How to Take Packet Capture?

Qosium needs to see the network traffic to be able to measure passively. Qosium Probe also comes with an optional feature to take packet captures, Pcap files, from the measured traffic. The packet trace is taken from the traffic that matches your measurement filter. You can open the Pcap file with the preferred packet analyzer tool. This guide demonstrates how you can perform packet capturing with Qosium Scope. Packet capturing is something that can also be taken off from a Qosium delivery.

Table of Contents

1. Introduction

Your Qosium can be delivered with an optional feature to enable full packet trace capturing. This enables you to write Pcap files of all the measured traffic. These files can be opened with packet analyzer tools, such as Wireshark.

2. Step-by-Step Guide

2.1. Verify Packet Capture Feature

First, verify that the Qosium Probe with which you plan to take the packet capture has pcap forwarding enabled. When Qosium Probe is launched, the following text should appear in the console.

```
Optional features: Pcap forwarding supported
```

Alternatively, you can simply test packet capturing, and if the feature is not enabled in your Qosium Probe, you will get an error message of that.

If pcap forwarding is not enabled in your distribution of Qosium Probe, please contact us via Tukipyyntö.

2.2. Setup Measurement

Setup measurement scenario normally. Note that the packets are captured only from the primary measurement point, even if a two-point measurement has been configured.

To capture from the secondary measurement point, launch another Qosium Scope instance and perform a single point measurement targeting the secondary Probe

2.3. Set Packet Filter

Be careful with the packet filter when Qosium Probe is located on a different machine than Scope. The reason for this is that a packet capturing will also capture Qosium's control traffic, which also carries the packet capturing data when enabled. This results control traffic to grow until network capacity is reached. To filter out Qosium's own control traffic, simply exclude the Qosium communication port from the packet filter.

Qosium uses, by default, TCP destination port 8177, so it is easy to filter out. For example, if you wish to perform a remote capturing in machine 192.168.0.10 for all the traffic that involves the target machine, except Qosium's own traffic, then apply the following filter:

```
ip and host 192.168.0.10 and not port 8177
```

If Qosium's control traffic is not filtered out in a remote capture situation, the already captured traffic will be re-captured, leading to a chain reaction that will eventually fill all the available bandwidth between Probe and Scope.

2.4. Set Scope to Capture Packets

To enable pcap results in Qosium Scope, a few settings must be set. In the *Measurement Control* panel,

under the *Results* tab:

- Enable *Capture pcap results to file*
- Select the preferred *Save directory*

All results statistics and the cap file are written to the same given directory.

See Results Tab for more information.

3. Taking Packet Capture from Both Ends of Two-Point Measurement

When you have a two-point measurement configured and packet capture is enabled, the pcap file created includes only trace from the Primary Probe. If you want to take the capture also from the other end of the measurement path, you need to start another measurement. You can take packet captures from both ends in the following way:

- Scope with two-point measurement
  — Enable packet capture, and packet dump is taken from the interface Primary Probe measures
  — Give *Measurement description* so that you know from which measurement the dump file is taken from
- Start another Scope for one-point measurement
  — Connect to the other Secondary Probe in your two-point measurement
  — Set the same measurement filter as in the two-point measurement
  — Give *Measurement description* so that you know from which measurement the dump file is taken from
  — Enable packet capture

4. Performance Considerations

The amount of data can get very large fast when measuring a high-speed stream. If the measured stream is larger than the network path's bandwidth between the controlling entity and Qosium Probe, then Probe starts buffering the captured packets for sending. First, this increases the memory usage of Qosium Probe depending on the buffering need. Secondly, Pcap file writing will be delayed accordingly.

If the measured stream is continuously larger than the network path's bandwidth between Scope and Probe, the buffering continues, theoretically, until the computer runs out of memory. To prevent this, you need to pay attention to the measurement process. When you stop the measurement, also Pcap results sending is stopped. If unsent packets are buffered in the Qosium Probe, they will be erased.

Bear in mind that Qosium Scope has limited capability to process and write Pcap data. Thus, if you write Pcap files from a high-speed stream, Qosium Scope might halt its operation for a while when you stop the measurement. This is because Qosium Scope will collect and write all data that its receiver has locally buffered.