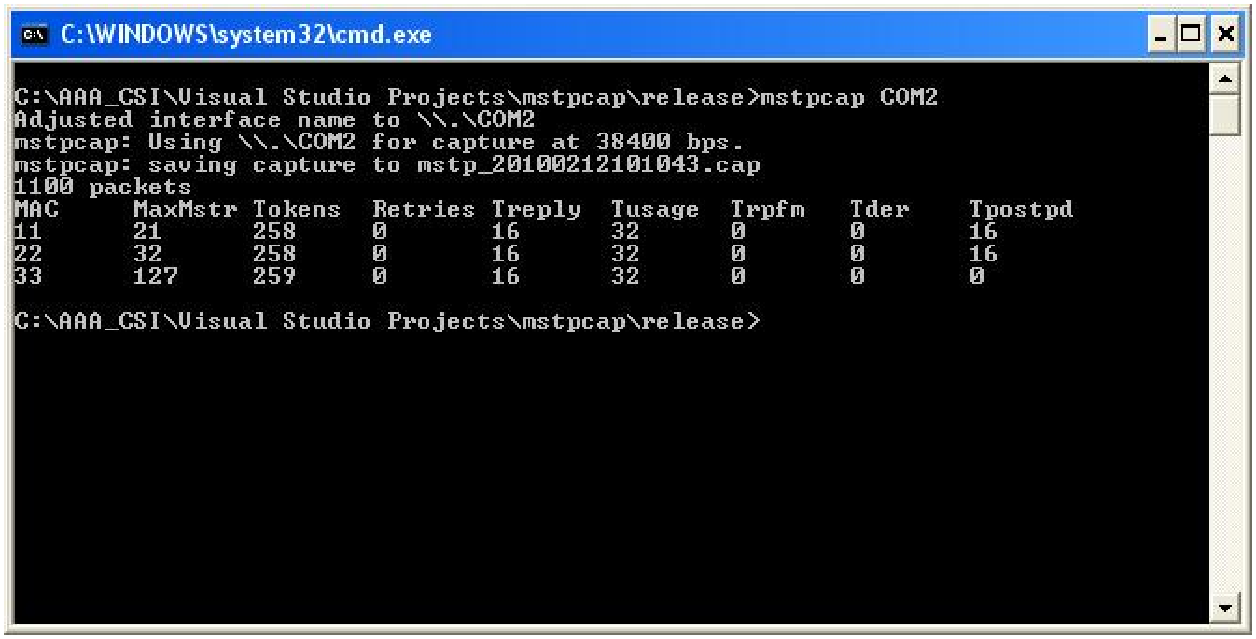
MS/TP Packet Capture using Wireshark

Wireshark (available at www.wireshark.org) is a well known, widely used packet capture tool for networks. It can be used to capture BACnet IP and all other forms of IP traffic by simply running it on your PC and connecting to your Ethernet interface.

The packet analysis of Wireshark can be used with MS/TP with the help of a packet capture tool that will receive MS/TP traffic on a COM port on your PC. The program mstpcap.exe provided at no charge at www.csimn.com is simply a compiled copy of Steve Karg’s original open source project at sourceforge.net, documented on Steve’s web site here: http://steve.kargs.net/bacnet/wireshark-and-bacnet-mstp/

Run the program by simply providing a COM port. While running, it will show the captured packet count. Type Ctrl-C to stop capture. The program will then display a summary of packets captured. It will also have created a .cap file which will display the Wireshark file icon if you have already installed Wireshark. If Wireshark is present, simply double click the file and it will open in Wireshark.



```
C:\AAA_CSI\Visual Studio Projects\mstpcap\release>mstpcap COM2
Adjusted interface name to \\.\COM2
mstpcap: Using \\.\COM2 for capture at 38400 bps.
mstpcap: saving capture to mstp_20100212101043.cap
1100 packets
MAC     MaxMstr Tokens  Retries Treply  Tusage  Trpfm   Tder    Tpostpd
11      21      258     0       16      32      0       0       16
22      32      258     0       16      32      0       0       16
33      127     259     0       16      32      0       0       0

C:\AAA_CSI\Visual Studio Projects\mstpcap\release>
```

Note: If you are using the MTX002 as your RS485 adapter with mstpcap, you first need to put the MTX002 into pass-through mode. The syntax for the passthru.exe command (from command prompt) is:

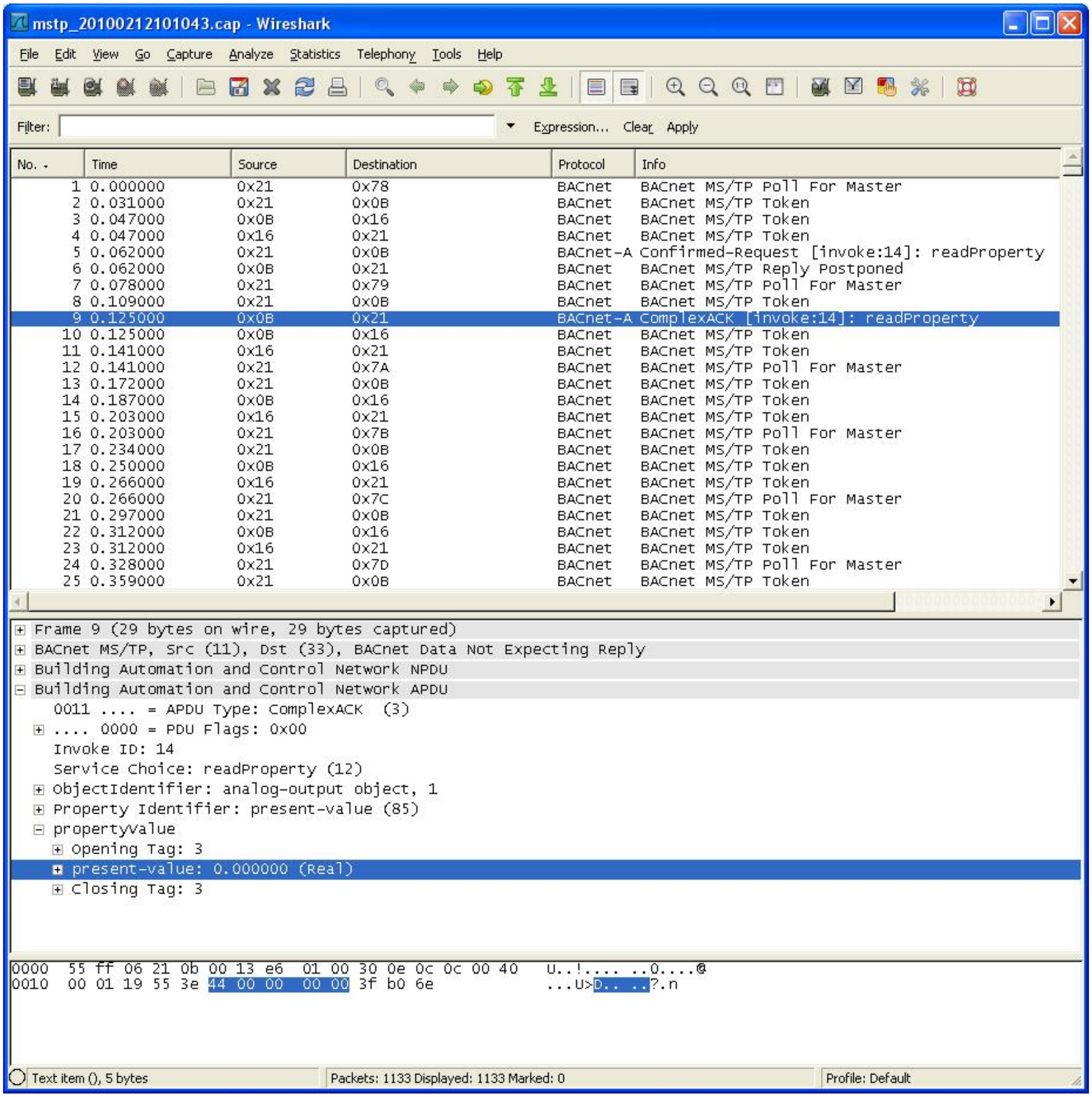
```
C:\> passthru COMx baud
```

where COMx is the comm. port number such as COM2, and ‘baud’ is the speed at which your MS/TP link is running. A typical command would be:

```
C:\> passthru COM2 38400
```

Once in pass-through mode, you need to unplug the MTX002 from the USB port and reconnect it (force hard reset of MTX002 adapter).

Example of MS/TP packet capture:


mstp_20100212101043.cap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. -  Time       Source   Destination   Protocol  Info
     1 0.000000   0x21     0x78          BACnet    BACnet MS/TP Poll For Master
     2 0.031000   0x21     0x0B          BACnet    BACnet MS/TP Token
     3 0.047000   0x0B     0x16          BACnet    BACnet MS/TP Token
     4 0.047000   0x16     0x21          BACnet    BACnet MS/TP Token
     5 0.062000   0x21     0x0B          BACnet-A  Confirmed-Request [invoke:14]: readProperty
     6 0.062000   0x0B     0x21          BACnet    BACnet MS/TP Reply Postponed
     7 0.078000   0x21     0x79          BACnet    BACnet MS/TP Poll For Master
     8 0.109000   0x21     0x0B          BACnet    BACnet MS/TP Token
     9 0.125000   0x0B     0x21          BACnet-A  ComplexACK [invoke:14]: readProperty
    10 0.125000   0x0B     0x16          BACnet    BACnet MS/TP Token
    11 0.141000   0x16     0x21          BACnet    BACnet MS/TP Token
    12 0.141000   0x21     0x7A          BACnet    BACnet MS/TP Poll For Master
    13 0.172000   0x21     0x0B          BACnet    BACnet MS/TP Token
    14 0.187000   0x0B     0x16          BACnet    BACnet MS/TP Token
    15 0.203000   0x16     0x21          BACnet    BACnet MS/TP Token
    16 0.203000   0x21     0x7B          BACnet    BACnet MS/TP Poll For Master
    17 0.234000   0x21     0x0B          BACnet    BACnet MS/TP Token
    18 0.250000   0x0B     0x16          BACnet    BACnet MS/TP Token
    19 0.266000   0x16     0x21          BACnet    BACnet MS/TP Token
    20 0.266000   0x21     0x7C          BACnet    BACnet MS/TP Poll For Master
    21 0.297000   0x21     0x0B          BACnet    BACnet MS/TP Token
    22 0.312000   0x0B     0x16          BACnet    BACnet MS/TP Token
    23 0.312000   0x16     0x21          BACnet    BACnet MS/TP Token
    24 0.328000   0x21     0x7D          BACnet    BACnet MS/TP Poll For Master
    25 0.359000   0x21     0x0B          BACnet    BACnet MS/TP Token
```

```
⊞ Frame 9 (29 bytes on wire, 29 bytes captured)
⊞ BACnet MS/TP, Src (11), Dst (33), BACnet Data Not Expecting Reply
⊞ Building Automation and Control Network NPDU
⊟ Building Automation and Control Network APDU
    0011 .... = APDU Type: ComplexACK   (3)
  ⊞ .... 0000 = PDU Flags: 0x00
    Invoke ID: 14
    Service Choice: readProperty (12)
  ⊞ ObjectIdentifier: analog-output object, 1
  ⊞ Property Identifier: present-value (85)
  ⊟ propertyValue
    ⊞ Opening Tag: 3
    ⊞ present-value: 0.000000 (Real)
    ⊞ Closing Tag: 3
```

```
0000   55 ff 06 21 0b 00 13 e6  01 00 30 0e 0c 0c 00 40    U..!.... ..0....@
0010   00 01 19 55 3e 44 00 00  00 00 3f b0 6e             ...U>D.. ..?.n
```

Text item (), 5 bytes | Packets: 1133 Displayed: 1133 Marked: 0 | Profile: Default