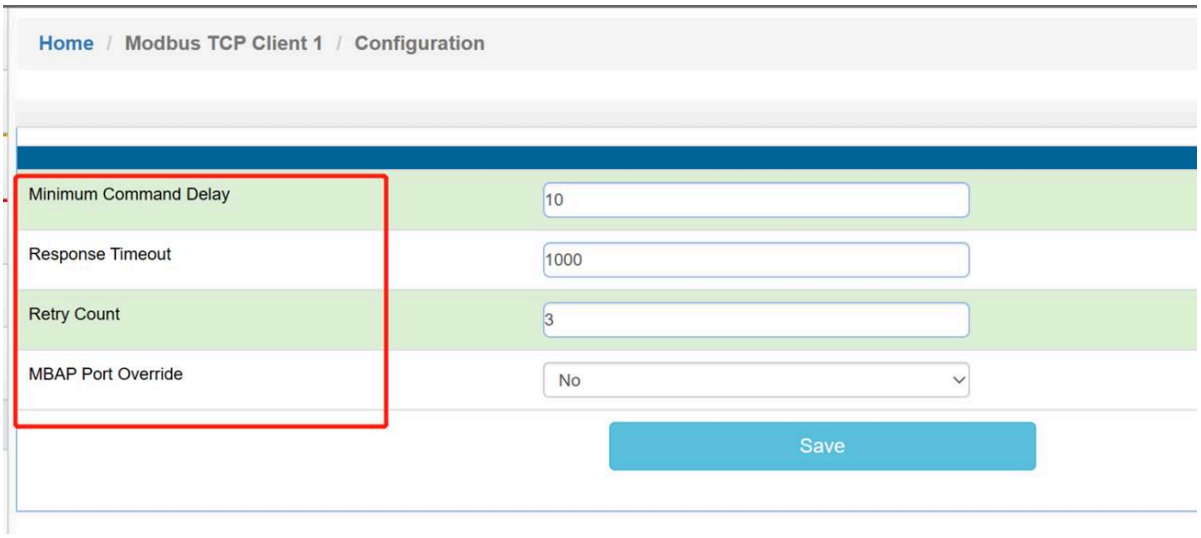
Overview of Modbus TCP/IP Protocol Module Functions

The new Modbus TCP/IP series communication gateway module from Beacon Global Technology can convert various industrial protocols into Modbus TCP/IP protocol for communication.

Modbus TCP/IP:	
Supported Modbus Function Codes	1: Read Coil Status 2: Read Input Status 3: Read Holding Registers 4: Read Input Registers 5: Force Single Coil 6: Preset Single Holding Register 15: Force Multiple Coils 16: Preset Multiple Holding Registers 22:Mask Write Holding Register (Slave only) 23: Read/Write Multiple Holding Registers (Slave only)
Supported Number of Clients	15
Supported Number of Servers	15
Command List	Each client can have up to 32 fully configurable commands.
Status Data	Each command reports error codes individually.
Command List Polling	Each command can be individually enabled or disabled; writing is only allowed when data changes.

Modbus TCP/IP Client Configuration (Master)

Click on Modbus TCP/IP Client > Client1 > Configuration as shown in the image to view the default settings.



This configuration is ready for use by default.

- **Minimum Command Delay**: The polling time for each client to execute commands, measured in milliseconds (0-65535).

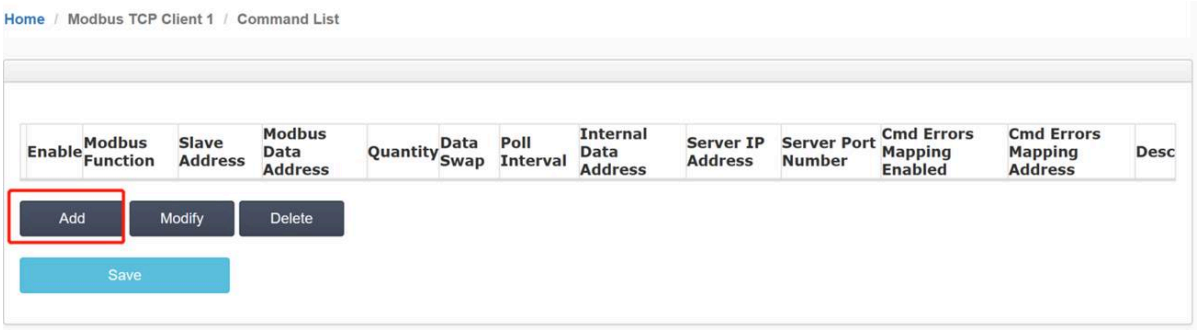
(Note: A smaller delay allows for faster command sending, but it ' s not always better. Check the documentation of the slave device to ensure it can respond in a timely manner to the commands sent by the master.)

- **Response Timeout**: The response time of the connected device, also measured in milliseconds (0-65535).

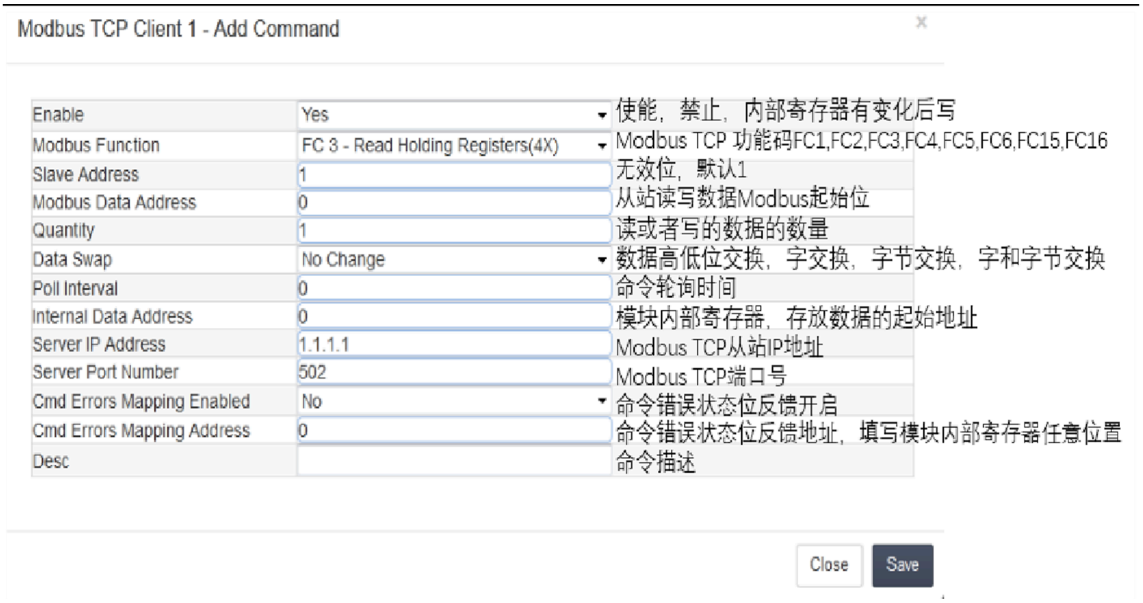
- **Retry Count**: The number of retry attempts for connection (0-65535).

- **MBAP Port Override**: Port 502 override options (NO/YES).

Next, click on Modbus TCP/IP Client > Client1 > Commands.

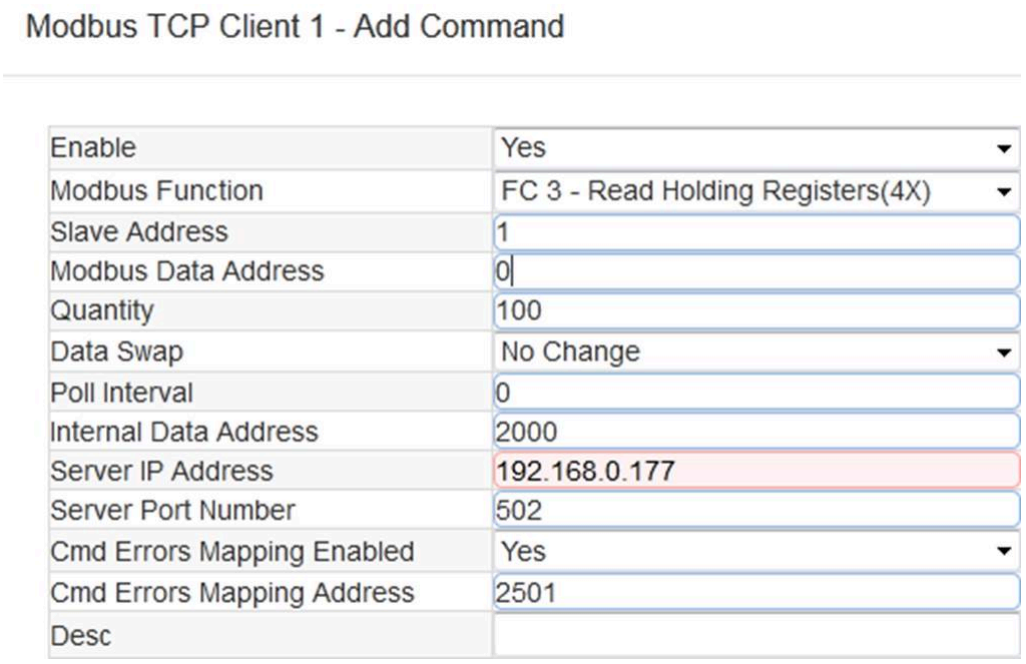


Click "Add" to create a new command with the following settings:



Command Description: Use function codes to control reading and writing areas. The module's internal registers are in 16-bit INT format. When reading or writing BOOL values, be aware of the 16-to-1 relationship.

(Note: First, confirm the size of the internal register data area of the module, as it varies by model. The following command configuration examples are based on a data area of 10,000 words. When configuring the module, strictly refer to the range of the internal data area.)



The above command has the following meaning: The module uses function code FC3, with the slave data starting address at 0, equivalent to 40001. The read quantity is 100. The module's internal register starting address is 2000. This means it reads from the slave at IP address 192.168.0.177, retrieving 100 words from the slave data address range 40001-40100 and placing them into the module's internal registers 2000-2099. If the command does not return correctly, an error will be reported in internal register 2051.

If the function code is FC4 (read-only), the slave data starting address is 0, equivalent to 30001. The read quantity is still 100, with the internal register starting address at 2000. This indicates that it reads from the slave at IP address 192.168.0.177, retrieving data from the slave address range 30001-30100 and storing it in internal registers 2000-2099. If the command fails to return correctly, an error will again appear in internal register 2051.

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	

The above command has the following meaning: When the module uses function code FC1, the slave data starting address is 0, equivalent to 00001. The read quantity is 16 (reading 16 bits is equivalent to reading one word). The module's internal register starting address is 32000 (this is a bit address; reading 16 bits equals one word, so the actual starting address for internal registers is 32000/16 = 2000). This indicates that it reads from the slave at IP address 192.168.0.177, retrieving data from the slave address range 00001-00160 and placing it in the module's internal register starting at address 2000 (since reading 16 bits of data occupies only one internal register address). If the command does not return correctly, an error will be reported in internal register 2051.

If function code FC2 (read-only) is used, the slave data starting address is still 0, with a read quantity of 16. The internal register address remains at 32000, which again indicates reading from the slave at IP address 192.168.0.177, retrieving data from the slave address range 00001-00160 and storing it in internal register 2000. If the command fails to return correctly, an error will appear in internal register 2051.

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	

The above command is described as follows: When **Conditional** is enabled, the module uses function codes FC6 or FC16, with a write quantity of 20. The internal register starting address is 2000, which means that whenever any register within the range of 2000-2049 changes, it triggers a write command. The data is sent from the module to the slave at IP address 192.168.0.177, with the slave receiving data in the address range of 40051-40071. If the command does not execute correctly, an error will be reported in internal register 2051.

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	

The above command is described as follows: When the module uses function codes FC6 or FC16, the write quantity is 20, and the internal register starting address is 2000. This means that the data from internal registers in the range of 2000-2049 will be continuously written to the slave at IP address 192.168.0.177, with the slave receiving data in the address range of 40051-40071. If the command does not execute correctly, an error will be reported in internal register 2051.

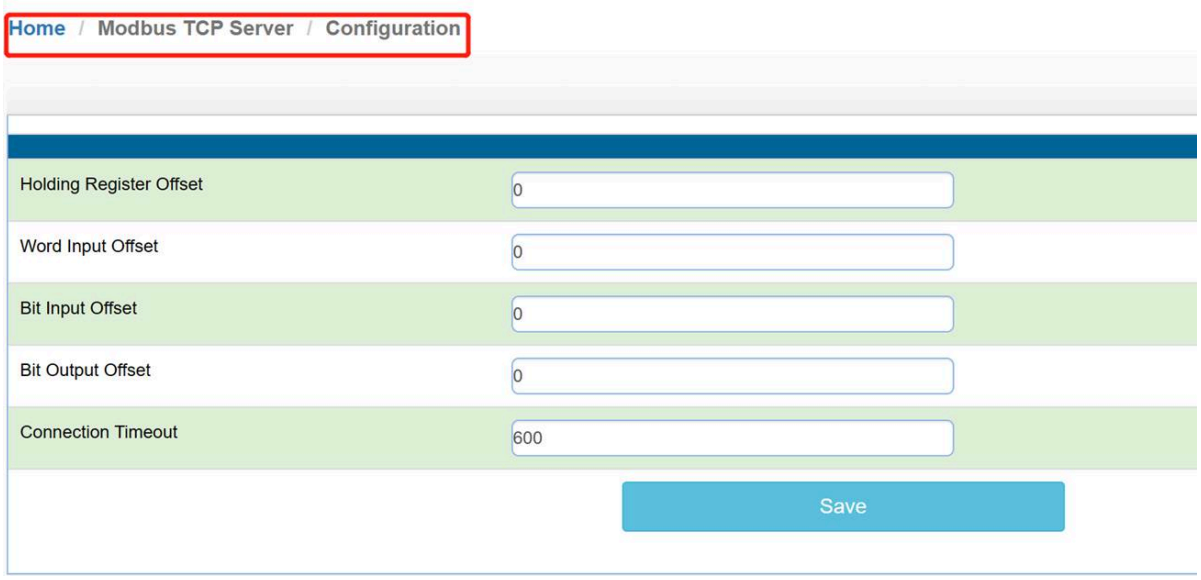
Modbus TCP Client 1 - Add Command

Enable	命令使能	Yes
Modbus Function	功能码	FC 15 - Force (Write) Multiple Coils (0X)
Slave Address	默认1	1
Modbus Data Address	从站数据起始地址	0
Quantity	数量	160
Data Swap	数据高低位交换	No Change
Poll Interval	轮训时间	0
Internal Data Address	内部寄存器地址	16000
Server IP Address	从站IP地址	192.168.2.177
Server Port Number	从站端口号	502
Desc		

The above command is described as follows: When using function code FC15, the slave data starting address is 0. The module writes a quantity of 160 BOOLs (which is a multiple of 16, as 160 bits equals 10 words of 16 bits each). It references the internal register starting address of 16000 (also a multiple of 16, with the actual starting address being 1000), indicating that the 160 bits of data (10 integer values) from internal word registers 1000-1009 will be written to the slave address range 00001-00160.

Modbus TCP/IP Server Configuration (Slave)

The configuration of the Modbus TCP/IP Server typically uses the default initial settings.

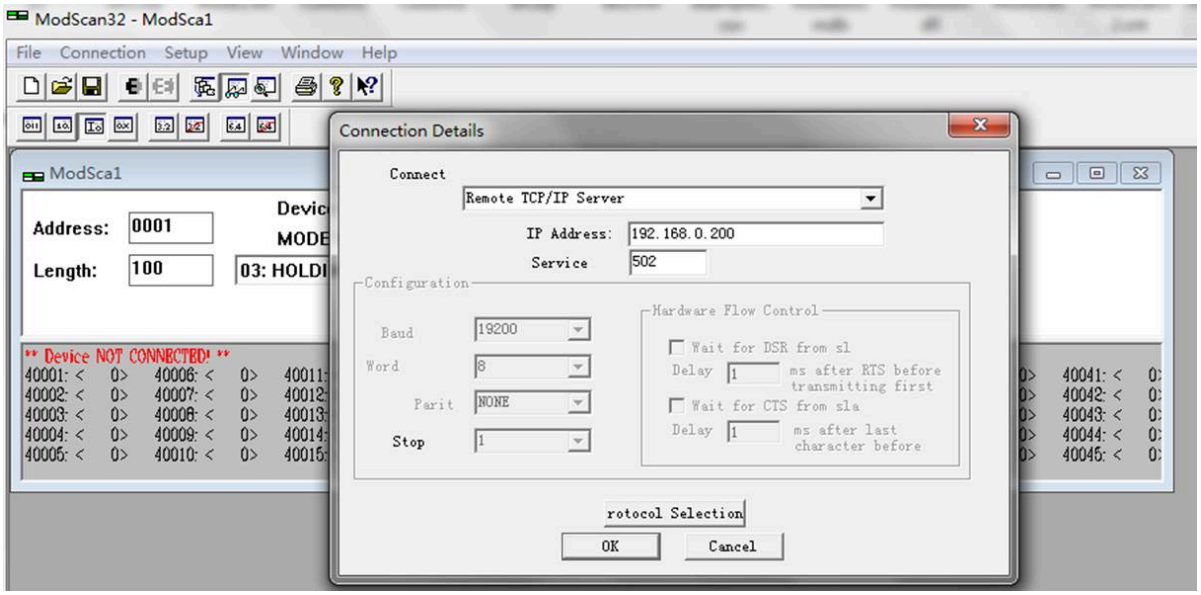


The internal registers of the module correspond to the following Modbus TCP/IP addresses:

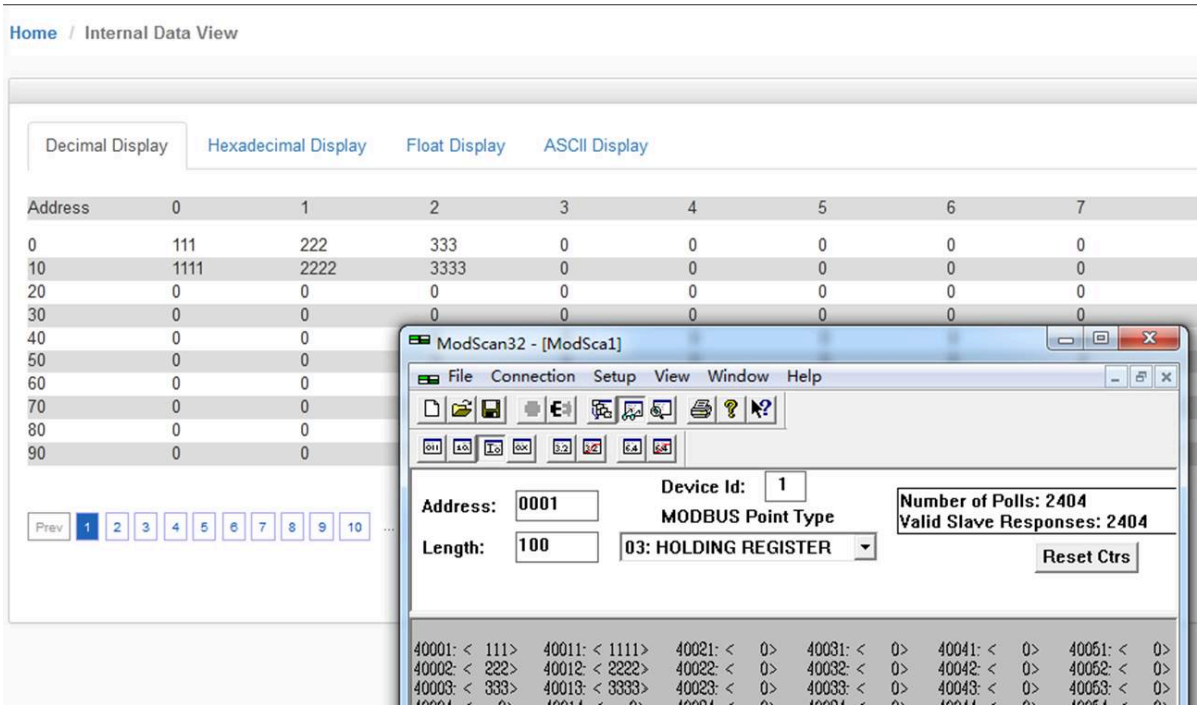
Internal registers of the module	**0**	**1**	**100**	**1000**	**2000**
Modbus Address (Register 4)	40001	40002	40101	41001	42001
Modbus Address (Register 3)	30001	30002	30101	31001	32001
Modbus Address (Register 1)	10001-10016	10017-10032	11601-11616	26001-26016	42001-42016
Modbus Address (Register 0)	00001-00016	00017-00032	01601-01616	16001-16016	32001-32016

Users can use the Modbus TCP/IP simulation software ModScan32 to test the connection to the module's Modbus TCP/IP Server. Change the local computer's IP address to 192.168.0.177 (in the same subnet as the Modbus TCP/IP gateway port).

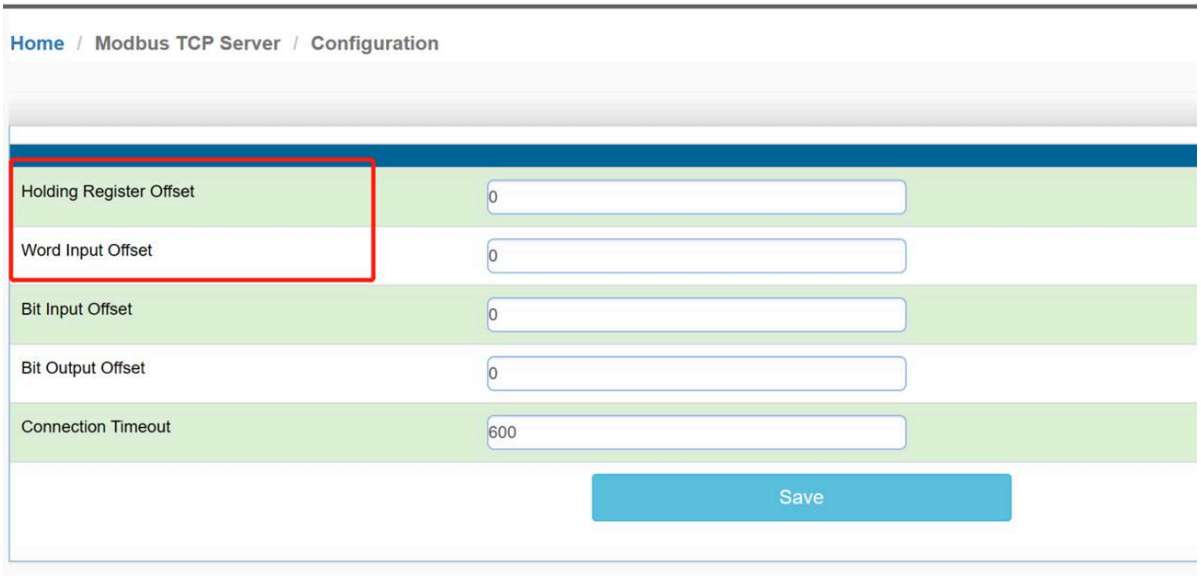
For example: Open the Modbus TCP simulation software ModScan32, which simulates the Modbus TCP master. Use function code FC03 to read and write 100 consecutive words of internal data from registers 0 to 99. Address 40001 corresponds to internal register 0, and 40100 corresponds to internal register 99, and so on. Select "Connection," then choose " Remote TCP/IP Server," and enter the IP address of the module's E1 port (192.168.0.200) with the default port number 502. Then click OK.



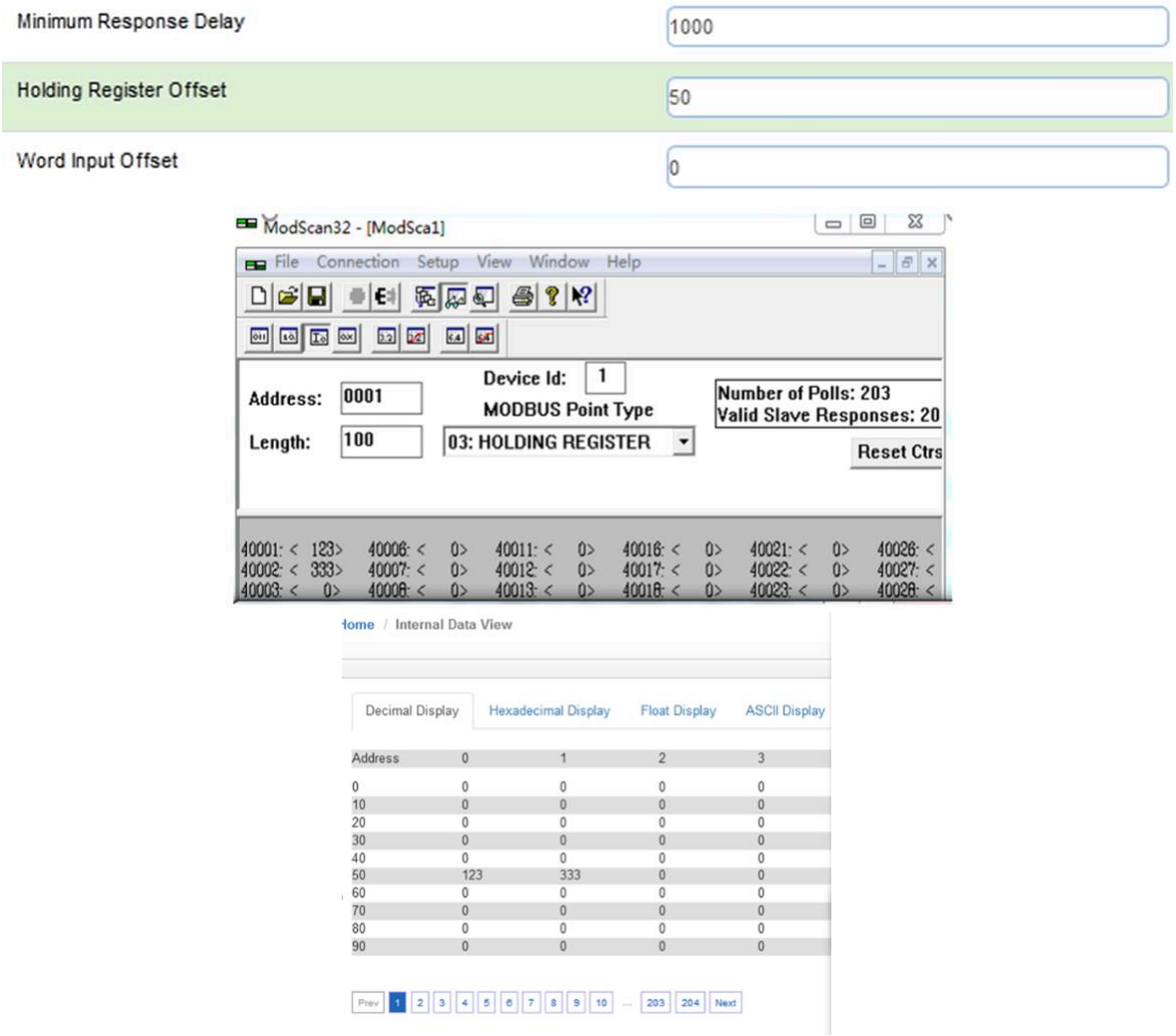
The ModScan32 software allows simultaneous reading and writing of internal registers. Write some data to addresses 40001-40003 and 40011-40013, then check the data in internal registers 0-2 and 10-12. The data should correspond correctly. You can also see that the software has sent and received 2404 times in the upper right corner. If there are any errors, the number of sent and received data packets will not be equal.



When the module is set as a Modbus TCP/IP slave, you can see the following two options in the configuration interface.



Usage of Holding Register Offset:
When the Modbus TCP/IP master writes data to the module, entering two values at addresses 40001 and 40002 should normally write these values to internal registers 0-1. However, if the offset is set to 50 (as shown in the image), the data will be written directly to internal registers 50-51. This principle also applies to registers in other areas, such as 4, 3, 1, and 0.



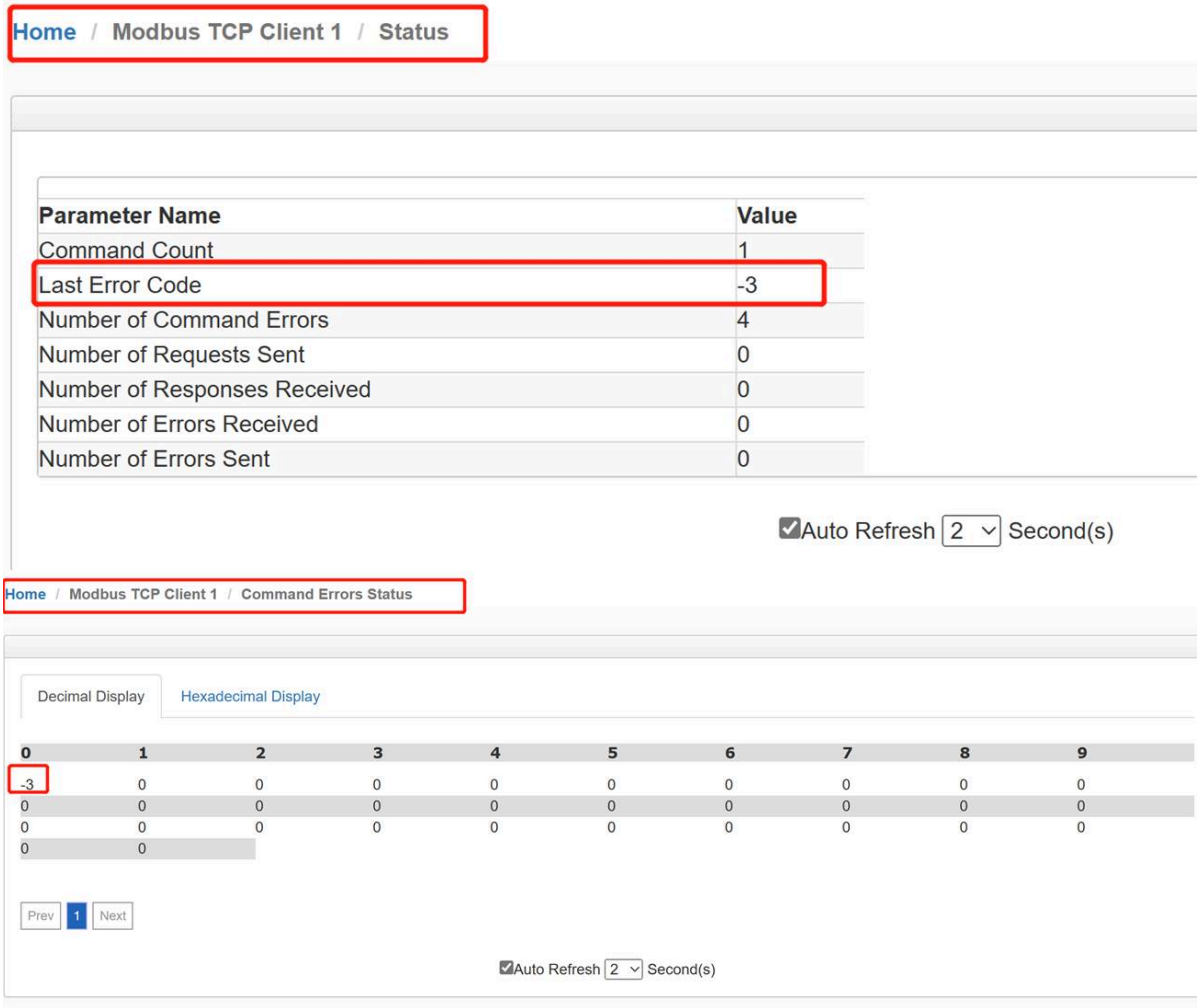
Usage of Word Input Offset:
If the offset is set to 50 (as shown in the image), when the Modbus TCP/IP master inputs two values at addresses 30001 and 30002 in area 3, the data will be directly offset to internal registers 50-51 in the module. Note that the ModScan32 simulation software cannot load values from area 3; please enter the actual data area from the field device.

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

Modbus TCP/IP Protocol Error Diagnosis

Error Codes

When using the Modbus TCP/IP protocol, users can check the communication status and command error codes on the module page to quickly identify the source of the issue.



The relevant error code details are as follows:

Code	Code (Hexadecimal)	Description
-2	0xFFFE	Command Timeout
-3	0xFFFD	Send Timeout
-5	0xFFFB	Connection Terminated
-6	0xFFFA	Message Length Error