



Capture Filters

Wireshark Filters

» What is a filter?

- Used to limit what appears in the Packets List pane

» Wireshark filters are used to

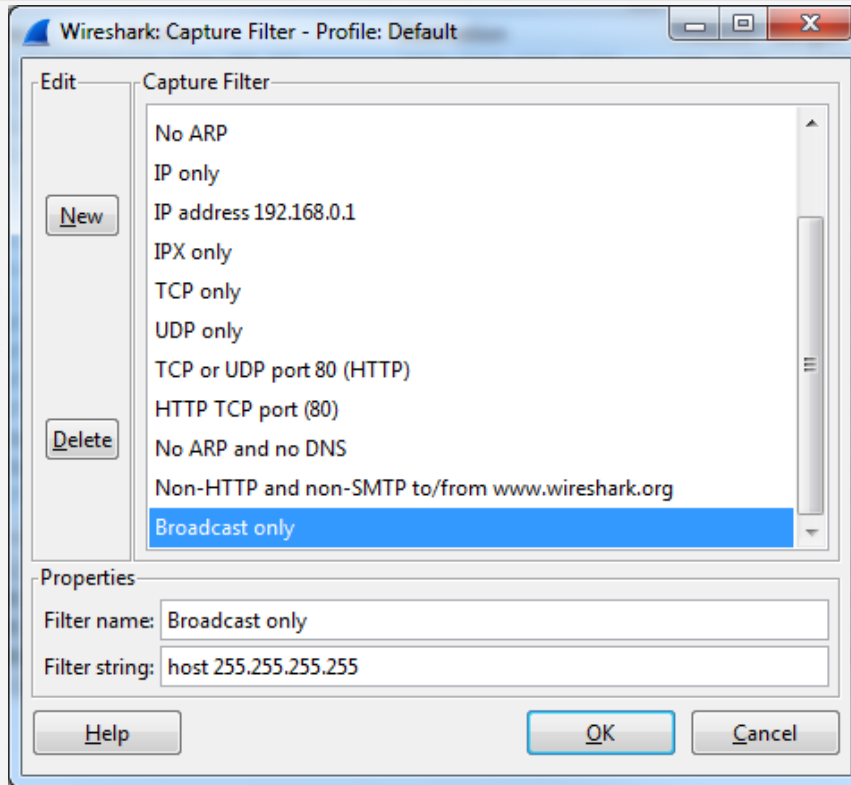
- Aid in troubleshooting efforts
- Refine the view
- Assist with only collecting only what you need

Wireshark Filters

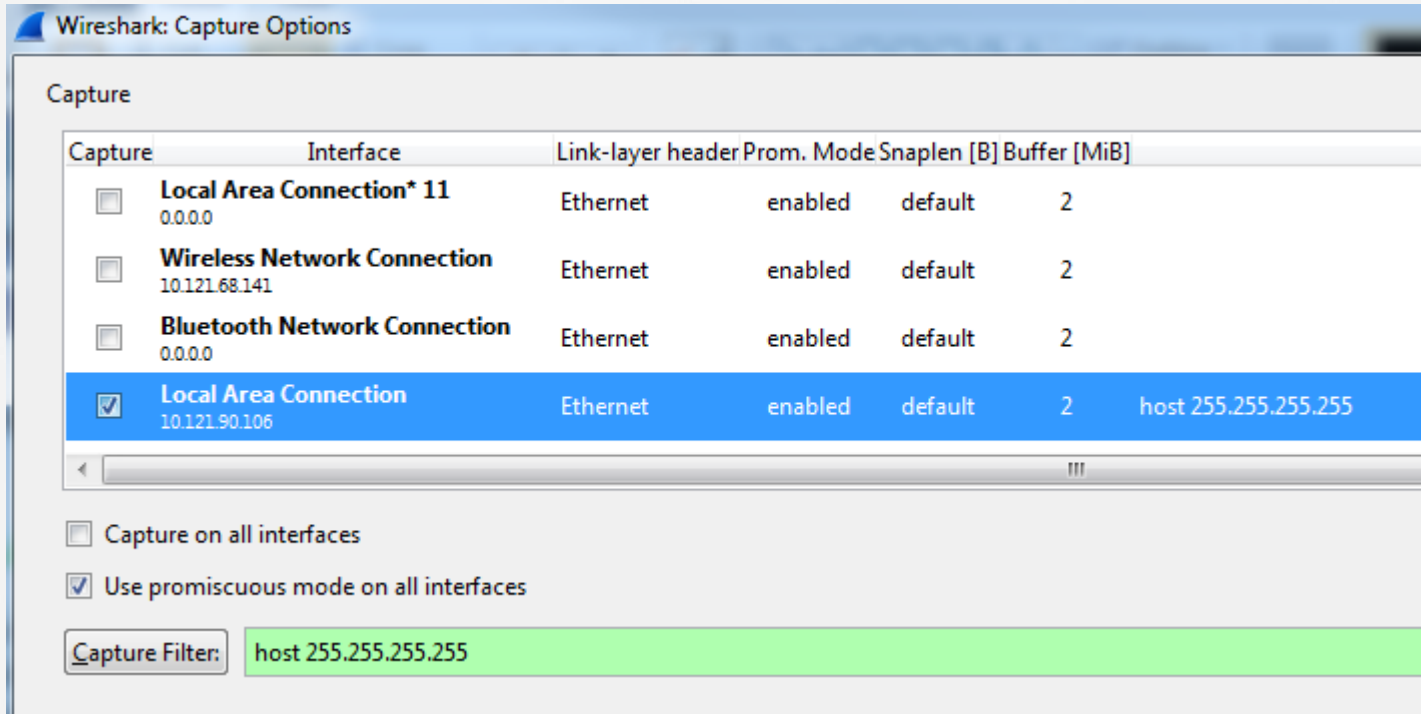
» Filter types

- 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 Capture Filter



Configuring a Capture Filter



The image shows the 'Wireshark: Capture Options' dialog box. The 'Capture' section contains a table with the following data:

Capture	Interface	Link-layer header	Prom. Mode	Snapplen [B]	Buffer [MiB]	
<input type="checkbox"/>	Local Area Connection* 11 0.0.0.0	Ethernet	enabled	default	2	
<input type="checkbox"/>	Wireless Network Connection 10.121.68.141	Ethernet	enabled	default	2	
<input type="checkbox"/>	Bluetooth Network Connection 0.0.0.0	Ethernet	enabled	default	2	
<input checked="" type="checkbox"/>	Local Area Connection 10.121.90.106	Ethernet	enabled	default	2	host 255.255.255.255

Below the table, there are two checkboxes:

- Capture on all interfaces
- Use promiscuous mode on all interfaces

At the bottom, the 'Capture Filter:' field is set to 'host 255.255.255.255'.

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?