Ограничиваем скорость на маршрутизаторе Cisco. Технология rate-limit

Иванов Михаил

Всем привет. Хочу поделиться своим опытом по настройке ограничений скорости на маршрутизаторах Cisco.
Итак, для начала немного расскажу о том, зачем это понадобилось. Скажем, построили мы небольшую Hub-and-Spoke сеть. Каналы связи у нас небольшие, например, 2 Мбит/с каждый. Сеть небольшого предприятия, которое со временем начинает разрастаться и трафик в этих каналах тоже увеличивается.
Пример из жизни. Есть центральный офис и несколько филиалов. Основной трафик — это ERP-системы и обновления софта. Каналы 2 Мбит/с не нагружены, все работает, всех устраивает. Тут в филиале появляется сервер видеонаблюдения, с которого идут видеопотоки на центральный офис, когда там служба безопасности просматривает камеры. При этом канал загружается под 100% и начинаются проблемы. То есть, необходимо весь трафик, идущий к видео серверу урезать.
Как это сделать. Сразу же приходят на ум два варианта:

- rate-limit
- traffic-shape

Чем эти два способа отличаются?
Traffic-shape работает только на выходных интерфейсах. Так же traffic-shape умеет работать с очередями. Rate-limit работает как на входных так и на выходных интерфейсах и режет все пакеты, что выходят за полосу, но можно устанавливать максимальное значение всплеска.

Rate-limit команда вводится в режиме конфигурирования физического интерфейса и имеет следующий синтаксис:

```
rate-limit input|output [access-group [rate-limit] acl-index] [limit-bps] [nbc] [ebc] conform-action [action] exceed-action [action]
```

Разберем более детально:

- access-group — указываем номер нашего ACL, в который ловим трафик, который будем ограничивать.

Далее идут три значения скорости limit bps, nbc, ebc

- limit bps — скорость ограничения(в битах!)
- nbc — допустимый предел трафика
- ebc — максимальный предел трафика

Для расчета всех значений используем такую формулу:

nbc=limit(bit/s)/8(bit/s)*1,5sec

ebc=2nbc

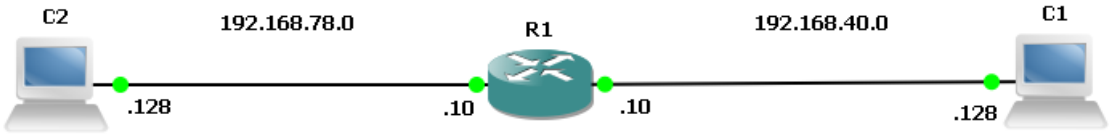
Или же используем готовый калькулятор .
Далее по синтаксису:

- conform-action — что делать с трафиком при соответствии ограничения
- exceed-action action — что делать с трафиком при превышении ограничения.

И тут есть несколько действий:

- drop — отбросить пакет
- transmit — передать пакет
- set-dscp-transmit — пометить пакет

Теперь давайте посмотрим на практике. Возьмем GNS3, один маршрутизатор и две виртуальные машины.



Топология простейшая, чтобы просто показать как это работает.

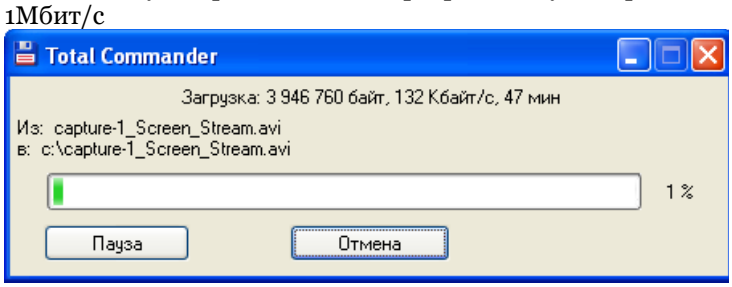
Ограничим весь трафик из сети 192.168.40.0/24 в сеть 192.168.78.0/24. Для этого на R1 создаем ACL.

- R1(config)#access-list 101 permit ip 192.168.40.0 0.0.0.255 192.168.78.0 0.0.0.255
- R1(config)#access-list 101 deny ip any any

Ограничиваем абсолютно весь трафик. Пример простой, могут быть более сложные ACL, чтоб ограничивать скорость по каким-то сервисам, портам и пр.

Проверим скорость в сети до ограничений.

На хосте C1 у нас работает FTP-сервер, C2 — будет ftp-клиентом. Скорость виртуальной сети у меня 1Мбит/с

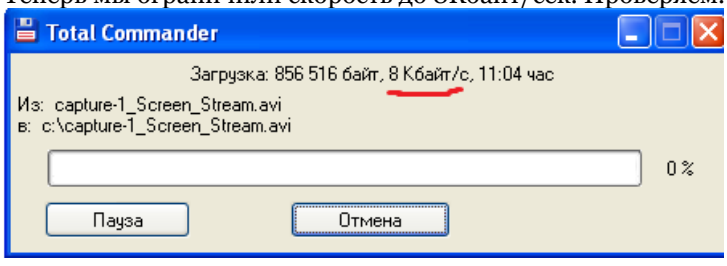


Видим что скорость закачки около 1Мбит/с.

После этого вешаем на физический интерфейс rate-limit, который смотрит в сеть 192.168.40.0/24

- R1(config)#int fa 0/0
- R1(config-if)#rate-limit output access-group 101 64000 12000 24000 conform-action transmit exceed-action drop

Теперь мы ограничили скорость до 8Кбайт/сек. Проверяем.



Скорость стала 64 Кбит/с. Все работает.

Благодарю за внимание.