Packet Filters in Qosium

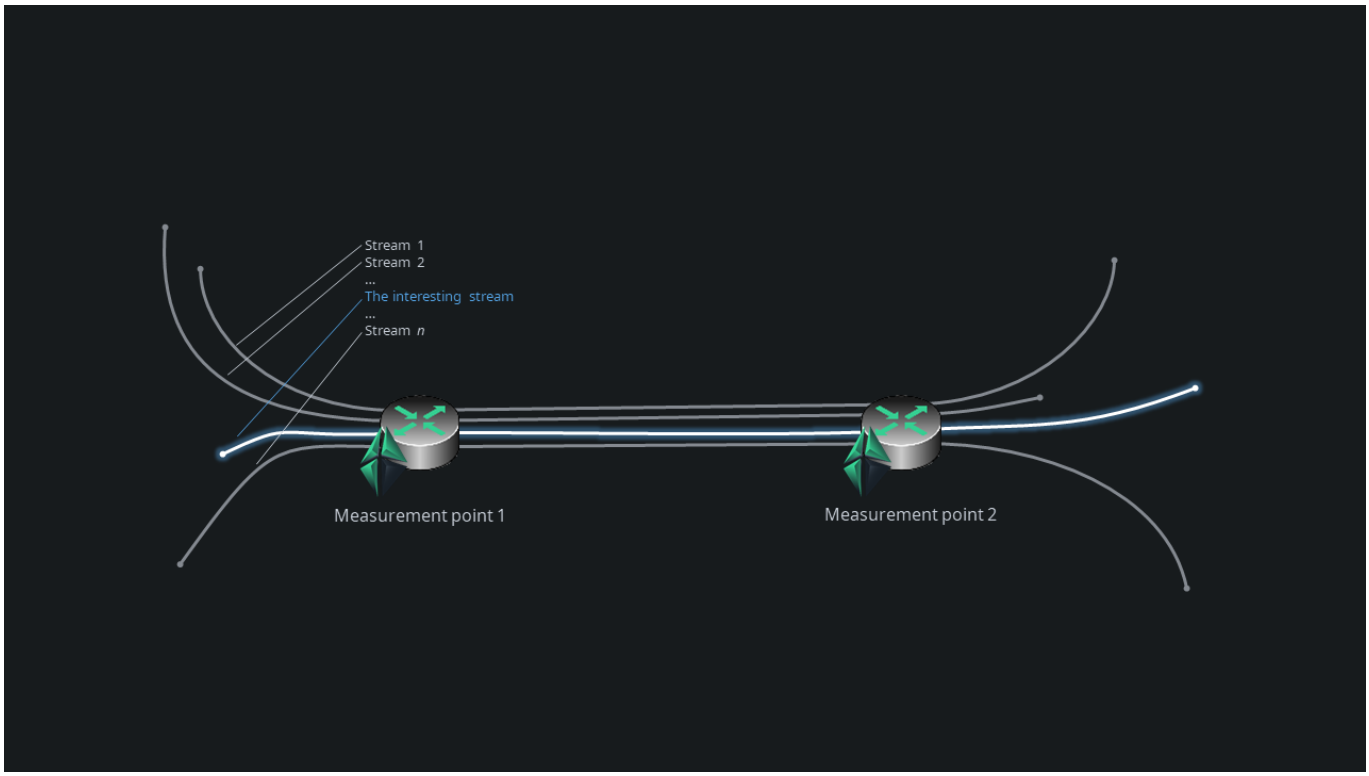
Packet filter is one of the essential concepts in passive measurement. An active measurement tool pushes a predetermined data stream into the network, so the traffic to be measured is always known. In passive measurement, on the other hand, existing traffic is measured, so filters are needed to define what part, in particular, of the total traffic is the interesting one to be taken into the measurement.

Table of Contents

1. Filtering in General

In passive measurement, existing traffic in the network is being measured. By default, when tapping into a network interface, all the traffic traveling there is shown. Sometimes that is what is desired. However, often you may wish to examine only a specific part of the total traffic.

Consider the figure below, which depicts two measurement points through which several independent traffic streams flow, originating from different applications/services. If we were, for example, interested only in the QoS of a particular single flow between these two measurement points, we would need to filter out all the other flows during measurement. This enables us to measure the QoS solely from the perspective of that interesting traffic flow. Similarly, we could be interested in multiple flows of a specific kind, which would require another kind of filter. This is what filtering in the context of passive QoS measurements is all about.



2. Filtering in Qosium

Qosium has some automation in filtering. For example, in an end-to-end measurement scenario, Qosium will, by default, assume that all traffic between the two points is included in the measurement and generate an automatic filter accordingly. In many measurement cases, that is enough. If, however, you are interested only in a specific part of the total traffic, tell that to Qosium by defining *a manual filter*. All Qosium measurement controllers allow defining a filter.

Defining a filter in Qosium follows the well-known Pcap syntax. A typical end-to-end filter could look like this:

```
ip and host 192.168.0.10 and host 192.168.0.101
```

This instructs Qosium to measure all IPv4 based traffic between hosts 192.168.0.10 and 192.168.0.101. If, for example, the interesting part would be a VoIP-stream traveling between these two machines, we need

to focus the filter. Let us assume that the VoIP software uses UDP port 7000 on one end and UDP port 7001 on the other. Now we can define the filter as

```
ip and host 192.168.0.10 and host 192.168.0.101 and udp and port 7000 and port 7001
```

This is now a so-called *strict filter*, as there can be only one two-way stream that fits the filter. The previous filter was an example of a *loose filter* as many potential streams can be caught with that.

3. Additional Information

Writing filters in Qosium is mostly straightforward. An up-to-date full instruction of the Pcap syntax is given here. See our article on Pcap syntax instructions, which includes keywords, functionalities, and examples typically needed when using Qosium.

Qosium's packet filter is a capture filter, so the traffic filtered out cannot be added in the measurement later.