Правильное использование Fast Path и FastTrack в Mikrotik

interface31.ru/tech_it/2021/09/pravilnoe-ispolzovanie-fast-path-i-fasttrack-v-mikrotik.html

С самого основания данного ресурса мы не перестаем придерживаться мнения, что практика всегда должна опираться на необходимый теоретический минимум, давая в своих статьях порой обширные теоретические отступления. Без теории практика превращается в подобие шаманских камланий с бубном, когда вроде сделал все тоже самое, но ничего не работает. В этом плане технология FastTrack в Mikrotik, несмотря на всю свою простоту, держит пальму первенства по количеству возникающих с ней проблем, которые, в большинстве своем, возникают именно от незнания и непонимания работы этой технологии.

Что такое Fast Path

Основной проблемой роутеров Mikrotik, особенно недорогих моделей, является достаточно слабая вычислительная мощность процессора, являющаяся сдерживающим фактором для реализации многих сложных сетевых сценариев. Причина этого кроется в достаточно сложном процессе обработки трафика роутером, в чем можно убедиться подробно изучив диаграммы Packet Flow, показывающие порядок прохождения пакетов через устройство. Если вы собираетесь серьезно работать с устройствами Mikrotik, то данный раздел документации рекомендуется знать хотя бы на твердую четверку, так как именно здесь находятся ответы на многочисленные вопросы типа: "я все сделал по инструкции, но ничего не работает" или "работает, но как-то не так".

Более подробное рассмотрение данного вопроса выходит за рамки нашей статьи, поэтому вернемся к нагрузке на процессор. Очевидно, что причина этого - сложный путь обработки трафика, который полностью ложится на плечи CPU. Можно ли этого как-либо избежать? Можно, в RouterOS v6 для этого появилась новая технология - **Fast Path** (*быстрый путь*), которая позволяет направить трафик по быстрому пути, без обработки ядром ОС, что позволяет существенно снизить нагрузку на систему.

Основная мысль, положенная в основу этой технологии такова, что пакеты уже установленных соединений, а также тех участков передачи трафика, где не требуется фильтрация и контроль, можно отправить по быстрому пути, тем самым разгружая процессор и ускоряя передачу данных. Fast Path - это расширение драйвера интерфейса, которое позволяет ему напрямую взаимодействовать с некоторыми подсистемами RouterOS и пропускать остальные.

В настоящий момент Fast Path можно использовать для:

- Трафика IPv4
- Транзитного трафика IPv4 (FastTrack)
- Traffic Generator
- MPLS
- Мосты (Bridge)

Однако использование данной технологии имеет ряд ограничений, так для IPv4 FastPath требуется среди прочего:

- Отсутствие правил брандмауэра
- Отсутствие списков адресов
- Отсутствие политик IPsec
- Отсутствие очередей
- Отсутствие отслеживания соединений

Для мостов требуется:

- Отсутствие правил брандмауэра
- Отсутствие фильтрации VLAN

Это не полный список, с полным списком ограничений вы можете ознакомиться в официальной документации. Но уже этого достаточно, чтобы понять, с Fast Path не все так просто и за производительность приходится расплачиваться возможностями. Если мы хотим использовать быстрый путь, то нам следует отказаться практически от любого контроля и фильтрации трафика.

Также помним, что Fast Path - это расширение драйвера интерфейса и оно может поддерживаться не для всех портов и типов интерфейсов. Так в современных моделях серии RB9xx и RB2011/3011/4011 Fast Path поддерживается для всех портов, а вот более старые модели могут иметь ограничения, поэтому советуем снова обратиться к документации. Также Fast Path можно использовать для PPPoE, L2TP, IP-IP, GRE и EoIP, мостов, VLAN и беспроводных интерфейсов.

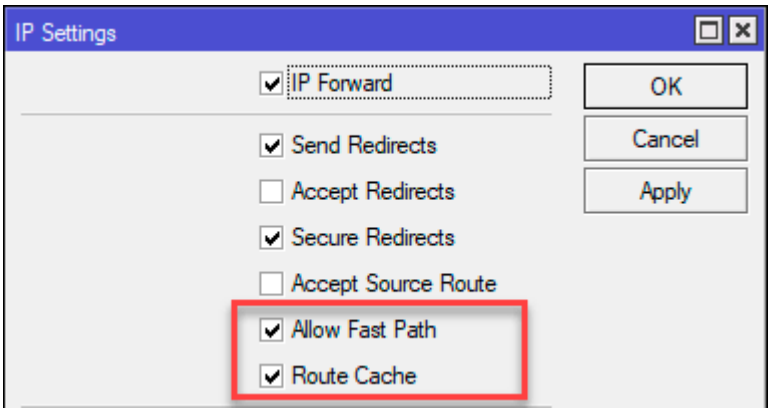
При этом может возникнуть ситуация, когда один из интерфейсов поддерживает Fast Path, а другой нет. В этом случае возможны два варианта: если **входящий интерфейс** поддерживает Fast Path, то часть пути (насколько это возможно) пакеты пройдут через него, а затем перейдут на Slow Path (**медленный путь**) с полной

обработкой трафика на CPU. Если интерфейс входа не поддерживает Fast Path, то трафик проделает весь путь по Slow Path, вне зависимости от того, поддерживает Fast Path интерфейс выхода или нет.

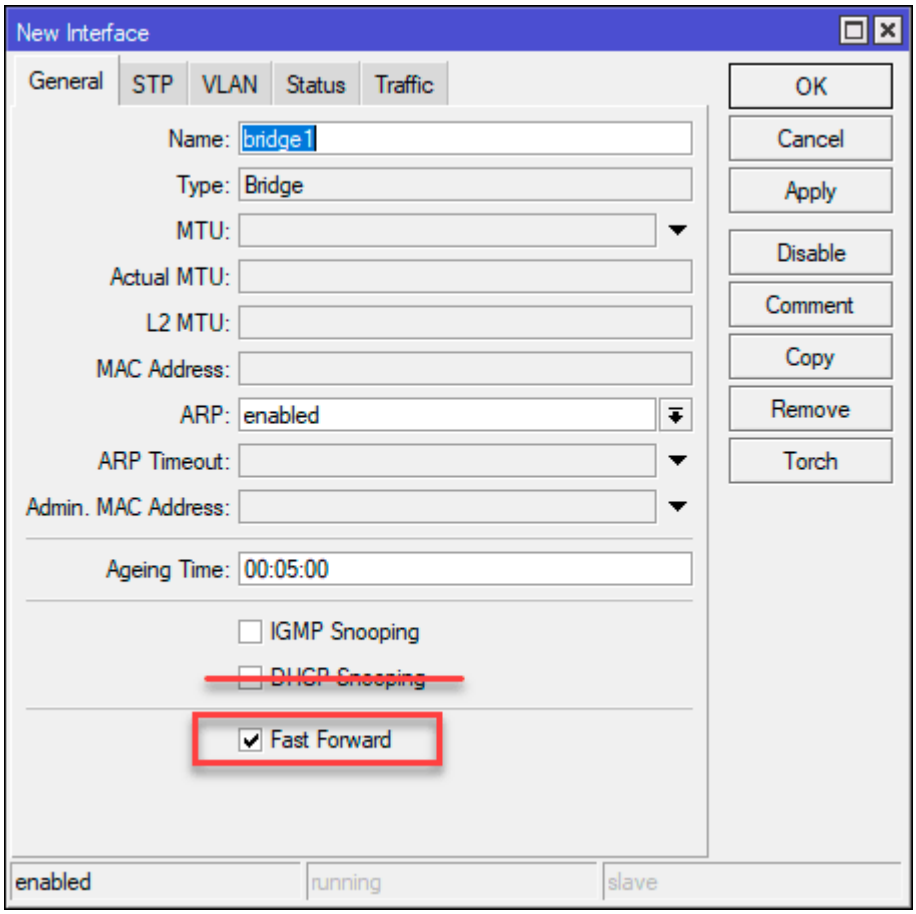
Еще один важный момент: Fast Path можно использовать **только для IPv4 TCP или UDP соединений**. Однако в правилах нет необходимости указывать протокол, для всего неподдерживаемого трафика Fast Path будет игнорироваться.

Практическое применение Fast Path

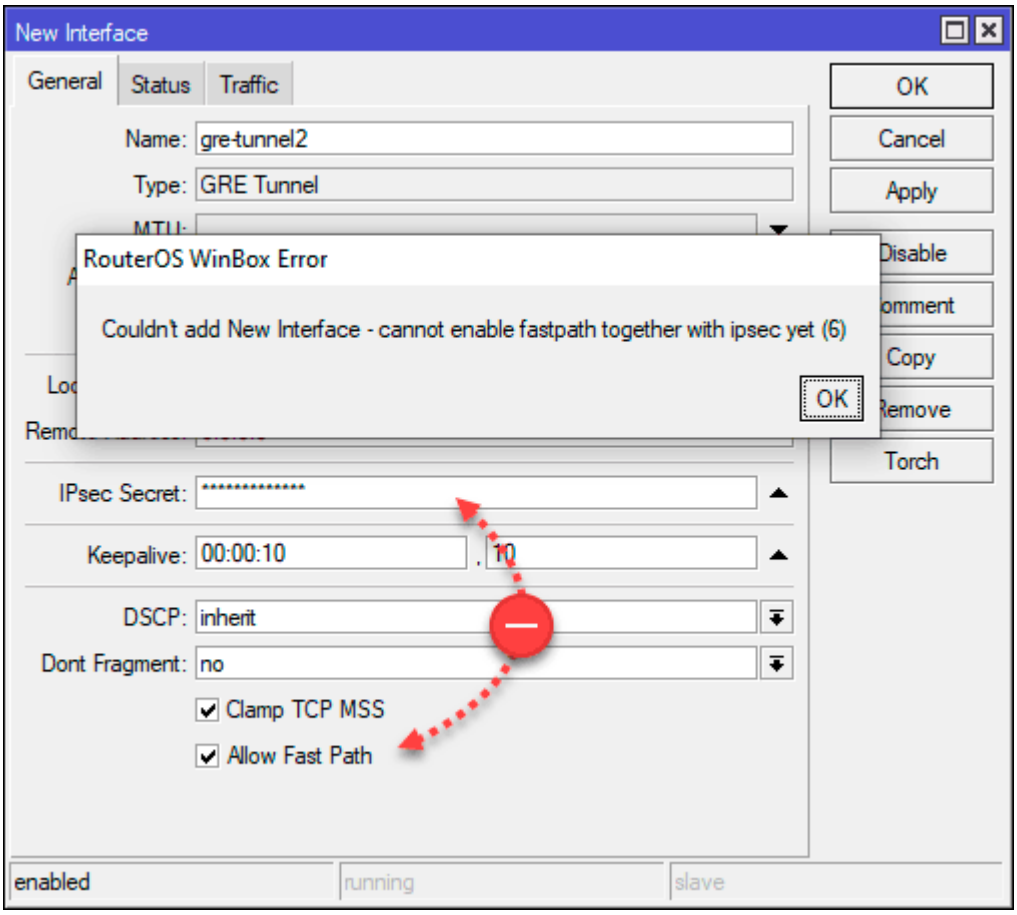
Прежде всего перейдем в **IP - Settings** и убедимся, что флаги **Allow Fast Path** и **Route Cache** установлены. В современных моделях это настройки по умолчанию, поэтому данная рекомендация носит чисто академический характер. В данной конфигурации IPv4 TCP и UDP-трафик, удовлетворяющий перечисленным выше условиям, будет автоматически отправлен по быстрому пути.



Для мостов по умолчанию активируется опция **Fast Forward**, включающая для передаваемых пакетов быстрый путь, но при этом помним, что **DHCP-snooping** не должен быть включен, а также отсутствовать любая фильтрация трафика или VLAN внутри моста.

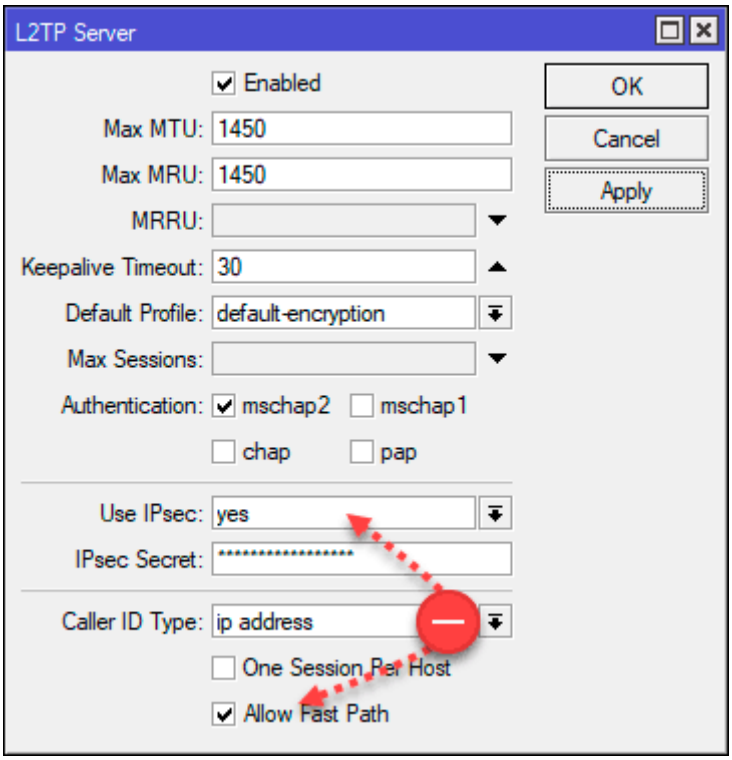


А вот дальше уже становится интереснее. Туннельные соединения и L2TP поддерживают Fast Path, но это лишает нас возможности использовать IPsec, поэтому от Fast Path для данных видов соединений придется отказаться. Тем более что система не даст нам создать интерфейс, сочетающий Fast Path и IPsec.



Правда для L2TP-соединений вы можете одновременно установить обе опции, но при включённом IPsec Fast Path будет игнорироваться. Тем не менее мы категорически не рекомендуем использовать такие неоднозначные варианты настройки, потому как при обновлении RouterOS поведение системы может измениться, что способно привести к неожиданным и непредсказуемым результатам.

Коротко подведем итоги. RouterOS по умолчанию сама будет использовать Fast Path там, где это возможно, наша задача - понимать, что влияет на возможность использования данной технологии и делать правильный выбор между Fast Path или возможностями дополнительного контроля и защиты трафика.



Практическое использование Fasttrack

Fasttrack можно без преувеличения назвать самой неправильно настраиваемой опцией. Если выполнить поиск в сети интернет, то можно увидеть множество материалов про то, как решить те или иные проблемы с Fasttrack. Но большинство этих проблем также связаны с непониманием работы данной технологии. Давайте разберемся, что же такое Fasttrack, это сочетание Fast Path + Connection Tracking, проще говоря мы можем отправить все уже установленные и связанные с ними соединения по быстрому пути.

При этом нам окажутся недоступны брандмауэр, очереди, IPsec и многое другое. По сути, пакеты, попадающие в Fasttrack проскакивают роутер без обработки, что значительно снижает нагрузку на процессор, но лишает нас возможности гибко управлять трафиком. Насколько это оправдано? Нужно смотреть по задачам, скажем если это выход внутренних устройств в интернет, то Fasttrack тут вполне к месту, позволяя существенно разгрузить роутер. Насколько это безопасно? Безопасность в данном случае не пострадает, так как по быстрому пути идут уже установленные соединения, новый пакет обязательно пройдет по медленному пути с полной обработкой брандмауэром.

Для включения Fasttrack перейдем в **IP - Firewall - Filter Rules** и добавим следующее правило: **Chain - forward, Connection State: established, related**, на закладке **Action** установим действие **fasttrack connection**. Это отправит все установленные и связанные соединения по короткому пути, но лишит нас возможности обработки и контроля такого трафика.

Еще один важный момент, вы обязательно должны указать **Connection State** для этого правила, если вы этого не сделаете, то получите огромную дыру в безопасности, так как мимо брандмауэра по короткому пути пойдут все пакеты. Мы бы не стали заострять на этом внимание, но в нашей практике были случаи, когда администраторы включали Fasttrack для всего транзитного трафика.

Сразу после него добавим еще одно правило: **Chain - forward, Connection State: established, related**, на закладку **Action** можно не переходить, так как **accept** - действие по умолчанию. Для чего это нужно? Как мы помним, Fast Path работает только для TCP и UDP соединений, остальной трафик пойдет по этому правилу, кроме того, некоторая часть пакетов попадающих под действие Fasttrack направляется по медленному пути и без этого правила они бы были отброшены.

```
/ip firewall filter
add chain=forward action=fasttrack-connection connection-state=established,related
add chain=forward action=accept connection-state=established,related
```

Это самая простая реализация Fasttrack, которая приведена в большинстве инструкций, и она же вызывает большинство проблем. Почему так? Да потому, что приведенное выше правило отправляет по быстрому пути все установленные и связанные соединения, без учета их направления и назначения. При этом становятся недоступны фильтрация и маркировка трафика брандмауэром, очереди и политики IPsec. Стоит ли удивляться, что все завязанные на данные технологии настройки перестают работать.

Как быть? Нужно конкретизировать правила, основная наша цель - снизить нагрузку на устройство, поэтому мы хотим использовать Fasttrack для обычного интернет трафика, но исключим оттуда все остальные соединения. Поэтому вместо одного правила используем два:

```
add action=fasttrack-connection chain=forward connection-state=established,related
in-interface=bridge1 out-interface=ether10
add action=fasttrack-connection chain=forward connection-state=established,related
in-interface=ether10 out-interface=bridge1
```

Где **bridge1** - внутренний мост, а **ether10** - внешний интерфейс, смотрящий в интернет.

Что изменилось? Теперь по быстрому пути идут пакеты только из локальной сети в интернет и обратно. Все остальные соединения полноценно обрабатываются ядром RouterOS и могут полностью использовать все ее возможности.

Если направлений трафика, который мы хотим направить по быстрому пути несколько, скажем, несколько каналов в интернет, либо межсетевой трафик, то создаем для каждого направления свою пару правил, с указанием входящего и исходящего интерфейсов.

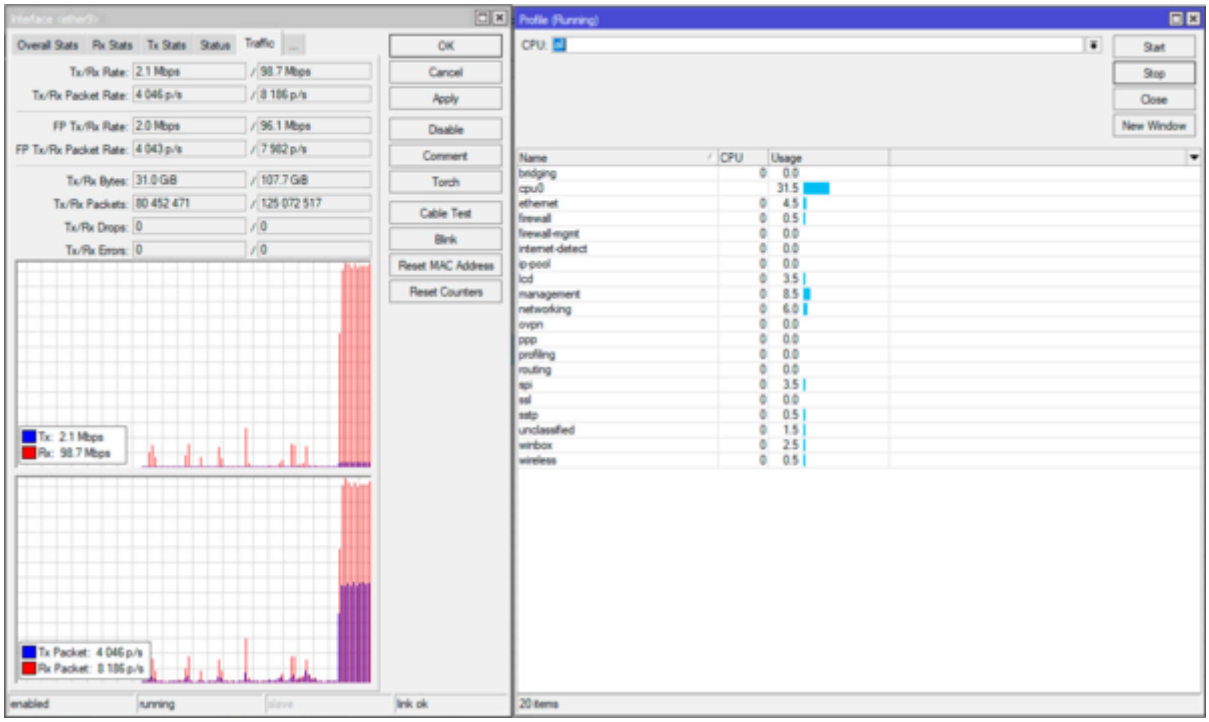
Для IPsec в самое начало цепочки forward (т.е. обязательно выше правил с fasttrack) следует добавить еще два правила:

```
/ip firewall filter
add action=accept chain=forward ipsec-policy=in,ipsec
add action=accept chain=forward ipsec-policy=out,ipsec
```

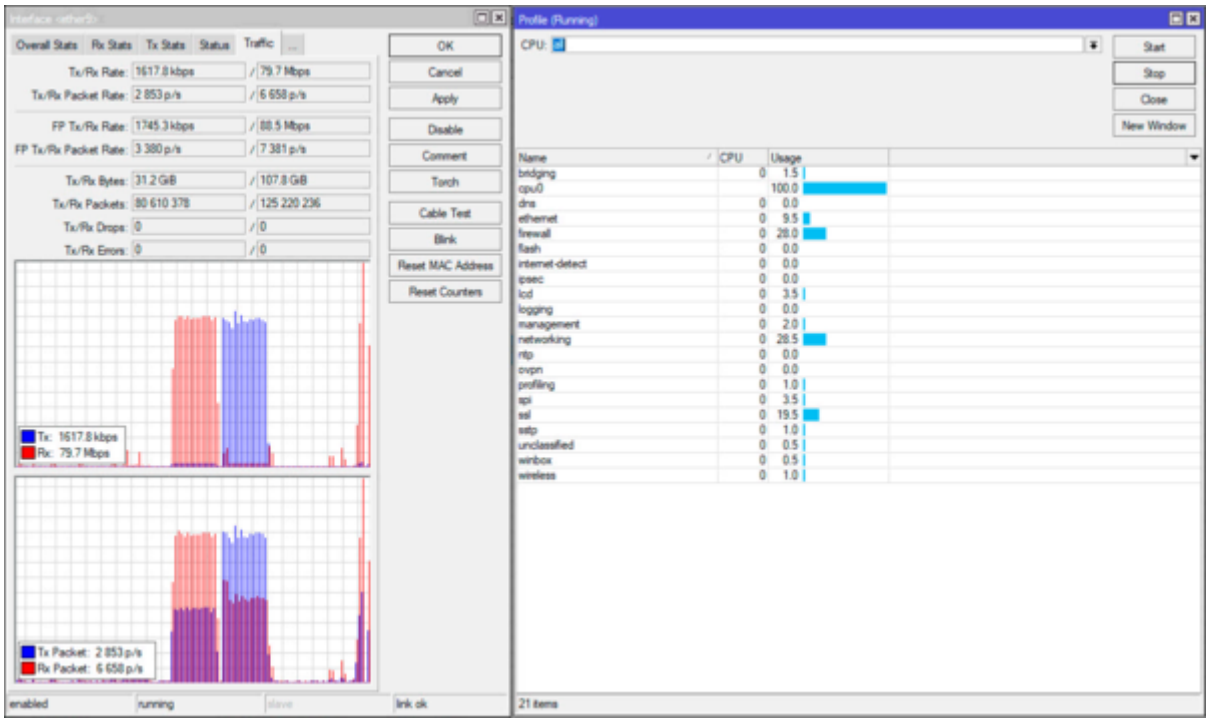
Важно! Обратите внимание, так как Fast Path - это расширение драйвера интерфейса, то и в качестве критериев в правилах мы должны использовать именно интерфейсы, что позволит максимально корректно обрабатывать потоки трафика и избежать логических ошибок.

Также обратите внимание, что Fasttrack применяется именно для **транзитных** соединений, не влияя на входящие и исходящие соединения самого роутера. Мы бы не заостряли на этом внимание, но в сети нам попадались инструкции, когда пакеты маркировались в цепочках INPUT и OUTPUT, а затем эти метки соединений пытались использовать в цепочке FORWARD, надо ли говорить, что подобные конструкции работать не будут.

Ну и логическое завершение нашей статьи - практическая польза от Fasttrack. Мы провели простой тест, запустили на одном из узлов сети **Speedtest от Ookla** используя для выхода в интернет RB2011. С включенным Fasttrack роутер прокачал все 100 Мбит/с тарифа при нагрузке на CPU в пределах 30-32%:



А теперь выключаем Fasttrack и видим, что роутер полностью лег, но при этом даже не смог прокачать тариф, упершись в планку 80 Мбит/с:



Становится очевидно, что Fast Path и FastTrack - важные технологии, позволяющие существенно увеличить производительность Mikrotik, но применять их следует обдуманно, учитывая все плюсы и минусы данного решения. Надеемся, что данная статья окажется вам полезна и вы теперь будете использовать все возможности Fast Path без каких-либо затруднений и будете понимать как именно это работает.

Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на углубленном курсе по администрированию MikroTik. Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.