Instructions for capturing Wireshark data for troubleshooting EtherNet/IP and BACnet MSTP

Overview

Wireshark® is a network protocol analyzer that lets you capture and interactively browse the traffic running on a computer network. Wireshark is a free software that has a rich and powerful feature set and runs on most computing platforms including Windows®, macOS, Linux, and UNIX®.

Steps for capturing Wireshark data for EtherNet/IP

Step 1: Download wireshark from the link below:

https://www.wireshark.org/download.html

Depending on the laptop configuration of OS, choose the suitable platform and version shown in the screenshot below.

Download Wireshark

The current stable release of Wireshark is 3.4.2. It supersedes all previous releases.

Stable Release (3.4.2)	~
 Windows Installer (64-bit) Windows Installer (32-bit) Windows PortableApps[®] (32-bit) macOS Intel 64-bit .dmg Source Code 	
Old Stable Release (3.2.10)	

Step 2: Connect the EtherNet/IP PLC to one of the switch ports, for example, Port P2.

Step 3: From the switch user interface, configure one port, in this case P1, for mirroring which will send all data coming to port P2. Port P2 is the source and Port P1 is the destination for mirroring. For more information on mirroring, please review the port mirroring procedure for the Hirschmann[™] switch, which is the switch in use.

Step 4: Connect the drives on the remaining ports, which can be one or more.

Step 5: Configure the PLC to talk to the drives connected to these switch ports, for instance P3, P4, and so on.



Step 6: Connect the laptop that has Wireshark installed and running to Port P1, on which port mirroring is activated.

Step 7: Now you will be able to log all the data that Port P2 sees from the connected PLC.

The table below clarifies the description for the ports mentioned in the steps above.

P1	P2	P3	P4	P5	P6	P7	P8
Port mirroring is	Connected						
activated from P2	to PLC	to drive					

Steps for capturing Wireshark data for BACnet MSTP

Step 1: Install the mstpcap.exe. Details are available from the link below:

https://bravocontrols.com/troubleshooting-bacnet-mstp-traffic-wireshark

If mstpcap.exe is not available, please contact Eaton.

Step 2: Open Wireshark. You will notice that it now recognizes the assigned com ports, which are shown in the screenshot below.

The lifebase lifebase lifebase lifebase File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help		- a ×
Apply a display filter <ctrl-></ctrl->	E3 •	Expression +
Welcome to Wireshark		
Open		
C/Uken\E4502166\Desktop\PowerXL_BACnet_Testing\DG1\DG1_BACnet_Testing6_fix_pcapng (221 MB)	^	
C-{Users}E4502166\Desktop\DG1 BACnet Testing\DG1_BACnet_Testing_5pcaping (not found)		
C\Users\E4502166\Desktop\DG1 EACnet Testing\DG1_BACnet_Testing_Aproppig (not found)		
C1/Users1E4S021661Desktop1DG1 BACnet Testing1DG1_BACnet_Testing,2pcapng (not found)		
C\Users\E4502166\Desktop\D51 BACnet Testiny\DG1_BACnet_Testing_1proppg (not found)		
and have a second s	*:	
Capture		
using this filter: 📕 Enter a capture filter	All interfaces shown*	
Bluetooth Network Connection Image: BaCnet MS/IP on COM10 Image: BaCnet MS/IP on COM3 Image: BaCnet MS/IP on COM7	į	
Learn User's Guide · Wiki · Questions and Answers · Mailing Lists You are running Wireshark 2.6.9 (v2.6.9-0-gf1627e90). You receive automatic updates.		
Z Ready to load or capture No Packets	ă.	Profile: Default

Step 3: Click on the settings icon beside the com port you want to monitor BACnet MSTP on and set the appropriate baud rate. Note that it has to be a separate com port from the one you are using for Yabe.

📕 Weeshalk - Interface Options: RACent MD/TP on COMP				7	×
Baud Rate	9600			•	
Save parameter on capture start					
Restore Defaults		Start	Close	Help	

Step 4: Click Start. The process is complete.

Eaton 1000 Eaton Boulevard Cleveland, OH 44122 United States Eaton.com



© 2022 Eaton All Rights Reserved Printed in USA Publication No. AP040232EN / Z25726 August 2022

Eaton is a registered trademark.

All other trademarks are property of their respective owners.