University of New Hampshire
InterOperability Laboratory

Wireshark Color Filters for PTP (Tutorial)

by Jeff Laird, May 2012

What are color filters?

Along with capture filters and display filters, Wireshark has *color filters*, which allow the user to customize packet coloring. You can view and edit the color filters through the **View → Coloring Rules...** dialog box.

Why you want to use color filters for PTP

Wireshark comes preconfigured with some color filters, but it does not know about the various PTP message types. Therefore by default all PTP messages appear in the same color, which is hard to read. Distinguishing the various PTP message types by color greatly improves readability.

The IOL PTP color filters

The IOL has devised a set of ten color filters for the ten PTP message types. Because the filters are based on the PTP message type they are equally effective with layer-2 (Ethernet) and layer-3 (IP) transport. To use the IOL color filters in your Wireshark captures do the following.

1. Download the file `IOL_PTP_Wireshark_color_filters.txt` from our website (where this tutorial document was found).
2. Using the **View → Coloring Rules...** dialog box mentioned above, import that color filter file. Importing *appends to* rather than overwrites the existing color filters. If you are using layer-2 transport you must move the "Broadcast" coloring rule to below the ten PTP rules you just added. This is because Wireshark applies the rules from top to bottom. Similarly, if you are using layer-3 transport you must move the "UDP" coloring rule down.

hex	message type
00	Sync
01	Delay_Req
02	Pdelay_Req
03	Pdelay_Resp
08	Follow_Up
09	Delay_Resp
0a	Pdelay_Resp_Follow_Up
0b	Announce
0c	Signaling
0d	Management

IOL Color Filters

FYI (unimportant details)

The ten colors used in the IOL PTP color scheme are the following X11 colors: pink, lightblue, mediumaquamarine, lightgreen, dimgray (font color), mistyrose, lightcyan, aquamarine, goldenrod, hotpink, palegoldenrod).

Another method of distributing a set of color rules is to copy Wireshark's color filter file from one computer to another, eliminating the use of the **View → Coloring Rules...** dialog box altogether. Wireshark stores the filtering rules in a file called "colorfilters". There are two instances of this file: a global instance which Wireshark uses by default until a user makes changes, and a user instance which Wireshark creates after the user makes changes. In Linux the global file is

```
/usr/share/wireshark/colorfilters
```

, and the user file is

```
/home/<username>/.wireshark/colorfilters
```

. In Windows the global file is

```
C:\Program Files\Wireshark\colorfilters
```

, and the user file is

```
C:\...\<username>\Application Data\Wireshark\colorfilters
```

(in XP) or

```
C:\...\<username>\AppData\Roaming\Wireshark\colorfilters
```

(in Vista/7).

To configure a computer to use a particular set of color filters, overwrite the user file with the desired colorfilter file.