站读取DP从站的数据，整体高低8位字节相互交换
Output Byte Swap	NO	模块作为DP主站写给DP从站的数据，整体高低8位字节相互交换

在该窗口中可以配置Profibus主站的输入数据量（Input data size）和输出数据量（Output data size）此参数可根据用户的实际应用进行设置。此页面中：

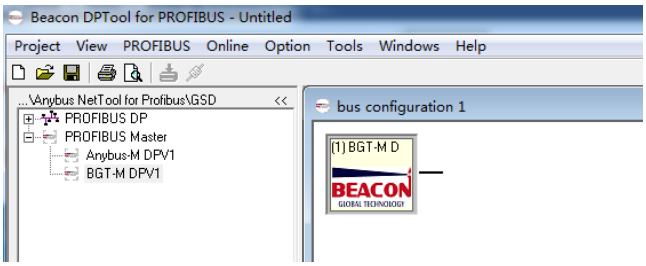
DP从站对于模块的输入起始地址为0，代表模块作为DP主站读取DP从站数据，存储在模块内部数据区的起始地址。

模块对于 DP 从站输出起始地址为 1500，代表模块作为 DP 主站写给 DP 从站数据，调用模块内部数据区的起始地址。

在电脑中双击

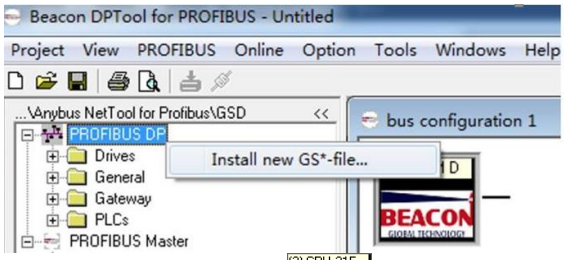
软件，进入PROFIBUS-DP组态页面，点击左上角新建项目。之后拖动BGT-MDPV1图标到右侧

bus configuration1的空白页面里面，



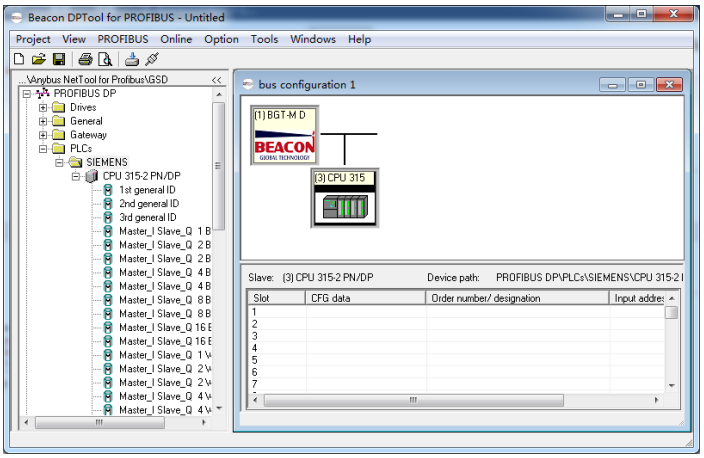
然后双击 图标显示DP主站配置的界面，对主站参数进行配置，具体内容请参考前文“组态Profibus-DP主站”。

之后安装新的DP从站GSD文件。鼠标右键点击PROFIBUS DP，出现Install new GS*-file…，选择导入对应的DP从站GSD文件。

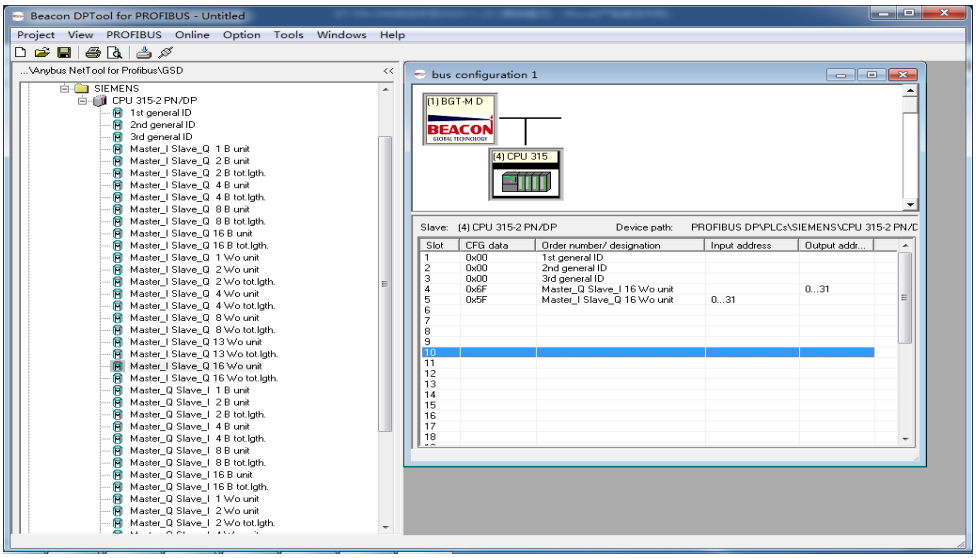


拖动DP从站设备加入到DP网络中进行组态，双击图标 。从站会弹出从站属性对话框，我们在这里可以对从站设备的一些属性参数进行设置。具体内容请参考前文“组态Profibus-DP从站”。

这时DP从站的IB0—IB31和QB0—QB31的数据就可以和这个Profibus-DP主站模块进行数据交换了。如果增加两个或多个输入输出模块，Input address和Output address会随着模块的增加自动分配Profibus地址。



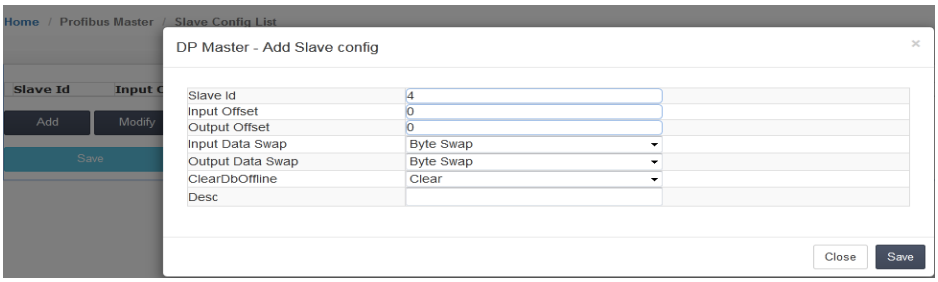
首先我们展开导入的从站设备，展开后我们可以看到一个配置数据列表，该列表根据所选从站设备的不同，GSD文件的不同，配置列表也不同。添加西门子315-2PN/DP PLC的GSD文件，点击从站设备，会弹出从站的配置表格，从这里我们添加从站的IO模块，左键点住16 words input拖到右下表格中，这样一个16个word的输入模块我们就添加进来了，同理我们还可以添加一个16 words output的输出模块。



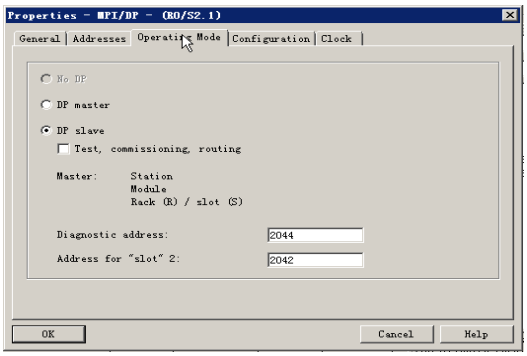
点击保存Profibus DP网络配置并返回到主站设置窗口，将配置文件下载到模块里面。

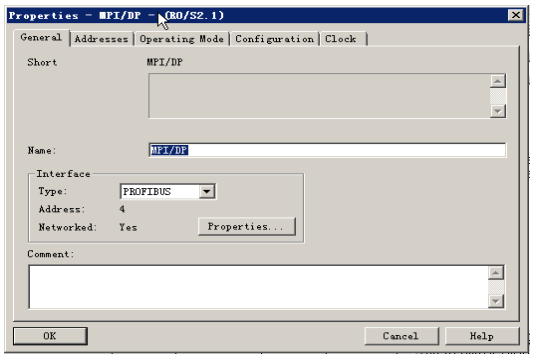
回到模块的网页配置界面（登录后操作）点击Slave ConfigList，点击Add按钮可以增加配置4号从站输入输出字节的高位和低位交换。“ClearDbOffline”表示DP从站离线或者发生断线情况下，是否保留断线之前的数据，这里可以选择不清零或者清零。

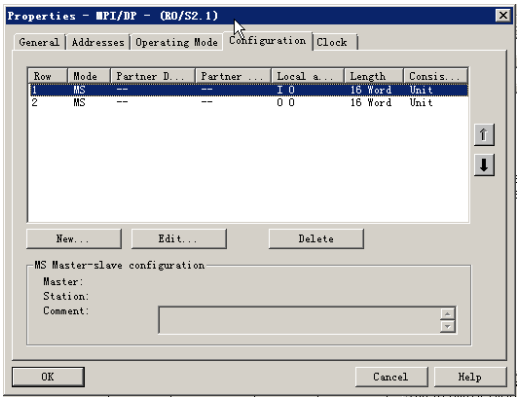
配置完成后，点击Save，提示Success成功。再点击配置列表里面的Save保存所有的配置。



然后点击重启模块，使配置生效。以上步骤便完成了DP主站模块和一个DP从站的通讯配置。同时西门子315-2PN/DP PLC作为DP从站的硬件设置如下：







配置好硬件后，下载到西门子CPU，之后点击PLC变量表查看输入输出关系，如下图：

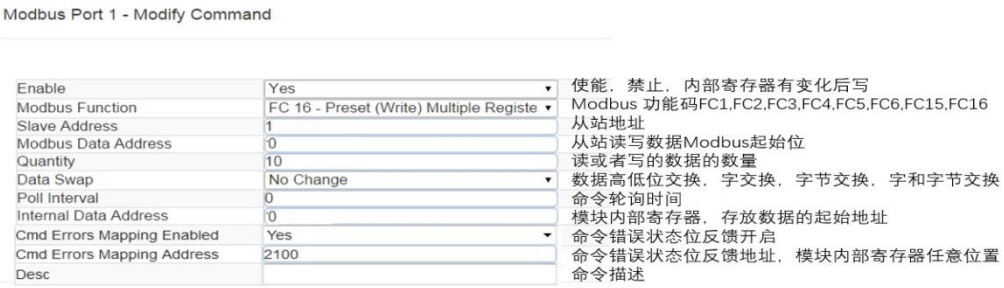
4	0x6F	Master_Q Slave_I 16 Wo unit		0...31
5	0x5F	Master_I Slave_Q 16 Wo unit	0...31	

第一行是DP从站输入的16个字，对应模块（DP主站）输出区域，模块内部寄存器地址1500-1515。

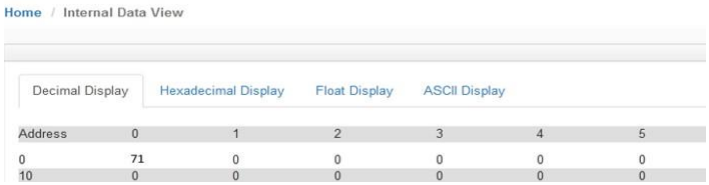
第二行是DP从站输出的16个字，对应模块（DP主站）输入区域，模块内部寄存器地址0-15。

下图为模块内部寄存器地址区域分配的配置：

如下图，我们在模块Modbus RTU主站一侧，使用功能码FC16建立一条写指令，从模块对1号Modbus从站写出一些数据，将调用模块内部寄存器地址0-9里面的数据，写入到Modbus从站40001-40010中去。

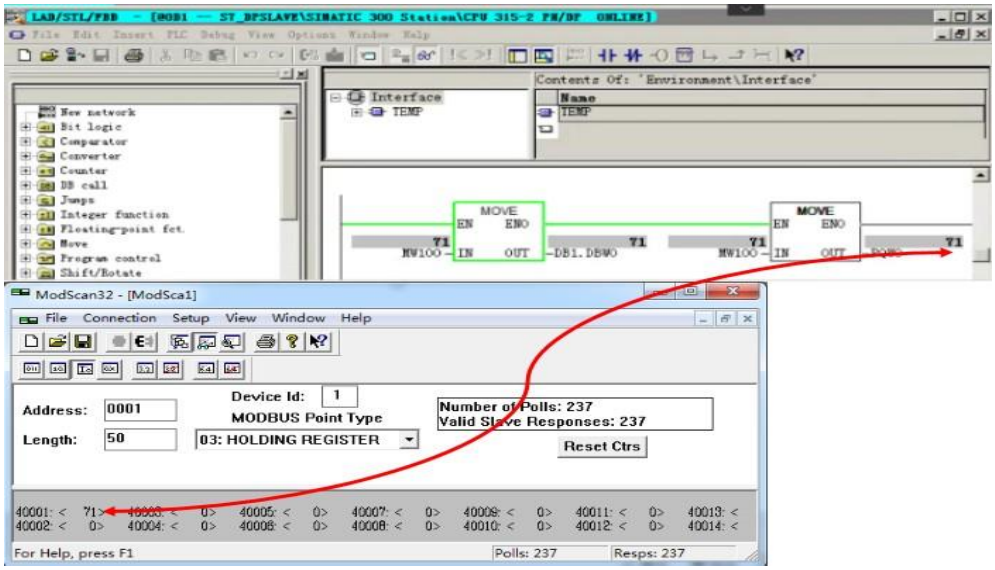


之后在西门子PLC（DP从站）的程序内给定PQW0的输出一个值，查看模块内部寄存器0收到了该数值。



我们采用ModScan32模拟Modbus从站与模块S1端口连接。

同时查看ModScan32仿真软件里面40001获取到模块Modbus主站端口写入的该数值。

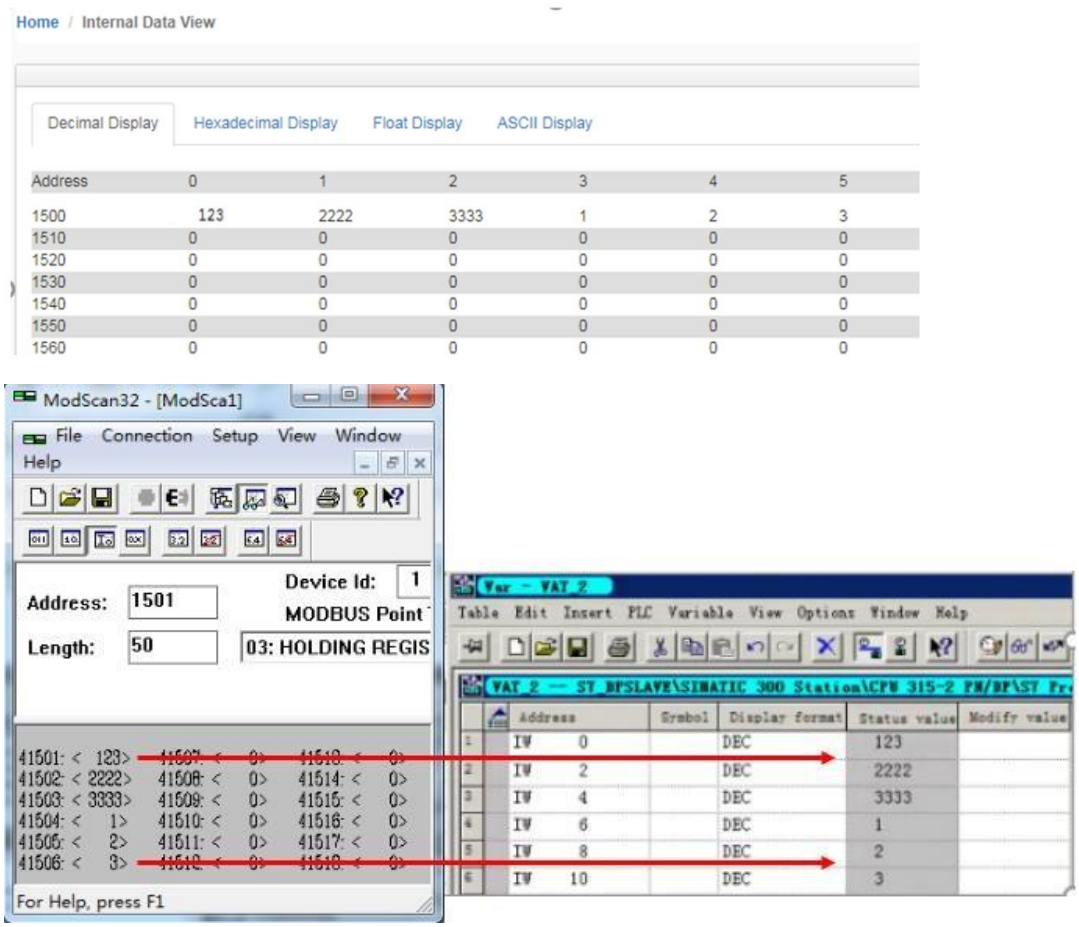


如下图，我们在模块Modbus RTU一侧使用功能码FC3建立一条读指令，读取1号Modbus从站数据，从41501-41510这10个数放到模块内部寄存器1500-1509里面。

Modbus Port 1 - Modify Command

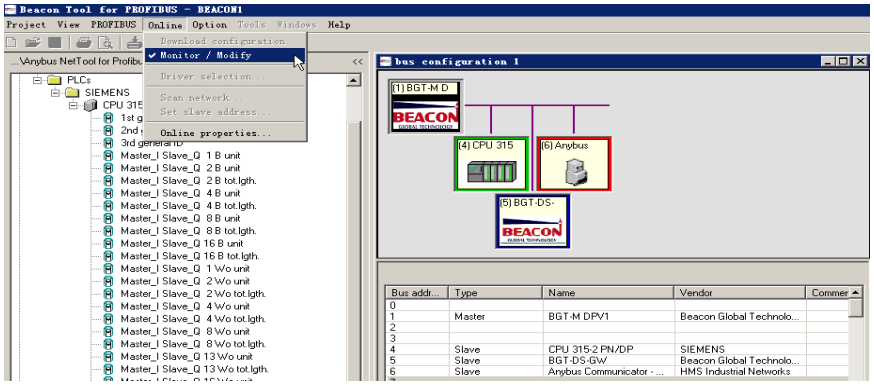
Enable	Yes	使能，禁止，内部寄存器有变化后写
Modbus Function	FC 3 - Read Holding Registers(4X)	Modbus 功能码FC1,FC2,FC3,FC4,FC5,FC6,FC15,FC16
Slave Address	1	从站地址
Modbus Data Address	1500	从站读写数据Modbus起始位
Quantity	10	读或者写的数据的数量
Data Swap	No Change	数据高低位交换，宇交换，宇节交换，宇和宇节交换
Poll Interval	0	命令轮询时间
Internal Data Address	1500	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

ModScan32与模块S1端口连接，仿真软件中对41501，41502，41503，41504，41505，41506地址给定一些数值，同时查看模块内部寄存器1500起始地址区域，这些数值被模块S1端口读取到正确地址，并且在西门子PLC（DP



从站），可看到PIW0-PIW10的输入值，与ModScan32中给出的数值一致。

同样可以使Modbus串口从站获取DP从站在线和离线状态。



在配置软件中，从站绿色外框表示从站GSD文件正确；从站蓝色外框（红色外框偶尔闪烁）表示从站GSD文件不正确，或者GSD文件配置的输入和输出与从站的输出和输入字节数不相符DP线路正确；从站红色外框表示从站线路不正确，有可能是DP中断电阻拨码不对或者是线路没有按照Profibus-DP标准来接线。

Decimal Display | Hexadecimal Display | Float Display | ASCII Display

Address	0	1	2	3	4	5	6	7	8	9
800	4	3	4	4	0	0	4	4	4	4
810	4	4	4	4	4	4	4	4	4	4
820	4	4	4	4	4	4	4	4	4	4
830	4	4	4	4	4	4	4	4	4	4
840	4	4	4	4	4	4	4	4	4	4
850	4	4	4	4	4	4	4	4	4	4
860	4	4	4	4	4	4	4	4	4	4
870	4	4	4	4	4	4	4	4	4	4
880	4	4	4	4	4	4	4	4	4	4
890	4	4	4	4	4	4	4	4	4	4

Prev 1 2 ... 4 5 6 7 8 9 10 11 12 13 ... 32 33 Next

在模块的内部寄存器页面中，如上图：

800数据为4，表示Profibus-DP0号站地址没有使用设备；

801数据为3，表示1号站地址是主站，主站正常运行状态；

802数据为4，表示Profibus-DP2号站地址没有使用设备；

803数据为4，表示Profibus-DP3号站地址没有使用设备；

804数据为0，表示Profibus-DP4号站地址设备正常运行；

805数据为0，表示Profibus-DP5号站地址设备正常运行；

806及以后的地址，数据均为4，表示Profibus-DP6号站地址（及以后站号）没有设备。

从802以后的状态值0表示从站正常运行，4表示从站离线状态。

如下图，在模块Modbus RTU一侧，点击Port 1----commands建立一条如下指令。将模块内部数据区800-899的连续100个整型数，写出给1号Modbus从站40101-40200，这样DP从站的在线状态，将会发送给Modbus从站。

Enable	Yes
Modbus Function	FC 16 - Preset (Write) Multiple Register
Slave Address	1
Modbus Data Address	100
Quantity	100
Data Swap	No Change
Poll Interval	0
Internal Data Address	800
Cmd Errors Mapping Enabled	
Cmd Errors Mapping Address	
Desc	

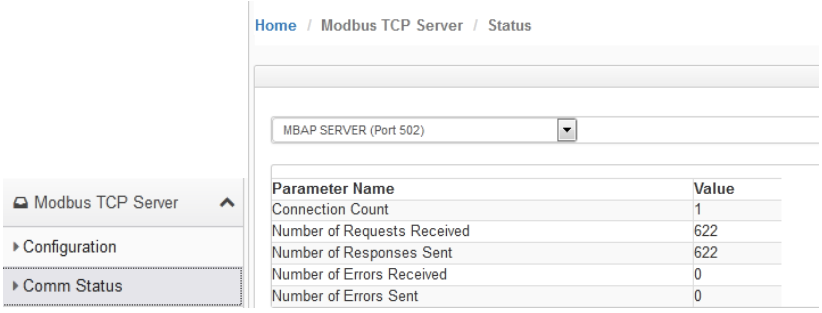
关于如何通过模块的 Modbus RTU 协议，配置成为 Modbus 从站，连接各类 Modbus 主站例如 DCS，PLC，HMI 等设备的内容，可以参考前文提到的“配置模块做 Modbus RTU 从站”或者和 BEACON 办事处进行咨询。

举例 3.Modbus TCP 和 Modbus RTU 之间数据交换

此案例中，模块的Modbus TCP驱动采用server方式，Modbus RTU驱动采用master方式。

打开MODBUS TCP仿真软件MODSCAN32,作用是仿真MODBUS TCP主站,连接模块的Modbus TCP Server。

登录浏览器，进入模块配置页面。在左侧导航栏的 Modbus TCP 下拉菜单中，点击 Comm status。模块默认做MODBUS TCP从站，不需要任何设置。可同时被多个MODBUS TCP主站访问。



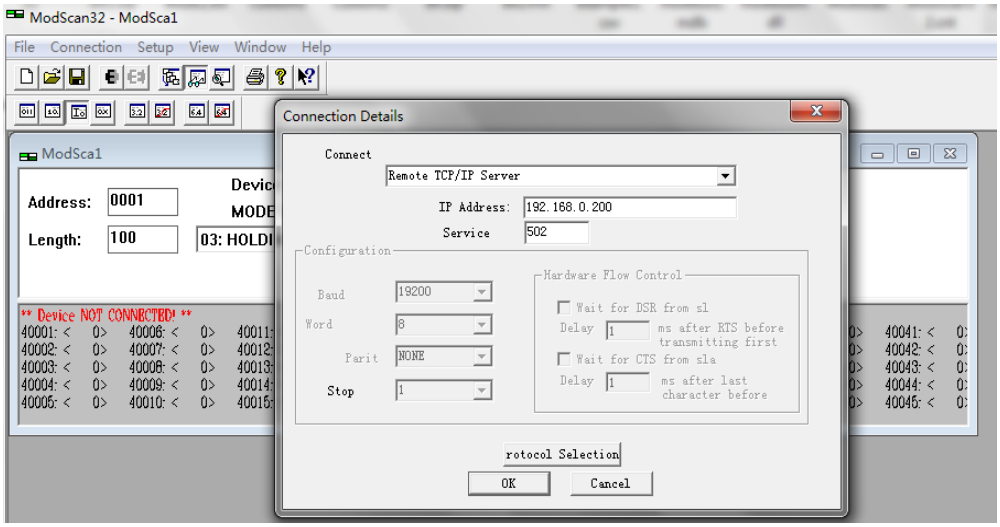
模块内部寄存器 Internal Data 同时提供MODBUS 4区 ，3 区，1 区，0区的访问。

模块内部寄存器对应着MODBUS TCP地址如下：

模块内部寄存器0对应着40001，同时对应着30001，同时对应着10001-10016，同时对应着00001-00016。

详细内容以及 Modbus 功能码和指令的使用方式，可以参考前文“配置模块作为 Modbus TCP server”中的内容。

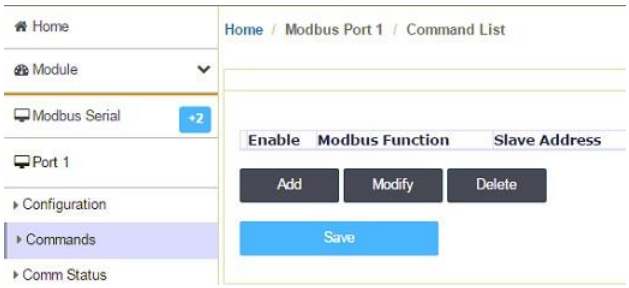
在软件中使用功能码FC03，读写模块内部数据区0-99的连续100个字的数据，40001对应着内部寄存器0，40100 对应着内部寄存器 99,以此类推。选择 Connection，选择 Remote TCP/IP Server，填写模块 E1 口的 IP 地址 192.168.0.200，端口号默认502。然后点击OK。



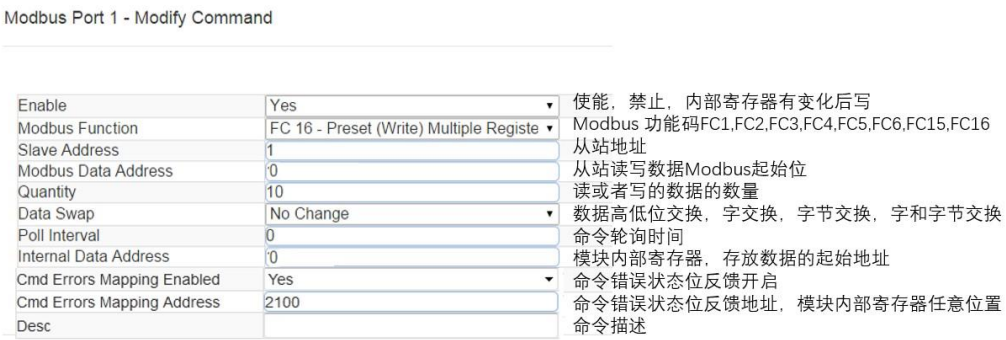
ModScan32 软件可以对内部寄存器读写同时进行，在软件中 40001-40010 写一些数据，如下图查看模块内部寄存器 0-9 里面的数据情况，模块已经接收到这些数据。

在模块主页面左侧导航栏中，找到“Modbus Serial”，在下拉菜单中点击“Port1”为选择模块的 S1 串口，点击“configuration”对该串口进行配置，设置为做 Modbus 主站，采用 RS485 方式，点击保存。

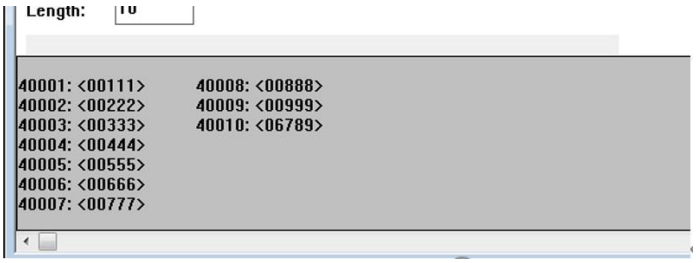
接着点击 Port1 里面的“Commands”显示 S1 端口命令的配置页面，点击 Add。



如下图，我们在模块 Modbus RTU 主站一侧使用 FC16,建立一条写指令，对 1 号 Modbus 从站写入一些数据，将模块内部寄存器地址 0-9 里面的数据，写入到 Modbus 串口 1 号从站 40001-40010 中去。 详细内容以及 Modbus 功能码和指令的使用方式，可以参考前文“配置模块作为 Modbus RTU Master”中的内容。



仍然采用另一台电脑的串口，作为 Modbus 1 号从站的仿真，可以看到相应数据被写入到 Modbus 串口 1 号从站 40001-40010 中。



特别注意

该Profibus-DP主站模块，根据不同型号，可以采用多种协议进行数据的相互转换和传输。

配置不同协议驱动，对于模块内部数据区写数据时，不要出现不同协议重复写入模块相同内部数据区地址的情况。例如，下图中已经配置了内部寄存器0-768（16位字）作为DP从站数据的采集区，则 Modbus TCP 或者 RTU 驱动，不能再对该区域进行数据的输入，否则数据将出现混乱。

同理，如果想对DP从站进行数据输出，请将 Modbus TCP 或者 RTU 驱动采集到的数据，对应保存到模块内部寄存器地址1500-2268（16位字），这样采集到的数据才会输出给DP从站。

同样的模块内部数据区，如果作为对外输出使用时，可以重复被多种协议调动。

例如模块 Modbus TCP 主站或者 Modbus RTU 主站驱动，读取到 Modbus TCP 或者 RTU 从站的数据，存放到了模块内部数据区的地址范围 1500-3000，这个地址区域内的数据可以被模块的 DP 主站驱动调用写出给 DP 从站，同时也可以被调用写出给 Modbus TCP 或者 Modbus RTU 从站，或者被其他作为主站的 Modbus TCP、Modbus RTU 设备从模块中读取。

反之，模块内部寄存器0-768（16位字）作为DP从站数据的采集区，这个地址区域内的数据可以被模块的 Modbus TCP或者Modbus RTU主站驱动调用写给Modbus TCP或者Modbus RTU从站，或者被其他作为主站的Modbus TCP、Modbus RTU 设备从模块中读取。

模块硬件前端的指示灯状态说明

序号	名称	状态	描述
1	MasterStatus	绿色	操作模式
		绿色闪烁	清除模式
		红色	停止模式
		红色闪烁	被动操作HSBY主站
		不亮	离线模式
2	Slave/TokenHold	绿色	全部从站正常，令牌正常
		不亮	没有从站，没有令牌
3	DatabaseStatus	绿色	数据库正常
		绿色闪烁	数据库正在下载中
		红色	数据库无效
		不亮	未下载数据库
4	CommunicationStatus	绿色	主站与所有从站在交换数据
		绿色闪烁	有从站丢失
		红色	总线控制错误，
		不亮	主站和从站没有数据交换

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。

联系电话 （中国大陆）	销售经理13910136425， 技术经理15910883727
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