

PilotFish for WireShark

Purpose

PilotFish is a software tool designed to be used with WireShark (v1.1 or later) to capture and decode BACnet MS/TP messages.

Background

To troubleshoot BACnet problems, very often we need to capture, decode and analyze the communication messages down to the byte and bit level. Since the structure of BACnet messages is not trivial, we need tool to help us to comprehend the complexity. For BACnet IP datalink, one of the most common and effective approaches is to use WireShark. WireShark (a free and open source tool) is a very well known, mature, sophisticated and widely used general network message analyzer for Ethernet based communications. For BACnet MS/TP datalink, however, things become not so easy. WireShark just cannot "see" MS/TP messages directly because the communications is on RS485 serial bus but not Ethernet. A gateway is therefore needed for the purpose. However, free tool of this type is still very rare on the market. PilotFish is therefore written to fill the missing link. This tool acts as a bridge between WireShark and MS/TP trunk to let us analyze MS/TP messages as well as IP messages on WireShark at the same time.

Theory

The whole idea was inspired by an article from Steve Karg (<http://steve.kargs.net/2008/11>).

Advantages

1. User can use only a single tool to analyze both BACnet IP and MS/TP messages.
2. It makes use of WireShark's built-in BACnet decoder (very sophisticated and well supported by the community). So the decoding is fast, accurate and consistent with the analysis done for the IP datalink.
3. Very often, there is a strong correlation between the communications of the IP and MS/TP datalinks. Using this approach, user can examine all IP and MS/TP messages alongside at the same time and study any the chronological causes and effects across the two datalinks.

Features

- Online mode – It can capture and send MS/TP packets to WireShark directly in real time
- Offline mode – It can capture and save MS/TP packets in a file. The file can then be opened with WireShark later.

Requirements

Software:

1. Microsoft Windows XP SP3 or later.
2. WireShark version 1.1 or later.

Hardware:

1. A desktop or notebook PC with a spare RS232 port or a spare USB port
2. For using RS232 port, a RS232-to-RS485 converter, or
for using USB port, an USB-to-RS232 converter and a RS232-to-RS485 converter, or
an USB-to-RS485 converter

Installation

No real installation is needed. Just copy the file "PilotFish.exe" to a desired directory.

Operation

There are two modes of operation:

Online mode:

1. Connect the PC to the MS/TP bus via any necessary hardware
2. Run WireShark. Select a network interface and start capture.
3. Run PilotFish (execute the "PilotFish.exe" file)
4. In the "Get input from" panel, fill in the parameters for connecting the MS/TP trunk.
5. In the "Send output to" panel, select the tab "WireShark (Online mode)". Select the same network interface being used by WireShark in step 1.
6. Click the "Start" button to start the capture.
7. Now, real time MS/TP messages can be seen on WireShark.
8. If desired, in order not to be overwhelmed by the messages received, capture or display filters can be set in WireShark.
9. Click the "Stop" button to finish the capture.

Offline mode:

1. Connect the PC to the MS/TP bus via any necessary hardware
2. Run PilotFish (execute the "PilotFish.exe" file)
3. In the "Get input from" panel, fill in the parameters for connecting the MS/TP trunk.
4. In the "Send output to" panel, select the tab "File (Offline mode)". Specify the full path name for the capture file.
5. Click the "Start" button to start the capture.
6. Wait for a certain period of time enough for your need.
7. Click the "Stop" button to finish the capture.
8. Run WireShark to open the captured file.

Tips

1. By nature, the MS/TP datalink is never silent. There are always messages (especially those for PFM and Token) going on even when there is no application data exchange. These datalink messages are massive and may sometimes prevent you from following application level activities easily. In this case, you can use the filter function in PilotFish to filter out those messages you don't want to see. For normal use, PFM and Token messages can be screened out without missing any significant application event.
2. To just focus on BACnet messages in WireShark, you can use the following display filters in WireShark.
 - 2.1. "bacapp" for all BACnet application messages (of both IP & MS/TP datalinks)
 - 2.2. "bacnet" for all BACnet network and application messages (of both IP & MS/TP datalinks)
 - 2.3. "mstp.frame_type" for all BACnet MS/TP messages (in both online & offline mode)
 - 2.4. "mstp" for all BACnet MS/TP messages (in offline mode)
3. In online mode, if your PC has no physical network connection (standalone, no network cable plugged-in), WireShark will not see packets sent by PilotFish (even if you don't care about the IP messages). This is in fact not a problem of either WireShark or PilotFish. It's actually a problem of Microsoft Windows. The solution is to use Microsoft Loopback Adapter.
 - 3.1. Install Microsoft Loopback Adapter
 - 3.1.1. For Windows XP, see this (<http://support.microsoft.com/kb/839013>)
 - 3.1.2. For Windows 7, see this (<http://www.windowsreference.com/windows-7/how-to-install-a-loopback-adapter-in-windows-7/>)
 - 3.2. Assign an arbitrary IP to the Loopback Adapter
 - 3.3. Reboot the PC (very important!)
 - 3.4. In online mode operation, select the Loopback Adapter instead of a physical network adapter.