ECHELON

IzoT™ Plug-in for WireShark

Monitor, analyze, and troubleshoot IzoT networks using the Wireshark packet analyzer.

078-0511-01A

Printed in the United States of America.

Echelon Corporation
www.echelon.com

Contents

The IzoT Plug-in for WireShark

The IzoT Plug-in for WireShark lets you use WireShark's free and open-source packet analyzer to troubleshoot and analyze LonTalk/IP networks. If you don't have a copy of WireShark, go to *www.wireshark.org/download.html* to download it.

Introduction

Wireshark is a free and open-source packet analyzer for IP networks. It is used for network troubleshooting and analysis. The IzoT Plug-in for Wireshark enables Wireshark to decode LonTalk/IP packets.

You can use the IzoT Plug-in for Wireshark to monitor LonTalk/IP traffic on a LAN channel. You can also use the IzoT Plug-in for Wireshark to monitor LonTalk/IP traffic on an FT channel if you have an IzoT Router that is configured as a repeater and is attached to both your LAN and your FT channel, and if you have a hub connecting your computer and your IzoT Router. The IzoT Router is configured as a repeater by default. When operating as a repeater, the IzoT Router forwards all packets on the FT channel to the LAN channel.

You can configure an IzoT Router to operate as a configured or learning router using the IzoT Commissioning Tool. If the IzoT Router is operating as a configured or learning router, it will not forward all packets on the FT channel to the LAN channel, and as a result, you will not see all FT traffic in Wireshark. If you are using the IzoT Commissioning Tool to commission an IzoT Router, change the operating mode to be a repeater when you are using Wireshark to troubleshoot or analyze the FT channel. You can change the operating mode back to a configured or learning router when you are not using Wireshark.

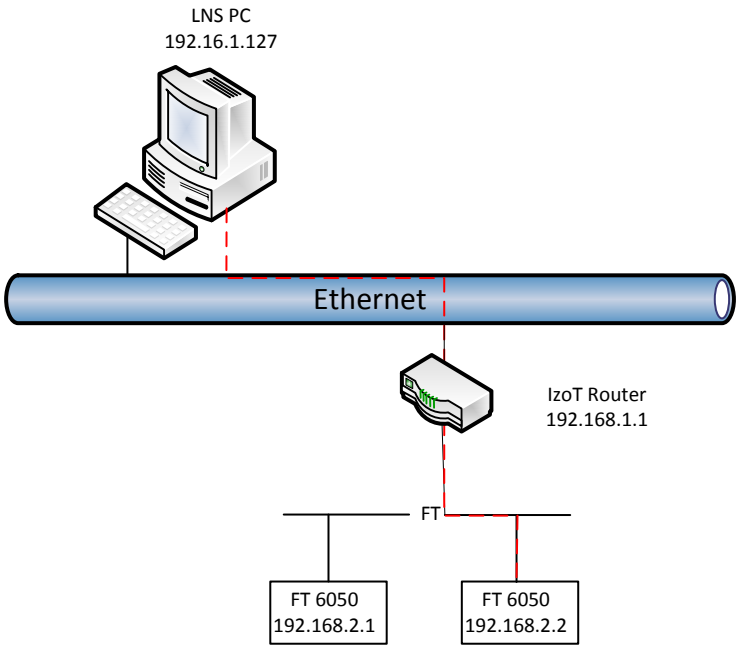
Installing the Wireshark Plug in

The IzoT Plug-in for Wireshark is included as part of your IzoT NodeBuilder software. To install the IzoT Plug-in for Wireshark, follow these steps:

1. Install the IzoT NodeBuilder software as described in the *IzoT NodeBuilder User's Guide*.
2. Download the Wireshark software for Windows from *www.wireshark.org/download.html*.
3. Install the Wireshark for Windows software.
4. Copy **lontalkip.dll** from your LONWORKS Wireshark Plugin folder into your Wireshark plugins directory. In a typical installation, the default LONWORKS folder is **C:\Program Files (x86)\LonWorks\Wireshark Plugin**, and the default Wireshark Plugs folder is **C:\Program Files\Wireshark\Plugins\1.10.6**, where 1.10.6 is the version of Wireshark you have downloaded. The WireShark Plugin folder comes with DLLs compiled for both 32-bit and 64-bit Windows. Use the ones that match your installation.

Monitoring Packets

Once you have set up Wireshark, you can monitor LonTalk/IP traffic. If you have LonTalk/IP-FT devices and an IzoT Router connecting your FT channel to a LAN, packets will flow from FT devices, through the IzoT Router, over the Ethernet LAN and to your computer. The red line shows the flow of the packets.



Adding a Switch to the Network

When using Wireshark, there are some potential limitations in monitoring traffic on an Ethernet channel. A protocol analyzer can only decode the traffic that it receives. Typically, networks use switches, and switches do not forward all traffic to all ports, but instead attempt to only forward traffic to ports that should be receiving that traffic. This means that only LonTalk/IP traffic that is broadcast, multicast, or sent directly to the computer running Wireshark will be received and decoded by Wireshark.

Adding a Hub to the Network

If you use a hub on your network, then all traffic received by that hub is forwarded to all ports on the hub. This means that all traffic can be decoded by a computer running Wireshark, regardless of the destination of the traffic. You can find a more thorough discussion of hub traffic at wiki.wireshark.org/CaptureSetup/Ethernet.

Reading the Wireshark Logs

You can use Wireshark filters to select packets to be logged or displayed, and you can use Wireshark statistics reports to analyze displayed data. For more information on using Wireshark, download the Wireshark documentation from www.wireshark.org/docs. The *Wireshark User's Guide* is available in several formats, you can browse it on the Web, download a zip file, or grab it as a PDF file.