Using Wireshark with MS/TP

Using Wireshark for MS/TP

Problems are sometimes not obvious and you will want to see what is actually going out over the network. Most people are already with using Wireshark to capture network traffic on Ethernet, but you can also use Wireshark to analyze data captured on MS/TP. The capture is not live like it is for Ethernet, but analysis with Wireshark can be very helpful.

Control Solutions has created an MS/TP data capture utility that works in conjunction with the MTX002 MS/TP to USB adapter. This is not a generic RS-485 adapter. The MTX002 is an intelligent device that is itself an MS/TP device. A special driver has been included in the data capture utility to recognize MS/TP packets sent via USB by the MTX002.



Start by downloading and installing the USB driver for the MTX002. Do not plug in the MTX002 until you have installed the correct USB driver. The driver installation package is found on the product page for the MTX002 at csimn.com.

Download the MS/TP packet capture utility from the Tool Links page at csimn.com. To run the capture utility, start by putting the MTX002 in pass-through mode. Refer to your PC's device manager to see where the MTX002 was installed, and refer to that COM port in the passthru command. Select the baud rate that matches your network.



Now run mstpcap referring to the COM port that the MTX002 is on. Type Ctrl-C to stop capture.



When capture is stopped, you will get the capture summary that looks something like the illustration below. Note the file name that starts with "mstp_" and ends with .cap. Find this file and double click it (assuming you have Wireshark installed on your PC).

Con Con	nmand Prompt								
c:\mst	tpcap>pass	thru COM	3 38400						*
USB Ad Discor	dapter goi nnect and	ng into reconnec	pass-thre t to USB	ough mod port to	e. exit pa	ss-throu	ıgh mode		
c∶∖mst Adjust mstpca mstpca	tpcap>mstp ted interf ap: Using ap: saving	cap COM3 ace name \\.\COM3 capture	to \\.\ for cap to mstp	COM3 ture at _2016092	38400 bp 8095521.	s. cap			
2000 j MAC 21 22 27	packets MaxMstr Ø 26 127	Tokens 521 521 521 521	Retries 0 0 0	Treply 20 16 16	Tusage 0 32 39	Trpfm 0 0 0 0	Tder 0 32 Ø	Tpostpd 0 0 0 0	
c:\ms1	tpcap>	12.23		57-73 -	17.8				

Double clicking the .cap file created will automatically open it in Wireshark and display packets as illustrated below.

Image: Source Destination Protocol Length Image: Source Depression Clear Apply Sove Time Source Destination Protocol Length Info 10.000000 0x15 0x16 BACnet 8 BACnet ReadProperty[88] analog-value.1 present-value 20.000000 0x15 0x16 BACnet 8 BACnet Sacnet <	and then UU	Capture Analyz	1.12.2 (v1.12.2-0-g89) e Statistics Telepho	9988222 from master-1.12)]
Image: Source Destination Protocol Length Info 10.000000 Ox1b Ox15 BACnet 8 BACnet MS/TP Token 20.000000 Ox15 Ox16 BACnet 8 BACnet MS/TP Token 30.00000 Ox16 Ox16 BACnet 8 BACnet MS/TP Token 40.000000 Ox16 Ox16 BACnet 22 Confirmed-REQ readProperty[88] analog-value,1 present-value 50.000000 Ox16 Ox16 BACnet 22 Confirmed-REQ readProperty[88] analog-value,1 present-value 60.000000 Ox16 Ox15 BACnet 8 BACnet MS/TP Poll For Master 70.000000 Ox16 Ox15 BACnet 8 BACnet MS/TP Poll For Master 70.000000 Ox16 Ox15 BACnet 8 BACnet MS/TP Token 80.000000 Ox15 Ox16 BACnet 8 BACnet MS/TP Token 90.000000 Ox16 Ox16 Dx16 BACnet 8 BACnet MS/TP Token 90.000000 Ox16 Ox16 BACnet & BACnet MS/TP Token BACnet BACnet MS/TP Token <t< th=""><th>• ()</th><th></th><th>9 Q @ # #</th><th>ର୍କି 💈 🗐 🗐 ପ୍ରାର୍ଟ 🗉 🗃 🖬 🥵 % 🙀</th></t<>	• ()		9 Q @ # #	ର୍କି 💈 🗐 🗐 ପ୍ରାର୍ଟ 🗉 🗃 🖬 🥵 % 🙀
Time Source Destination Protocol Length Info 1 0.000000 0x1b 0x15 BACnet 8 BACnet MS/TP Token 2 0.000000 0x15 0x16 BACnet 8 BACnet MS/TP Token 3 0.00000 0x16 0x1b BACnet 8 BACnet MS/TP Token 4 0.000000 0x1b 0x16 BACnet 22 complex=ACK read#roperty[88] analog-value,1 present=value 5 0.000000 0x1b 0x15 BACnet 8 EACnet MS/TP Poll For Master read#roperty[88] analog=value,1 present=value 6 0.000000 0x1b 0x15 BACnet 8 EACnet MS/TP Poll For Master 7 0.000000 0x1b 0x15 BACnet 8 EACnet MS/TP Token 8 0.000000 0x1b 0x16 BACnet 8 EACnet MS/TP Token 9 0.000000 0x1b 0x16 BACnet 8 EACnet MS/TP Token 9 0.000000 0x16 0x16 BACnet 8 EACnet MS/TP Token 9 0.000000 0x16 0x16 BACnet 8 EACnet MS/TP Token 9 0.000000 0x16 0x16 BACnet 8 EACnet MS/TP Token <td< td=""><td>er:</td><td></td><td></td><td>Expression Clear Apply Save</td></td<>	er:			Expression Clear Apply Save
1 0.000000 0x1b 0x15 BACnet 8 BACnet MS/TP Token 2 0.000000 0x15 0x16 BACnet 8 BACnet MS/TP Token 4 0.000000 0x16 0x1b BACnet 23 Confirmed-REQ readProperty[88] analog-value,1 present-value 5 00.00000 0x16 0x1b BACnet 29 Complex-Ack readProperty[88] analog-value,1 present-value 6 0.00000 0x1b 0x15 BACnet 8 BACnet MS/TP Token 8 0.00000 0x1b 0x15 BACnet 8 BACnet MS/TP Token 8 0.00000 0x1b 0x15 BACnet 8 BACnet MS/TP Token 9 0.00000 0x15 0x16 BACnet 8 BACnet MS/TP Token 9 0.00000 0x15 0x16 BACnet 8 BACnet MS/TP Token m m m m errame 5: 29 bytes on wire (232 bits). 29 bytes captured (232 bits) BACnet MS/TP, Src (22), Dst (27), BACnet Data Not Expecting Reply Suilding Automation and Control Network MPDU 0011 = APDU Type: Complex-ACK (3) 9 0000 = PDU Flags: 0x00 Invoke ID: 88 Service Choice: readProperty (12) BobjectIdentifier: present-value (85) 8 [[Time	Source	Destination	Protocol Length Info
2 0.000000 0x15 0x16 BACnet 8 BACnet MS/TP Token 3 0.000000 0x1b 0x16 BACnet 23 Confirmed-REQ readProperty[88] analog-value,1 present-value 5 0.000000 0x1b 0x16 BACnet 29 Complex-ACK readProperty[88] analog-value,1 present-value 6 0.000000 0x1b 0x15 BACnet 29 Complex-ACK readProperty[88] analog-value,1 present-value 6 0.000000 0x1b 0x15 BACnet 8 BACnet MS/TP Poll For Master 7 0.00000 0x1b 0x15 BACnet 8 BACnet MS/TP Token 8 0.000000 0x15 0x16 BACnet 8 BACnet MS/TP Token 9 0.000000 0x15 0x16 BACnet 8 BACnet MS/TP Token 9 0.00000 0x15 0x16 BACnet 8 BACnet MS/TP Token 9 0.00000 0x16 0x16 BACnet 8 BACnet MS/TP Token 9 0.00000 0x16 0x16 BACnet 8 BACnet MS/TP Token 0x0000 0x16 0x16 BACnet 8 BACnet MS/TP Token 0x0000 0x16 0x16 BACnet 8 BACnet MS/TP Token <tr< td=""><td>1 0.000000</td><td>0x1b</td><td>0x15</td><td>BACNET 8 BACNET MS/TP Token</td></tr<>	1 0.000000	0x1b	0x15	BACNET 8 BACNET MS/TP Token
3 0.000000 0x16 0x1b BACnet 8 BACnet M5/TP Token 4 0.000000 0x1b 0x16 BACnet- 23 Confirmed-REQ readProperty[88] analog-value,1 present-value 5 0.000000 0x1b 0x36 BACnet- 23 Comfirmed-REQ readProperty[88] analog-value,1 present-value 6 0.00000 0x1b 0x36 BACnet- 8 BACnet M5/TP Token readProperty[88] analog-value,1 present-value 8 0.000000 0x15 0x16 BACnet 8 BACnet M5/TP Token 9 0.000000 0x15 0x16 BACnet 8 BACnet M5/TP Token # """"""""""""""""""""""""""""""""""""	2 0.000000	0x15	0x16	BACnet 8 BACnet MS/TP Token
4 0.000000 0x1b 0x16 BACnet- 23 Confirmed-REQ readProperty[88] analog-value,1 present-value 5 0.000000 0x1b 0x36 BACnet- 29 Complex-ACK readProperty[88] analog-value,1 present-value 6 0.000000 0x1b 0x36 BACnet- 29 Complex-ACK readProperty[88] analog-value,1 present-value 7 0.00000 0x1b 0x36 BACnet 8 BACnet MS/TP Poll For Master 8 0.000000 0x15 0x16 BACnet 8 BACnet MS/TP Token 9 0.00000 0x16 0x16 BACnet 8 BACnet MS/TP Token 9 0.00000 0x16 0x1b BACnet 8 BACnet MS/TP Token """"""""""""""""""""""""""""""""""	3 0.000000	0x16	0x1b	BACnet 8 BACnet MS/TP Token
S 0.000000 0x16 0x1b BACnet- 0 0.00000 29 Complex-Ack readProperty[88] analog-value,1 present-value 6 0.000000 0x1b 0x36 BACnet 8 BACnet M5/TP Poll For Master 7 0.00000 0x1b 0x15 BACnet 8 BACnet M5/TP Token 8 0.000000 0x15 0x16 BACnet & BACnet M5/TP Token 9 0.000000 0x16 0x1b BACnet M5/TP Token Trame 5: 29 bytes on wire (232 bits), 29 bytes captured (232 bits) SACnet M5/TP, Src (22), DSt (27), BACnet Data Not Expecting Reply Balanet M5/TP Token Trame 5: 29 bytes on wire (232 bits), 29 bytes captured (232 bits) SACnet M5/TP, Src (22), DSt (27), BACnet Data Not Expecting Reply Balanet M5/TP Token Town of a PDU Type: Complex-ACK (3) 0	4 0.000000	0x1b	0x16	BACnet- 23 Confirmed-REQ readProperty[88] analog-value,1 present-value
6 0.00000 0x1b 0x36 BACnet 8 BACnet M5/TP Poll For Master 7 0.00000 0x1b 0x15 BACnet 8 BACnet M5/TP Token 8 0.00000 0x15 0x16 BACnet 8 BACnet M5/TP Token 9 0.00000 0x16 0x1b BACnet 8 BACnet M5/TP Token m rame 5: 29 bytes on wire (232 bits), 29 bytes captured (232 bits) Accnet M5/TP, Src (22), BACnet Data Not Expecting Reply tuilding Automation and Control Network NPDU tuilding Automation and Control Network APDU 0011 = APDU Type: Complex-ACK (3) 9 0000 = PDU Flags: 0x00 Invoke ID: 88 Service Choice: readProperty (12) 0 ObjectIdentifier: present-value (85) 8 [[3] 0 S5 ff 06 1b 16 00 13 81 01 00 30 58 0c 0c 00 80 U 0X 0 00 01 19 55 3e 44 42 33 a3 d7 3f dc d0U>DB3?	5 0,000000	0x16	0x1b	BACNET- 29 Complex-ACK readProperty[88] analog-value,1 present-value
7 0.00000 0x1b 0x15 BACnet 8 BACnet MS/TP Token 8 0.00000 0x15 0x16 BACnet 8 BACnet MS/TP Token 9 0.00000 0x16 0x1b BACnet 8 BACnet MS/TP Token m trame 5: 29 bytes on wire (232 bits), 29 bytes captured (232 bits) AACnet MS/TP, Src (22), DSt (27), BACnet Data NOT Expecting Reply tuilding Automation and Control Network NPDU 10011 = APDU Type: Complex-ACK (3) 0 0000 = PDU Flags: 0x00 Invoke ID: 88 Service Choice: readProperty (12) 0 objectIdentifier: present-value (85) 8 [3] 0 of 55 ff 06 1b 16 00 13 81 01 00 30 58 0c 0c 00 80 U	6 0.000000	0x1b	0x36	BACnet 8 BACnet MS/TP Poll For Master
8 0.00000 0x15 0x16 BACnet 8 BACnet MS/TP Token 9 0.00000 0x16 0x16 BACnet 8 BACnet MS/TP Token m rrame 5: 29 bytes on wire (232 bits), 29 bytes captured (232 bits) BACnet MS/TP, Src (22), Dst (27), BACnet Data Not Expecting Reply wilding Automation and Control Network NPDU suilding Automation and Control Network APDU 0011 = APDU Type: Complex-ACK (3) 0 0000 = PDU Flags: 0x00 Invoke ID: 88 Service Choice: readProperty (12) 0 ObjectIdentifier: present-value (85) 8 [3] 0 55 ff 06 1b 16 00 13 81 01 00 30 58 0c 0c 00 80 U	7 0.000000	0x1b	0x15	BACnet 8 BACnet MS/TP Token
9 0.00000 0x16 0x1b BACnet 8 BACnet MS/TP Token T Tame 5: 29 bytes on wire (232 bits), 29 bytes captured (232 bits) BACnet MS/TP, Src (22), DSt (27), BACnet Data Not Expecting Reply suilding Automation and control Network APDU 0011 = APDU Type: Complex-ACK (3) 0 0000 = PDU Flags: 0x00 Invoke ID: 88 Service Choice: readProperty (12) 0 bjectIdentifier: analog-value, 1 Property Identifier: present-value (85) 8 [3] 0 55 ff 06 1b 16 00 13 81 01 00 30 58 0c 0c 00 80 0 00 01 19 55 3e 44 42 33 a3 d7 3f dc d0 U>DB3?	8 0.000000	0x15	0x16	BACnet 8 BACnet MS/TP Token
<pre>m. rame 5: 29 bytes on wire (232 bits), 29 bytes captured (232 bits) AACnet MS/TP, Src (22), DSt (27), BACnet Data Not Expecting Reply wilding Automation and Control Network NPDU 0011 = APDU Type: Complex-ACK (3) 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 0011 9 55 3e 44 42 33 a3 d7 3f dc d0 001 9 55 3e 44 42 33 a3 d7 3f dc d0 001 9 55 3e 44 42 33 a3 d7 3f dc d0 001 9 55 3e 44 42 33 a3 d7 3f dc d0 001 9 55 3e 44 42 33 a3 d7 3f dc d0 001 9 55 3e 44 42 35 001 9 56 56 56 56 56 56 56 56 56 56 56 56 56</pre>	9 0.000000	0x16	0x1b	BACnet 8 BACnet MS/TP Token
<pre>rame 5: 29 bytes on wire (232 bits), 29 bytes captured (232 bits) AACnet M5/TP, Src (22), Dst (27), BACnet Data Not Expecting Reply wilding Automation and Control Network NPDU oulding Automation and Control Network APDU 0011 = APDU Type: Complex-ACK (3) 0000 = PDU Flags: 0x00 Invoke ID: 88 Service Choice: readProperty (12) ObjectIdentifier: analog-value, 1 Property Identifier: present-value (85) [[3] 0 55 ff 06 1b 16 00 13 81 01 00 30 58 0c 0c 00 80 U 00x 0 00 01 19 55 3e 44 42 33 a3 d7 3f dc d0U>DB3?</pre>		0.000		
10 55 5f 06 1b 16 00 13 81 01 00 30 58 0c 00 80 0	0011 = 0000 = Invoke ID: 8 Service Choi ObjectIdenti Property Ide	APDU Type: Co PDU Flags: 0x 8 ce: readPrope fier: analog- ntifier: pres e: 44.910000	mplex-ACK (3) 00 value, 1 ent-value (85) (Real))
	8 {[3] 9 present-valu 8 }[3]			

If mstpcap says it saved a file but you cannot find it, check to see that mstpcap.exe is not blocked. It will appear to run but not be allowed to save a file on your PC if blocked. Click Unblock if necessary.

ieneral	Comp	atibility	Security	Details	Previous Versions			
		mstpcap.exe						
Type of file:		Application (.exe)						
Descrip	tion:	mstpca	p.exe					
Location:		C:\mstpcap						
Size:		14.5 KB (14,848 bytes)						
Size on disk:		16.0 KB (16,384 bytes)						
Created:		Friday, February 12, 2010, 9:07:16 AM						
Modified:		Today, September 28, 2016, 12 minutes ago						
Accessed:		Friday, February 12, 2010, 9:07:16 AM						
Attribute	es:	<u> R</u> ea	ad-only	Hidder	A <u>d</u> vanced.			
Security:		This file came from another computer and might be blocked to help protect this computer.						

Article ID: 37 Created On: Tue, Dec 6, 2016 at 9:46 PM Last Updated On: Tue, Dec 6, 2016 at 9:46 PM