Modbus:

Remote Lab instructions

Modbus Serial RTU

V7

Created By:	Danie Stoop, Edwin Wright	Date:	Pre-3/10/14
Reviewed By:	Steve Steyn	Date:	3/10/14
Revised By:	Edwin Wright	Date	7/4/20



Instructions Basics

Getting Started

- Logon to Electromeet (Follow the New_Remote_Lab_Instructions document)
- The Modbus software **MB Poll** and **MB Slave** is installed on various labs.

Hardware:

Normally we would run the Modbus simulation software (client and server a.k.a. master and slave) on two separate computers, via a null modem cable. However, in this case we are running them both on one machine, via a virtual null modem.

Software used:

- Modbus Poll v8.0.0
- Modbus Slave v7.0.0
- TAL Virtual Null Modem(taltech.com)
- All the above is installed on the Remote Lab computers

Modbus Serial

You can complete this practical assignment by logging into the Electromeet Remote Lab computer as per above.

You do not need any specialised hardware of your own, as was the case in the past. There is a virtual null modem running which creates two linked virtual serial ports.

We will be using COM1 and COM2

Open TAL Virtual Null Modem by clicking on the icon (on desktop or taskbar)



Use the default settings for COM1 on COM Port - A and COM2 on COM Port - B Then Tick the two Boxes:

"Auto-activate when launched" and "Auto-minimize when activated"

Ý

😽 Virtual Null M	-		\times
COM Port - A	СОМ СОМ	Port - B	•
Auto - activate	when la when a	aunched activated	
Acti	vate		

Now click the "Activate" button and the window will be minimized to taskbar.

Now run both the MODBUS Master (ModbusPoll) and the Modbus Slave (ModbusSlave) by clicking on the desktop icons.



The easiest approach is to run them side-by-side, adjusting them to fit in next to each other like this:

Madbus Slave - Mitslave1 File Edit Connection Setup Display View Window Help	× 4	1월 Madbus Poll - Mbpoll1 File Edit Connection Setup Functions Display View Window Help □ ☞ 晶 ● × □ 二 色 小 05 06 15 16 17 22 23 TC 定	×
Motion Image: Control of the second sec		Metpoliti Tx = 0. D = 1; F = 03. SR = 1000ms No connection 4 0 3 0 4 0 3 0 4 0 9 0	
For Help, press F1. Port 1: 9600-8-E-1	Fo	or Help, press F1. Port 1: 960	J-8-E-1

Let's start with the Slave.

First we are going to configure the way in which the information is displayed, viz. (a) binary (all 1's and 0's) and (b) Base 0 i.e. protocol address notation, starting from 0 (as opposed to PLC addresses, starting from 1).

Click *Display* and select *Binary*, then click *Display* again and select *Protocol Addresses (Base 0)*. You will end up with something like this:

Disp	olay View Window Help		
	Signed	Alt+Shift+S	
	Unsigned	Alt+Shift+U	
	Hex	Alt+Shift+H	
~	Binary	Alt+Shift+B	
	32 Bit signed	>	
	32 Bit Unsigned	>	
	64 Bit Signed	>	
	64 Bit Unsigned	>	Big-endian
	32 Bit Float	>	Little-endian
	64 Bit Double	>	Big-endian byte swap
	PLC Addresses (Base 1)		Little-endian byte swap
~	Protocol Addresses (Base Ø)		
	Communication		

Now hit F2 or click *Setup-> Slave definition*. Set the slave up as follows.

Slave Defin	ition ×
Slave ID:	1 ОК
Function:	01 Coil Status (0x) V Cancel
Address:	0 Protocol address. E.g. 11 > 10
Quantity:	19
View Rows 10 Hide	O 20 O 50 O 100 O Fit to Quantity Alias Columns □ PLC Addresses (Base 1)
Error Sim Skip r 0	esponse Insert CRC/LRC error (Not when using TCP/IP) [ms] Response Delay Return exception 06, Busy

The slave address in this case is 1. Function Code (FC) = 01 (Coil status). Address = 0 refers to the logical address of the first coil, and Quantity = 19 means that there are 19 consecutive coils (numbered 0 thru 18). This is just an arbitrary number in our case.

	Alias	00000	Alias	00010
i i		0		0
		0		0
		0		0
		0		0
		0		0
		0		0
		0		0
		0		0
		0		0
		0		

To edit any coil, just double-click on it and toggle the radio buttons on Edit Coil between on and off. You can do this once the simulation is running.

	Alias	00000	Alias	00010	
0		0		0	
1		0		0	
2		q		0	
3		0		0	
4		0		0	
5		0		0	
6		0		0	
7		0	Edit Coil	-	~
8		0	Eurecon		~
9		0	Value On	OOff	OK
			Auto chi	ange	Cancel

Click *Connection->Connect* and set up the serial communications parameters as shown using the VSPE Connector COM port – COM 1 for default configuration. Ensure that RTU mode is selected. Then click OK.

📓 Modbus Slave - Mbslave1	
File Edit Connection Set	up Display View Window Help
🗅 📽 🖬 🚭 🛅 🗏 😫	ä ? ₩?
Price Edit Connection Set D Image: Connection D Image: Connection Image: D Image: Connection Alias 0 1 1 2 1 3 1 4 5 6 7 8 9	O0000 Alias O0000 Alias Outer of the second s
	127.0.0.1 🗸 502
	Any Address © IPv4 Ignore Unit ID O IPv6

Check the port settings carefully, as the Master side settings have to match. The configuration here is COM1 9600,8,N,1.

Now let's turn our attention to the Master side.

Click *Display* and set it up as follows (the same as for the Slave).

Disp	lay View Window Help		
	Signed Unsigned Hex	Alt+Shift+S Alt+Shift+U Alt+Shift+H	
~	32 Bit signed 32 Bit Unsigned 64 Bit Signed 64 Bit Unsigned	AIC+SUITC+B	Big-endian
	32 Bit Float 64 Bit Double PLC Addresses (Base 1)	>	Little-endian Big-endian byte swap Little-endian byte swap
~	Protocol Addresses (Base 0) Communication		

웹 Modbus Poll - Mbpoll1
File Edit Connection Setup Functions Display View Window Help
🗅 📽 🖬 🎒 🗙 🛅 🗒 🚊 💷 05 06 15 16 17 22 23 TC 🗵 💡 🛠
Tx = 0: Err = 0: ID = 1: F = 03: SR = 1000ms
No confliction
Alias 00000
Read/Write Definition
3 Slave ID: 1 OK
4 Function: 01 Read Coils (0x) V Cancel
5
6 Address: 10 Protocol address. E.g. 11 -> 10
7 Quantity: 2
9 Scan Rate: 1000 [ms] Apply
Disable
Read/Write Disabled
Disable on error Read/Write Once
View
Rows
● 10 ○ 20 ○ 50 ○ 100 ○ Fit to Quantity
Hide Alias Columns DLC Addresses (Base 1)
Address in Cell Enron/Daniel Mode

In the poll definition above, coils 10 and 11 (starting with 10, total =2) on slave 1 will be read once every second. Click *OK*.

Hit F3 or click *Connection->Connect*. Select COM 2 by default ensuring that the settings are the same as for the Slave. COM2 : 9600,8,N,1. Also ensure that RTU mode is selected.

诸 Modbus Poll - N	/bpoll1				
File Edit Connec	tion Setup Function	ns Display View	Window Help		
🗅 🚔 🖬 🎒 🏅	х 🗖 🗏 👜 л	05 06 15 16	17 22 23 TC	P. 💡 📢	
Mbpoll1					
Tx = 0: Err = 0:	ID = 1: F = 01: SR	= 1000ms			
No connection					
Alia	sl 00010				~
1	Connection Setup				^
2	Connection			1 [ОК
3	Serial Port		~		
4	Serial Settings			; L	Cancel
5	COM2		~	Mode	
7		1		€RTU	○ ASCII
8	9600 Baud ~			D	There are at
9	8 Data bits 🛛 🗸			1000	froc [*]
	None Parity ~	1		1000	Luis-
	nono r onc,	1		Delay Bet	ween Polls
	1 Stop Bit 🗸 🗸		Advanced	20	[ms]
	Remote Modbus Se	rver			
	IP Address or Node	e Name			
J	127.0.0.1				~
	Server Port	Conne	t Timeout	⊚ IPv4	
	502	3000	[ms]	O IPv6	

If all goes according to plan, connection will be established.

If a red 'timeout' message appears on either side, do the following.

- Click Disconnect on both sides
- Check that the communications parameters are the same for both sides
- Reconnect on both sides

If a red 'illegal' message appears on either side, do the following.

- Click Disconnect on both sides
- Check if the poll definitions match (slave addresses and function codes)
- Check that the coils read by the Poll program are a SUBSET of the coils defined by the Slave program, and not the other way around
- Reconnect on both sides

Click *Display->communications* and observe the traffic between master and slave. Remember that it is as seen from the master's perspective, the display on the slave will be the other way around i.e. Tx on the master will be Rx on the slave.

×

📧 Communication Traffic

Exit	Con	tinue	•		Clea	r		Save	Сору	Log	Stop on Error	Time stamp
Tx:000000-01	01	00	0A	00	02	9D	C9					
Rx:000001-01	01	01	00	51	88							
Tx:000002-01	01	00	ΟA	00	02	9D	C9					
Rx:000003-01	01	01	00	51	88							
Tx:000004-01	01	00	0A	00	02	9D	C9					
Rx:000005-01	01	01	00	51	88							
Tx:000006-01	01	00	0A	00	02	9D	C9					
Rx:000007-01	01	01	00	51	88							
Tx:000008-01	01	00	0A	00	02	9D	C9					
Rx:000009-01	01	01	00	51	88							
Tx:000010-01	01	00	0a	00	02	9D	C9					
Rx:000011-01	01	01	00	51	88							

Tx refers to the Modbus request, because we are looking at the Master here. 0x means Hex.

- Slave = 0x01 (i.e. 1 decimal)
- Function code = 0x01 (1 = Read coil status)
- Initial coil address = 0x000A (i.e. decimal 10 protocol or decimal 11 PLC)
- Number of coils = 0x0002
- CRC = 0x9DC9

Rx refers to the Modbus Rx response:

- Slave = 0x01
- Function = 0x01
- Byte count = 0x01
- Coil status = 0x00 = 00000000 (both coils cleared)You might have to reinitialise or plug in the modems just to make sure it is running.
- •
- CRC = 0x5188

When you have finished lab make sure you close ALL Modbus windows. Click on TAL icon in TaskBar and then click "Deactivate" before closing the window and logging off the Remote Lab.

Modbus TCP

Although not required for this Lab, if you do wish to play with MODBUS over TCP/IP, you can do a loopback by writing and reading from **IP address 127.0.0.1 Port 502** (which is your PC's default local loopback IP address) with both ModbusPOLL and ModbusSLAVE.

The purpose of this document is to introduce you to the Modbus/TCP concept. You may, however, be asked in your assignments to use other registers, etc. Also take care to use the IP address in bold (above) and not the one in the screenshots below. The following shows setup for FunctionCode 03 - Holding Registers.

🗿 Modbus Slave - Misslave1	– 🗆 X	월 Modbus Poll - Mbpoll1	- 🗆 ×
File Edit Connection Setup Display View Window Help		File Edit Connection Setup Functions Display View Window Help	
D 🚅 🖬 🚭 🛅 📃 🚊 😵 😵		D 🖨 🖬 🕾 📉 🛅 🗒 🙏 🗅 05 06 15 16 17 22 23 TC 🖳 🤋 🎇	
Mislavel Image: Commention D = 1: F = 01 0 No connection 0 Aliss 00000 Aliss 00000 0 0 1 Save Defmition 2 Slave Defmition 3 Slave Defmition 4 Function: 5 Function: 6 Addees: 1 Pholocol address. E.g. 40011 > 10 0 Quantity: 10 20 9 View @ Not Fit to Quantity: 10 20 9 View @ Not Fit to Quantity: 10 20 50 10 20 50 10 20 50 10 20 50 10 20 50 10 20 50 10 20 50 10 20 50 10 20 <	*	Mappelit Image: Constraint of the second secon	

Run the Modbus Poll and Modbus Slave from the desktop icons as shown above for for serial

Setup the Modbus TCP connection on both Master and Slave as shown below. Note the Master uses loopback IP address of Slave : 127.0.0.1.

🔄 Modbus Slave - Mbslave1 - 🗆 🗙	🖸 Modbus Poll - Mbpoll1 — 🗆 🗙
File Edit Connection Setup Display View Window Help	File Edit Connection Setup Functions Display View Window Help
D 📽 🖬 🚳 🛅 🗏 🛕 🔋 🕺	D 🖆 🖬 🚭 🗙 🛅 🗒 🚊 🕮 05 06 15 16 17 22 23 TC 🗵 🔋 😵
Modelsve1 Image: Connection Setup Alias 00000 Alias 00000 Connection Setup X 1 Connection Setup 2 Connection 3 Mode 4 Senid Setings 6 COM1 9 Boad 9 Boad 0 Serid Setings OK 1 Cancel 9 Serid Setings 6 COM1 9 Boad 9 Boad 1 Stop Bit Flow Control None Paily DSR 1 Stop Bit Image: Pot 127.0.1 So2 Any Address IPv4 I gnore Unit ID IPv6	Mode OK Alias 0000 Alias 0000 Alias 0000 Connection OK Alias 0000 Connection OK Serial Settings Cancel Serial Settings Cancel Serial Settings Cancel 9 B Data bits Incol 1000 Ims; Delay Between Pols 20 Ims; Remote Modbus Server IP Address or Node Name I27.0.1 V Server Port Connect Timeout @IPv6

Set the Register ranges for both Master and Slave as follows and Click *OK* on both. This time we will be using FC03.

🗿 Modbus Slave - Mbslave1	– 🗆 X	📽 Modbus Poll - Mbpoll1 - 🗆 >										
File Edit Connection Setup Display View Window Help		File Edit Connection Setup Functions Display View Window Help										
		🗅 🖆 🖬 🚭 🗙 🛅 🗒 🚊 几 05 06 15 16 17 22 23 TC 🕺 🤋 🎗										
Image: Constraint of the constraint		Image: Contract of the state of th										

In the poll definition above, holding registers 0 thru 9 inclusive (protocol) i.e. 40001 thru 40010 will be read once every second. Click *OK*.

붭	Modbus Poll - M	Ibpoll1			
File	Edit Connect	tion Setup Functions	Display View	Window Helj	р
	🚔 🖬 🕾 🔁	(미분희)지(05 06 15 16	17 22 23 TC	: 🖻 🛛 🖇 🕅
	Mbpoll1				
Ъ	< = 520: Err = (0: ID = 1: F = 03: SR	= 1000ms		
	Alias	00000	Alias	00010	
0	0			0	
1	1	0000 0000 0000 0000			
2	2	0000 0000 0000 0000			
1	3	0000 0000 0000 0000			
4	1	0000 0000 0000 0000			
5	5	0000 0000 0000 0000			
e	5	0000 0000 0000 0000			
2	7	0000 0000 0000 0000			
1	3	0000 0000 0000 0000			
9	9	0000 0000 0000 0000			

B Data bits I [1000 [ms]	ТСРЛР 🔽	Mode © BTU C ASCI	ОК
8 Data bits I 1000 [ms]	9600 Baud 🗾	- Besponse Timeout	Cancel
	8 Data bits 🔄	1000 [ms]	
Odd Parity 🔄 🔤 Delay Between Polls	Odd Parity 🗾	Delay Between Polls	
1 Stop Bit 🗾 10 [ms] Advance	1 Stop Bit 🖃	10 [ms]	Advanced
	IP Address	Port	_
IP Address Port	192.168.2.4	502	

If all goes according to plan, connection will be established. If a red 'timeout' message appears on either side, do the following.

- Click Disconnect
- Check the IP address and port number
- Reconnect

If it still does not work, click *Display->Communication* and check if you are at least getting messages sent (Tx). If this is the case, the Slave is not responding. Check Modbus Slave sett 192.168.1.30

Let's proceed.

Click *Display->communications* and observe the traffic between master and slave. Remember that it is as seen from the master's perspective.

Communication	n Traff	fic																							Х
Exit	Con	itinue	9		Clea	r		S	ave			Сор	y		l	.og			Stop (on Er	ror	П	ime s	tamp	I
Tx:000012-00	0A	00	00	00	06	01	03	00	01	00	0A														~
Rx:000013-00	ΟA	00	00	00	17	01	03	14	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	I.
Tx:000014-00	ŌВ	00	00	00	06	01	03	00	01	00	0Å														
Rx:000015-00	Oв	00	00	00	17	01	03	14	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	I.
Tx:000016-00	0C	00	00	00	06	01	03	00	01	00	0A														
Rx:000017-00	0C	00	00	00	17	01	03	14	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	I.
Tx:000018-00	ΟD	00	00	00	06	01	03	00	01	00	0A														
Rx:000019-00	ΟD	00	00	00	17	01	03	14	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	I.
Tx:000020-00	ΟE	00	00	00	06	01	03	00	01	00	0A														
Rx:000021-00	ΟE	00	00	00	17	01	03	14	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1
Tx:000022-00	0F	00	00	00	06	01	03	00	01	00	0a														
Rx:000023-00	0F	00	00	00	17	01	03	14	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	I.
Tx:000024-00	10	00	00	00	06	01	03	00	01	00	0a														
Rx:000025-00	10	00	00	00	17	01	03	14	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	١v
<																								3	

Let's now compare the messages with the ones you obtained with Modbus RTU earlier.

When we look at the Modbus/TCP messages, as opposed to the Modbus Serial messages, we notice the original PDU in there (03 00 00 00 0A), plus several extra bytes in the beginning (e.g. 0F 00 00 00 06, as well as the absence of a two-byte checksum at the end.

Notice how the Transaction Identifier increments after every Request/Response pair.