Additional Setup Instructions for Modbus: RTU, ASCII, TCP, Omni & Enron

Table of Contents

Table of Figures

SETUP INSTRUCTIONS FOR MODBUS RTU, ASCII, TCP, OMNI, AND ENRON

Setup for Modbus RTU and ASCII

Modbus ASCII and Modbus RTU protocols have three selections on the launcher menu. The appropriate selection depends upon physical characteristics of your network.

If your system is running over a physical layer that is 2-Wire RS-422/485, select either the Modbus RTU on 2Wire RS422/485 or the Modbus ASCII on 2-Wire RS422/485, depending upon which protocol your system is using. In this case there are no special wire-tapping instructions. If your system is not a 2-wire RS422/485 system, you must select the correct launcher item based upon the following information.

There are two decodes for Modbus RTU: Modbus RTU Master and Modbus RTU Slave. Similarly, there are two decodes for Modbus ASCII: Modbus ASCII Master and Modbus ASCII Slave. The Master and Slave refer to where in the circuit NetDecoder is connected. The rest of this topic will simply refer to Modbus Master or Modbus Slave, as the principles are the same.

Modbus Master assumes that data from the Master is on the DTE side (i.e. master data is on the TxD pin and slave data on the RxD pin). If NetDecoder is connected to a Master device, choose the Modbus Master decode.

Modbus Slave assumes that data from the slave is on the DTE side (i.e. slave data is on the TxD pin and master data on the RxD pin). If NetDecoder is connected to any Slave device, choose the Modbus Slave decode.

The diagram below illustrates conceptually which decoder to choose. Your configuration may be different from the diagram. The important thing is to choose Modbus Master if the master data is on the transmit line, or Modbus Slave if the slave data is on the transmit line.

Once you have selected the correct protocol, be sure to set the Register Display Settings so your data is decoded correctly. See the section titled Modbus Register Display Format Settings below for information.
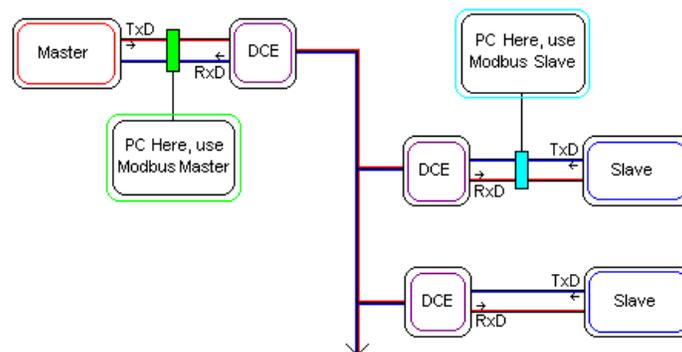
Figure 1 Modbus Cable Connection Diagram

Setup for Modbus TCP

Generally, Modbus conversations tend to be between just two devices and it's easy to define Master and Slave. On more complex TCP networks, the relationship can be less certain. It is possible for a device to function as both Master and Slave. It is certainly possible to have more than two devices in a Modbus TCP conversation.

NetDecoder uses two methods to determine whether a frame is from a Master or a Slave. If an IP address is explicitly defined then NetDecoder will always decode frames that way. If an IP address is not defined then NetDecoder will still make an attempt. The first time it encounters the combination of IP Address+Transaction ID+Modbus Function Code, it will assume that it came from a Master. When it sees that same combination again, the decoder will assume that it came from a Slave. For this method to work, Modbus TCP transaction IDs must be unique.

To explicitly define an IP Address as Master or Slave, follow the steps below to enter this information into NetDecoder.

1. Start NetDecoder. Choose NetDecoder from Start | Programs | Frontline NetDecoder [version#] | Frontline NetDecoder | Frontline NetDecoder. Then from the *Choose Protocol to Analyze* dialog, expand the *Modbus* folder, select the *Modbus TCP* icon, and click the *Run* button. Then choose *Set Initial Decoder Parameters* from the *Options* menu on the Control window and select the *Modbus TCP* tab.
2. Enter the IP Address of the Master in the *IP Address* box.
3. In the *Node Type* box, select *Master*.
4. Click *Add*.
5. Enter the IP Address of a Slave in the *IP Address* box.
6. In the *Node Type* box, select *Slave*.
7. Click *Add*.
8. Repeat for each additional Slave.
9. When finished, click *OK*.
10. Set the Register Display Format Settings below.

That's all the information NetDecoder needs. You can fill in the rest of the information if you choose, but it isn't required. When you start NetDecoder, Modbus TCP frames should be correctly decoded depending on whether their type is Master or Slave. Follow the above steps to add or delete nodes as needed.

You can include nodes for more than one location. For example, if you have 3 sites, each with a Master and Slaves, you can include the IP Addresses for all 3 sites in one node file.

Modbus Register Display Format Settings

Modbus protocol messages do not provide data formatting information but simply transmit holding and input registers as byte streams. The Modbus Register Display Settings dialog provides a method for users to define display formats to be utilized when displaying the values in these registers.

> To access this dialog, go to the *Options* menu on the Control window and choose *Set Initial Decoder Parameters*, and select the *Modbus* tab.

> To add a new entry, fill in the fields and click the *Add* button.

> Double-clicking a setting copies its values to the input fields.

> To replace a setting with a new setting created from the input fields, click the setting to replace and then click the *Modify* button.

When you close a capture file, you will be asked whether you want to save the current register settings into it. To save settings independent of a specific capture file, type any string in the "Apply Template" field and click Save. To restore those settings to the dialog, select the desired setting in the "Apply Template" dropdown list.

New settings will not take effect in a currently opened capture file until the frame display is closed and then reopened.

Register Display Settings

Default Display Format_Bits

This field specifies the default display format for registers that have no user defined setting (such registers are always assumed to be 2 bytes long). The default display format is limited to single-register display formats to prevent implicit register range overlap and to ensure that explicitly defining a setting in which one display format item uses multiple registers does not change the locations of subsequent default settings.

Station Address

The IP Address or Station Address field (its name changes to reflect the loaded decoder) is used to enter the desired IP or station address for each setting. Enter an asterisk to specify that a setting applies to all IP or station addresses. Station address ranges are from 0 to 248 and IP address ranges can be any valid IP Address.

Register Type

The Register Type field specifies the type of register, either HOLDING or INPUT.

Bytes Per Register

This field will default to 2, indicating that standard Modicon registers are 2 bytes each. If you are dealing with a third party implementation of Modbus, you may need to adjust this field to reflect the actual number of bytes in a single register.

Register Start Address

Enter the address of the first register you want to specify settings for.

Display Format_Bits

The Display Format_Bits field specifies the desired display format. Display formats ASCII and HEX are variable-length and display a char or hex byte respectively for each byte in a register. The other display formats (INT_16, FLOAT_32, etc) have a bit count suffix in their names and use as many registers as they need, based on the bytes per register field. Choose a format for the specified register range.

Length

This field is the desired number of data items (e.g. INT_32s), not the number of registers. The number of registers will be calculated and displayed in the text description.

Example

If you want to specify Station 3's input registers 0-99 as INT_16s, you would enter 3 for the Station Address, INPUT for the Register Type, 0 for the Start Address, 2 for Bytes Per Register, INT_16 for the Display Format and 100 for the Length, indicating that you have 100 INT_16s starting at Input Register Address 0 where each register is 2 bytes long.

Setup for Modbus Omni

As discussed in Section 1.3, Modbus protocol messages do not provide data formatting information but simply transmit holding and input registers as byte streams. The Modbus-Omni standard defines a particular display format for the values in the registers. To make it easy for the end-users, Frontline provides a predefined template that users can load while monitoring Modbus-Omni networks.

The Modbus Register Display Settings dialog provides a method for users to load the Modbus-Omni template.

1. To access this dialog, go to the *Options* menu on the Control window and choose *Set Initial Decoder Parameters.*

2. Select the *Modbus* tab.

The File Open icon should now be enabled.

3. Click on it and select *Omni.*
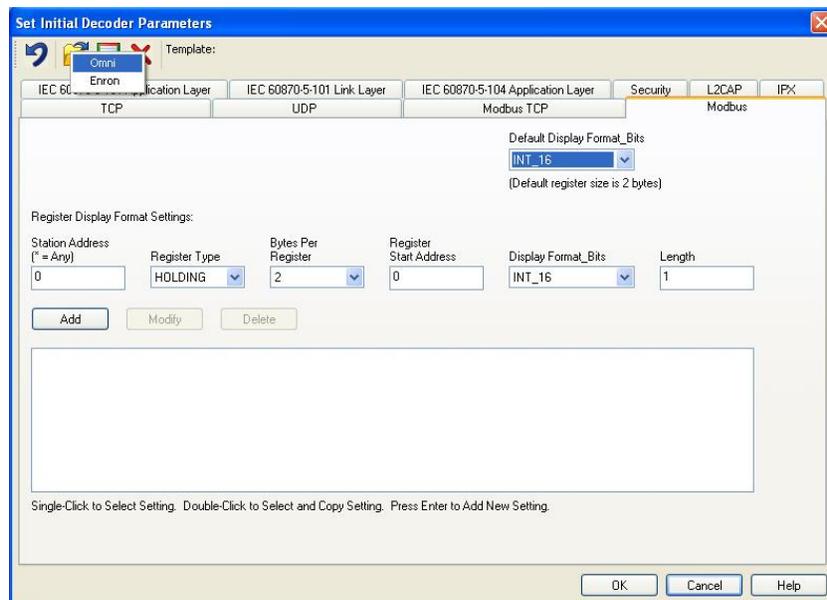
Figure 2 - Omni

This should load up the register display settings for Modbus-Omni standard.

Set Initial Decoder Parameters

Template: Omni

| IEC 60870-5-101 Application Layer | IEC 60870-5-101 Link Layer | IEC 60870-5-104 Application Layer | Security | L2CAP | IPX |
| TCP | | UDP | Modbus TCP | | Modbus |

Default Display Format_Bits
INT_16
(Default register size is 2 bytes)

Register Display Format Settings:

| Station Address (* = Any) | Register Type | Bytes Per Register | Register Start Address | Display Format_Bits | Length |
| * | HOLDING | 4 | 17001 | FLOAT_32 | 1199 |

Add   Modify   Delete

Station * - Display HOLDING Registers 4001 thru 4999 (8 bytes each) as ASCII (Number of ASCII's = 999)
Station * - Display HOLDING Registers 5001 thru 5999 (4 bytes each) as DINT_32 (Number of DINT_32's = 999)
Station * - Display HOLDING Registers 6001 thru 8999 (4 bytes each) as FLOAT_32 (Number of FLOAT_32's = 2999)
Station * - Display HOLDING Registers 9001 thru 9499 (128 bytes each) as ASCII (Number of ASCII's = 499)
Station * - Display HOLDING Registers 14001 thru 14399 (16 bytes each) as ASCII (Number of ASCII's = 399)
Station * - Display HOLDING Registers 15001 thru 15299 (4 bytes each) as FLOAT_32 (Number of FLOAT_32's = 299)
Station * - Display HOLDING Registers 17001 thru 18199 (4 bytes each) as FLOAT_32 (Number of FLOAT_32's = 1199)

Single-Click to Select Setting. Double-Click to Select and Copy Setting. Press Enter to Add New Setting.

OK   Cancel   Help

Figure 3 - Load Register Display Settings for Modbus-Omni

4. Click *OK* and continue with your data capture and analysis.

Setup for Modbus Enron

As discussed in Section 1.3, Modbus protocol messages do not provide data formatting information but simply transmit holding and input registers as byte streams. The Modbus-Enron standard defines a particular display format for the values in the registers. To make it easy for the end-users, Frontline provides a predefined template that users can load while monitoring Modbus-Enron networks.

The Modbus Register Display Settings dialog provides a method for users to load the Modbus-Enron template.

1. To access this dialog, go to the *Options* menu on the Control window and choose *Set Initial Decoder Parameters*.

2. Select the *Modbus* tab.

The File Open icon should now be enabled.

3. Click on it and select *Enron.*
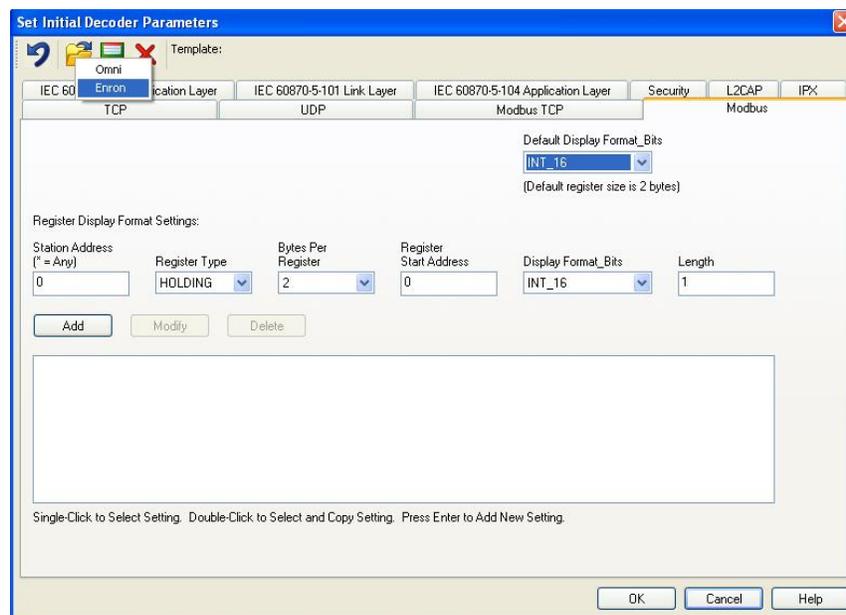
Figure 4 - Enron

This should load up the register display settings for Modbus-Enron standard.
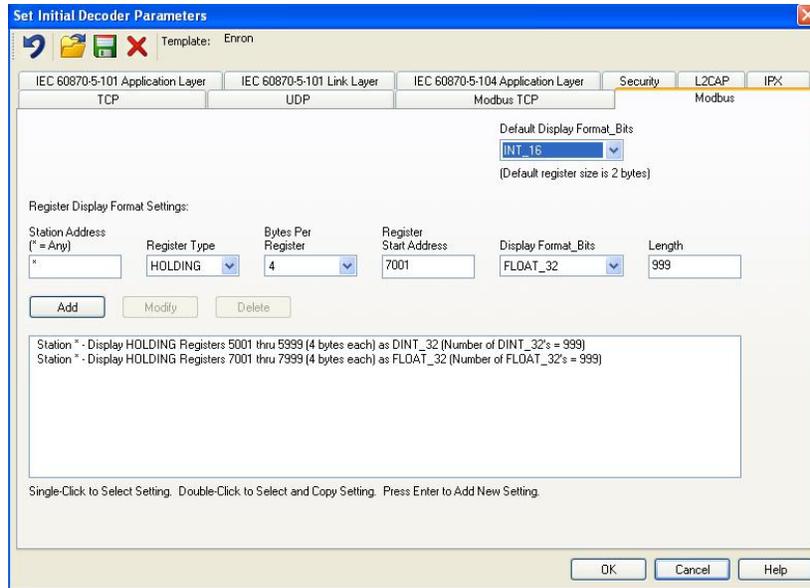
Figure 5 - Load Register Display Settings for Modbus-Enron

4. Click *OK* and continue with your data capture and analysis.