How-to Guides

These guides introduce features and functionalities of Qosium, and how to use them.

Table of Contents

For learning material, please refer to [Get Started with Qosium](#) instead.

1. 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.

1.1. 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](#).

1.2. Step-by-Step Guide

1.2.1. 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 [Support Request](#).

1.2.2. 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.

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

1.2.3. 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.

1.2.4. 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.

1.3. 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

1.4. 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.

2. How to Discover Probes

When you have a large network with many Qosium Probes installed, keeping track of each Probe and their IP addresses can become cumbersome. Qosium comes with a feature that allows you to find all your Qosium Probes in the network.

2.1. Concept

Qosium comes with a feature to find your Qosium Probes in the network and take them into a measurement. The *Probe Discovery* feature overcomes the difficulty of recalling IP addresses and device reachability issues with dynamic IP addresses. Instead of IP addresses, Qosium Probes are identified based on their unique ID given by you. Probes in the network periodically register their existence to a selected *Central Probe*.

Using Probe discovery is useful when:

- You are monitoring a wide network with dozens of Probes.
- Remembering the IP addresses/hostnames of Qosium Probes is difficult.
- The IP addresses/hostnames of Qosium Probes are dynamic.
- Devices in which Qosium Probes run are not meant to be connected at all times, or the devices change.
- You want to monitor the overall availability of network devices (i.e., Ping like testing that a device is up and connected)

> (i) The Probe Discovery feature can also be used as a network health inspection tool. If a Qosium Probe you have set to register to a Central Probe has not done that, the device is either disconnected or powered off. You also see the time for how long the device has been connected.

2.2. Configure Qosium Probes

2.2.1. Central Probe

Choose the Qosium Probe that acts as the Central Probe to which other Probes register.

Any Probe can act as the Central Probe. Thus, choose the Probe, e.g., based on availability: the Probe is always on and accessible by other Probes in the monitored system.

2.2.2. Registering Probes

- Open the QosiumProbe.ini file.
- Find the *Server connectivity parameters* section, which is up in the config file.
- Set a unique *Service ID* for the Probe.
- Scroll down to the *Central server registration* section .
- Therein give the IP address of the Central Probe (**central_server_address**), modify **central_server_port** according to Central Probe, and set the interval for how often the Probe registers to the Central Probe in seconds.
- After modifying QosiumProbe.ini file, restart Qosium Probe to activate the new configuration.

See [Qosium Probe's parameters](#) for a detailed description of the key parameters related to this.

2.3. Utilizing Probe Discovery

The Probe Discovery functionality is implemented to Qosium Scope, Qosium Scope Lite, and can also be used by your own software, which implements that feature from the QMCP API.

2.3.1. Discover Probes with Qosium Scope

Follow these instructions if you have the Central Probe configured.

- Open Qosium Scope
- In the top menu bar, select *Control > Discover Probes...*
- Set your Central Probe address and port and press *Update*
- After a few seconds, a list of available Qosium Probes should appear. Select a Probe from the list to be used as the Primary Probe. Then press the button *Use as Primary Probe*
  - If a two-point measurement: select another Qosium Probe from the list to be used as the Secondary Probe. Then press the button *Use as Secondary Probe*
- Close the *Discover Probes* dialog

Now Probes have been selected, and the measurement setup proceeds as usual.

2.3.2. Discover Probes with Qosium Scope Lite

The registered Qosium Probes can be checked with a command `getservices` when in a subscribed state.

Qosium Scope Lite does not integrate an automated functionality to select the Probes for a measurement. Therefore, you need to type the IP addresses of the desired Probes to be included in the measurement manually in the Scope Lite's configuration file.

3. How to Measure over NAT

NAT changes packet content, which brings a new challenge on passive QoS measurement. However, Qosium can manage this and you can measure QoS over a network path where there is a NAT deployed between.

3.1. Define the Topology

There are a couple of specific actions you need to take in the parameterization when measuring over a *NAT* or proxies that change the protocol header content of IP packets. The following instructions tell how to do the measurement parameterization with Qosium Scope. Qosium Scopemon and Scope Lite has the corresponding parameters and the procedure is the same than with Scope.

On the bottom of the *Topology* tab, enable *NAT between Probes* as shown below.
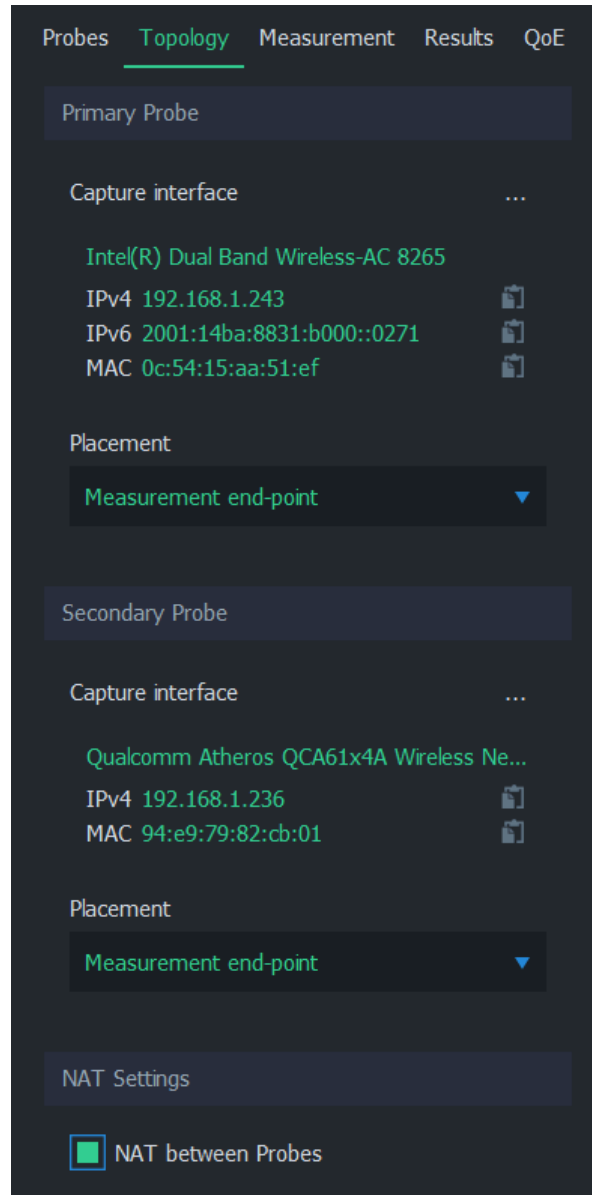
3.2. Set the Filter

Filtering differs from the typical measurement scenario where a NAT is not present. There are two ways how to set the filter. In the most common one, set the filter how the Primary Probe sees the traffic flow(s), while the secondary Probe filter is set automatically. Alternatively, you can define a complex filter that includes parts for both sides of the NAT. This, naturally, requires that you are aware of how the desired traffic looks on the other side of the NAT.

Give *Packet filter* manually in the *Measurement* tab. After selecting *Manual filter*, you have three options in the *Secondary Probe filter mode* selection.
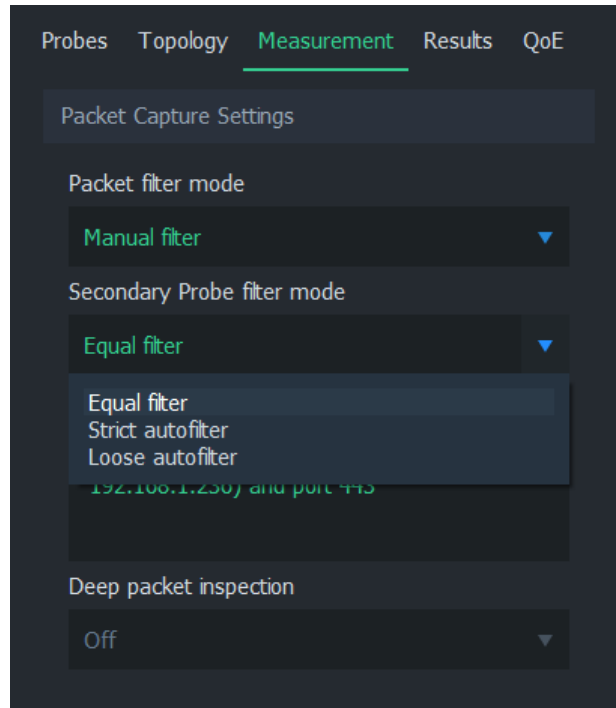
3.2.1. Loose autofilter

Use this when you wish to include all the flows between two IP addresses in the measurement. Define only the IP addresses in the filter. Do this from the primary Probe perspective – the secondary Probe filter is calculated automatically.

If, for example, IP addresses of the interesting traffic flows (as seen from the perspective of the Primary measurement point) are: 192.168.0.100 and 10.0.0.10, then the filter here would be:

```
ip and host 192.168.0.100 and host 10.0.0.10
```

Thus, the general format of the filter to set here is:

```
ip and host <IP address 1> and host <IP address 2>
```

3.2.2. Strict autofilter

Use this when you wish to measure the QoS of only a single flow between the two measurement points. In addition to IP addresses, use source and destination port definitions and also add the transport level protocol in the filter. This ensures that only a single flow will hit the filter. Do this from the primary Probe perspective – the secondary Probe filter is calculated automatically.

If, for example, the interesting traffic flow is TCP 192.168.0.100:56838 <=> 10.0.0.10:8177 as seen from the perspective of the Primary measurement point, then the filter here would be:

```
ip and tcp and host 192.168.0.100 and port 56838 and host 10.0.0.10 and port 8177
```

Thus, the general format of the filter to set here is:

```
ip and <protocol> and host <IP address 1> and port <port 1> and host <IP address 2> and
port <port 2>
```

3.2.3. Equal filter

This selection means that exactly the same filter is used in both measurement point ends. As known, NAT will change the addressing and ports of the traffic, so a single-flow filter won't do the trick. It is, of course, possible that there is something similar and also unique in the desired traffic that remains over the NAT, allowing you to generate a simple filter based on that. Generally, however, this is not the case. Thus, typically, you need to define a two-part filter:

```
<filter for the desired traffic in the Primary end> or <filter for the desired traffic in
the Secondary end>
```

Since especially the latter part of the filter can be quite troublesome to conclude, *Loose autofilter* or *Strict autofilter* are typically being used.

4. How to Create QoS Heatmaps

When Qosium Probe is involved in measurement having geographical location information, you can visualize all Qosium statistics as a heatmap. This feature is useful when measuring wireless networks to determine the network's performance in relation to location. Problem areas can be found out quickly, which helps optimize network coverage and initiate recovering actions.
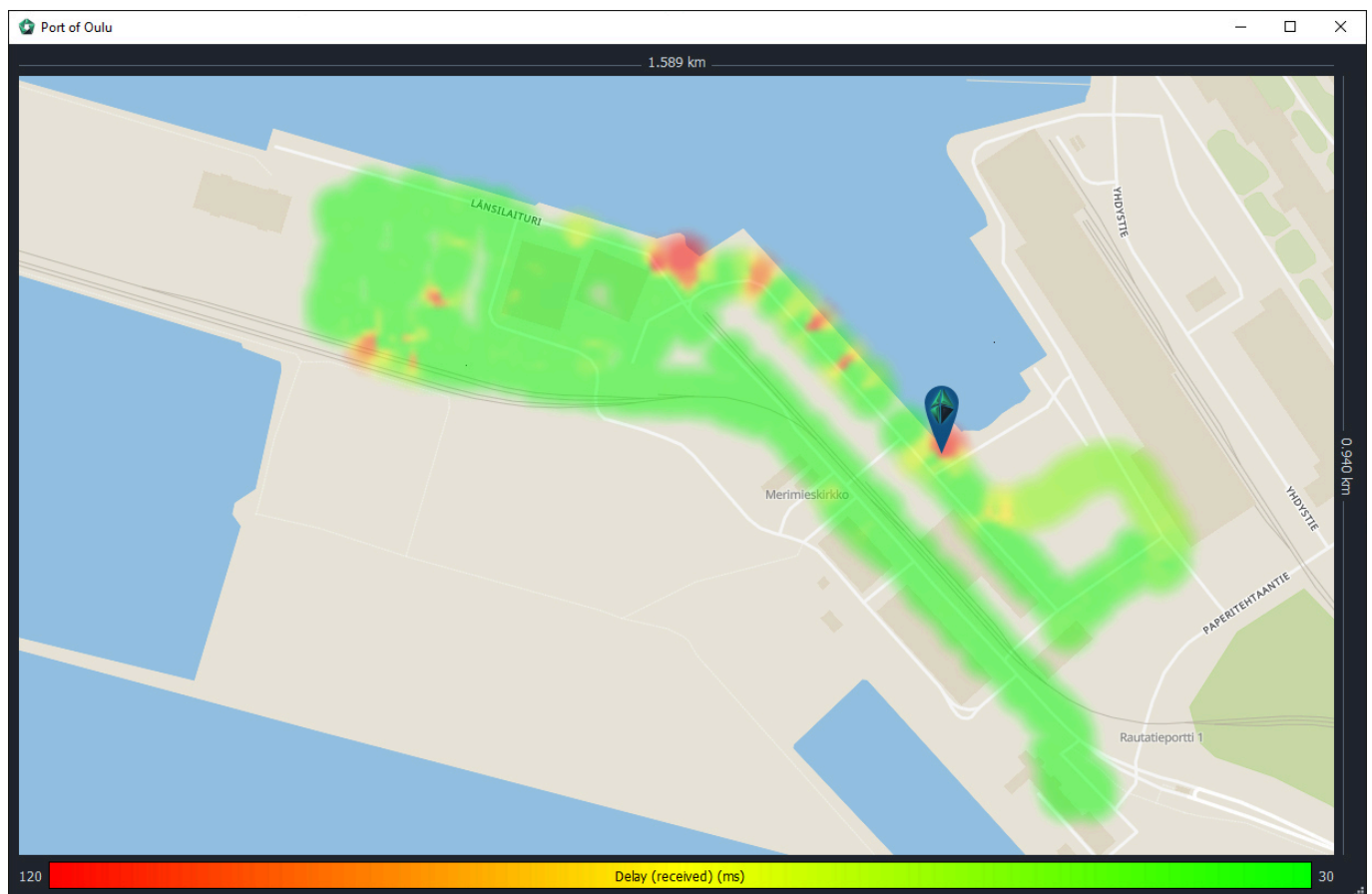
If you are measuring or monitoring moving objects, enable positioning to Qosium Probe, and you will get

into the world of heatmaps. This is a very useful way of visualization, allowing you to see the possible problem areas easily. Qosium lets you draw a heatmap of any performance statistic available, enabling QoS heatmaps instead of pure signal heatmaps, as seen typically.

Heatmaps can be drawn with Qosium Scope or Qosium Storage. The philosophy between these two is a bit different. Qosium Storage is typically used for real-time monitoring, while it can also be used to draw heatmaps from stored data of multiple measurements simultaneously. It allows easy separation of different measurements, and e.g., different devices in the field. The customization of the heatmap drawing style, however, is quite limited. Qosium Scope, in contrast, has extensive possibilities in customizing the visualization, but it can, without special actions, visualize only a single measurement at time.

An example of a heatmap visualization snapshot with Qosium Scope is shown above. It is from Port of Oulu while monitoring actual cargo handling daily operations. To start drawing heatmaps with Qosium Scope, see the detailed instructions [here](#).

5. Glossary

Network Address Translation

A technique for remapping an IP address space

[Wikipedia article on Network Address Translation](#)