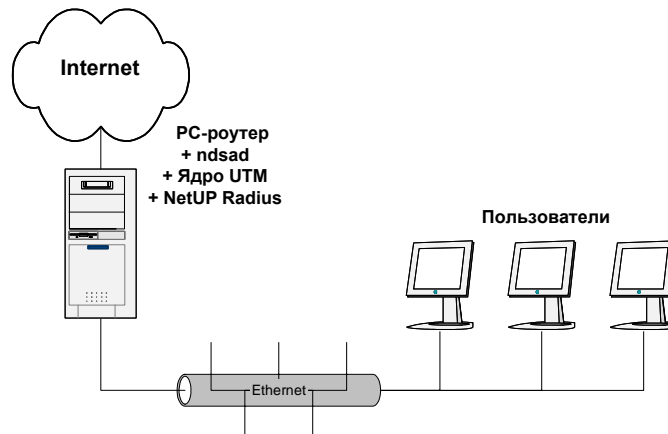


## Ограничение потоков трафика на PC-роутерах под управлением операционных систем Linux и FreeBSD, и использование шейпинга совместно с NetUP UTM.

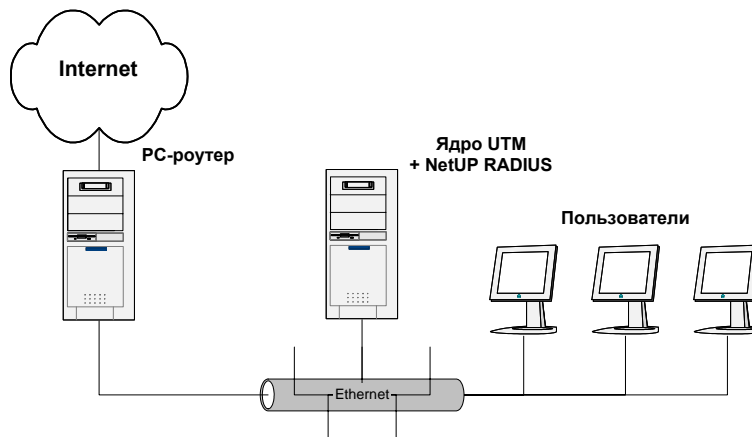
Ограничению пропускной способности канала ("шейпинг", от англ. "shaping" - придание формы, формирование) в ОС Linux посвящено довольно много литературы, но в большинстве своем она достаточно сложна для начинающего в этой области пользователя. В частности, сложность объясняется изобилием вариантов ограничения пропускной способности канала и трудностью выбора между этими вариантами.

Здесь будут описаны наиболее легковоспроизводимые варианты шейпинга, функциональности которых хватает в большинстве случаев.

Простейшим способом организации сети, при котором возможно шейпирование, является установка на PC-роутер пакетов роуптор (авторизует и создает виртуальное подключение), ndsadm (подсчитывает трафик), **NetUP Radius** (обеспечивает передачу запроса на авторизацию от роуптор к ядру **NetUP UTM** и передачу разрешения/запрета авторизации в обратном направлении), файерволла (вводит ограничение по скорости) и ядра биллинговой системы **NetUP UTM**:



При больших количествах клиентов и потоках трафика можно разгрузить PC-роутер, выделив ядро биллинговой системы **NetUP UTM** и **NetUP Radius** на отдельную машину, причем связь роутера с биллинговым сервером может осуществляться как через локальную сеть, так и через интернет:



## Настройка шейпинга на PC-роутере под управлением Linux и использование совместно с NetUP UTM.

Здесь будет рассмотрена схема, где биллинг и Radius-сервер установлены на роутере. Для организации шейпинга используется пакет iproute2, который есть в любом дистрибутиве Linux. Возможно, он уже установлен на вашем сервере, что можно проверить, набрав команду "tc" (именно эта команда будет использоваться далее):

```
server# tc
Usage: tc [ OPTIONS ] OBJECT { COMMAND | help }
where OBJECT := { qdisc | class | filter }
      OPTIONS := { -s[tatistics] | -d[etails] | -r[aw] | -b[atch] file }
server#
```

Для реализации шейпинга нужно создать очередь, класс и фильтр. Создание очереди:

```
tc qdisc add dev eth0 root handle 1: htb
```

Создание классов:

```
tc class add dev eth0 parent 1: classid 1:1 htb rate 100mbit ceil 100mbit burst 200k
tc class add dev eth0 parent 1:1 classid 1:10 htb rate 1mbit burst 20k
```

Здесь класс 1:1 задает общую скорость канала, класс 1:10 задает ограничение скорости в 1Мб/с. Чтобы задать величину скорости в килобитах, нужно использовать обозначение "kbit". Можно задать неограниченное количество классов с разной пропускной способностью. Для обеспечения гарантированной полосы пропускания для клиента рекомендуется следить за тем, чтобы суммарная скорость, описанная в классах, не превышала пропускной описанной в родительском классе 1:1. Далее создается фильтр, заворачивающий трафик в класс:

```
tc filter add dev eth0 parent 1: protocol ip prio 3 handle 1 fw classid 1:10
```

Здесь следует обратить внимание на значение параметра handle - в нашем случае это "1". Параметр "handle" это метка, которая проставлена пакету в iptables, т.е. пакеты, скорость которых нужно ограничивать, нужно метить соответствующей меткой. Делается это следующим образом:

```
iptables -t mangle -A FORWARD -d 1.1.1.1/32 -j MARK --set-mark 1
```

эта запись означает, что пакеты, направляющиеся к адресу 1.1.1.1, будут попадать в фильтр, в котором указан параметр "handle 1".

### Настройка utm5\_rfw.

Исходя из соображений безопасности, utm5\_rfw лучше запускать от непривилегированного пользователя. В качестве firewall\_path указываем в конфиге /usr/bin/sudo. В разделе "правила файерволл" будем полностью прописывать команду для выполнения.

В файле /etc/sudoers нужно разрешить пользователю, от которого будет запускаться utm5\_rfw, запускать процессы iptables и tc:

```
nobody ALL= NOPASSWD: /sbin/tc
nobody ALL= NOPASSWD: /sbin/iptables
```

Файл rfw5.cfg:

```
rfw_name=127.0.0.1
firewall_path=/usr/bin/sudo
core_host=127.0.0.1
core_port=11758
rfw_login=radius
rfw_password=radius
```

## Настройка файерволла в администраторском интерфейсе.

Заводим в биллинге брендмауэр, тип "local", IP-адрес 127.0.0.1. Создаем пять правил, - два для разрешения доступа в iptables, одно - для маркировки пакетов в iptables, одно для создания фильтра в TC и одно для создания класса в TC:

1. включение: `iptables -A FORWARD -s 0/0 -d UIP/UBITS -j ACCEPT`  
выключение: `iptables -D FORWARD -s 0/0 -d UIP/UBITS -j ACCEPT`

2. включение: `iptables -A FORWARD -d 0/0 -s UIP/UBITS -j ACCEPT`  
выключение: `iptables -D FORWARD -d 0/0 -s UIP/UBITS -j ACCEPT`

3. включение: `iptables -t mangle -A FORWARD -s 0/0 -d UIP/UBITS -j MARK --set-mark RULE_ID`  
выключение: `iptables -t mangle -D FORWARD -s 0/0 -d UIP/UBITS -j MARK --set-mark RULE_ID`

4. включение: `tc filter add dev eth0 parent 1: protocol ip prio 3 handle RULE_ID fw classid 1:RULE_ID`  
выключение: `tc filter del dev eth0 parent 1: protocol ip prio 3 handle RULE_ID fw classid 1:RULE_ID`

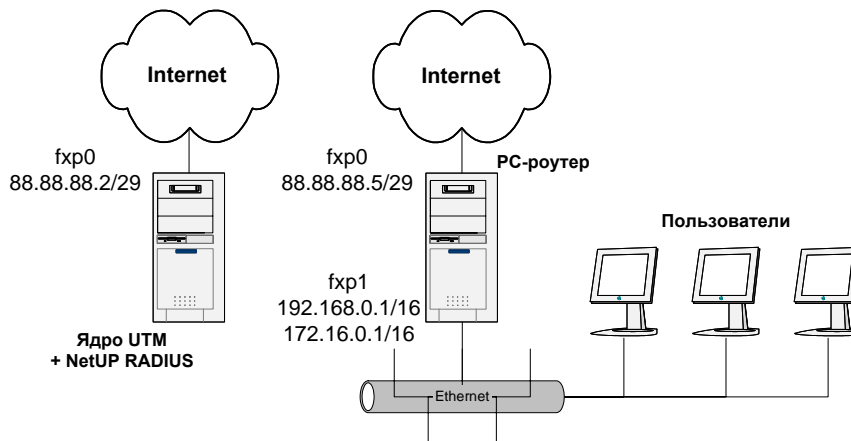
5. включение: `tc class add dev eth0 parent 1:1 classid 1:RULE_ID htb rate 1mbit burst 20k`  
выключение: `tc class del dev eth0 parent 1:1 classid 1:RULE_ID htb rate 1mbit burst 20k`

Здесь UIP/UBITS будет заменяться на IP-адрес пользователя вида 1.1.1.1/32, RULE\_ID будет принимать значение ID пользователя + 5000. На автозагрузку системы нужно проставить создание очереди и родительского класса:

```
echo "/sbin/tc qdisc add dev eth0 root handle 1: htb" >> /etc/rc.local
echo "/sbin/tc class add dev eth0 parent 1: classid 1:1 htb rate 100mbit ceil 100mbit burst 200k" >> /etc/rc.local
```

## Настройка шейпинга на PC-роутере под управлением FreeBSD и использование совместно с NetUP UTM.

Здесь будет рассмотрен пример, когда биллинг установлен не на PC-роутер, а на отдельный сервер, причем соединены они не через локальную сеть, а через интернет:



## Конфигурирование ограничения полосы пропускания на PC-роутере под управлением FreeBSD.

**Настройка файерволла ipfw.** Для того чтобы при загрузке роутера автоматически устанавливались правила файерволла, указанные в файле /etc/ipfw.conf, необходимо в /etc/rc.conf, добавить строки:

```
firewall_enable="YES"
firewall_type="/etc/ipfw.conf"
```

А сам файл /etc/ipfw.conf должен содержать настройки:

```
add 0001 allow all from any to any via lo0
add 0010 divert natd all from 172.16.0.0/16 to not 172.16.0.0/16 out via fxp0
dd 0010 divert natd all from not 172.16.0.0/16 to me in via fxp0
```

```
add 0010 divert natd all from 192.168.0.0/16 to not 192.168.0.0/16 out via fxp0
add 0010 divert natd all from not 192.168.0.0/16 to me in via fxp0
add 0020 allow ip from me to any
add 0020 allow ip from any to me
```

**Настройка пакета ndsad.** Настройки коллектора статистики ndsad, устанавливаемого на роутер, хранятся в файле ndsad.cfg, который имеет следующее содержание:

```
ip 88.88.88.2 [IP-адрес машины, принимающей пакеты статистики]
port 9996 [порт, принимающий пакеты статистики]
hash lo 64
hash all 32
heap 65536
log /netup/utm5/log/ndsad.log [адрес лог-файла]
```

**Настройка пакета rportp** производится в трех файлах, расположенных в /etc/ppp/: ppp.conf, pptpd.conf и radius.conf. Основные настройки хранятся в ppp.conf:

```
loop:
set timeout 0
set device /dev/ppp
local
# Server (local) IP address, Range for Clients, and Netmask
set ifaddr 172.16.0.1 172.16.0.2-172.16.0.254 255.255.255.255
set server /tmp/loop "" 0177
pptp:
load loop
enable chap
# enable pap
set radius /etc/ppp/radius.conf
```

Настройка демона pptpd производится в /etc/ppp/pptpd.conf:

```
option /etc/ppp/ppp.conf
localip 172.16.0.1
pidfile /var/run/pptpd.pid
```

Параметры процесса авторизации по протоколу Radius устанавливаются в /etc/ppp/radius.conf:

```
auth 88.88.88.2:1812 secret
acct 88.88.88.2:1813 secret
```

**Настройки rfw** указываются в файле /netup/utm5/rfw5.cfg:

```
rfw_name=router
sudo_path=
shell_path=/usr/local/bin/bash
firewall_path=/sbin/ipfw
core_host=88.88.88.2
core_port=11758
rfw_login=rfw
rfw_password=rfw
```

**Общие настройки системы.** Так же необходимо внести настройки в файлы: /etc/rc.local и /etc/sysctl.conf следующим образом. В /etc/rc.local следует добавить строки:

```
/usr/local/sbin/pptpd -c /etc/ppp/pptpd.conf &  
/netup/utm5/bin/ndsad -w -d -c /netup/utm5/ndsad.cfg &  
/netup/utm5/bin/utm5_rfw -f &
```

А в sysctl.conf – такие:

```
net.inet.ip.fw.one_pass=1
```

На этом настройка шейпинга на роутере завершена. Модифицировав конфигурационные файлы на роутере, можно приступить к настройке сервера, на котором установлен биллинг.

### Конфигурирование биллингового сервера.

Файл rc.conf должен содержать следующие директивы:

```
firewall_enable="YES"  
hostname="billing"  
ifconfig_fxp0="88.88.88.2/29"  
defaultrouter="88.88.88.1"
```

В конфигурационном файле rc.local необходимо указать три правила файерволла по умолчанию:

```
/sbin/ipfw add 64000 allow ip from me to any  
/sbin/ipfw add 64000 allow ip from any to me  
/sbin/ipfw add 65000 deny ip from any to any
```

Так же в Java-интерфейсе администратора необходимо создать:

- тариф передачи трафика, который будет ограничен по скорости (в примере его ID 410);
- соответствующего системного пользователя;
- брандмауэр и правила файерволла.

**Добавление системного пользователя** производится во вкладке «пользователи и группы – системные»; по нажатию кнопки «добавить» появится окно с полями, которые необходимо заполнить:

Системные группы		
Идентификатор группы	Имя группы	Информация

**Добавление брандмауэра** производится во вкладке «настройки – список брандмауэров»; по нажатию кнопки «добавить» появится окно с полями, которые необходимо заполнить:

Завершающей стадией настройки является добавление четырех правил файерволла во вкладке «настройки – правила firewall»; по нажатию кнопки «добавить» появится окно с полями, которые необходимо заполнить:

Правило №6 задает ширину канала;

правило №7 направляет пакеты на шейпирование;

правило №8 разрешает выход пакетов;

правило №9 разрешает вход пакетов.

© Компания NetUP, 2001-2005.

г.Москва, Лужнецкая набережная, д.2/4, строение 1, 5 этаж, офис 1

Почтовый адрес: 119311, Москва, а/я 87

Телефоны: +7 (095) 543-9220 (многоканальный)

+7 (095) 540-9652

+7 (095) 540-9653

