Содержание

Аналитика Full NetFlow

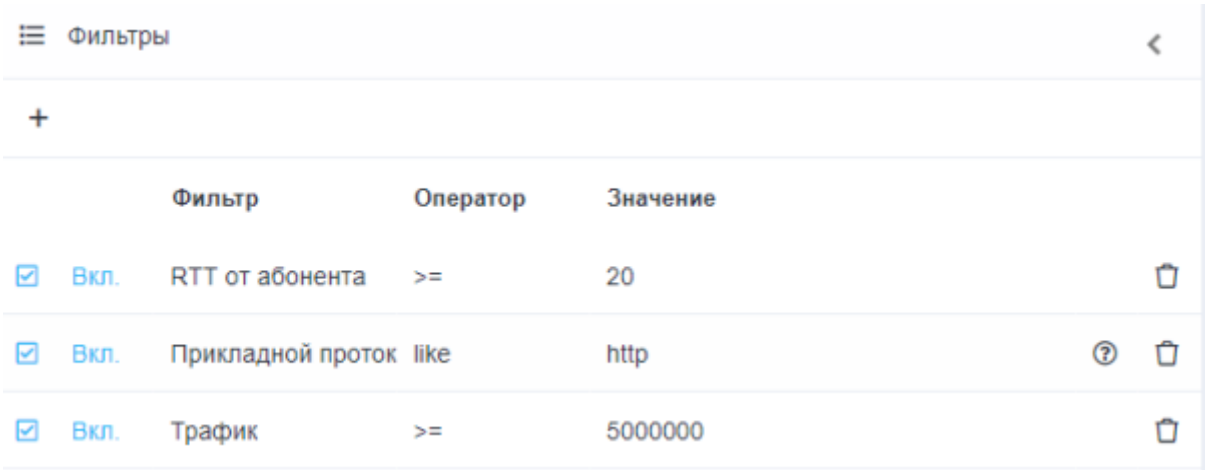
DPI выгружает информацию о всех сессиях клиентов в формате IPFIX (NetFlow v10).

1. Поиск ухудшения качества доступа к интернет

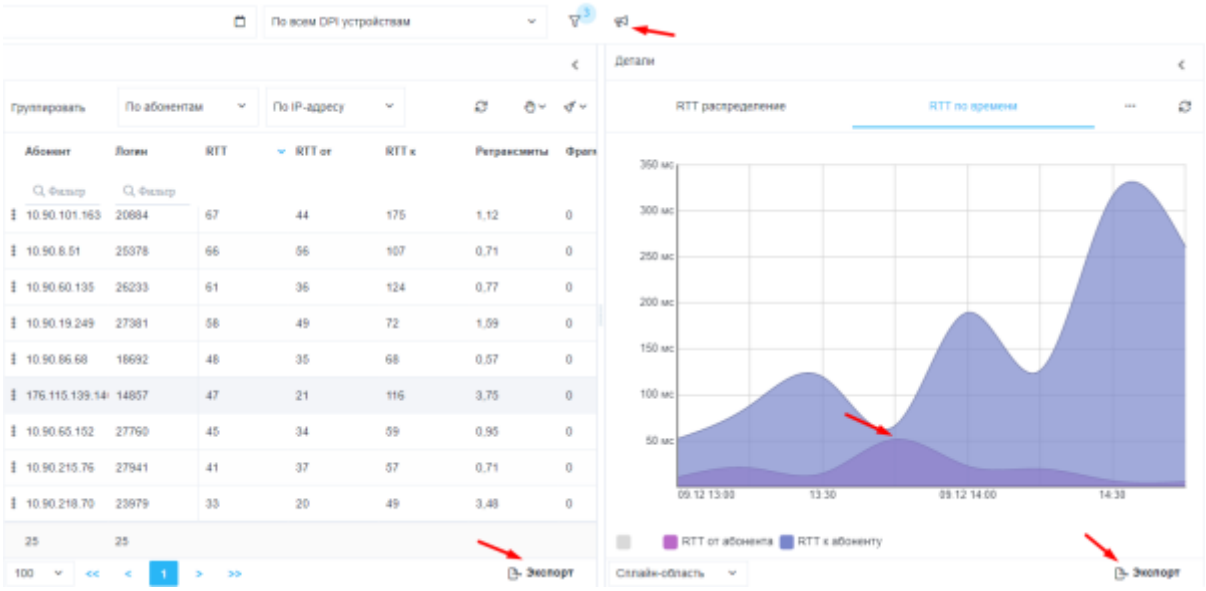
DPI выгружает информацию о задержках между клиентом и DPI и между DPI и хостом во время установления TCP соединения - RTT. В статистике фиксируется задержка в рамках каждого протокола с привязкой к UserAgent (берется из ClickStream), что дает возможность отследить работу конкретного устройства.
Необходимые действия для поиска:

1. перейти в раздел QoE Аналитика - > Абоненты - > Нетфлоу
2. создать фильтр, где

- предлагается ограничить поиск по протоколу http/https, чтобы отсеять возможные особенности других протоколов при установке TCP соединения
- указать среднюю скорость, чтобы делать выборку из абонентов, активно пользующихся интернет
- указать нижний порог RTT от клиента



Интерпретация полученной статистики:



- Фильтр вывел 25 потенциальных клиентов, у которых могут быть проблемы с доступом.
- Подробнее с задержками по времени, которые у них фиксируются, можно ознакомиться в окне **"Детали"**.
- Используя рупор, можно перенести их в маркетинговую кампанию и провести уведомление или опрос через браузер по удовлетворенности услугами.
- Возможна выгрузка отчета в удобном формате.

2. Сервис "Мониторинг аплинков"

Термины и определения

Аплинк (Uplink, восходящая линия) — это канал связи от оператора к вышестоящему и/или магистральному оператору, откуда оператор берет интернет.
RTT (Round-Trip Time, время приема-передачи) — это время, затраченное на отправку сигнала, плюс время, которое требуется для подтверждения, что сигнал был получен. Это время задержки, следовательно, состоит из времени передачи сигнала между двумя точками.

Назначение

Сервис "Мониторинг аплинков" позволяет без специальных экспертных знаний онлайн выявлять проблемы с доступностью сервиса у пользователей, которые могут возникнуть из-за канала между провайдером и интернет-ресурсом:

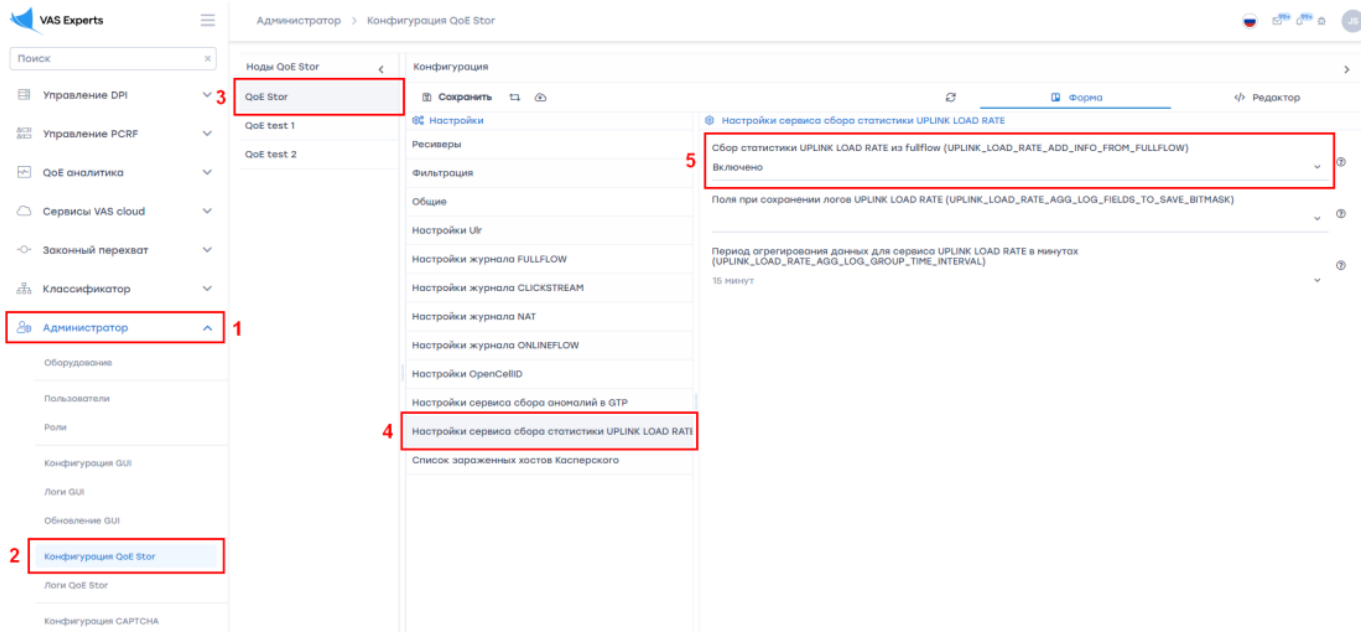
- Проблемы или загруженность вышестоящего оператора (аплинка).
- Медленная работа или недоступность самого сервиса.

Начало работы

Перед началом работы необходимо включить возможность сбора статистики. Для этого нажать на иконку ☰ в левом верхнем углу экрана и

1. Выбрать в открывшемся меню пункт *Администратор*
2. Выбрать пункт *Конфигурация QoE Stor*
3. *QoE Stor*
4. *Настройки сервиса сбора статистики UPLINK LOAD RATE*
5. В пункте *Сбор статистики UPLINK LOAD RATE* выбрать *Включено*

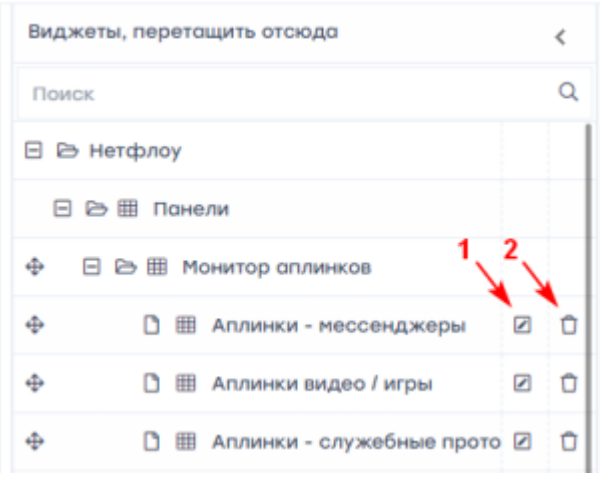
После выполненных действий нажать кнопку *Сохранить* в верхней части экрана.



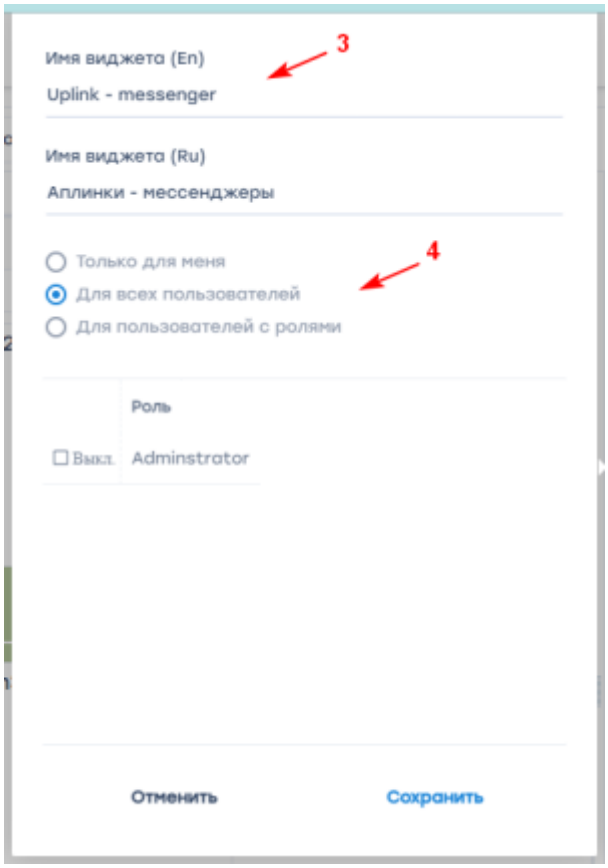
Внешний вид

Сервис располагается в *QoE аналитика → QoE дашборд.* Чтобы добраться до виджета для мониторинга аплинков, в боковой панели с виджетами необходимо выбрать *Нетфлоу → Панели → Мониторинг аплинков* и перетащить виджет на дашборд.

На боковой панели можно настроить (1) и удалить (2) каждый виджет.



В окне настройки виджета (1) можно изменить имя виджета на английском и русском языках (3) и его видимость (4).



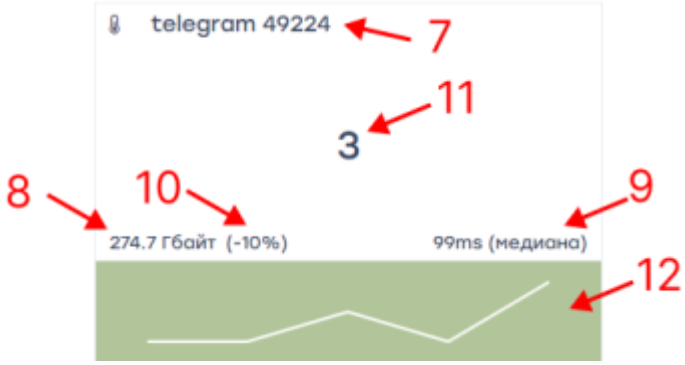
В верхней части экрана можно выбрать, за какой период будет отображаться трафик (5), выбрать источник данных (6).

Для каждого протокола в его плитке отображается:

- **Наименование** протокола (7)
- **Объем** трафика на выбранный период (8)
- **Медиана** по RTT к абоненту, ms (9)
- **Дельта** трафика, % (10). Это разница между трафиком за выбранный период времени и трафиком из статистики, который обычно бывает за аналогичный период в тот же день недели
- Общая **оценка** здоровья сервиса (11):

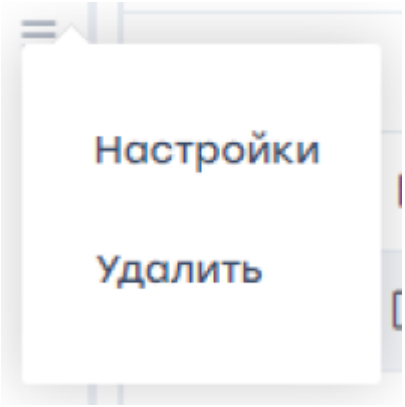
1. 0-3 балла — хорошо, кривая зеленого цвета
2. 4-7 баллов — удовлетворительно, кривая желтого цвета
3. 8-10 баллов — плохо, кривая красного цвета

- **Кривая** изменения оценки здоровья протокола (12). Кривая показывает, сколько раз менялась оценка протокола на выбранный период времени и не было ли плохих оценок.



Настройка протоколов в виджете

При наведении на виджет в его верхнем правом углу появится значок ☰. Нажав на него, можно перейти в настройки, либо удалить виджет.



При нажатии на пункт *Настройки* откроется форма настройки. Здесь представлен список протоколов (1), их количество — от 1 до 10. Чтобы отображать больше 10 протоколов, можно добавить на дашборд несколько виджетов. Например, можно сделать несколько тематических виджетов — на мессенджеры и соцсети, стримы и прочее, в каждом до 10 протоколов.

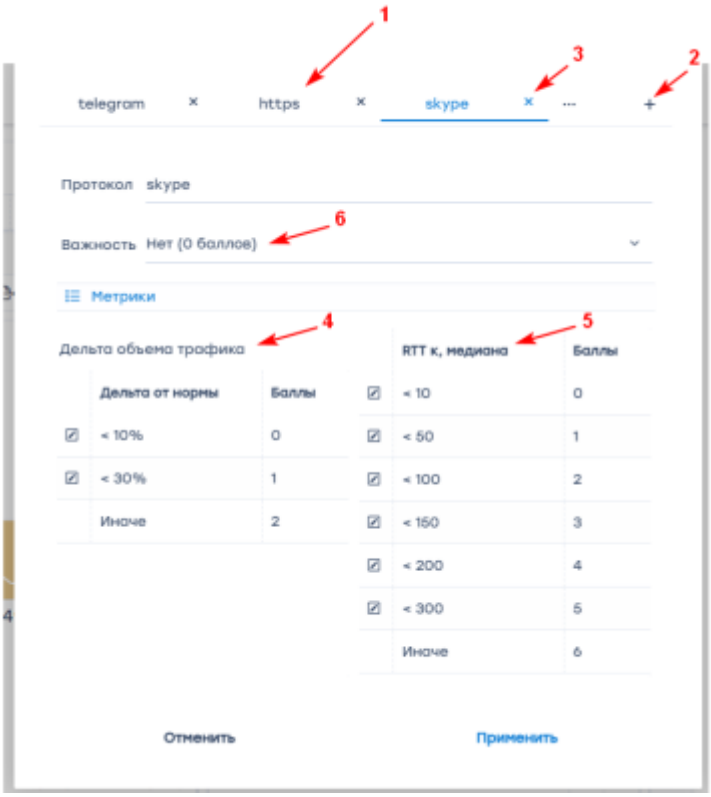
Добавлять (2) или удалять (3) можно все протоколы, которые есть в стандартном словаре. Для каждого протокола можно настроить оценки по дельте объема трафика (4) (в зависимости от того, насколько трафик изменится, будет добавлено от 0 до 2 баллов) и по показателю RTT (5). Данный показатель более важный, поэтому настройка более гибкая для сервисов, которые могут быть очень чувствительны к изменению этого показателя.

Также для каждого из протоколов можно задать категорию важности (6), которая будет добавлять от 0 до 2 баллов к итоговой оценке в случае, если сумма по оценкам трафика и медиане будет больше нуля. Ресурсы имеют разную "чувствительность". Важно не допускать даже небольших проблем с чувствительными ресурсами. Каждому ресурсу пользователем присваивается категория важности:

- Категория 1 — очень популярный сервис, крайне чувствительный к качеству и разрывам связи.
- Категория 2 — нишевый, но известный сервис, требовательный к качеству.
- Категория 3 — сервис только начинает набирать популярность, но сам не может гарантировать качества контента или контент не критически важный.

Рекомендованные значения влияния дельты объема трафика на оценку протокола (в %) и

показателей RTT определяются разработчиком и передаются оператору, который далее настраивает их исходя из особенностей своей сети.



Что делать в случае проблемы

В случае своевременного выявления и локализации проблем провайдер может решить их:

- Переключением на другой аплинк.
- Приоритизацией трафика (применением "аварийных" политик).
- Инициированием обращения к аплинку о проблемах.

Если решение невозможно (проблемы у сервиса или аплинк невозможно поменять), техническая поддержка провайдера сможет экономить время на выявлении проблем и своевременно информировать пользователей.

Описание RTT

Время приема-передачи (англ. round-trip time, RTT) — это время, затраченное на отправку сигнала, плюс время, которое требуется для подтверждения, что сигнал был получен. Это время задержки, следовательно, состоит из времени передачи сигнала между двумя точками в пределах одного flow.
За flow в DPI принимается вся сетевая активность в рамках source/destination socket (source IP:port /destination IP:port).
Так как весь flow между клиентом и сервером проходит через DPI, подсчет RTT на DPI производится для двух направлений:

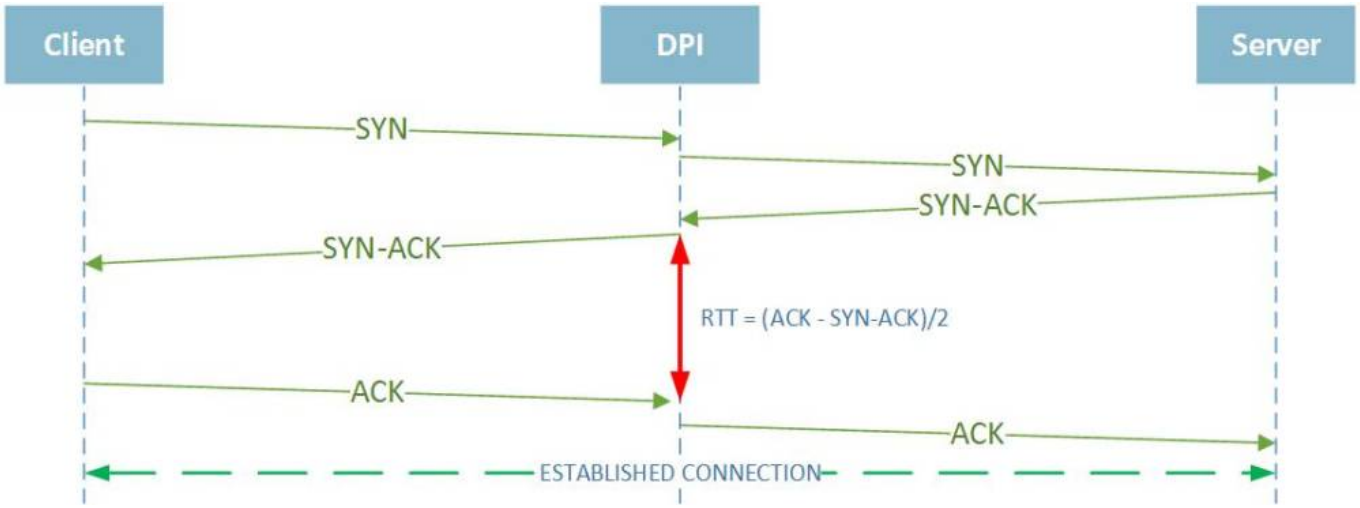
1. От клиента до DPI (обозначение в GUI **от абонента**)
2. От сервера до DPI (обозначение в GUI **к абоненту**)

Регистрация каждого нового flow на DPI производится не по сообщению SYN от инициатора TCP соединения, а при получении ответа SYN/ACK, поэтому подсчет RTT производится исходя из разницы передачи и приема последующих сообщений:

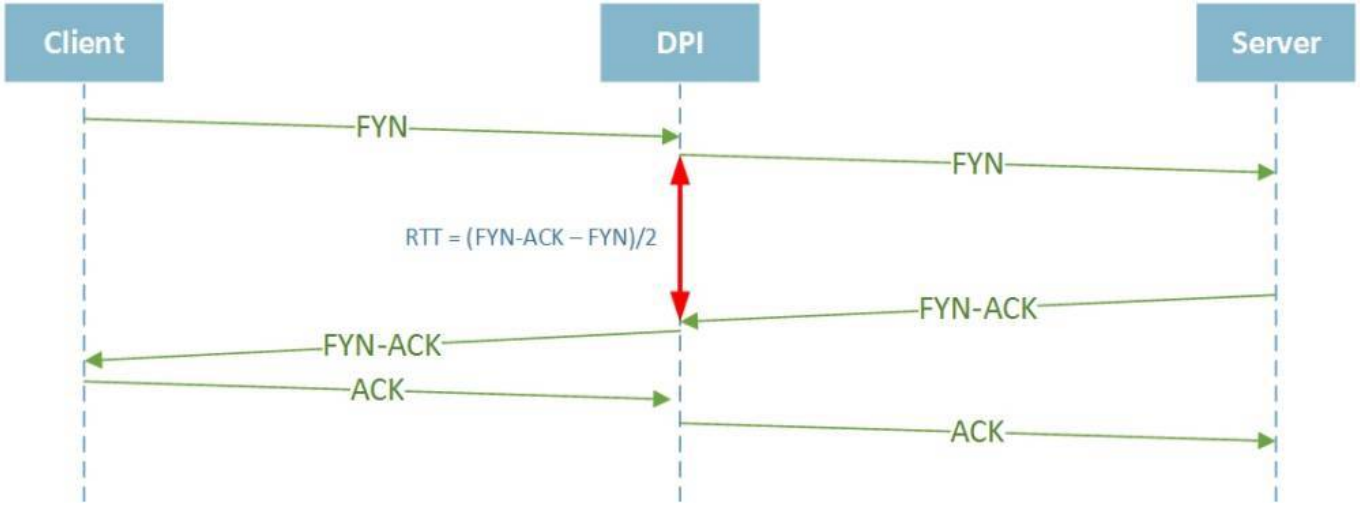
Клиент может являться сервером, а сервер - клиентом, в зависимости от того, кто инициализирует TCP соединение (TCP SYN). Соответственно, логика подсчета RTT тогда тоже меняется, и подсчет ведется наоборот.

!!! Важно понимать, что RTT считается только для session-oriented (TCP) соединений. Для UDP подсчет RTT не производится.

RTT от абонента до DPI



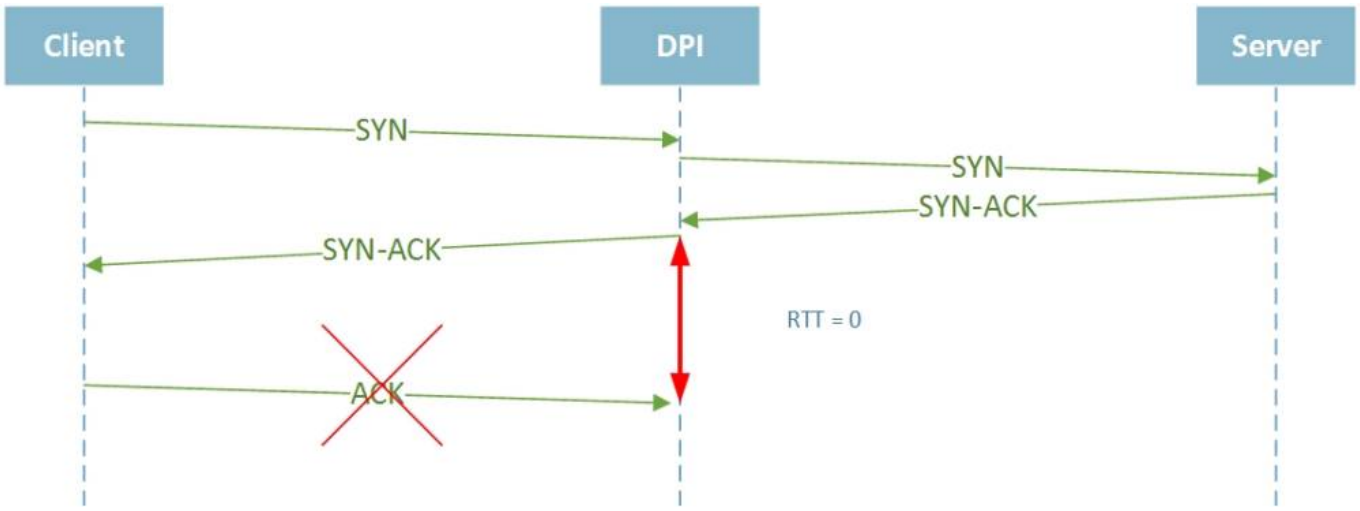
RTT к абоненту - от сервера до DPI (в случае если завершение было инициировано со стороны клиента)



Особенности протокола TCP и расчет RTT

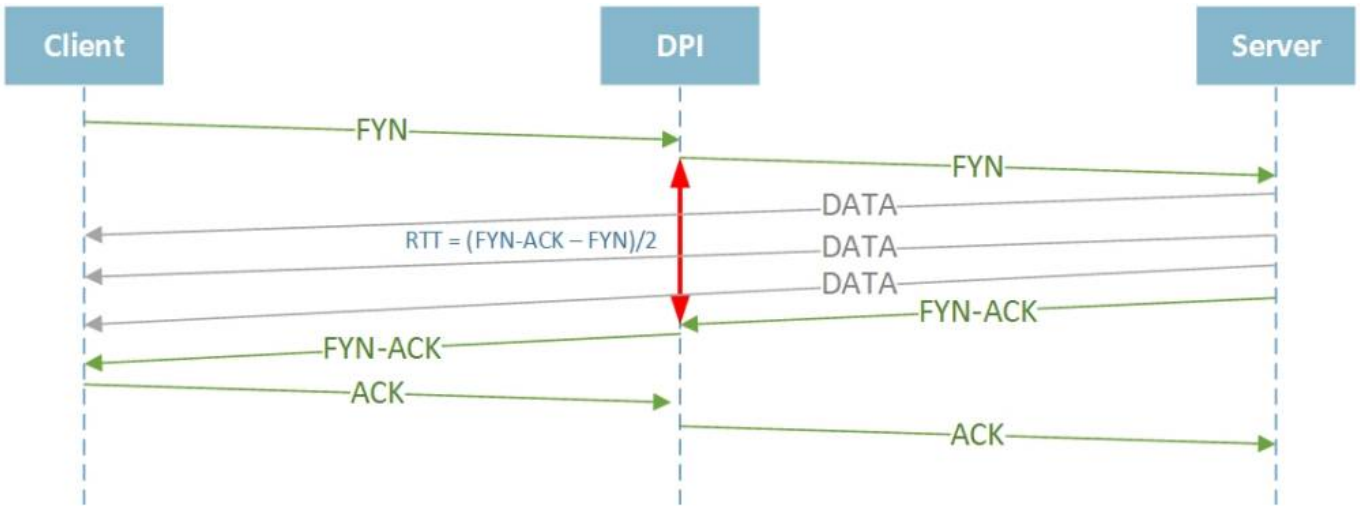
В виду особенностей протокола TCP, возможно множество различных ситуаций, влияющих на подсчет RTT для конкретного flow.

RTT от клиента до DPI для некоторых flow равен нулю



В случае, если DPI не получил ACK от клиента на отправленный SYN/ACK. Подобная ситуация может случиться по нескольким причинам, например, клиент разорвал соединение физически, либо прислал RST. Во всех подобных ситуация, DPI проставит значение “0” в RTT от клиента до DPI для данного flow.

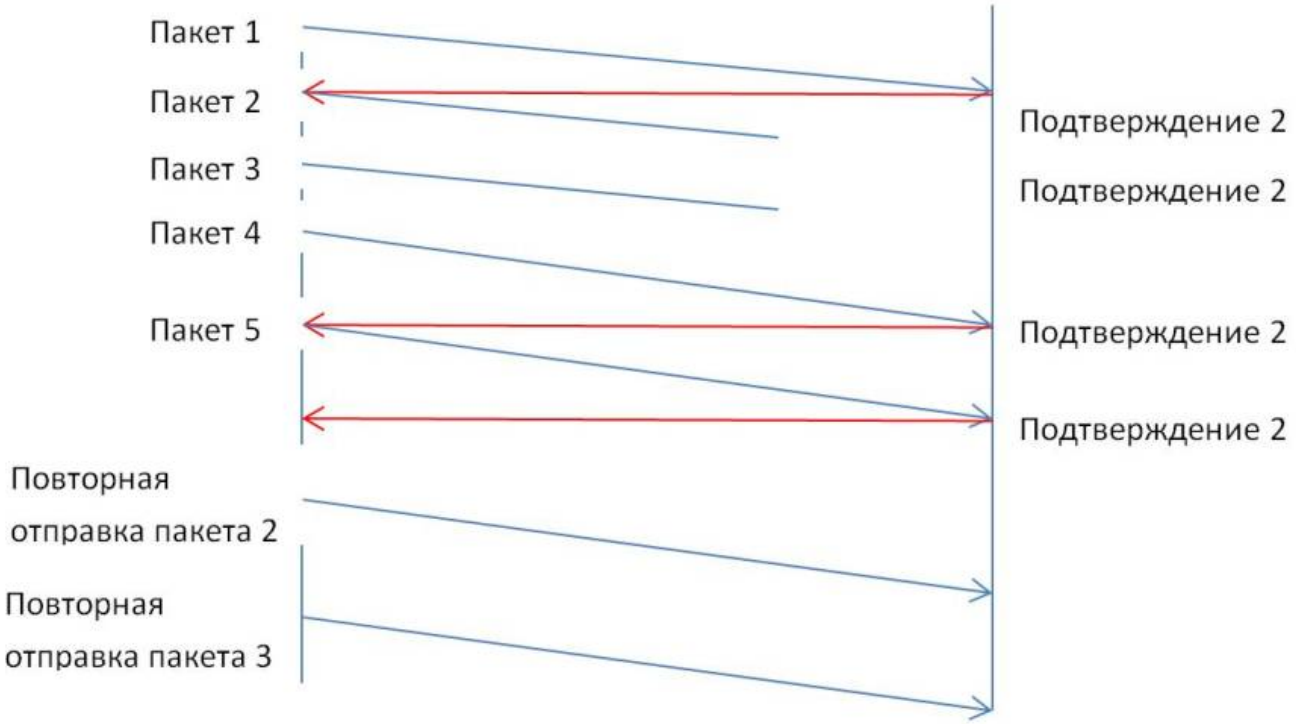
RTT для некоторых flow принимают очень большие значения (десятки секунд)



Например, такая ситуация может возникнуть в случае TCP HALF CLOSED CONNECTION (наполовину закрытый TCP), когда один из участников соединения прекращает передачу данных, однако все еще может получать данные от удаленной стороны. В таком случае, передающая сторона может послать FYN/ACK только после завершения передачи данных, в следствии чего, значение RTT значительно возрастет.

Описание ретрансмитов

1. Общий процент ретрансмитов
2. Процент ретрансмитов, когда трафик от абонета
3. Процент ретрансмитов, когда трафик к абонету



Виды перезапросов:

- TCP Retransmission – классический тип повторной передачи пакетов. Отправитель пакета, не получив подтверждения получения от адресата по истечении таймера retransmission timer, отправляет пакет повторно автоматически, предполагая, что он потерян по пути следования. Значение таймера подстраивается гибко и зависит от кругового времени передачи по сети для конкретного канал связи. Как он рассчитывается можно узнать в RFC6298 Computing TCP's Retransmission Timer.
- TCP Fast Retransmission – отправитель отправляет повторно данные немедленно после предположения, что отправленные пакеты потеряны, не дожидаясь истечения времени по таймеру (ransmission timer). Обычно триггером для этого является получение нескольких подряд (обычно три) дублированных подтверждений получения с одним и тем же порядковым номером.Например, отправитель передал пакет с порядковым номером 1 и получил подтверждение – порядковый номер плюс 1, т.е. 2. Отправитель понимает, что от него ждут следующий пакет с номером два. Предположим, что следующие два пакета потерялись и получатель получает данные с порядковым номером 4. Получатель повторно отправляет подтверждение с номером 2. Получив пакет с номером 5, отправитель все равно отправляет подтверждение с номером 2. Отправитель видит три дублированных подтверждения, предполагает, что пакеты 2, 3 были потеряны и шлет их заново, не дожидаясь таймера.
- Spurious Retransmission – этот тип повторной передачи появился в версии 1.12 сниффера Wireshark и означает, что отправитель повторно отправляет пакеты, на которые получатель уже отправил подтверждение.