



Display Filters

Wireshark Filters

» What is a filter?

- Used to limit what appears in the Packets List pane

» Wireshark filters are used to

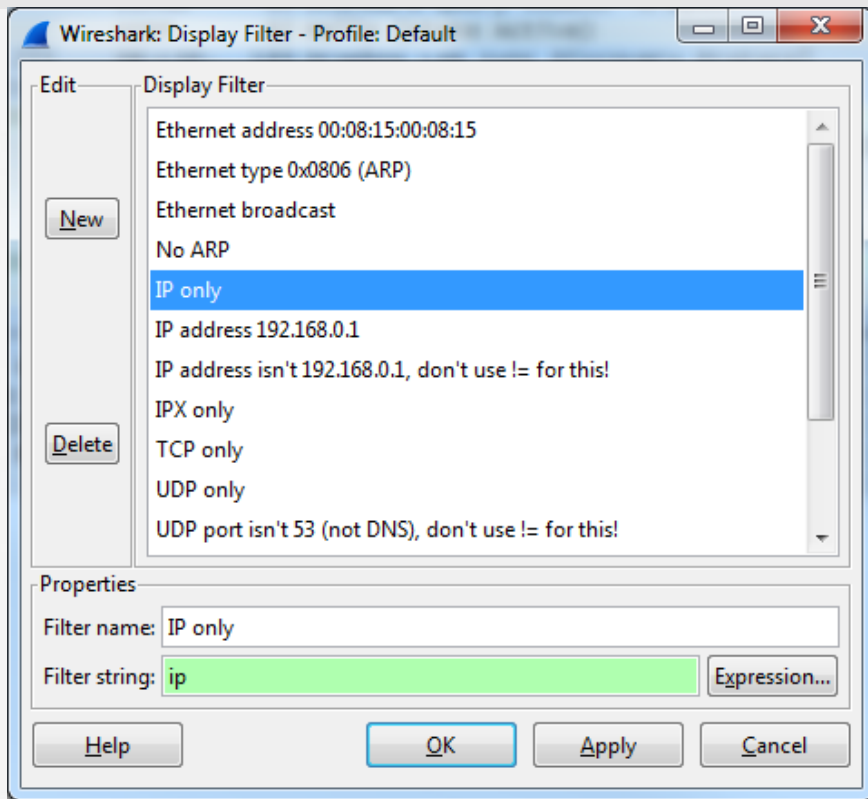
- Aid in troubleshooting efforts
- Refine the view
- Assist with only collecting only what you need

Wireshark Filters

» Filter types

- Capture – Used to filter data before it is captured by Wireshark. For example, you could configure Wireshark to capture only data supplied by a specific IP address.
- Display – Used to filter data after it is captured. This will help you refine the display to show only what you need to see.

Configuring a Display Filter



Wireshark Filters

» Troubleshooting with filters

- Streamline viewable traffic to find exactly what you need
- Remove anything that could cause confusion
- Give the analyst a clearer view of the root cause data

Questions?