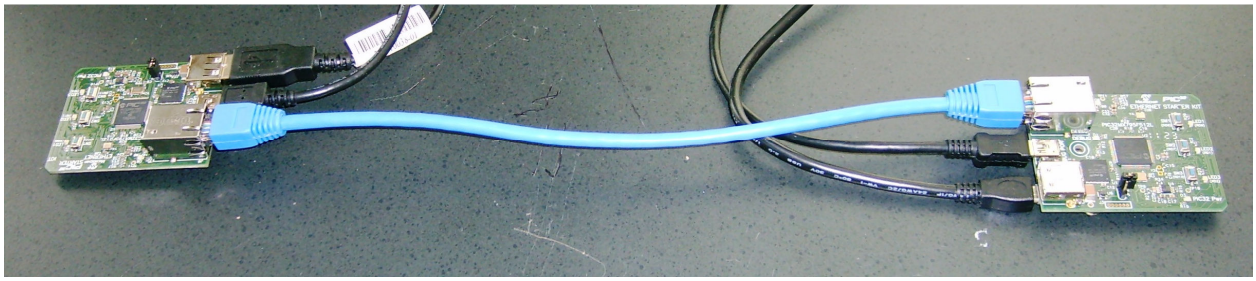
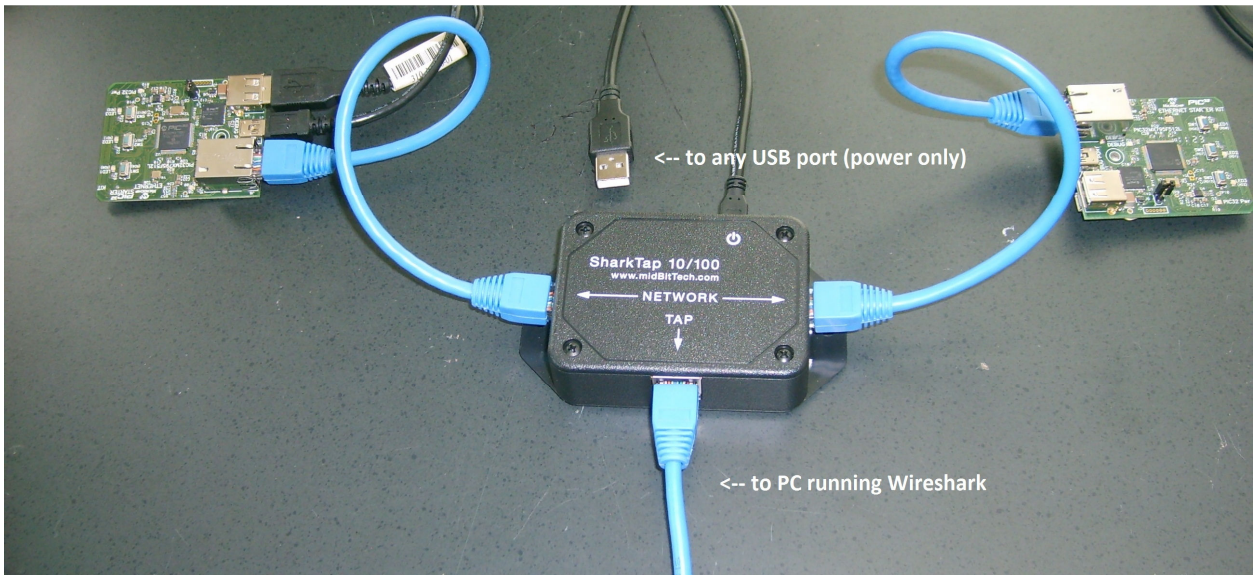
Quick Start Guide

In the example below, a developer is debugging a USB-over-ethernet extender. We want to view the packets on the blue CAT5 Ethernet cable:



To use the SharkTap to monitor the Ethernet packets on that link, connect the SharkTap as shown in the next picture:



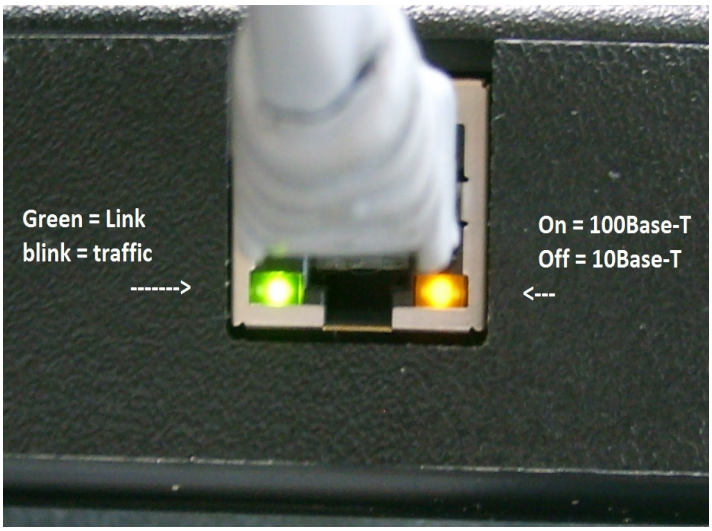
The two Ethernet devices connect to the two side ports marked ‘NETWORK’. All packets on either network port will be duplicated on the TAP port. The TAP port is typically connected to a PC running the Wireshark analyzer. Finally, connect the USB cable from the back port to any USB port, or use any cell phone charger with a micro-USB connector. The red LED on the back will light red to show power is attached. (The SharkTap will not show up as a device when connected to a PC, it only draws power)

That’s it! The open source (free!) Ethernet analyzer WireShark can be downloaded from www.wireshark.org. You’ll also see links for documentation there as well.

Indicators:

The Red LED glows when power is applied. The SharkTap uses the standard 5V power from a USB port, and draws 250mA or less current.

Each port jack has two LEDs. The Green LED is on when there is a valid link connection. (Note that the SharkTap has a feature called MDIX, meaning that it will automatically crossover Tx and Rx pairs, so no crossover cable is ever needed.) The Yellow LED is on if the link is 100Base-T, off if it's 10Base-T. The Green LED will blink when there are packets sent or received on that port.



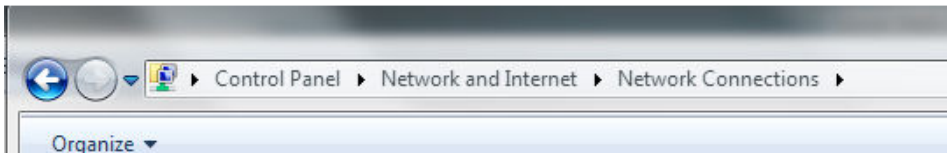
Questions? Send us an email at support@midbittech.com

www.midbittech.com

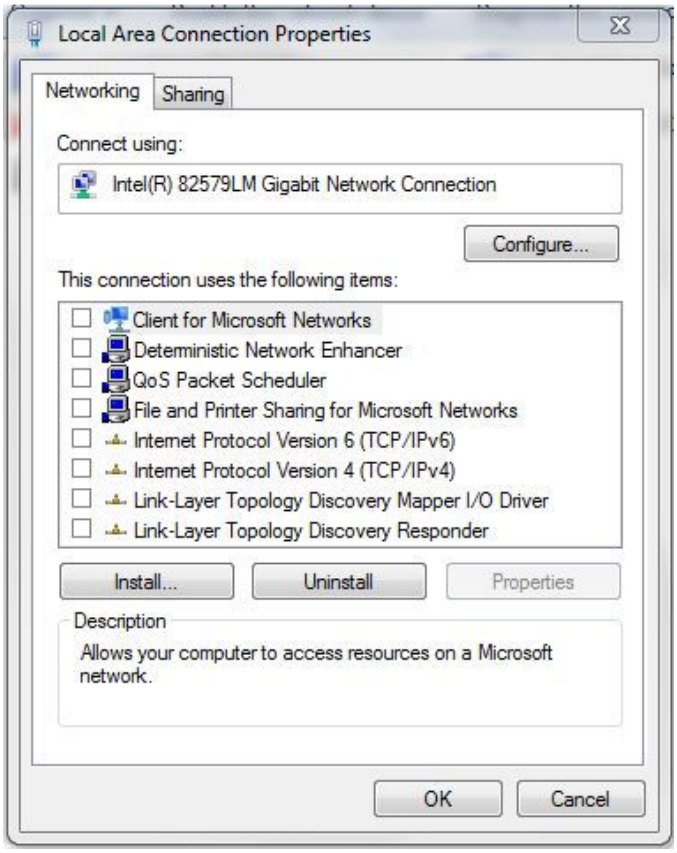
A Hint for your PC port:

For Windows setups that have a spare Ethernet port that you can use to connect to the SharkTap, such as a laptop that uses Wifi for internet access, here's a hint for setting up the wired port that will avoid Windows sending packets out the port, so you will only capture packets from the network you are monitoring. Note that the Sharktap will send any packets the PC sends to the Network ports. This can be useful for accessing the network you are monitoring, but can also be confusing if you don't realize your PC is generating packets.

Edit the properties for the spare port, which can be reached from



And then double clicking on the spare port. This will bring up a dialog like the following:



Click on the check boxes to remove the check marks from all the protocols that the connection uses. This will prevent Windows from trying to access the Internet or a Windows network over this port.