



**Application Note 51599**  
**(Revision -, 10/2018)**  
Original Instructions

## **MBEDrv for Modbus TCPIP Interaction with Woodward Controls**

**Re: Modbus Application Protocol Specification v1.1b3**

Woodward reserves the right to update any portion of this publication at any time. Information provided by Woodward is believed to be correct and reliable. However, no responsibility is assumed by Woodward unless otherwise expressly undertaken.

Copyright © Woodward, Inc. 2018  
All Rights Reserved

# MBEDrv

## Interaction with Woodward Controls

### Application

Any application using the MBEDrv for Modbus TCP/IP Ethernet communication and using Woodward controls

### Purpose

The purpose of this document is to diagnose Modbus TCP/IP communication issues with Woodward VxWorks based controls. The Modbus master (typically the HMI or DCS computer terminal) will exhibit communication errors.

### Assumptions

The engineer is familiar with the GE MBEDrv utility, Woodward tools such as AppManager, GAP, and Control Assistant, GE HMI packages such as iFix or Cimplicity. The user is also familiar with Wireshark and capturing packet capture (pcap) files from a network.

### Tools:

- Engineering workstation
- Network tap or port mirror on switch
- Wireshark & WinPcap
- MBEDrv
- GE iFix
- GAP
- AppManager

Table 1. Glossary

<b>Syscon</b>	Primary CPU
<b>Backup</b>	Backup CPU
<b>TCP</b>	Transport Control Protocol – reliable protocol for transmitting data over Ethernet
<b>UDP</b>	Unified Datagram Protocol – unreliable protocol for transmitting data over Ethernet
<b>NIC</b>	Network Interface Controller – the “network card” on the computer
<b>MBE or MBEDrv</b>	GE MBEDrv (Modbus Ethernet) driver
<b>Modbus</b>	An application layer messaging protocol, positioned at layer 7 of the OSI model, which provides client/server communication between devices connected on different types of buses or networks

### Symptoms:

The network will appear unstable after a period of use. TCP Modbus may exhibit time outs and errors with the CPU, this can lead to dropped connections and attempts to re-establish communications numerous times.

Communications between MBE and the CPU will exhibit instability by:

- Connecting and reconnecting often
- Stale data (not updating in a timely fashion)
- 

In extreme cases, communication between a CPU and RTN expansion rack will also be impacted because of the network conditions.

**Diagnosis:**

The issue can be identified by reviewing the MBE PowerTool utility for errors in the MBE driver configuration or through Monitor GAP. A high number of errors in the MBE power tool may be indicative of an issue. Additional information may be captured by network tools such as Wireshark and a network tap or mirror port.

**Wireshark analysis:**

This assumes a pcap exists of the network having an issue. This assumes a network map of IP addresses does not exist or is incomplete

**Determine the Woodward CPU**

To determine the Woodward CPU, follow the steps below.

1. Open wireshark and the pcap file
2. Apply a display filter:  
(eth.dst[0:3] == 00:12:8c) && (tcp.dstport==502)
3. Open the Conversations display (Statistics->Conversations)

Address A	Port A	Address B	Port B	Packets	Bytes
192.168.101.161	65229	192.168.101.1	502	27,813	1798 k
192.168.101.8	54215	192.168.101.1	502	18,208	1211 k
192.168.101.10	64905	192.168.101.1	502	17,402	1157 k
192.168.101.10	58331	192.168.101.1	502	4,390	274 k
192.168.101.7	54295	192.168.101.1	502	4,071	253 k
192.168.101.10	58293	192.168.101.1	502	2,511	158 k
192.168.101.161	53055	192.168.101.1	502	2,435	146 k
192.168.101.7	54384	192.168.101.1	502	2,198	137 k
192.168.101.8	54191	192.168.101.1	502	1,890	117 k
192.168.101.9	58156	192.168.101.1	502	1,257	75 k
192.168.101.8	54325	192.168.101.1	502	1,256	75 k
192.168.101.10	58294	192.168.101.1	502	1,256	75 k
192.168.101.8	54266	192.168.101.1	502	1,255	75 k
192.168.101.9	58154	192.168.101.1	502	1,255	75 k
192.168.101.9	58155	192.168.101.1	502	1,255	75 k
192.168.101.8	54330	192.168.101.1	502	1,254	75 k
192.168.101.8	54261	192.168.101.1	502	1,254	75 k
192.168.101.10	58298	192.168.101.1	502	1,254	75 k
192.168.101.161	57921	192.168.101.1	502	1,217	73 k
192.168.101.7	62079	192.168.101.1	502	5	294
192.168.101.7	62092	192.168.101.1	502	5	294
192.168.101.7	62097	192.168.101.1	502	5	294
192.168.101.7	62109	192.168.101.1	502	5	294
192.168.101.7	62120	192.168.101.1	502	5	294
192.168.101.7	62124	192.168.101.1	502	5	294
192.168.101.7	64124	192.168.101.1	502	5	294
192.168.101.7	64133	192.168.101.1	502	5	294
192.168.101.7	64149	192.168.101.1	502	5	294
192.168.101.7	64200	192.168.101.1	502	5	294
192.168.101.7	64206	192.168.101.1	502	5	294

Figure 1. Wireshark Conversations Display

4. Select "Limit to Display Filter"
  - a. The IP Addresses in Address B will be the Woodward control's IP address, annotate this value.
  - b. The IP Address in Address A will be the HMI or device creating the Modbus connections.
  - c. Sort on Packets (descending) to see which conversations have the most packets in the capture.

## Analyzing the Conversations

In general the conversations with the higher number of packets are valid Modbus TCP sockets. The conversations with a lower number of packets (5 or less) are conversations that indicate an error.

To analyze a conversation further, a filter may be applied from the Conversations dialog:

1. Right click on the conversation and follow the dropdowns as illustrated in Figure 2.

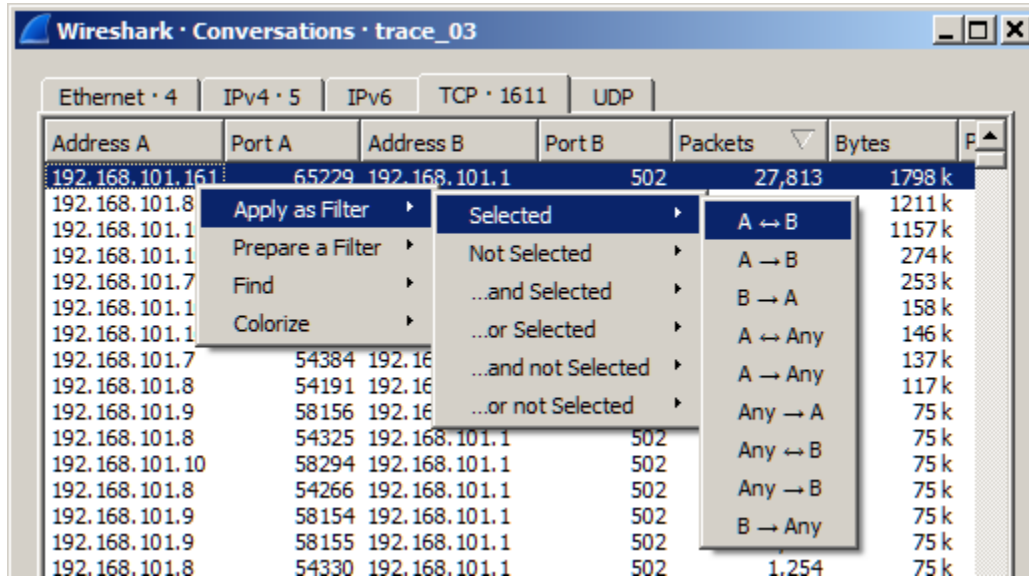


Figure 2. Conversations Dropdown Menu Series

The main Wireshark window will apply the filter from the conversations:

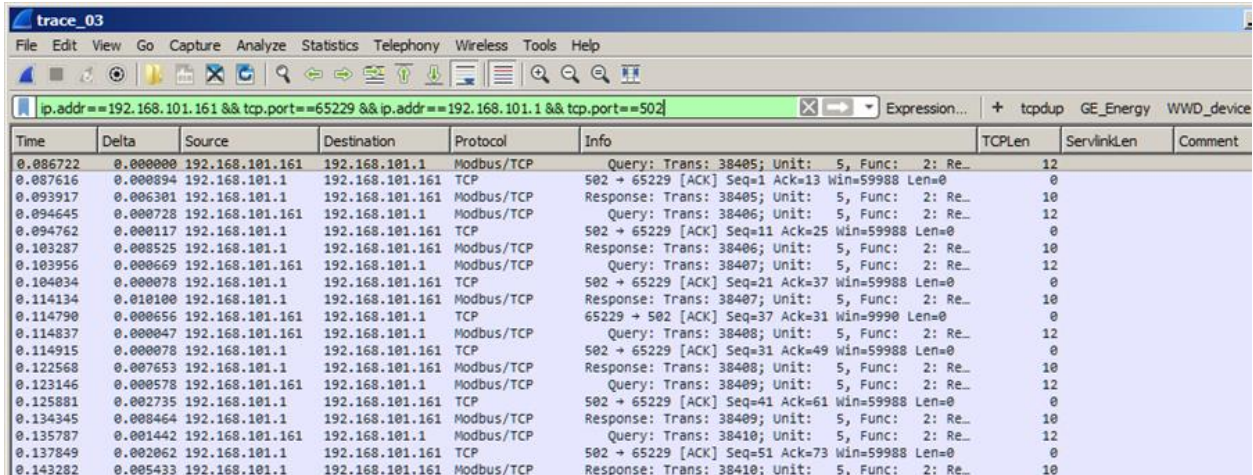


Figure 3. Filter from Conversations Applied

The above indicates a healthy Modbus session with the control. Notice there is consistent Query and Response traffic between the device and the Woodward control.

2. Select a conversation with a lower (5) number of packets:

Time	Delta	Source	Destination	Protocol	Info	TCPLen	Serv
8.812891	0.000000	192.168.101.10	192.168.101.1	TCP	61066 → 502 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 ...	0	
8.813162	0.000271	192.168.101.1	192.168.101.10	TCP	502 → 61066 [SYN, ACK] Seq=0 Ack=1 Win=60000 Len=...	0	
8.813420	0.000258	192.168.101.10	192.168.101.1	TCP	61066 → 502 [ACK] Seq=1 Ack=1 Win=65700 Len=0	0	
8.813456	0.000036	192.168.101.10	192.168.101.1	Modbus/TCP	Query: Trans: 46780; Unit: 4, Func: 16; Wr...	15	
8.813518	0.000062	192.168.101.1	192.168.101.10	TCP	502 → 61066 [ACK] Seq=1 Ack=16 Win=59985 Len=0	0	
10.498213	1.684695	192.168.101.1	192.168.101.10	TCP	502 → 61066 [FIN, ACK] Seq=1 Ack=16 Win=60000 Le...	0	
10.498272	0.000059	192.168.101.1	192.168.101.10	TCP	502 → 61066 [RST, ACK] Seq=2 Ack=16 Win=60000 Le...	0	
10.498431	0.000159	192.168.101.10	192.168.101.1	TCP	61066 → 502 [ACK] Seq=16 Ack=2 Win=65700 Len=0	0	
10.498458	0.000027	192.168.101.10	192.168.101.1	TCP	61066 → 502 [RST, ACK] Seq=16 Ack=2 Win=0 Len=0	0	
10.498570	0.000112	192.168.101.1	192.168.101.10	TCP	502 → 61066 [RST] Seq=2 Win=0 Len=0	0	

Figure 4. Selecting a Discrete Number of Packets

Notice there is a socket creation (SYN packet), a Modbus query, but no response, then a socket teardown (FIN, ACK). This pattern is an example of a misconfigured Modbus configuration. The creation and tear down of a socket is “expensive” on the embedded control.

## MBE Configuration

Locate the suspect computer and the MBE configuration. The MBE configuration may be accessed through the SCU utility in iFix or in the iFix project directory.

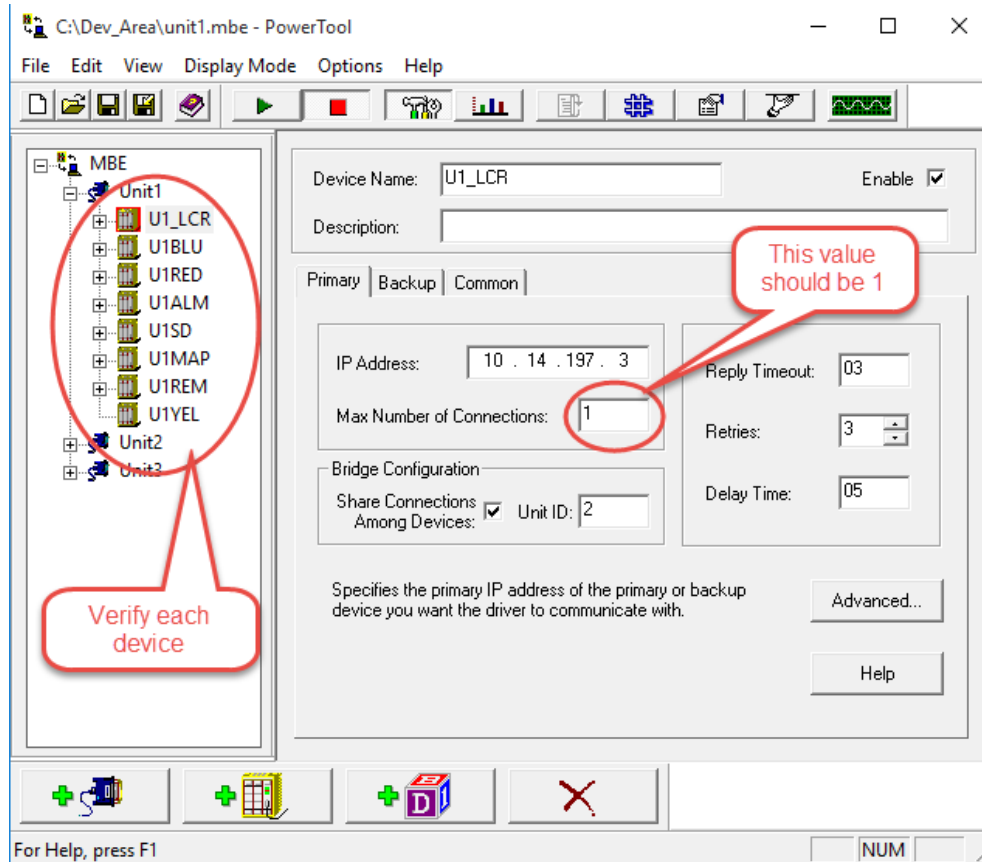


Figure 5. MBE Configuration Example

Examine each device in the MBE driver under the Channel, verify the max connection is set to “1”. The MBE Driver will default this value to “4” when creating new devices and channels. This needs to be verified on the Primary and Backup tabs.

The Common tab contains the strategy for Backup and Primary communications:

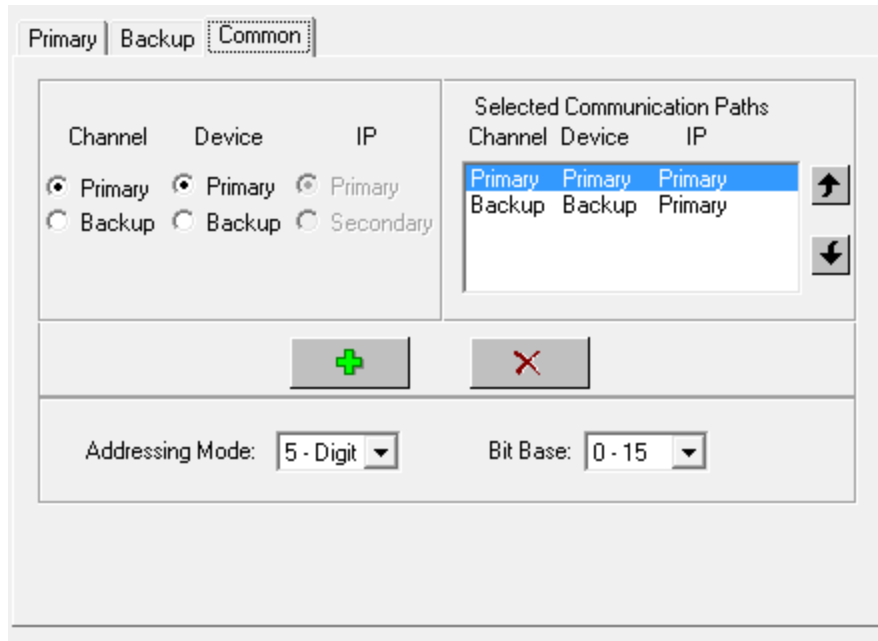


Figure 6. Common Tab Contents

Any changes made should be saved to the MBE driver.

### Validation of changes:

A pcap should be performed on the link to verify the elimination of small packet conversations. The Wireshark capture should demonstrate several conversations with consistent communications.

The screenshot shows a Wireshark capture of Modbus/TCP traffic. The filter is set to 'ip.addr==192.168.101.161 && tcp.port==53677 && ip.addr==192.168.101.1 && tcp.port==502'. The capture shows a series of queries and responses between the two IP addresses.

Time	Delta	Source	Destination	Protocol	Info	TCPLen	ServLinkLen	Comr
0.000000	0.000000	192.168.101.1	192.168.101.161	Modbus/TCP	Response: Trans: 34500; Unit: 5, Func: 4: Re...	11		
0.000602	0.000602	192.168.101.161	192.168.101.1	TCP	53677 → 502 [ACK] Seq=1 Ack=12 Win=9989 Len=0	0		
0.000656	0.000656	192.168.101.161	192.168.101.1	Modbus/TCP	Query: Trans: 34501; Unit: 5, Func: 4: Re...	12		
0.000771	0.000115	192.168.101.1	192.168.101.161	TCP	502 → 53677 [ACK] Seq=12 Ack=13 Win=59988 Len=0	0		
0.009655	0.008884	192.168.101.1	192.168.101.161	Modbus/TCP	Response: Trans: 34501; Unit: 5, Func: 4: Re...	11		
0.010311	0.000656	192.168.101.161	192.168.101.1	Modbus/TCP	Query: Trans: 34502; Unit: 5, Func: 4: Re...	12		
0.010404	0.000093	192.168.101.1	192.168.101.161	TCP	502 → 53677 [ACK] Seq=23 Ack=25 Win=59988 Len=0	0		
0.019700	0.009296	192.168.101.1	192.168.101.161	Modbus/TCP	Response: Trans: 34502; Unit: 5, Func: 4: Re...	11		
0.020252	0.000552	192.168.101.161	192.168.101.1	Modbus/TCP	Query: Trans: 34503; Unit: 5, Func: 4: Re...	12		
0.020343	0.000091	192.168.101.1	192.168.101.161	TCP	502 → 53677 [ACK] Seq=34 Ack=37 Win=59988 Len=0	0		
0.029714	0.009371	192.168.101.1	192.168.101.161	Modbus/TCP	Response: Trans: 34503; Unit: 5, Func: 4: Re...	11		
0.030292	0.000578	192.168.101.161	192.168.101.1	Modbus/TCP	Query: Trans: 34504; Unit: 5, Func: 5: Wr...	12		
0.030383	0.000091	192.168.101.1	192.168.101.161	TCP	502 → 53677 [ACK] Seq=45 Ack=49 Win=59988 Len=0	0		
0.039696	0.009313	192.168.101.1	192.168.101.161	Modbus/TCP	Response: Trans: 34504; Unit: 5, Func: 5: Wr...	12		
0.040273	0.000577	192.168.101.161	192.168.101.1	Modbus/TCP	Query: Trans: 34505; Unit: 5, Func: 5: Wr...	12		
0.040363	0.000090	192.168.101.1	192.168.101.161	TCP	502 → 53677 [ACK] Seq=57 Ack=61 Win=59988 Len=0	0		
0.049611	0.009248	192.168.101.1	192.168.101.161	Modbus/TCP	Response: Trans: 34505; Unit: 5, Func: 5: Wr...	12		
0.050253	0.000642	192.168.101.161	192.168.101.1	Modbus/TCP	Query: Trans: 34506; Unit: 5, Func: 5: Wr...	12		
0.050344	0.000091	192.168.101.1	192.168.101.161	TCP	502 → 53677 [ACK] Seq=69 Ack=73 Win=59988 Len=0	0		
0.059654	0.009310	192.168.101.1	192.168.101.161	Modbus/TCP	Response: Trans: 34506; Unit: 5, Func: 5: Wr...	12		
0.060215	0.000561	192.168.101.161	192.168.101.1	Modbus/TCP	Query: Trans: 34507; Unit: 5, Func: 5: Wr...	12		
0.060302	0.000087	192.168.101.1	192.168.101.161	TCP	502 → 53677 [ACK] Seq=81 Ack=85 Win=59988 Len=0	0		
0.069711	0.009409	192.168.101.1	192.168.101.161	Modbus/TCP	Response: Trans: 34507; Unit: 5, Func: 5: Wr...	12		

Figure 6. Wireshark Capture Example

## Conversation dialog:

Address A	Port A	Address B	Port B	Packets	Bytes
192.168.101.161	53677	192.168.101.1	502	31,682	2038 k
192.168.101.9	52595	192.168.101.1	502	22,086	1467 k
192.168.101.7	61061	192.168.101.1	502	9,758	648 k
192.168.101.9	52600	192.168.101.1	502	4,117	263 k
192.168.101.9	52597	192.168.101.1	502	3,430	218 k
192.168.101.9	52598	192.168.101.1	502	3,430	218 k
192.168.101.7	60955	192.168.101.1	502	3,270	217 k
192.168.101.7	60876	192.168.101.1	502	2,752	182 k
192.168.101.161	52554	192.168.101.1	502	2,078	128 k
192.168.101.9	52599	192.168.101.1	502	2,058	127 k
192.168.101.7	61068	192.168.101.1	502	1,540	97 k
192.168.101.7	61119	192.168.101.1	502	1,478	94 k
192.168.101.9	52601	192.168.101.1	502	1,373	82 k
192.168.101.9	52602	192.168.101.1	502	1,373	82 k
192.168.101.9	52604	192.168.101.1	502	1,373	82 k
192.168.101.9	52603	192.168.101.1	502	1,373	82 k
192.168.101.9	52605	192.168.101.1	502	1,373	82 k
192.168.101.161	59976	192.168.101.1	502	1,347	80 k
192.168.101.7	61062	192.168.101.1	502	620	37 k
192.168.101.7	61063	192.168.101.1	502	619	37 k
192.168.101.7	61064	192.168.101.1	502	618	37 k
192.168.101.7	61065	192.168.101.1	502	618	37 k
192.168.101.7	60951	192.168.101.1	502	609	38 k
192.168.101.7	61075	192.168.101.1	502	609	36 k
192.168.101.7	60882	192.168.101.1	502	520	33 k
192.168.101.7	60952	192.168.101.1	502	514	32 k
192.168.101.7	61039	192.168.101.1	502	494	32 k
192.168.101.7	60883	192.168.101.1	502	447	28 k
192.168.101.7	61067	192.168.101.1	502	339	21 k
192.168.101.7	61177	192.168.101.1	502	228	14 k
192.168.101.7	60946	192.168.101.1	502	213	17 k

Name resolution   
 Limit to display filter   
 Absolute start time   
 Conversation Types ▾

Copy ▾    Follow Stream...    Graph...    Close    Help

Figure 7. Conversation Dialog Example

We appreciate your comments about the content of our publications.

Send comments to: [icinfo@woodward.com](mailto:icinfo@woodward.com)

Please reference publication **51599**.



B 5 1 5 9 9 : -



PO Box 1519, Fort Collins CO 80522-1519, USA  
1041 Woodward Way, Fort Collins CO 80524, USA  
Phone +1 (970) 482-5811

Email and Website—[www.woodward.com](http://www.woodward.com)

Woodward has company-owned plants, subsidiaries, and branches, as well as authorized distributors and other authorized service and sales facilities throughout the world.

Complete address / phone / fax / email information for all locations is available on our website.