

# Software requirements

Students can Logon to Electromeet (Follow the "How to Connect to Remote Labs\_Electromeet\_HTML5\_Remote\_Lab" instructions document)

## The software is installed on Remote Lab 1 & 2

It is suggested that you run this in a virtual machine using a windows 7 32 bit image so that you do not break your real operating system – highly recommended. They are available for most virtualisation options here: <u>https://dev.windows.com/en-us/microsoft-edge/tools/vms/windows/</u>

**Software**: Wireshark, download and install to your own computer from <a href="http://www.wireshark.org">http://www.wireshark.org</a>

Tutorial video WireShark http://wiresharkdownloads.riverbed.com/video/wireshark/introduction-to-wireshark/

Follow the ModBus specific software supplied.

- SetupVSPE (serial port emulator)
- Modbus slave and master sw.

Modbus Poll - install "mbpollsetup" and use the registration information provided in the Word or RTF file "Modbus\_poll\_slave\_serial\_numbers". - Please note that everything is case sensitive!

Modbus Slave - install "mbslavesetup" as under Modbus Poll.

Virtual Serial Port Emulator – install "SetupVSPE.msi". - There is a registration string to use in the VSPE\_API\_32\_KEY.TXT file.

Screen Capture software if you don't have it already a good and free option at <a href="http://getgreenshot.org/">http://getgreenshot.org/</a>

Alternately this may be run on Remote Labs 1 and 2. The virtual com port software is different and this will be explained in a separate section.

#### Purpose / Background

The purpose of the first practical component of this assignment is for you to simulate a Modbus Master querying a Modbus Slave over a serial link.

Typically one would run Modbus Poll on one machine and Modbus Slave on another linked by means of a serial communication. If you have 2 machines with Serial ports and a Null Modem cable this can be done with ease. More typically recent machines do not have a serial port on them and as such one needs to work around this. One can install a USB-Serial converter on each machine and then again, link the 2 machines with a Null Modem cable.

However – we have software - a Virtual Port Serial Emulator (VSPE) where you can run virtual serial ports on ONE PC in a configuration to which both Master and Slave applications can connect.

### **Virtual Comm Ports**

After installing all the software you need to check which serial ports are available on the PC by going into Device Manager and checking. As the example below, this sample is all clear for any port a user wants to use.



One then needs to setup a Connector within VSPE. This then opens up a new virtual serial port which can be opened twice – thus allowing us to run Modbus Poll and Modbus Slave locally within the same machine



#### Select Connector and then Next

Specify device type	
VIRTI	Device type Connector  Unlike regular serial port, connector is a virtual device that can be opened twice. When opened, it creates data pipe between its clients. That allows separate applications use the same serial port to exchange data.
New serial port	💾 Existing serial port
	< Back Next > Cancel Help

Pick a free port from your device check and click on "Finish".

You should now have a virtual comm port that you can turn on and off at will

📚 Virtual Serial Ports Emulator (Emulation started)		
File View Language Emulation Device Help		
🖻 🖬 🕨 🔹 🎠 🕷 🗐	•	
Title	Device	Status
COM1	Connector	Ready
(Tuesday, November 11, 2014) [COM1] Initia	lizationOK	
(Tuesday, November 11, 2014) [COM1] Initia	lizationOK	

Once you have nominated the Connector within VSPE the infrastructure is in place. **Note** that you should use a Comm port Number up to and including 8 ONLY, because the Modbus software does not go beyond that. Once you have setup the VSPE Connector minimise it to the Task bar.

#### **Remote Lab Virtual comm ports**

On the remote lab you will find this icon



When double clicking it a window like this should appear



The comm ports shown are a connected pair and you need to set the Modbus Slave to one of them and the Modbus Poll to the other, they may vary between the labs so make sure to check. Ensure you use a pair that is port 8 or less to be compatible with the Modbus software.

If you don't get serial working in the modbus software you may need to unplug and plug back in the Virtual modem from the system menu



#### **Modbus Slave and Poll**

In order to get the link up and running go into Modbus Slave first. Go into Setup, Slave Definition

Change the Slave ID to 3 and Function to 01 – Coil Status. Alter the range (Address 1 for a length of 12 coils)

OK this.

Slave Defin	iition	×
Slave ID: Function: Address: Length:	3 01 COIL STATUS 1 12	OK Cancel

#### Go into Connection, > Connect.

Select the virtual Connector you have defined in VSPE (or one of the ports on the Lab) Set the rates ... typically 9600, 8 Data Bits, No parity, 1 Stop bit

Select RTU mode OK this.

Connection	vour port n	umber 🔀
Port 1	Mode © RTU O ASCII	ОК
9600 Baud 💌		Cancel
8 Data bits 💌	🔲 Ignore Unit ID	
None Parity 💌	Flow Control	
1 Stop Bit 💌	RTS Toggle 1 [ms] F	RTS disable delay

Then go into Modbus Poll.

Go into Setup, > Poll Definition

Change the Slave ID to 3 and Function to 01 – Read Coils. Alter the range (Address 1 for a length of 12 coils)

Leave the Scan rate as 1000 ms.

Click OK.

Poll Definit	ion	×
Slave ID:	3	ОК
Function:	01 Read Coils 🔹	Cancel
Address:	1	
Length:	12	Apply
Scan Rate:	1000 ms	
🔽 Auto Re	ead Enable	Read Once

Go into Connection, > Connect.

Select the **same** virtual Connector comm port you have defined in VSPE (or on the Lab the other comm port of the pair)

Set the rates ... To what you used in the Slave (note the defaults between Modbus Poll and Slave are different!!)

Select RTU mode Click OK.

Modbus Poll will then be sending messages to Modbus Slave. You will see this in the Modbus Poll window with Tx and Error count. The Tx should be going up and the error rate not going up (there may be a couple of errors initially).

To change a coil – you can double click on a coil within Modbus Slave and change it). On accepting (clicking OK), you will see the value change within Modbus Master ie. It has been successfully read.

📴 Mbslav1		
ID = 3		
00001 = 0 00002 = 0	Edit Coil	<b>—</b>
00003 = 0 00004 = 0	Value ⊂ On ⊙ Off	ОК
00005 = 0 00006 = 0	Auto change	Cancel
00007 = 0 00008 = 0		
00009 = 0 00010 = 0		
00011 = 0 00012 = 0		

Also please look at Display, Communication in either (the Tx/Rx will be reversed from one to the other) – which shows what is being sent across the network.

Communication Traffic	<b>—</b> ×
Exit Stop Save Copy Stop on Error	
000037-Rx:03 01 02 00 00 C0 3C 000038-Tx:03 01 00 00 00 0C 3D ED 000039-Rx:03 01 02 00 00 C0 3C 000040-Tx:03 01 00 00 00 0C 3D ED 000041-Rx:03 01 02 00 00 C0 3C	^
000042-Tx:03 01 02 00 00 0C 3D ED 000043-Rx:03 01 02 00 00 0C 3D ED 000044-Tx:03 01 02 00 00 0C 3C 000044-Tx:03 01 00 00 00 0C 3D ED 000045-Rx:03 01 02 00 00 C0 3C 000046-Tx:03 01 00 00 00 0C 3D ED 000047-Rx:03 01 02 00 00 C0 3C	
000048-Tx:03 01 00 00 00 0C 3D ED 000049-Rx:03 01 02 00 00 CO 3C 000050-Tx:03 01 00 00 00 0C 3D ED 000051-Rx:03 01 02 00 00 CO 3C 000052-Tx:03 01 00 00 00 0C 3D ED 000053-Rx:03 01 02 00 00 CO 3C	T T

You can play around with the software to familiarise yourself with it all – that is absolutely fine – but please revert to the settings above (in terms of COILS) for the practical unless given other instructions.

Please use screen capture software such as GreenShot to capture screenshots from Modbus Poll / Slave to paste into your Assignment Answer document where directed to support any questions/tasks asked .

PLEASE do not expect the assessor to interpret these Windows for you – these are backup to show what you have done. YOU must also explicitly answer all questions and if you have any difficulties setting up the software, please contact the module instructor.

# PART 2

We are running a Modbus server at IDC as a Remote Lab. So, instead of running MBSlave, use your MBPoll to connect to this server at IP address 203.59.72.226 with standard port number 502. If you are running this on the Remote Labs use IP address 192.168.1.30 port 502

Connection		<b>x</b>
TCP/IP	Mode	ОК
9600 Baud 💌	- Besponse Timeeut	Cancel
8 Data bits 💌	1000 [ms]	
Even Parity 💌	Delay Between Polls	]
1 Stop Bit 🛛 👻	10 [ms]	Advanced
Remote Server 👝		
IP Address 🛛 🥌	Port 🖊	
203.59.72.226	502	

Set Slave ID as 1. Execute an FC03, and read the contents of the first 10 registers using Base 0 addressing. (ie. Relative addresses 0 through 9, set through Display > Protocol Addresses)

Poll Definition	×
Slave ID:	OK
Function: 03 Read Holding Registers 💌	Cancel
Address: 0	
Length: 10	Apply
Scan Rate: 1000 ms	
🔽 Auto Read Enable	Read Once

You will see Registers set to values by previous students. Please alter one or two yourself.

#### Next: Make sure you have the latest version of wire shark.

Now lets grab some modbus packets with wireshark. Open up WireShark and click the "Capture Interfaces" button or "Capture > Interfaces"

In this window click options

Wireshark: Capture Interfaces		-			
Device	Description	IP	Packets F	Packets/s	
🔲 😥 Local Area Connection 3	TeamViewerVPN Adapter	fe80::546c:ba3e:6743:45f5	0	0	Details
🔲 🗊 VirtualBox Host-Only Network	Sun	fe80::6c52:bf8b:ad6:ade1	0	0	Details
📝 🚁 Local Area Connection	Realtek PCIe GBE Family Controller	fe80::ac49:18d4:45be:fe9a	254	105	Details
<u>H</u> elp	<u>S</u> tart	S <u>t</u> op	<u>O</u> ptions		<u>C</u> lose

Select your interface

Add a filter so we only capture modbus packets

Then click Start

anhene	Interface	Link-layer header	Prom. Mode	Snaplen [B] E	Buffer [M	B]	Capture Fi	ter 🗸
Local Area C fe80:a180:55b3: 10.0.2.15	onnection 2 da45:fbc0	Ethernet	enabled	262144	2	port 502		=
<								4
Canture on all inte	erfaces							
	mode on all inter	facer						Interfaces
	inoue on an inter	laces						
Capture Filter: port	t 502						-	Compile selected BPFs
pture Files							Display Options	
							bispidy options	
File:						Browse	Update list o	f packets in real time
File:						<u>B</u> rowse	Update list o	f packets in real time Iv scroll during live captur
File: Use <u>m</u> ultiple files		☑ Use pcap-ng forma	ıt			Browse	<ul> <li>✓ Update list o</li> <li>✓ Automatical</li> <li>✓ Hide capture</li> </ul>	f packets in real time ly scroll during live captur
File: Use <u>m</u> ultiple files √ Next file every	1	✓ Use pcap-ng forma megabyte(s)	ıt			Browse	✓     Update list o       ✓     Automatical       ✓     Hide capture	f packets in real time ly scroll during live captur e info dialog
File: ☐ Use <u>m</u> ultiple files √ Next file every Next file every		✓     Use pcap-ng forma       megabyte(s)     ▼       minute(s)     ▼	it -			<u>B</u> rowse	<u>Update list o</u> <u>Automatical</u> <u>Hide capture</u>	f packets in real time ly scroll during live captur e info dialog
File:       Use multiple files       Next file every       Next file every       Ring buffer with	1 × v	Use pcap-ng forma       megabyte(s)       minute(s)       files	rt -			<u>B</u> rowse	Image: Second	f packets in real time ly scroll during live captur e info dialog C addresses
File: Use <u>m</u> ultiple files Next file every Next file every Ring buffer with	1   A     1   A     2   A     v   v	Use pcap-ng forma       megabyte(s)       minute(s)       files	r <b>t</b>			<u>B</u> rowse	Update list o <u>Update list o     </u> <u>Automatical     <u>I Hide capture     Name Resolution     </u> <u>Resolve MAG     </u> <u>Resolve netve</u> </u>	f packets in real time ly scroll during live captur e info dialog C addresses vork-layer names
File: Use <u>multiple files</u> Vext file every Next file every Ring buffer with Capture Automatic	1   A     1   A     2   A     cally After	Use pcap-ng formation megabyte(s)	it 			<u>B</u> rowse	Update list o <u>Update list o     </u> <u>Automatical     <u>Hide capture     </u> <u>Hide capture     </u> <u>Resolve MAG     </u> <u>Resolve netv     </u> <u>Resolve tran </u></u>	f packets in real time ly scroll during live captur e info dialog C addresses vork-layer names sport-layer name
File: Use <u>multiple files</u> Next file every Next file every Ring buffer with po Capture Automation 1	1   4     1   4     2   4     r   r     cally After   r	Use pcap-ng forma       megabyte(s)       minute(s)       files	it 			<u>B</u> rowse	Update list o <u>Update list o     </u> <u>Automatical     <u>Hide capture     Hide capture     Resolve MAG     Resolve MAG     Resolve tran     Use external </u></u>	f packets in real time ly scroll during live captur e info dialog C addresses vork-layer names sport-layer name network name resolver

Once you have some packets "stop capture"

You should have something like this, open up the tree structure and explore the packets you have captured

<u> </u>	Local Are	a Conne	ection 2 (p	ort 502)	[Wiresh	ark 1.12.1	(v1.12.1-0-	g01b65ł	bf from ma	ster-1.1	2)]			
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew <u>G</u>	<u>io C</u> aptu	ure <u>A</u> na	alyze S	atistics	Telephony	<u>T</u> ools	s <u>I</u> nternal	s <u>H</u> elp	)			
0	0 🧹		(   E		2	Q 🖕	<b>→</b>	7 ⊉		<b>₽</b>   €		Q 🗹	₩.	¥ [
Filte	:r:		Instr	uctor	San	nple			▼ Exp	ression	. Clear	Apply	Save	
No.	Tin	ne	Sour	ce		D	estination		Pro	otocol	Length	Info		
	1 0.	00000	00010.	0.2.15		2	03.59.72	2.226	т	P	54	49309	→502	[ACK]
	20.	64815	30010.	0.2.15		2	03.59.72	2.226	Mo	odbus/	66	Qu	ery:	Tran
	30.	64851	700 203	. 59.72	.226	1	0.0.2.15	5	т	P	60	502→4	9309	[ACK
	4 0.	79304	900 203	. 59.72	.226	1	0.0.2.15	5	MC	odbus/	83	Respo	nse:	Tr an:
	5 0.	99323	00010.	0.2.15		2	03.59.72	2.226	т	P	54	49309	→502	[ACK
	61.	65291	00010.	0.2.15		2	03.59.72	2.226	MC	dbus/	66	Qu	ery:	Tran
	71.	65343	100 203	. 59.72	.226	1	0.0.2.15	5	т	P	60	502→4	9309	[ACK]
	81.	80352	700 203	. 59.72	.226	1	0.0.2.15	5	Mo	dbus/	83	Respo	nse:	Tran
	92.	00338	30010.	0.2.15		2	03.59.72	2.226	т	P	54	49309	→502	[ACK]
	10 2.	65857	80010.	0.2.15		2	03.59.72	2.226	Mo	dbus/	66	Qu	ery:	Tran
	11 2.	65884	200 203	.59.72	.226	1	0.0.2.15	5	т	P	60	502→4	9309	[ACK]
	12 2.	80582	600 203	.59.72	.226	1	0.0.2.15	5	Mo	dbus/	83	Respo	nse:	Tran
+ F	rame 2	: 66	bytes d	on wire	e (528	3 bits)	, 66 byt	tes ca	aptured	(528	bits)	on in	terfa	ice 0
÷Ε	therne	t II,	Src: 0	admus		31:98	(08:00:2	27:3c:	31:98),	Dst:	Realt	eku_1	2:35:	02 (
÷Ι	nterne	t Prot	tocol \	/ersion	n 4, s	Src: 10	.0.2.15	(10.0	). 2. 15)	Dst:	203.5	9.72.	226 (	203.
ΞΤ	ransmi	ssion	Contro	D Prot	tocol.	Src P	ort: 493	309 (4	19309),	Dst P	ort: 5	502 (5	02),	Seq:
	Sourc	e Port	t: 4930	9 (49)	309)									
	Desti	natio	n Port	502	(502)									