# Packet Capture - Best Practice

**In this section:**

This document describes the ideal settings for a packet capture. For information about how to capture a packet, download, or limitations, see Working with Packet Capture.

## Ideal Settings

The following list the ideal settings for Packet Capture.

1. Packet capture durations should be configured for the minimum amount of time necessary to capture the problem attempting to be reproduced.

2. When capturing a Media and/or SIP Signaling file, appropriate filters should be selected to minimize the volume of packets that must be captured. In particular, the following two filters should be utilized for Media and/or SIP Signaling file:

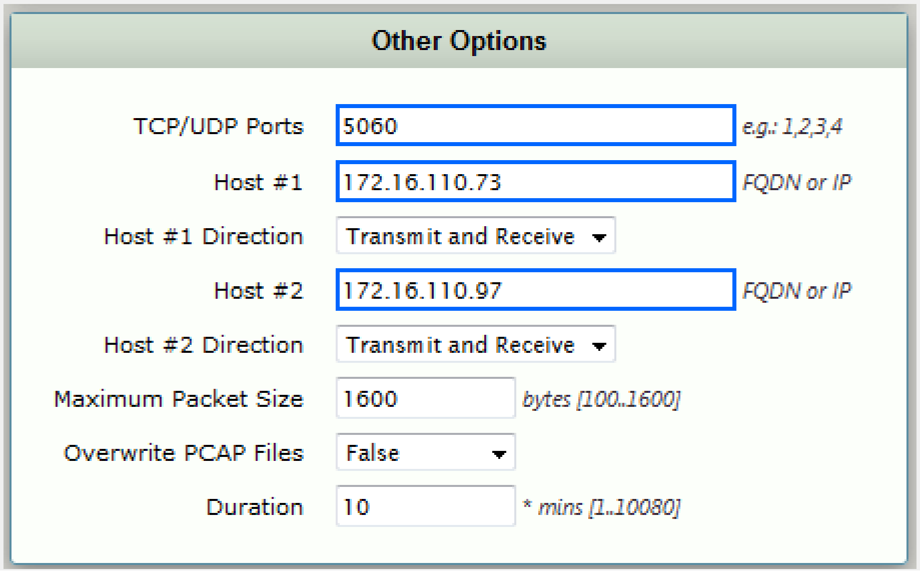
    - TCP/UDP Port filters
      Up to four filters can be listed. Separate the filters by using a comma.

    - Host IP address

      Up to two IP addresses can be configured. If possible, the host IP addresses should be used against termination points that are only terminating a single call.

    > ⓘ For each IP address entered (Host 1 or Host 2) a new option will become available to select capture direction.

**Figure 1:** Other Options Menu



Other Options

| | | |
|---|---|---|
| TCP/UDP Ports | 5060 | *e.g.: 1,2,3,4* |
| Host #1 | 172.16.110.73 | *FQDN or IP* |
| Host #1 Direction | Transmit and Receive ▾ | |
| Host #2 | 172.16.110.97 | *FQDN or IP* |
| Host #2 Direction | Transmit and Receive ▾ | |
| Maximum Packet Size | 1600 | *bytes [100..1600]* |
| Overwrite PCAP Files | False ▾ | |
| Duration | 10 | * *mins [1..10080]* |

## Maximum Duration

> The Packet Capture feature is intended for **short** duration packet captures. For that reason, a maximum duration of 120 minutes (2 hours) is permitted.

## Other Recommendations

### Wireshark

The packet time-stamps ("Time" field in Wireshark) of media packets in a packet capture may appear wrong, as large negative numbers. However, the ordering of the media packets based on packet numbers ("No." field in Wireshark) will be correct.

Also, if you use the "RTP Player" in Wireshark to decode and play the media packets, the wrong time-stamps may cause noise and/or distortion in the display and audio playback of the media packets. To work around this issue, in the RTP Player of Wireshark, select the "Use RTP timestamp" option and then click Decode.