Table of Contents

Full NetFlow analytics

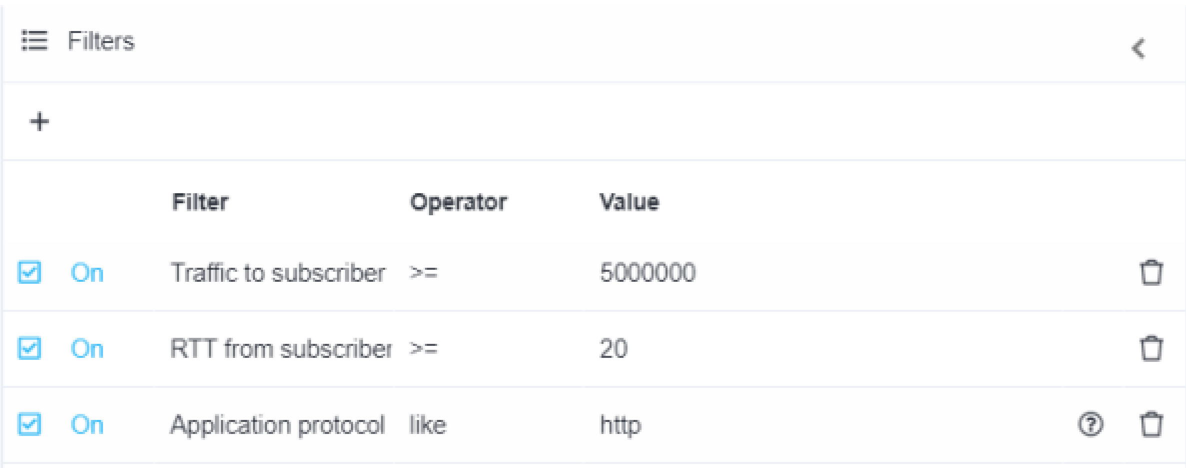
DPI exports information about all client sessions using IPFIX format (NetFlow v10)..

1. Troubleshooting of Internet access degradation

DPI exports information about delays between the client and the DPI and between the DPI and the host during TCP connection establishment - RTT. The statistics reflect a delay within each protocol with a reference to UserAgent (taken from ClickStream), which makes it possible to track the operation of a particular device.
Steps to follow:

1. switch to the QoE section Analytics → Subscribers → Netflow
2. create a filter designed to

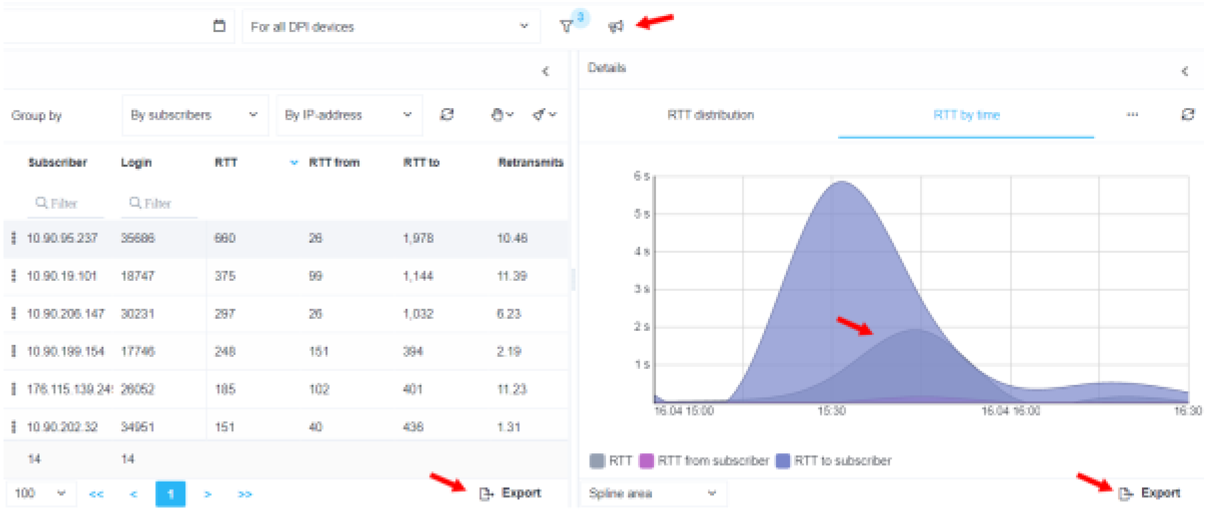
- filter information on http/https protocol to exclude from consideration all the parameters of other protocols when establishing a TCP connection
- set the mean speed to identify subscribers actively using the Internet and exceeding the the mean speed
- specify lower threshold for RTT from client


Filters

+

		Filter	Operator	Value
☑	On	Traffic to subscriber	>=	5000000
☑	On	RTT from subscriber	>=	20
☑	On	Application protocol	like	http

Interpretation of gathered statistics:



- The applied filter made it possible to display 25 potential subscribers who may have Internet access problems.
- More details about the time delays they were faced can be found in the **"Details"** window.
- Using a voice-tube pictogram, you can drag-and-drop them to marketing campaign and conduct a notification or survey on satisfaction with services using browser .
- You can export a report in a convenient format.

2. Uplink monitoring service

Terms & Definitions

Uplink is the link from the operator to the higher-level and/or backbone carrier, from where the operator accesses the Internet channels.
RTT (Round-Trip Time) is the time it takes to send the signal plus the time it takes to confirm that the signal has been received. This delay time, therefore, consists of the signal transmission time between the two points.

Purpose

The "Uplink monitoring" service allows you to detect problems with the service availability for users, which can occur in the channel between the provider and the Internet resource:

- Issues or congestion of the uplink operator.
- Slow operation or unavailability of the service itself.

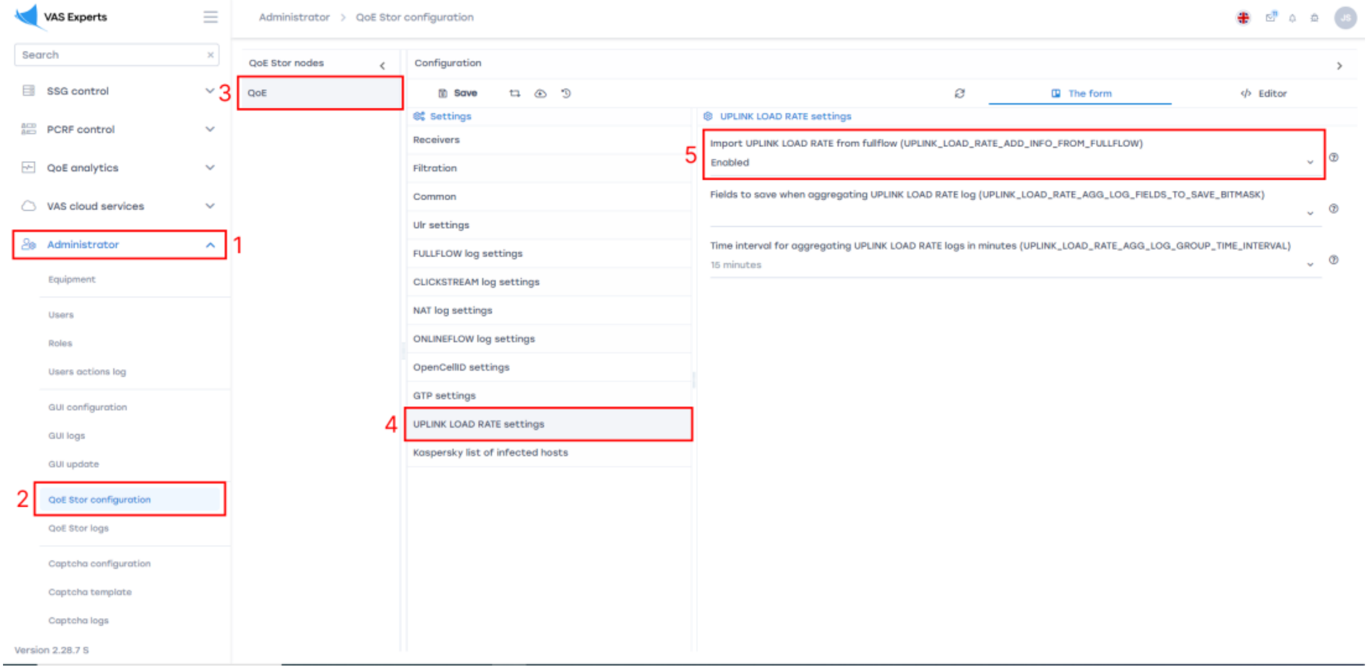
Getting started

Before you start, you need to enable the collection of statistics. To do so, click the icon ☰ in the top left and

1. Select the item *Administrator* in the menu
2. Select the item *QoE Stor configuration*
3. *QoE Stor*

4. *Settings of UPLINK LOAD RATE statistics gathering service*
5. At *UPLINK LOAD RATE* item select *ON*

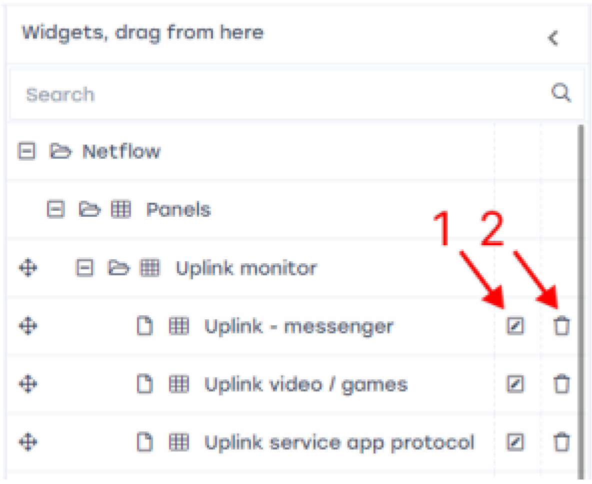
After that press the *Save* button at the top of the screen.



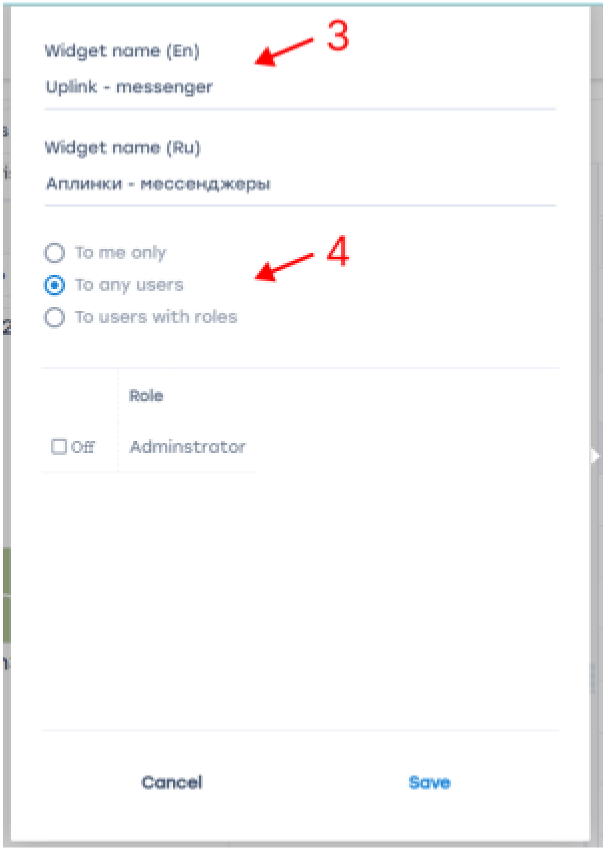
Appearance

The service is located in *QoE analytics → QoE dashboard.* To work with the widget for monitoring uplinks, in the sidebar with widgets select *Netflow → Panels → uplink monitoring* and drag and drop the widget to the dashboard.

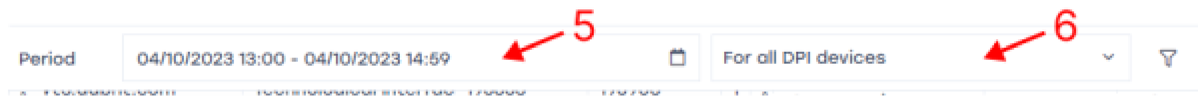
In the sidebar, you can adjust (1) and delete (2) each widget.



In the widget setup window (1) you can change the widget name in English and Russian (3) and its visibility (4).



At the top of the screen, you can select the period for which the traffic will be displayed (5), select the data source (6).

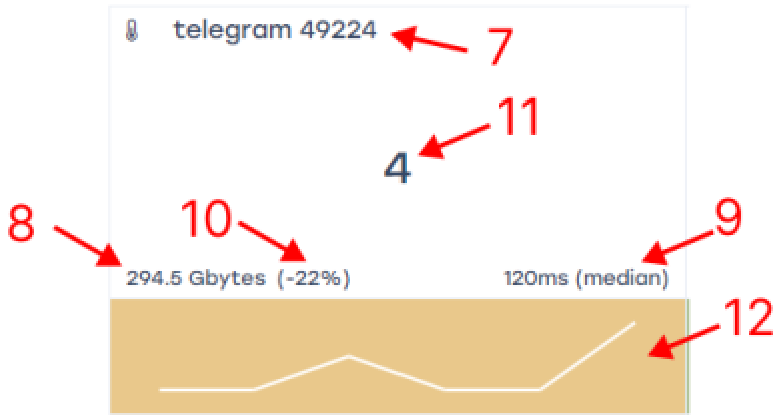


For each protocol, its tile displays:

- **Protocol name** (7)
- **Volume** of traffic for the selected period (8)
- **Median** RTT to subscriber, ms (9)
- **Traffic delta,** % (10). This is the difference between the traffic for the selected time period and the traffic from the statistics, which usually happens for the same period on the same day of the week
- Overall service health **score** (11):

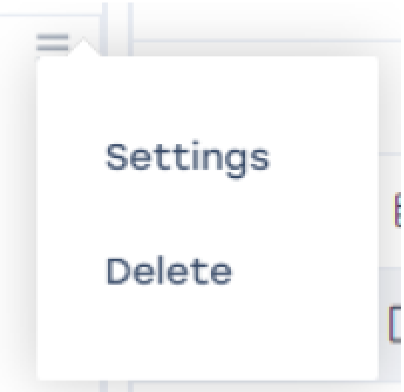
1. 0-3 points — good, graph is green
2. 4-7 points — satisfying, graph is yellow
3. 8-10 points — bad, graph is red

- The protocol health score **change curve** (12). The curve shows how many times the protocol score changed for the selected time period and whether there were no bad scores.



Setting up protocols in the widget

When you hover over the widget, a ☰ icon appears in the upper right corner of the widget. By clicking on it, you can go to the settings, or delete the widget.



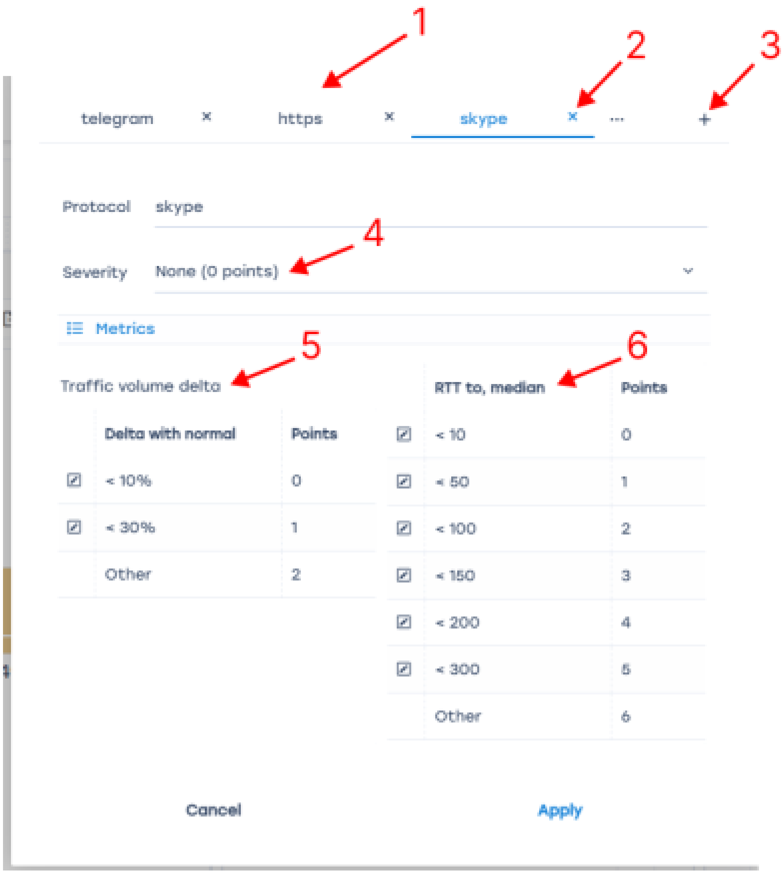
Clicking on *Settings* will open the setup form. Here is a list of protocols (1), their number – from 1 to 10. To display more than 10 protocols, you can add several widgets to the dashboard. For example, you can make several thematic widgets – on messengers and social networks, streams, etc., with up to 10 protocols in each.

You can add (2) or remove (3) all the protocols that are in the standard dictionary. For each protocol, you can adjust traffic delta score (4) (from 0 to 2 points will be added depending on how much the traffic changes) and RTT score (5). This indicator is more important, so its setting is more flexible for services that can be very sensitive to changes in this indicator.

You can also set an importance category (6) for each of the protocols, which will add from 0 to 2 points to the final score if the sum of the traffic and median scores is greater than zero. Resources have different "sensitivities". It is important to avoid even small problems with sensitive resources. Each resource is assigned an importance category by the user:

- Category 1 — a very popular service, extremely sensitive to quality and connection interruptions.
- Category 2 — a niche, but well-known service, demanding quality.
- Category 3 — the service is just gaining popularity, and cannot guarantee the quality of the content itself, or the content is not critical.

The recommended values of the impact of traffic volume delta on the evaluation of the protocol (in %) and RTT indicators are determined by the developer and transmitted to the operator, which then adjusts them based on the characteristics of its network.



What to do in case of a problem

In case of timely detection and localization of problems, the provider can solve them:

- By switching to another uplink.
- By prioritizing the traffic (application of “emergency” policies).
- By triggering an uplink to report problems.

If the solution is not possible (the service has problems or the uplink cannot be changed), the technical support of the provider can save time in identifying problems and inform users in a timely manner.

RTT Description

Round-trip time, RTT is the time taken to send the signal, plus the time it takes to confirm that the signal was received. This delay time, therefore, consists of the signal transmission time between two points within the same flow.
The term **flow** in DPI refers to all network activity within the source/destination socket (source IP:port / destinationIP:port).
Since the entire flow between the client and server goes through DPI, RTT calculation is performed by DPI for two directions:

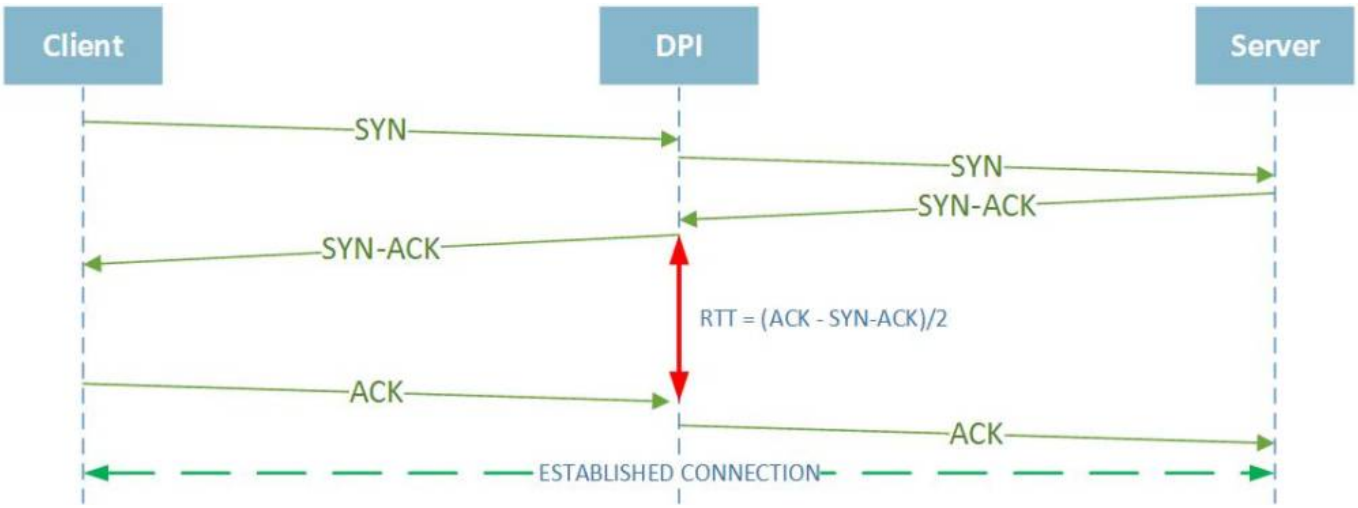
1. From subscriber to DPI (GUI has the following notation: **from subscriber**)
2. From server to DPI (GUI has the following notation: **from server**)

Registration of each new flow is performed by DPI on SYN/ACK received response basis instead of on SYN message sent from the initiator of the TCP connection, therefore, the RTT calculation is based on the difference between the transmission and reception of the following messages:

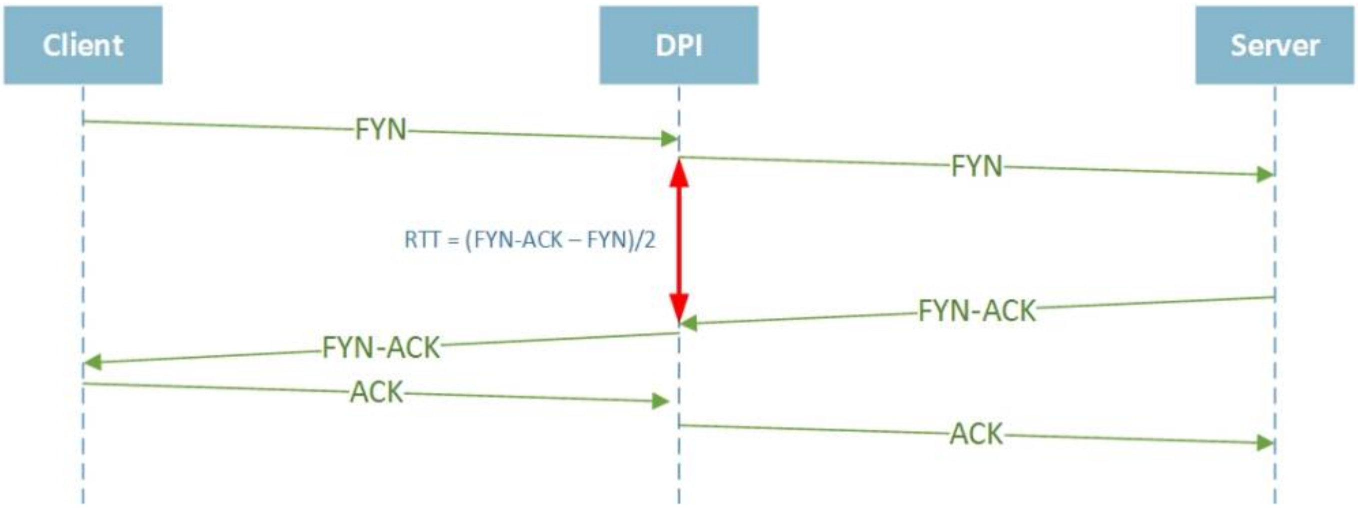
The client can be a server or the server can be a client depending on initiator of the TCP connection (TCP SYN). So the logic of RTT calculation also changes and calculation is done the other way around.

!!! It is important to know that RTT is only considered for session-oriented (TCP) connections. RTT calculation is not performed in case of UDP.

RTT from subscriber to DPI



RTT to subscriber - from server to DPI (in case the connection was closed at the initiative of the client)

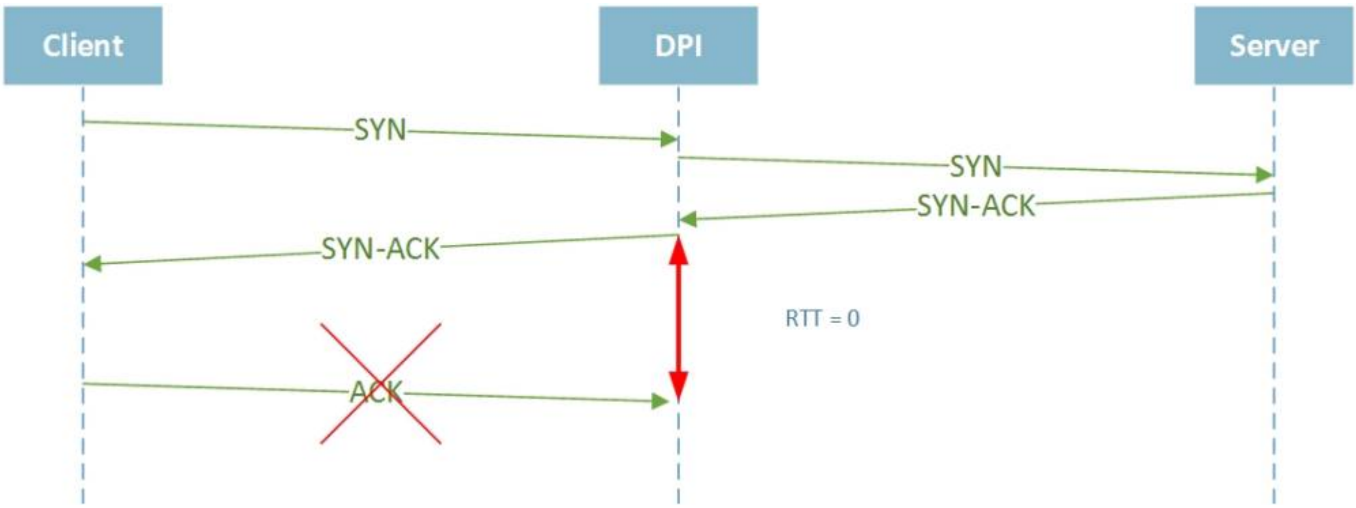


RTT to subscriber - from server to DPI (in case the connection was closed at the initiative of the server)

TCP protocol specificity and RTT calculation

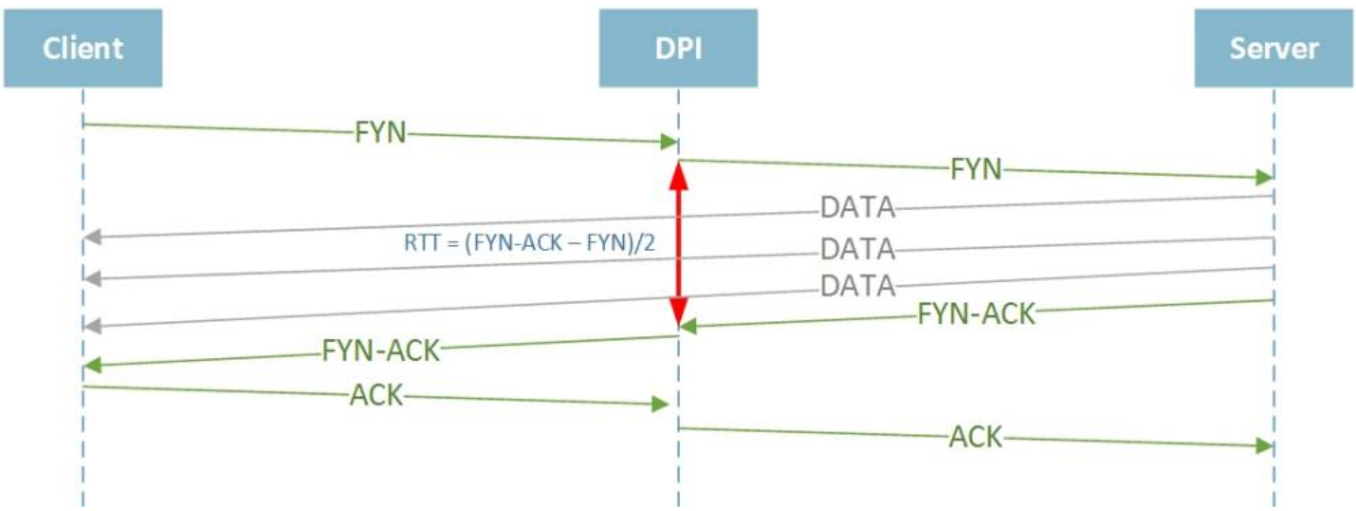
There are many different situations affecting the RTT calculation for a particular flow due to some TCP protocol features.

RTT from subscriber to DPI equals null for some flows



It corresponds the situation when DPI did not receive ACK sent from client to the DPI in response to received SYN/ACK. The situation can be caused by several reasons, for example, if the client physically disconnected the wire or sent RST. In all the situations mentioned above, the DPI will set “0” value in RTT from the client to the DPI for the given flow.

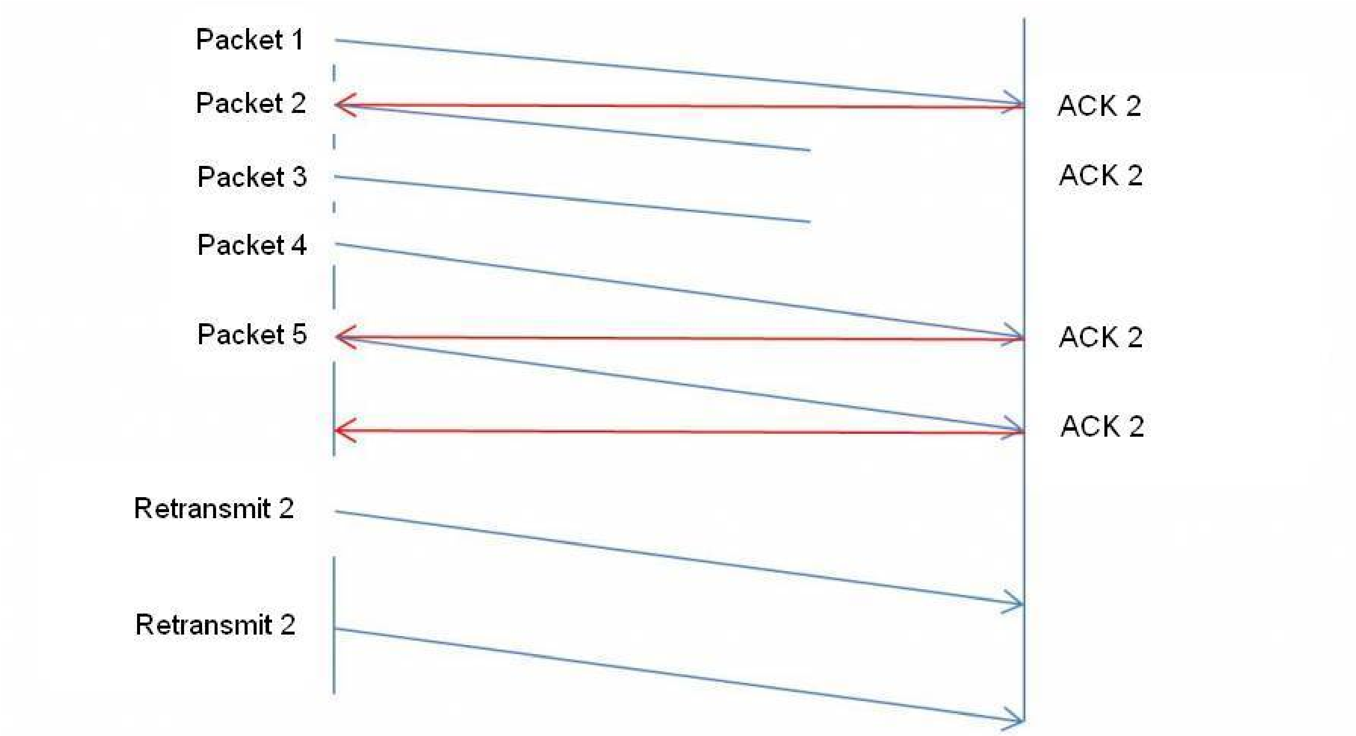
RTT for some flows take very large values (tens of seconds)



For example, this situation may occur in the case of TCP HALF CLOSED CONNECTION, i.e. when one of the connection participants terminates the data transmission, but still continues to receive the data from the remote side. In this case, the transmitting side can send FYN/ACK only after the data transfer is completed, so it will cause the significant increasing of RTT value.

Retransmits Description

1. Total retransmit percentage
2. The percentage of retransmissions when the traffic goes FROM subscriber
3. The percentage of retransmissions when the traffic goes TO subscriber



Retransmission types:

- **TCP Retransmission** is a classic type of packet retransmission. The packet sender having not received acknowledgment from the addressee after the retransmission timer expires, resends the packet automatically, assuming that it is lost along the route. The timer value is flexibly adjusted and depends on the circular transmission time over the network for a particular communication channel. RFC6298 (Computing TCP's Retransmission Timer) specifies the algorithm to calculate the timer.
- **TCP Fast Retransmission** corresponds for the following case: the sender resends the data immediately after assuming that the sent packets are lost without waiting for the expiration of the transmission timer. Usually it can be triggered by receiving several consecutive (usually three) duplicate acknowledgments with the same serial number. For example, the sender transmitted a packet with sequence number 1 and received an acknowledgment equal to sequence number plus 1, i.e. 2. The sender understands that the next packet with number two is expected. Suppose that the next two packets are lost and the recipient receives data with serial number 4. The recipient resends the acknowledgment with the number 2. Upon the receiving the packet with the number 5, the sender still sends the acknowledgment with the number 2. The sender sees three duplicate acknowledgments, assumes that the packets 2 and 3 were lost and resend them without waiting for a timer to expire.
- **Spurious Retransmission** is the type of retransmission appeared in the version 1.12 of Wireshark sniffer and means that the sender resends packets to which the recipient has already

sent acknowledgment.