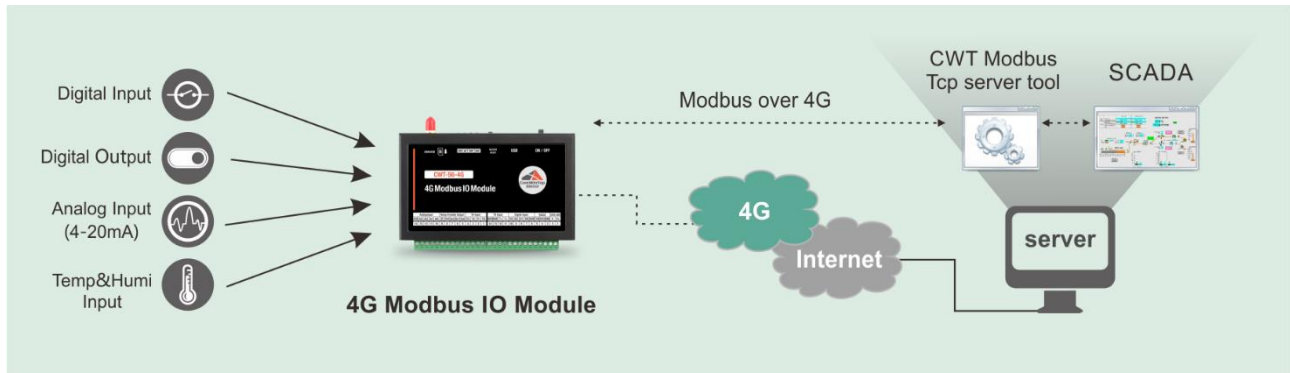


How to work with SCADA by Modbus

How does Scada system read and write the 4G module?

Usually, SCADA cannot directly send Modbus message to 4G module, because 4G network does not provide static public IP address for simcard (except VPN), For dealing with this issue, CWT provide a **Modbus TCP sever tool** to work with Scada in server , it forward SCADA Modbus TCP message to 4G module, and forward responds of 4G module to SCADA, So that realizes the connectivity of SCADA and 4G module.



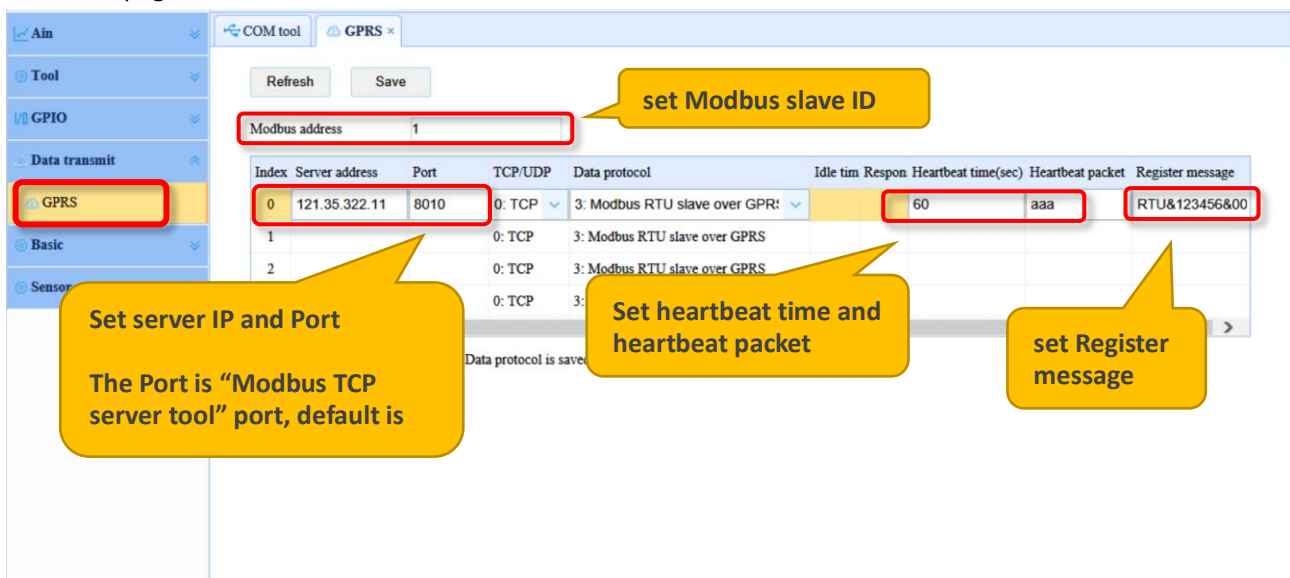
Communication process:

1. CWT 4g module build connection with Modbus TCP server according to server IP address (in this case, static public IP address or domain is necessary for server)
2. Scada system send Modbus TCP request command to Modbus TCP server tool
3. Modbus TCP server tool forward command to CWT 4g module
4. CWT 4g module responds

How to set 4G module and test

1. Set server parameters

In "GPRS" page



| Index | Server address | Port | TCP/UDP | Data protocol | Idle tim Respon | Heartbeat time(sec) | Heartbeat packet | Register message |
|-------|----------------|------|---------|-------------------------------|-----------------|---------------------|------------------|------------------|
| 0 | 121.35.322.11 | 8010 | 0: TCP | 3: Modbus RTU slave over GPR! | | 60 | aaa | RTU&123456&00 |
| 1 | | | 0: TCP | 3: Modbus RTU slave over GPRS | | | | |
| 2 | | | 0: TCP | 3: Modbus RTU slave over GPRS | | | | |

Note:

- 1) the **register message** must be setup, it's approval for connection between gateway and "Modbus TCP server too", the format is **RTU&123456&[ID]**, the [ID] is 8 numbers.
 In this demo, we set register message is **RTU&123456&00000001**
- 2) The heartbeat time and packet are necessary for holding connection between gateway and server. any characters can be heartbeat packet, and they don't affect Modbus communication.

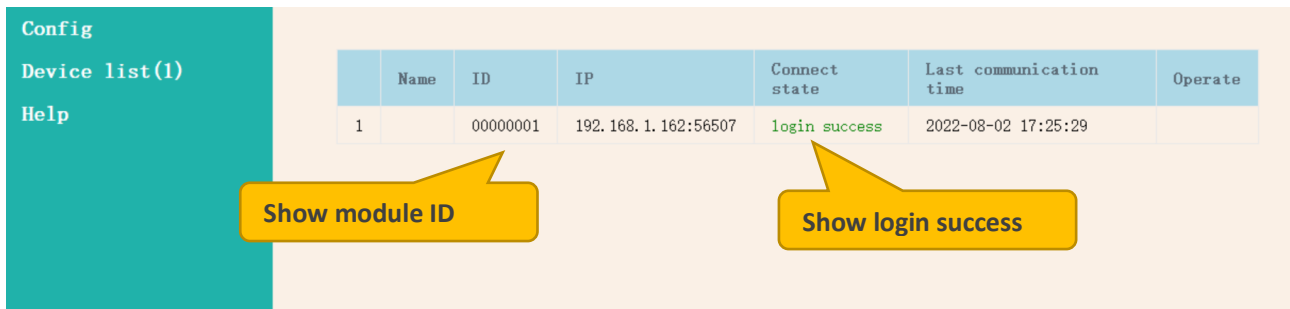
After setup, start the device to go to working mode.

2. Check connection in Modbus TCP server tool

Run the tool on server

System.Data.SQLite.dll
 System.Data.SQLite.EF6.dll
 System.Data.SQLite.Linq.dll
 System.Data.SQLite.xml
 TcpTransmissionTool.exe
 TcpTransmissionTool.exe.config

After 4G module connect up, Modbus TCP server tool show the connection.

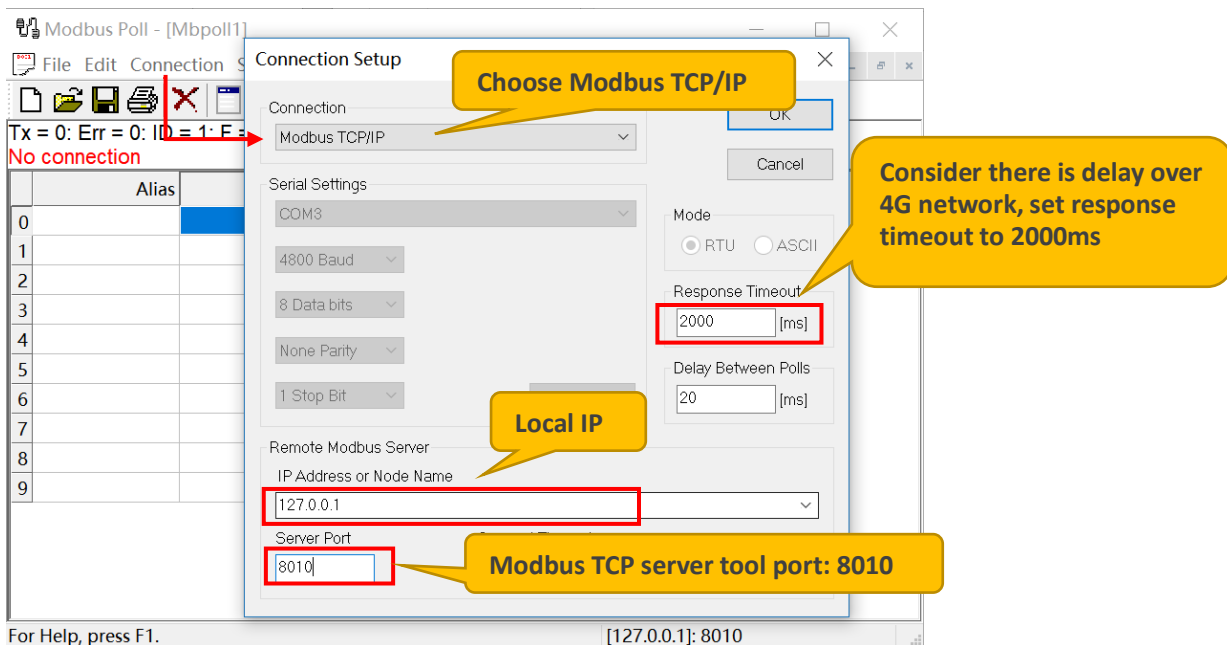


The screenshot shows the 'Config' window of the Modbus TCP server tool. On the left, there are tabs for 'Config', 'Device list(1)', and 'Help'. The 'Device list(1)' tab is active, displaying a table with connection details. A yellow callout points to the 'ID' column, labeled 'Show module ID'. Another yellow callout points to the 'Connect state' column, labeled 'Show login success'.

| Name | ID | IP | Connect state | Last communication time | Operate |
|------|----------|---------------------|---------------|-------------------------|---------|
| 1 | 00000001 | 192.168.1.162:56507 | login success | 2022-08-02 17:25:29 | |

3. Test by Modbus poll

Run Modbus Poll in the same server



The screenshot shows the 'Modbus Poll - [Mbpoll1]' window with the 'Connection Setup' dialog box open. The 'Connection' dropdown is set to 'Modbus TCP/IP'. The 'Serial Settings' section shows 'COM3', '4800 Baud', '8 Data bits', 'None Parity', and '1 Stop Bit'. The 'Remote Modbus Server' section shows 'IP Address or Node Name' as '127.0.0.1' and 'Server Port' as '8010'. A yellow callout points to the 'Connection' dropdown, labeled 'Choose Modbus TCP/IP'. Another yellow callout points to the 'Response Timeout' field, labeled 'Consider there is delay over 4G network, set response timeout to 2000ms'. A third yellow callout points to the 'IP Address or Node Name' field, labeled 'Local IP'. A fourth yellow callout points to the 'Server Port' field, labeled 'Modbus TCP server tool port: 8010'.

Connection Setup

Connection: Modbus TCP/IP

Serial Settings

COM3

4800 Baud

8 Data bits

None Parity

1 Stop Bit

Mode

RTU (selected) ASCII

Response Timeout: 2000 [ms]

Delay Between Polls: 20 [ms]

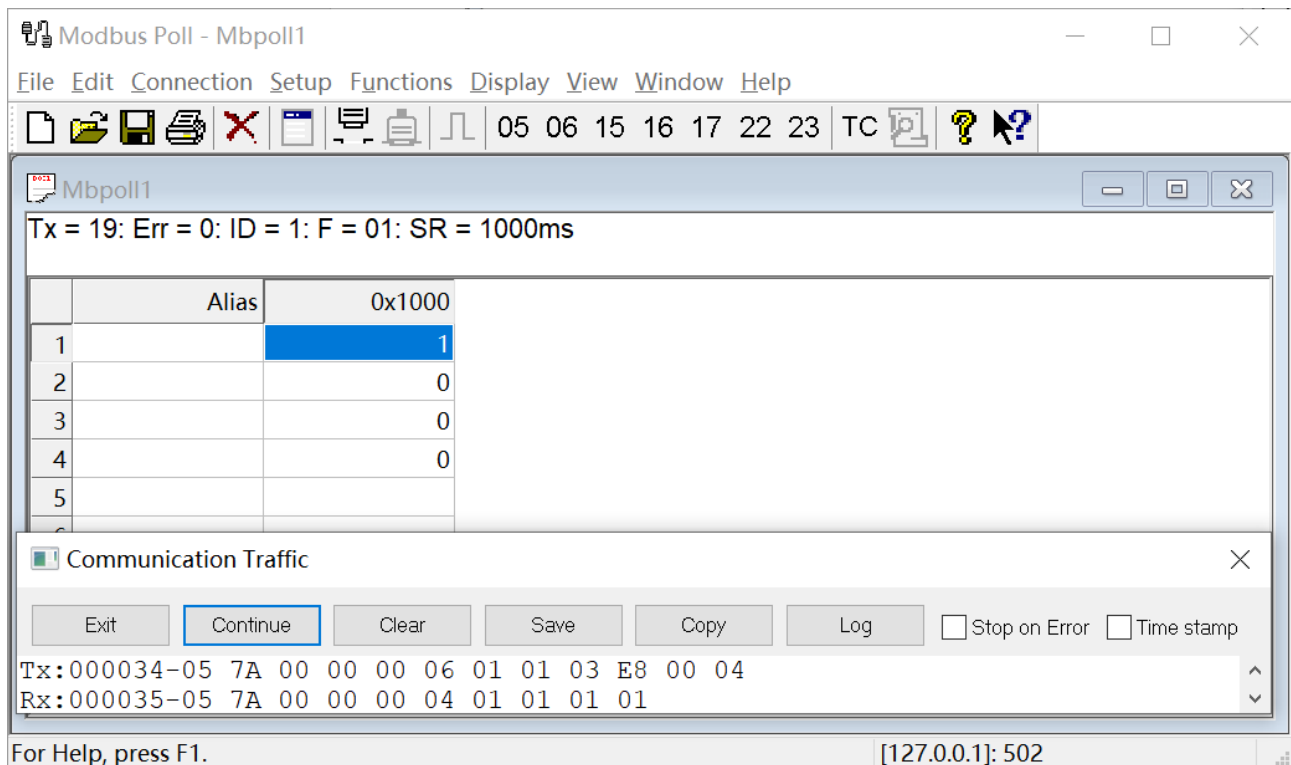
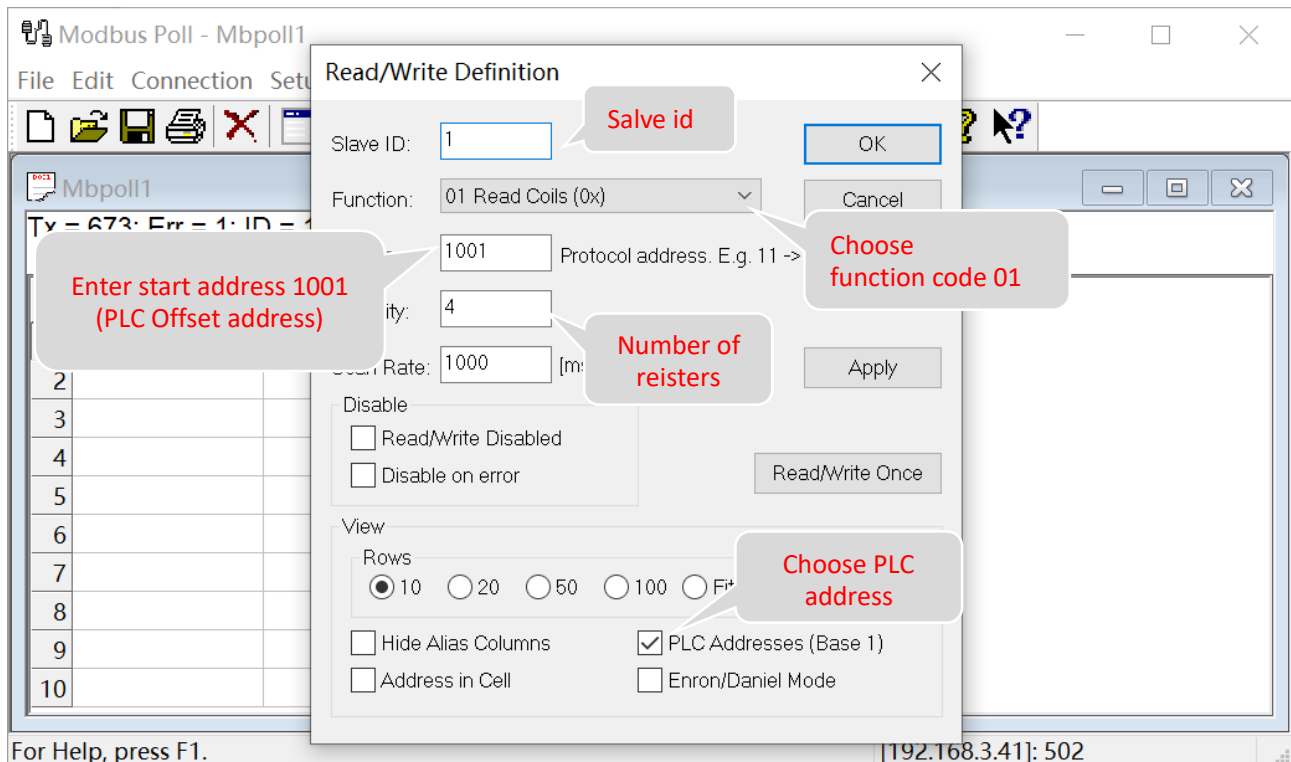
Remote Modbus Server

IP Address or Node Name: 127.0.0.1

Server Port: 8010

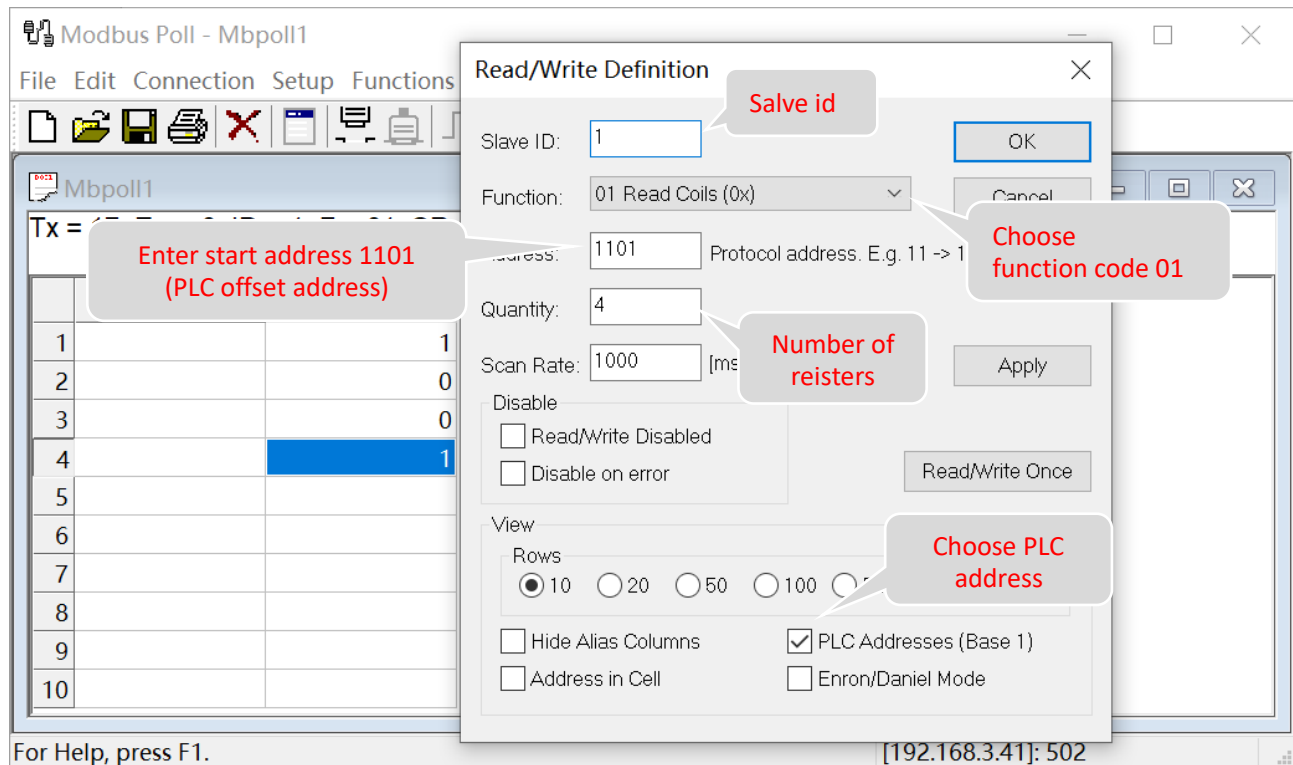
1) Read digital input

For example, read 4 channels of Di, slave id=1



2) Read digital output

For example, read 4 channels of Do, slave id=1

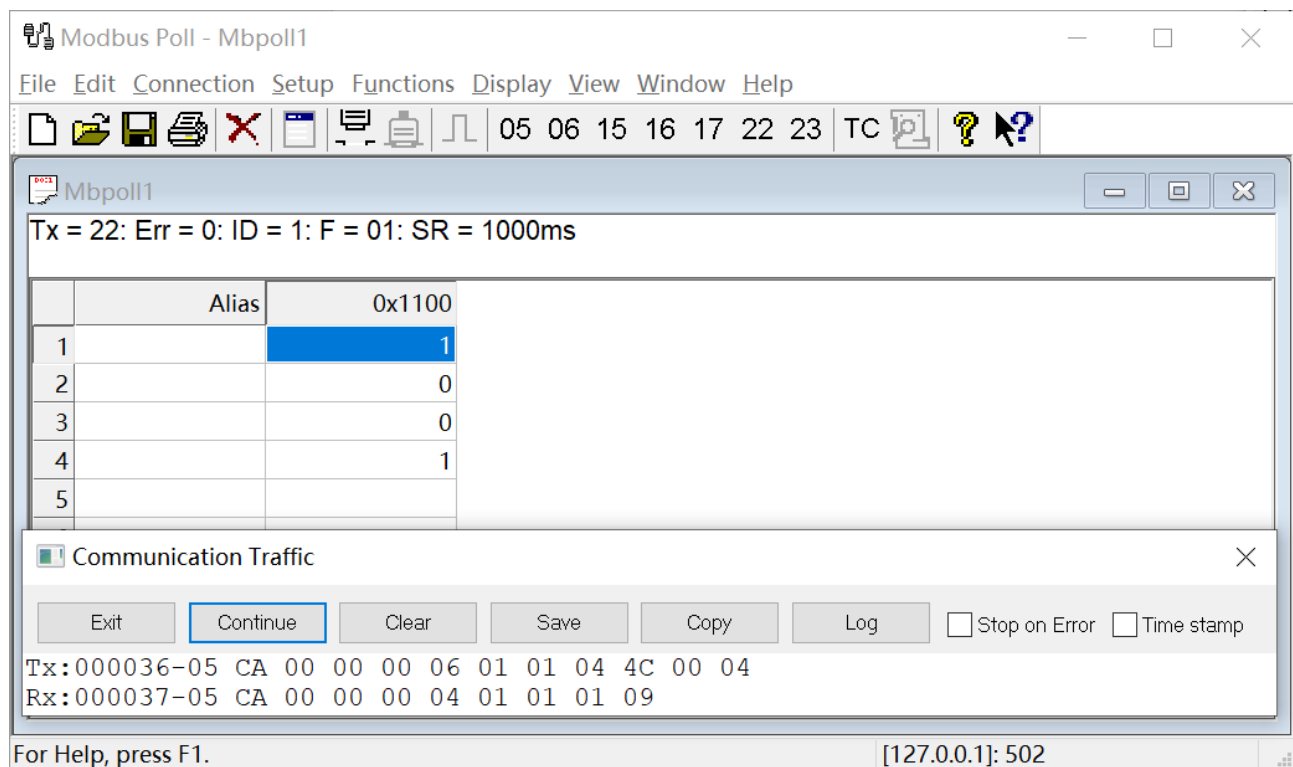


The screenshot shows the 'Modbus Poll - Mbpoll1' window with the 'Read/Write Definition' dialog box open. The dialog box contains the following fields and options:

- Slave ID:** 1 (Annotated: **Slave id**)
- Function:** 01 Read Coils (0x) (Annotated: **Choose function code 01**)
- Address:** 1101 (Annotated: **Enter start address 1101 (PLC offset address)**)
- Quantity:** 4 (Annotated: **Number of registers**)
- Scan Rate:** 1000 [ms]
- Disable:**
 - ☐ Read/Write Disabled
 - ☐ Disable on error
- View:**
 - Rows:** 10 (selected), 20, 50, 100, 200 (Annotated: **Choose PLC address**)
 - ☐ Hide Alias Columns
 - ☒ PLC Addresses (Base 1)
 - ☐ Address in Cell
 - ☐ Enron/Daniel Mode
- Buttons:** OK, Cancel, Apply, Read/Write Once

The background window shows a table with 10 rows and 3 columns. The 4th row is highlighted in blue, showing the value 1 in the third column.

For Help, press F1. [192.168.3.41]: 502



The screenshot shows the 'Modbus Poll - Mbpoll1' window with the 'Communication Traffic' window open. The main window displays the following information:

- Tx = 22: Err = 0: ID = 1: F = 01: SR = 1000ms**
- Table:**

| | Alias | 0x1100 |
|---|-------|--------|
| 1 | | 1 |
| 2 | | 0 |
| 3 | | 0 |
| 4 | | 1 |
| 5 | | |

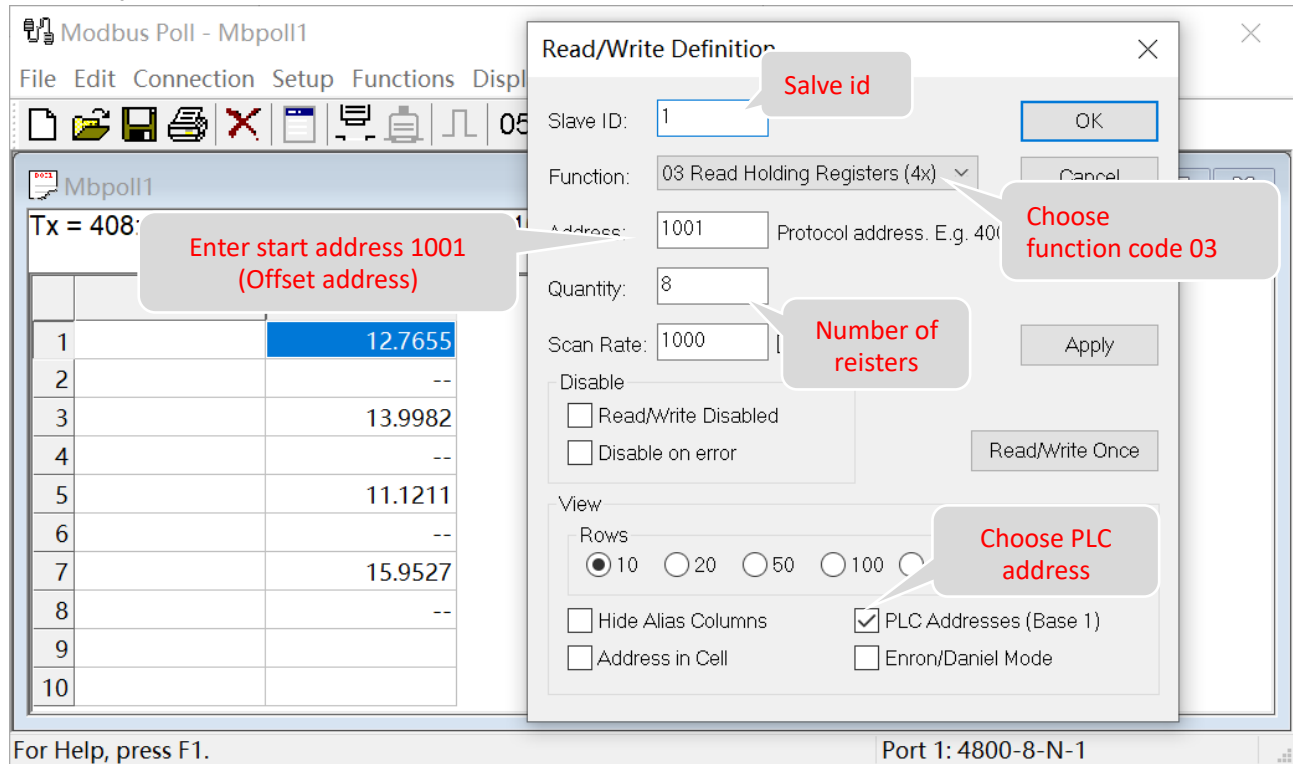
The 'Communication Traffic' window shows the following data:

- Buttons:** Exit, Continue (selected), Clear, Save, Copy, Log, Stop on Error, Time stamp
- Tx:** 000036-05 CA 00 00 00 06 01 01 04 4C 00 04
- Rx:** 000037-05 CA 00 00 00 04 01 01 01 09

For Help, press F1. [127.0.0.1]: 502

3) Read analog input

Fox example, read 4 channels of Ai, slave id=1

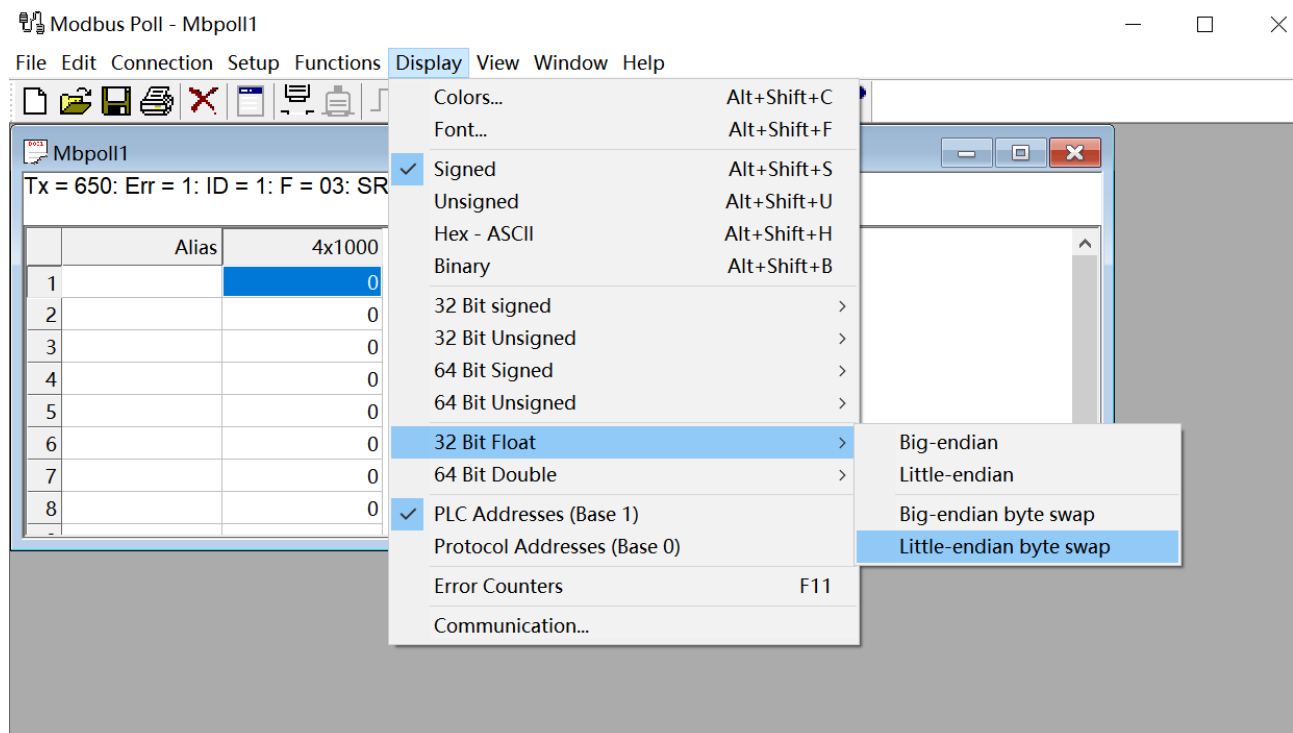


The screenshot shows the Modbus Poll interface with a table of data and a 'Read/Write Definition' dialog box. The table displays data for 10 channels, with the first channel (1) showing a value of 12.7655. The dialog box is configured for a Slave ID of 1, Function 03 (Read Holding Registers), Address 1001, and Quantity 8. Annotations highlight key settings: 'Slave id' (1), 'Choose function code 03', 'Number of registers' (8), and 'Choose PLC address' (Base 1).

| Channel | Value |
|---------|---------|
| 1 | 12.7655 |
| 2 | -- |
| 3 | 13.9982 |
| 4 | -- |
| 5 | 11.1211 |
| 6 | -- |
| 7 | 15.9527 |
| 8 | -- |
| 9 | -- |
| 10 | -- |

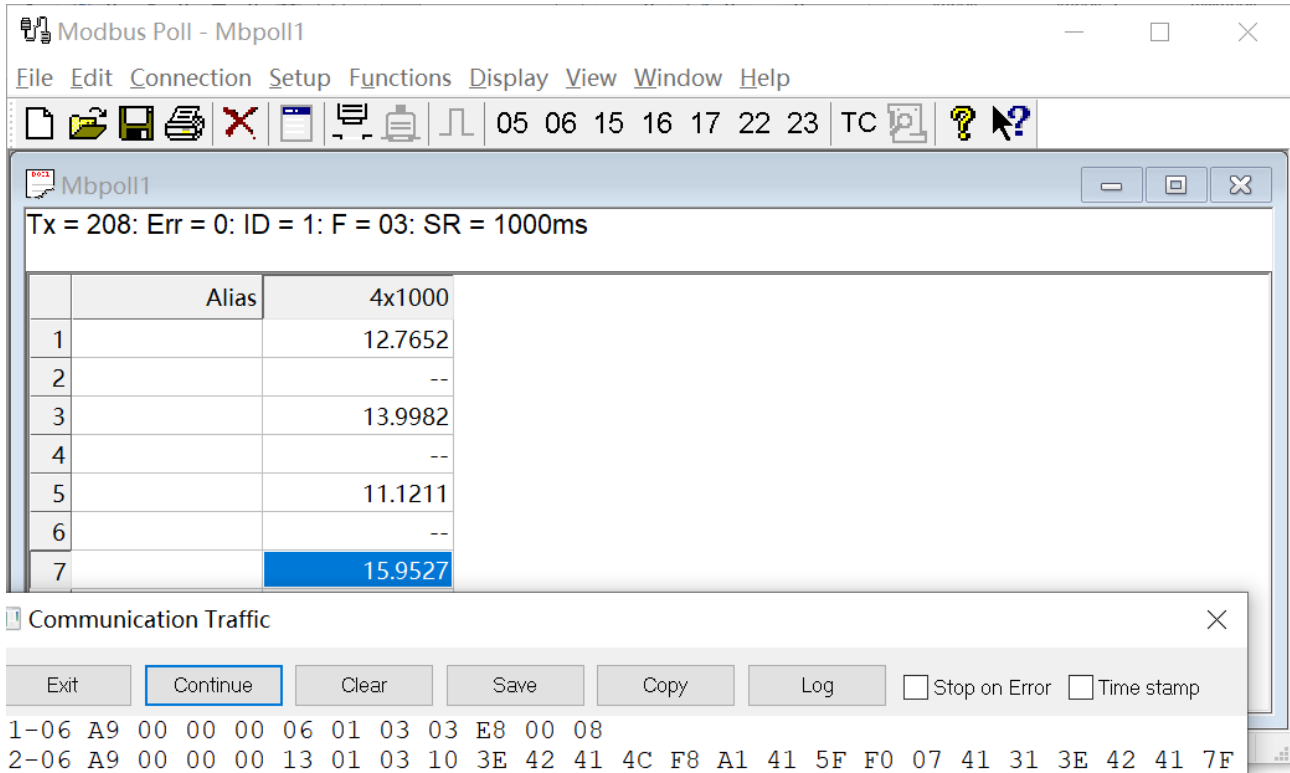
For Help, press F1. Port 1: 4800-8-N-1

Choose 32 Bit Float



The screenshot shows the 'Display' menu in Modbus Poll. The '32 Bit Float' option is selected, and the 'PLC Addresses (Base 1)' option is also checked. The menu also shows options for 'Colors...', 'Font...', 'Signed', 'Unsigned', 'Hex - ASCII', 'Binary', '32 Bit signed', '32 Bit Unsigned', '64 Bit Signed', '64 Bit Unsigned', '32 Bit Float', '64 Bit Double', 'PLC Addresses (Base 1)', 'Protocol Addresses (Base 0)', 'Error Counters', and 'Communication...'. The '32 Bit Float' option is highlighted in blue.

| Channel | Alias | Value |
|---------|-------|-------|
| 1 | | 0 |
| 2 | | 0 |
| 3 | | 0 |
| 4 | | 0 |
| 5 | | 0 |
| 6 | | 0 |
| 7 | | 0 |
| 8 | | 0 |



Modbus Poll - Mbpoll1

File Edit Connection Setup Functions Display View Window Help

Tx = 208: Err = 0: ID = 1: F = 03: SR = 1000ms

| | Alias | 4x1000 |
|---|-------|---------|
| 1 | | 12.7652 |
| 2 | | -- |
| 3 | | 13.9982 |
| 4 | | -- |
| 5 | | 11.1211 |
| 6 | | -- |
| 7 | | 15.9527 |

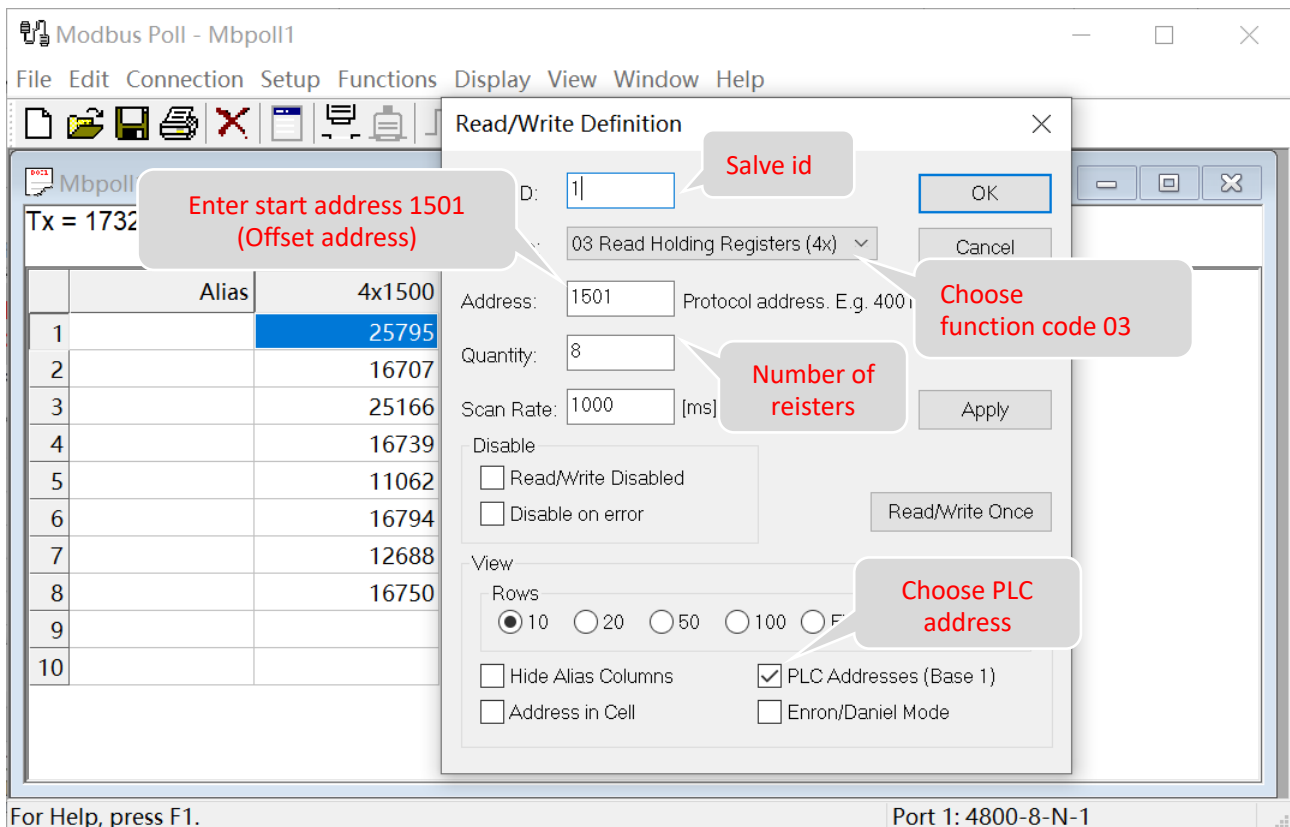
Communication Traffic

Exit Continue Clear Save Copy Log ☐ Stop on Error ☐ Time stamp

1-06 A9 00 00 00 06 01 03 03 E8 00 08
 2-06 A9 00 00 00 13 01 03 10 3E 42 41 4C F8 A1 41 5F F0 07 41 31 3E 42 41 7F

4) Read temperature input

For example, read 4 channels of Ti, slave id=1



Modbus Poll - Mbpoll1

File Edit Connection Setup Functions Display View Window Help

Tx = 1732

| | Alias | 4x1500 |
|----|-------|--------|
| 1 | | 25795 |
| 2 | | 16707 |
| 3 | | 25166 |
| 4 | | 16739 |
| 5 | | 11062 |
| 6 | | 16794 |
| 7 | | 12688 |
| 8 | | 16750 |
| 9 | | |
| 10 | | |

Read/Write Definition

Slave id: 1

Function: 03 Read Holding Registers (4x)

Address: 1501 Protocol address. E.g. 4001

Quantity: 8

Scan Rate: 1000 [ms]

Disable

☐ Read/Write Disabled

☐ Disable on error

View

Rows: ☒ 10 ☐ 20 ☐ 50 ☐ 100 ☐ Full

☐ Hide Alias Columns ☒ PLC Addresses (Base 1)

☐ Address in Cell ☐ Enron/Daniel Mode

OK Cancel Apply Read/Write Once

Enter start address 1501 (Offset address)

Salve id

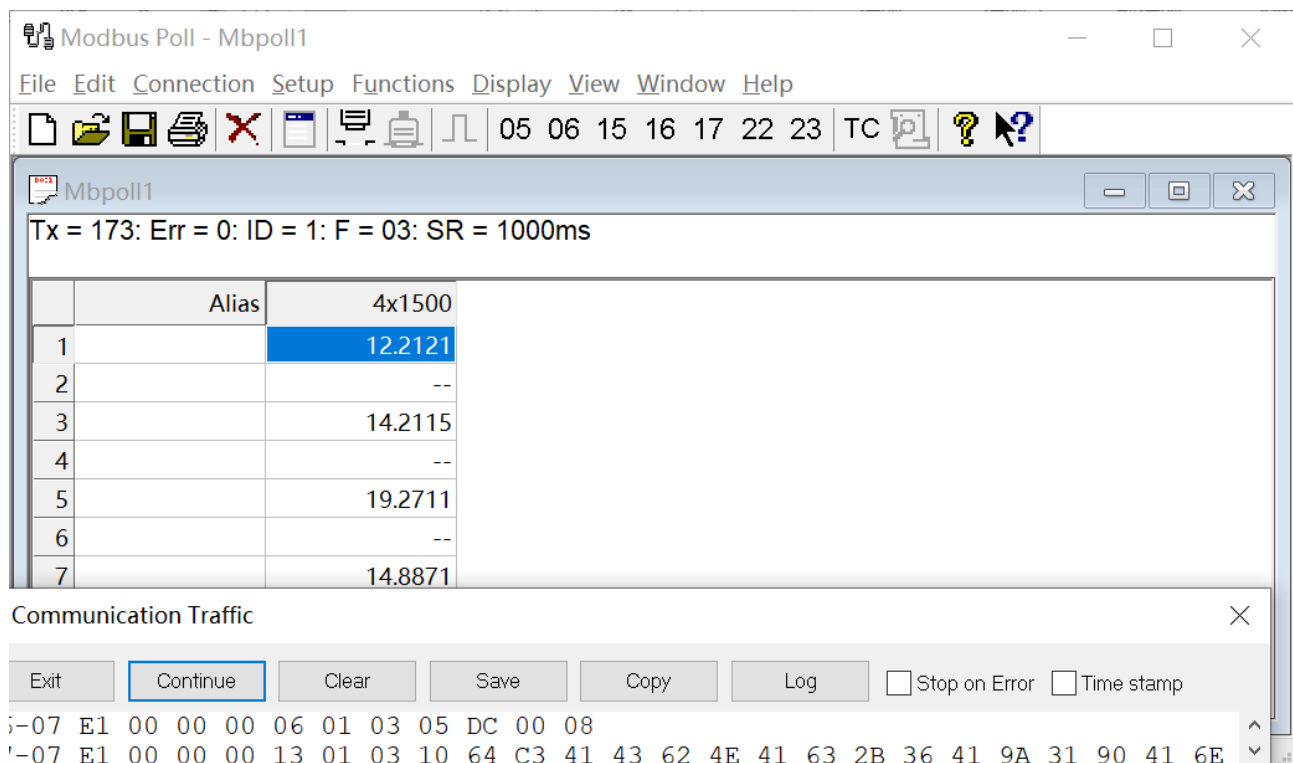
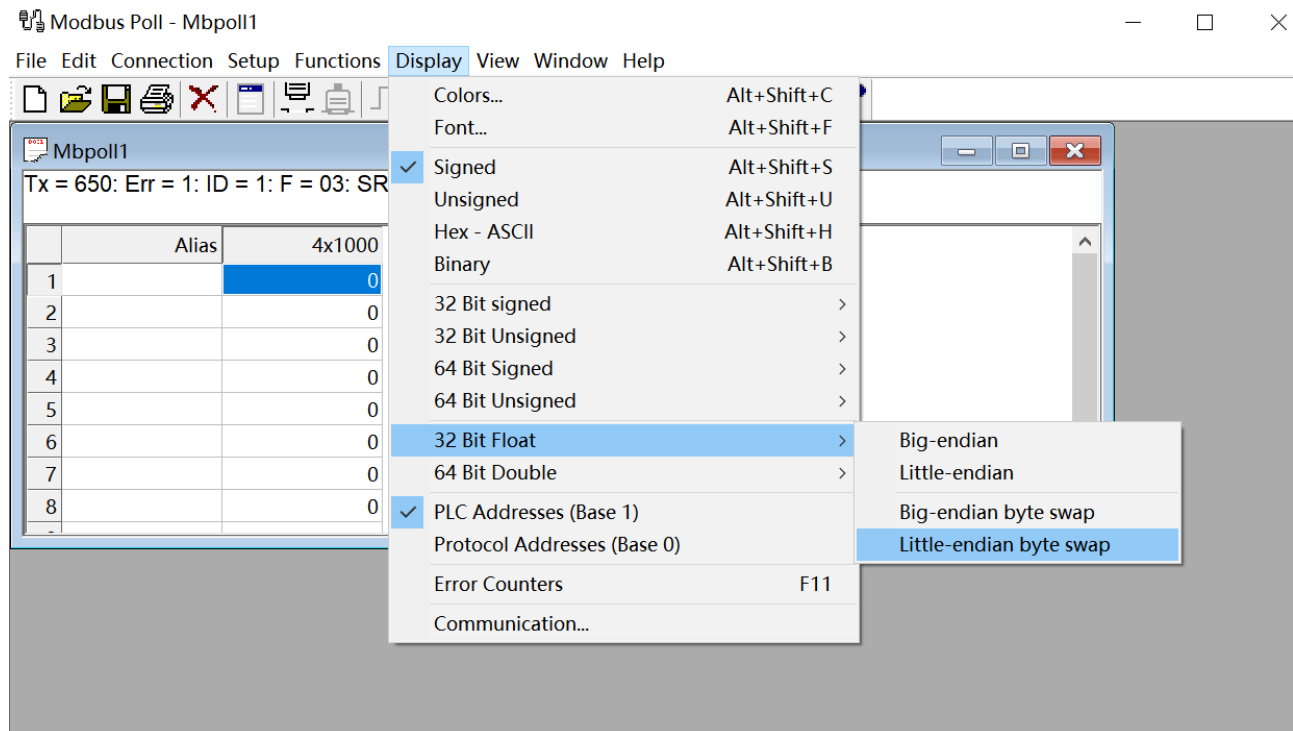
Choose function code 03

Number of registers

Choose PLC address

For Help, press F1. Port 1: 4800-8-N-1

Choose 32 Bit Float



Modbus poll connection is shown in Modbus TCP to RTU tool

| Config | | | | | | |
|----------------|------|-----------------|---------------------|--------------------|-------------------------|---------|
| Device list(2) | | | | | | |
| Help | | | | | | |
| | Name | ID | IP | Connect state | Last communication time | Operate |
| 1 | | 00000001 | 192.168.1.162:56507 | data communication | 2022-08-02 18:09:53 | |
| 2 | | 127.0.0.1:57331 | 127.0.0.1:57331 | data communication | 2022-08-02 18:09:54 | |

It's Modbus poll connection