Tech Tips

Wireshark Capture Instructions

SUMMARY

If you experience network communications problems with CTI products, we will often recommend getting a Wireshark capture of the communications activity while the problem is occurring. By analyzing the collected data, we can often determine the cause of the problem. Wireshark is a free software which records communication data in real time, capturing it to a file for later analysis.

Downloading Wireshark

Wireshark can be downloaded free from http://www.wireshark.org.

Other Equipment

NOTE: If the existing switch setup includes port mirroring capability that will allow capturing traffic between the CTI Ethernet product and the network, you may not need this. However, I recommend that you have this available as a backup.

Besides your laptop and the Wireshark software, you will need a managed Ethernet switch that that supports port mirroring. If you don't already have one, an inexpensive 5 port switch should be easy to find. You will need to configure one of the switch ports as a mirror port, which means that the switch will forward a copy of packets from designated ports to the mirror port.

You will need to place the switch in between the network and the CTI Ethernet port. In the illustration in Figure 1 on the following page, Port 1 is connected to the local area network, port 2 is connected to the CTI Ethernet port (CTI PLC is illustrated), and the laptop is connected to port 3, which has been configured to mirror traffic from ports 1 and 2.

Instead of a managed switch, you can also use the Dualcomm 10/100/1000Base-T Gigabit Ethernet Network TAP, which comes already configured for network capture.

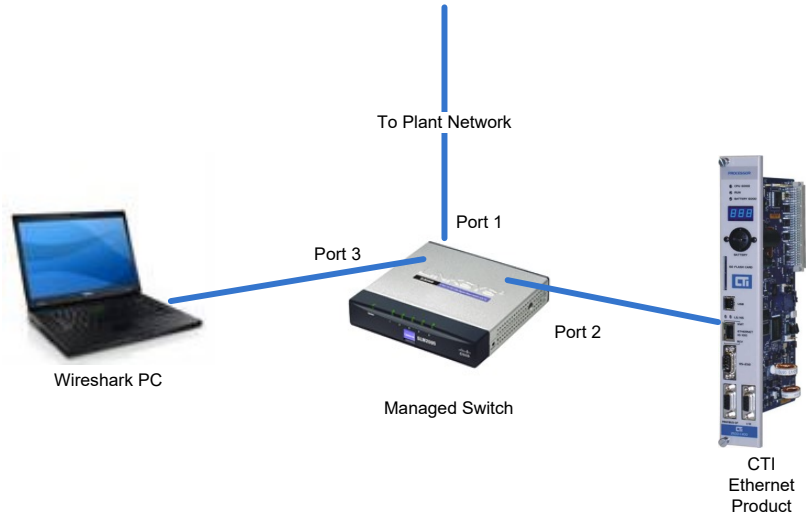
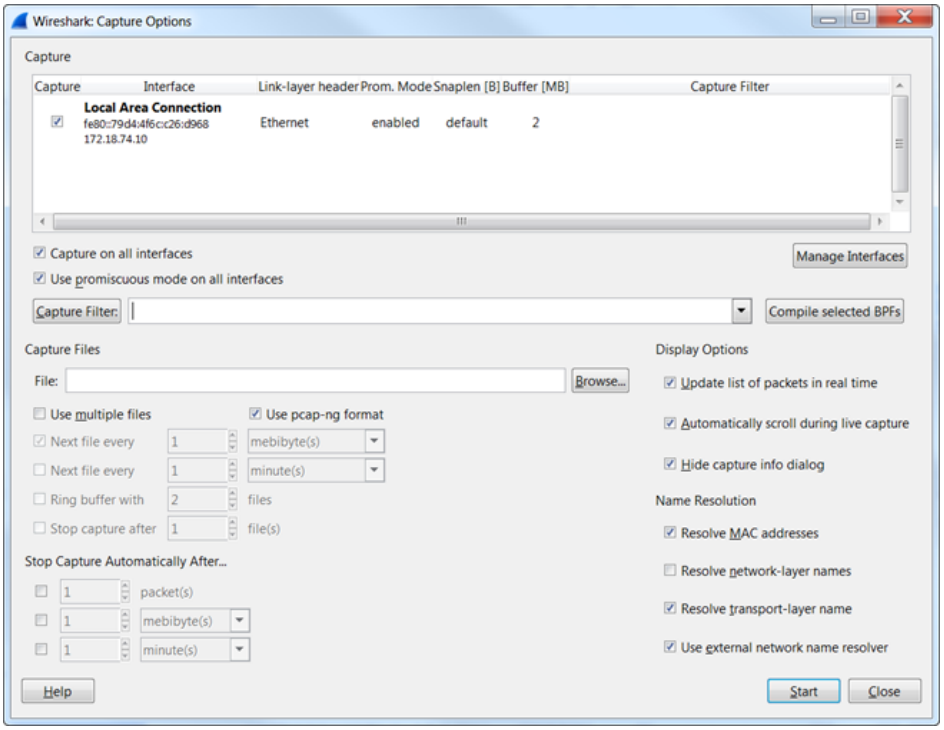


Figure 1. Network Capture Setup

Starting and Testing the Capture

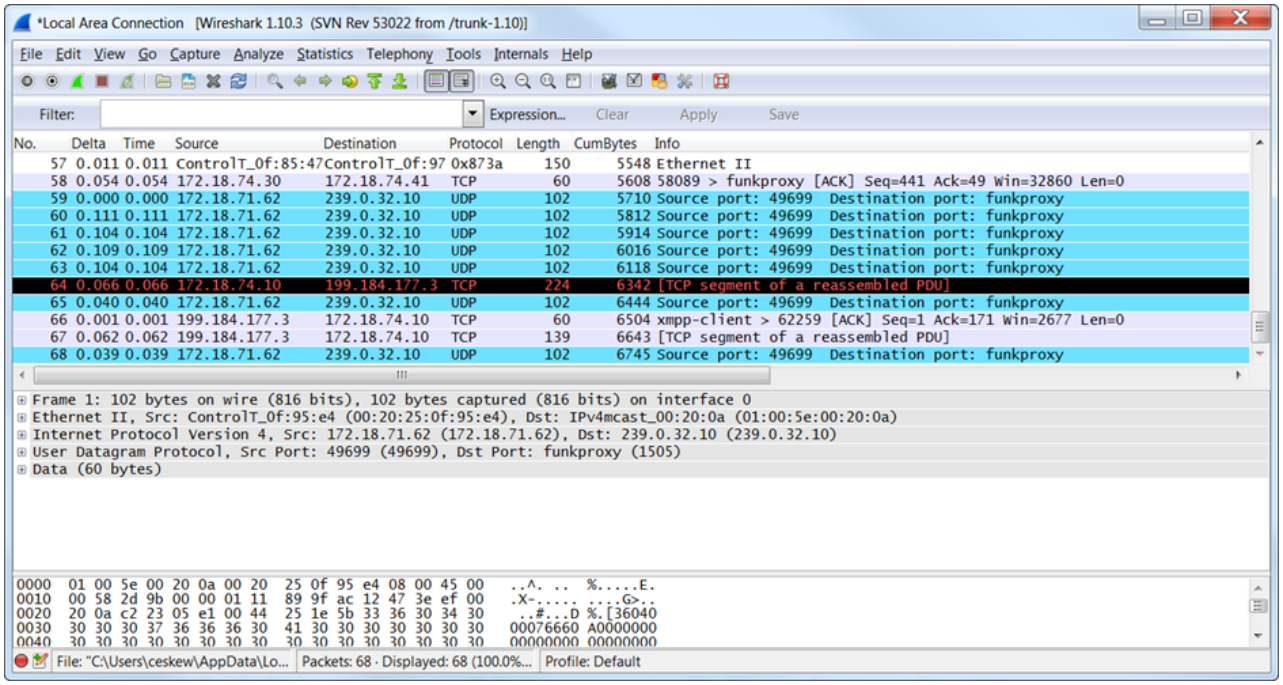
After starting Wireshark, you may need to specify the Capture Interface (your Ethernet Interface). Click on the Capture Options to display the following window.



This Capture Options dialog should display your Ethernet interface. Make sure that the “Capture on all interfaces” and “Use Promiscuous Mode” boxes and the “Update List of Packets in Real Time” and “Automatically Scroll during Live Capture” boxes are checked.

In the Capture Files area, click on the Browse button to select a path and file name used to store the capture data. Captures over an extended period of time (several hours) can result in large files, which may be difficult to transfer and slow to load. In this case you can check the Use Multiple Files box, which will create a new file when the specified condition is reached. I usually find the file size to be the best criteria and 10-15 MB to be a reasonable size. If you are emailing files, you may wish to determine the maximum size file that can be emailed from the site and us this value.

After doing so, click on the start button. You should see the main capture window with packet information scrolling in the upper section. If this is not happening, you will need to check your connections. If everything appears to be working, stop the capture.



Captures

In order to diagnose problems, we need an Ethernet capture taken while the problem is occurring. If the problem occurs only occasionally, it may be required to run the capture for hours, or even days. By properly specifying the Capture Files setup, you can allow automatic creation of new files on a periodic basis, or when the capture file reaches a certain size.

CONTROL TECHNOLOGY, INC.

5734 Middlebrook Pike
Knoxville, TN 37921 USA
+1.865.584.0440
www.controltechnology.com
sales@controltechnology.com

6FEB2020