ОсОО «Оптима-Телеком»

Разделение и ограничения скорости среди нескольких подключенных доступов интернет, в условиях разделения направлений трафика в зарубежную сеть интернет и локальную зону Кыргызстана

Яковенко Виктор
sales@prohost.kg

г. Бишкек

22.11.2015г.

Цель:

Разработать схему обеспечения офиса доступом к сети интернет в круглосуточном режиме.

Требования:

1.Обеспечение пользователей круглосуточным доступом к сети интернет.
2.Ограничение входящей и исходящей скорости каждого пользователя в зарубежную сеть интернет и сеть Кыргызстана.
3.Автоматизация резервирования доступа к сети интернет.
4.Распределение нагрузки между подключениями от различных провайдеров.
5.Демократичная цена решения.
6.Отказоустойчивость оборудования в среде с периодическими перебоями в электросети.
7.Компактные размеры оборудования и небольшое энергопотребление.

Аналоги на рынке Кыргызстана

ZyXEL Keenetic Lite III

TP-LINK TL-WR1043ND

Системный блок персонального компьютера с предустановленной системой Linux

Анализ аналогов

Аналоги обеспечены неплохим функционалом, но имеют ряд недостатков:

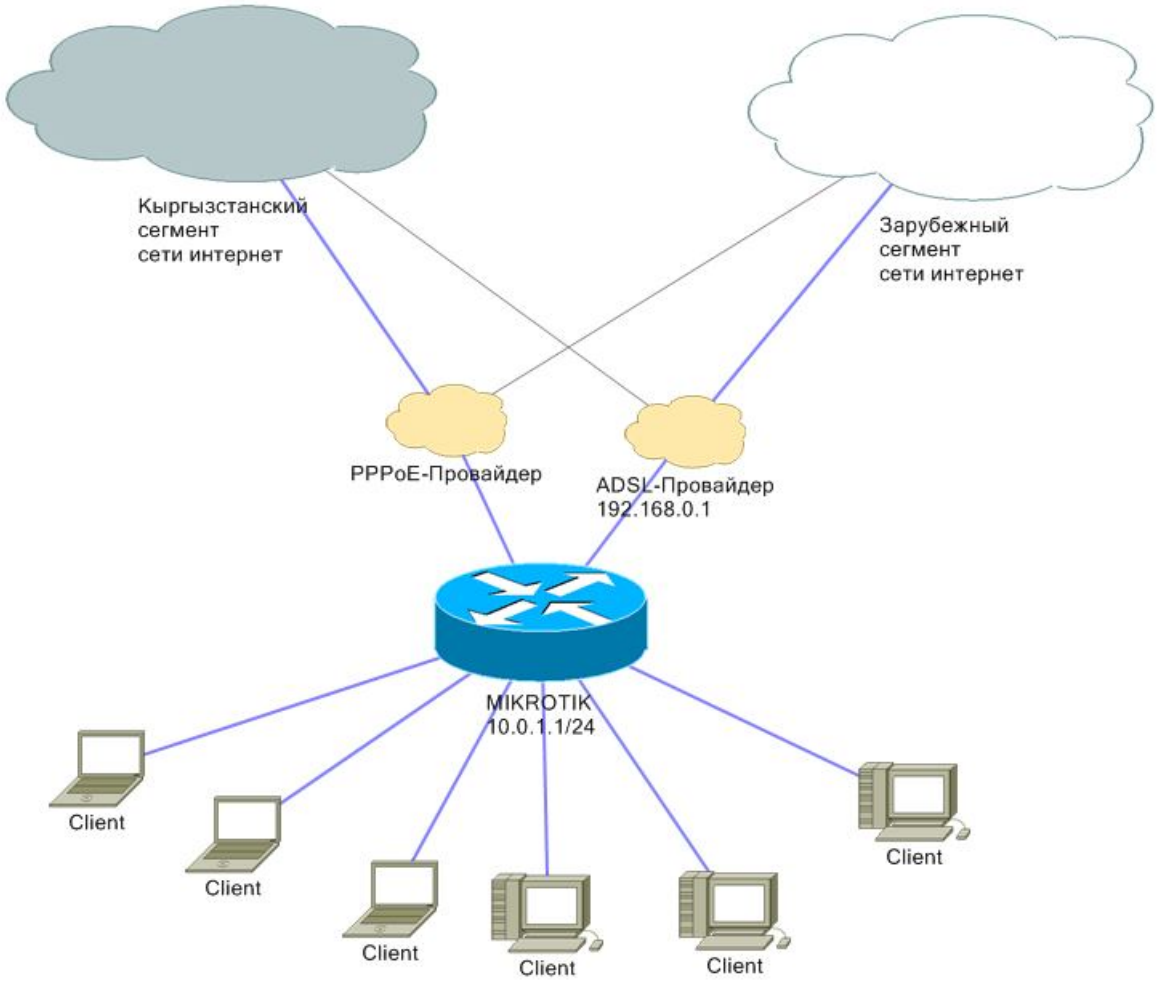
Роутеры:

- Отсутствие резервирования доступа к сети интернет
- Отсутствие ограничения пользователей по скорости
- Отсутствие распределения нагрузки между несколькими подключениями
- Работа роутера Zyxel критична к перебоям электроэнергии
- Отсутствие PoE

Системный блок ПК:

- высока вероятность отказа работы (собран либо из б/у деталей, либо из дешевых новых)
- необходимо содержание Linux специалиста
- шум вентиляторов
- большие габариты в сравнении с роутером

Схема сети


Кыргызстанский
сегмент
сети интернет
Зарубежный
сегмент
сети интернет
PPPoE-Провайдер
ADSL-Провайдер
192.168.0.1
MIKROTIK
10.0.1.1/24
Client
Client
Client
Client
Client
Client

Выбор модели RouterBOARD MIKROTIK

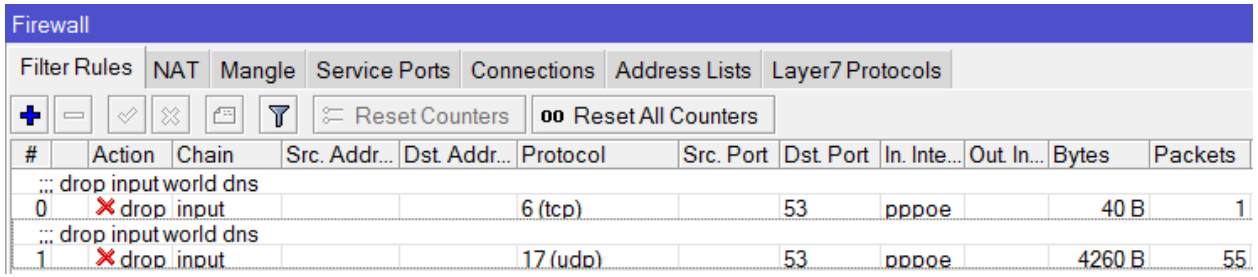
RB951Ui-2HnD
(802.11b/g/n Up to 7W,USB,CPU 600MHZ,128MB MEMORY, 5 ETHERNET PORTS,PoE)

RB951G-2HnD
(802.11b/g/n Up to 7W, USB, CPU 600MHZ, 128MB MEMORY, 5 ETHERNET GIG PORTS, PoE)

RB2011UiAS-2HnD-IN
(802.11b/g/n Up to 11W, USB, CPU 600MHZ, 128MB MEMORY, 5-1000Mbit and 5-100Mbit ETHERNET PORTS, 1 SFP PORT, PoE)

Настройка RouterBOARD MikroTik

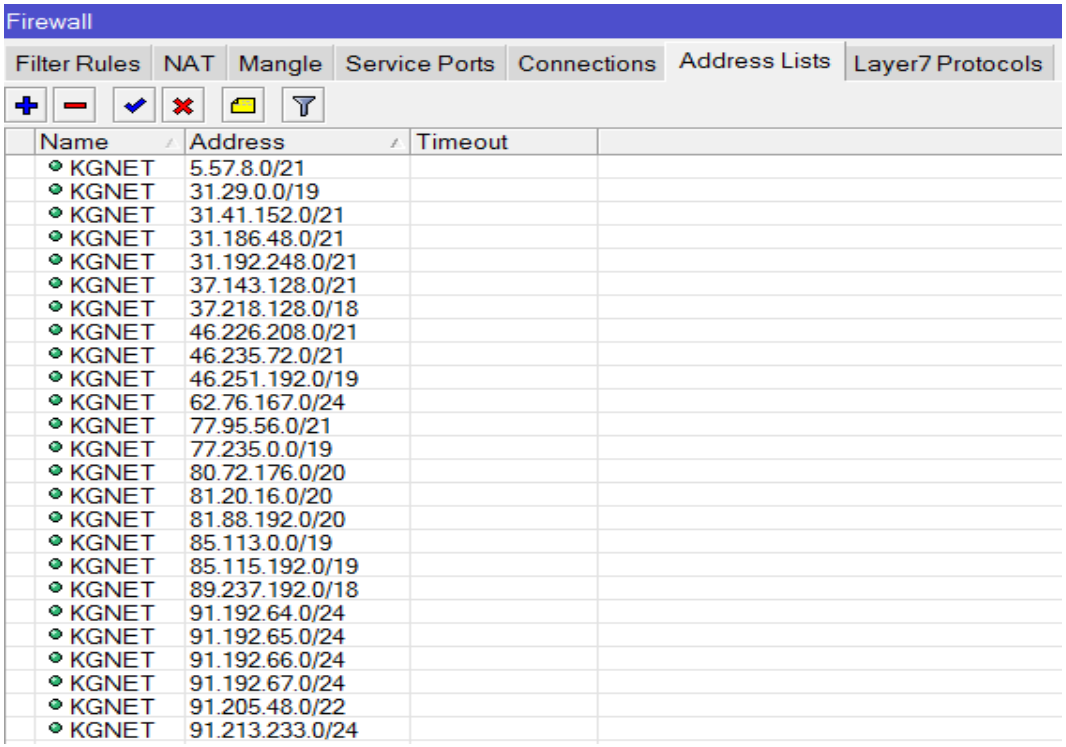
1) Закрываем DNS сервис на Mikrotik от внешнего мира т.к. роутер может стать частью атакующей сети и будет создаваться дополнительная нагрузка до 10 Мбит/с зарубежного трафика и до 90% нагрузки на процессор роутера. Блокировка необходима только для PPPoE провайдера, т.к. ADSL модем выступает в качестве брандмауэра и выдает нам адрес из собственного серого адресного пространства



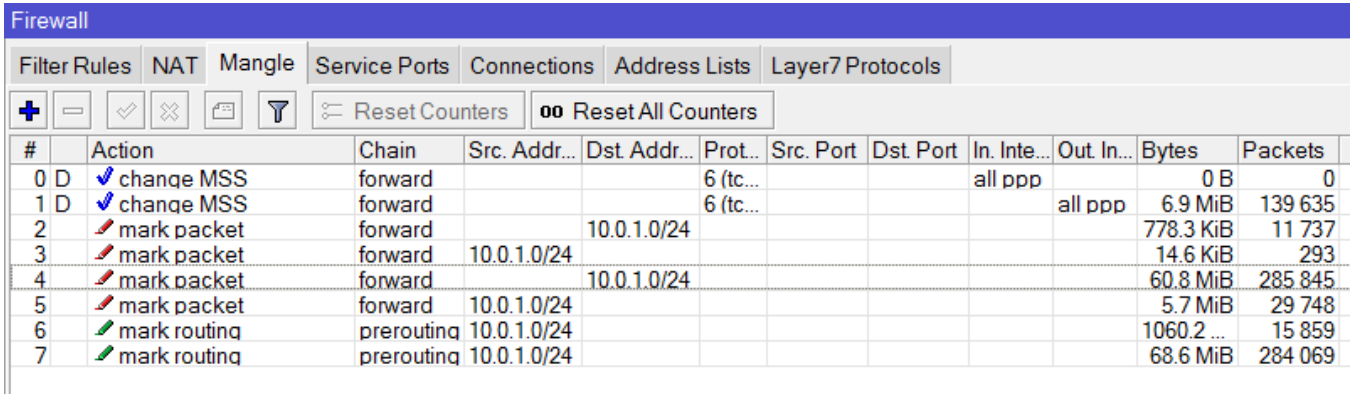
/ip firewall filter add chain=input action=drop protocol=udp in-interface=pppoe dst-port=53
/ip firewall filter add chain=input action=drop protocol=tcp in-interface=pppoe dst-port=53

2) Создадим адрес-лист KGNET, куда добавим список сетей провайдеров Кыргызстана
Список можно взять на официальном сайте каждого провайдера.

/ip firewall address-list add address=5.57.8.0/21 list=KGNET
/ip firewall address-list add address=89.237.192.0/18 list=KGNET
/ip firewall address-list add address=80.72.176.0/20 list=KGNET
/ip firewall address-list add address=212.112.96.0/20 list=KGNET
/ip firewall address-list add address=212.112.112.0/20 list=KGNET
/ip firewall address-list add address=94.143.192.0/21 list=KGNET
/ip firewall address-list add address=178.217.168.0/21 list=KGNET
/ip firewall address-list add address=46.226.208.0/21 list=KGNET
/ip firewall address-list add address=194.176.111.0/24 list=KGNET
/ip firewall address-list add address=62.76.167.0/24 list=KGNET
/ip firewall address-list add address=185.54.254.0/24 list=KGNET
/ip firewall address-list add address=31.148.30.0/24 list=KGNET
/ip firewall address-list add address=185.54.253.0/24 list=KGNET
/ip firewall address-list add address=31.41.152.0/21 list=KGNET
/ip firewall address-list add address=185.88.32.0/22 list=KGNET
……..



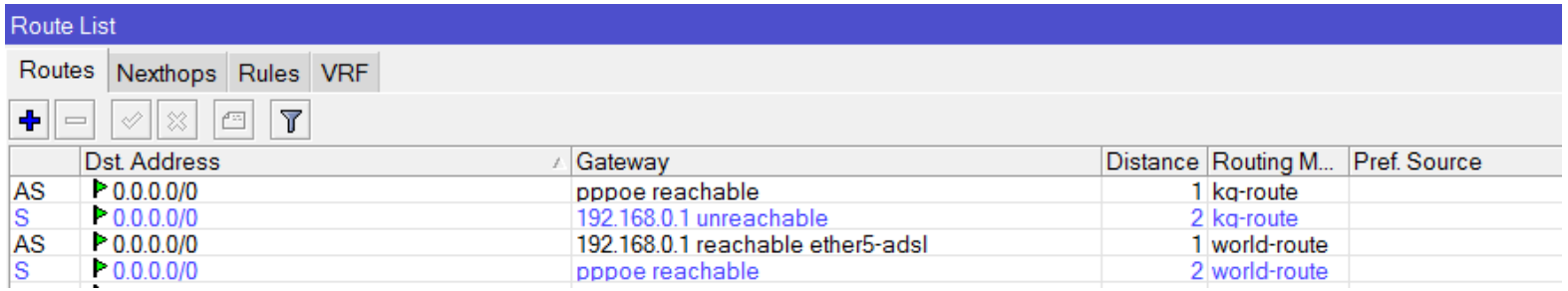
3) Наметим пакеты в стороны Кыргызстанской зоны сети интернет и зарубежной, чтобы в дальнейшем проводить ограничения по скорости.
Входящий и исходящий трафик зарубежной сети будут соответственно с наметкой world и kg.
Также наметим для маршрутизации исходящий трафик в зону KG и исходящий в зону МИР.



#		Action	Chain	Src. Addr...	Dst. Addr...	Prot...	Src. Port	Dst. Port	In. Inte...	Out. In...	Bytes	Packets
0	D	change MSS	forward			6 (tc...			all ppp		0 B	0
1	D	change MSS	forward			6 (tc...				all ppp	6.9 MiB	139 635
2		mark packet	forward		10.0.1.0/24						778.3 KiB	11 737
3		mark packet	forward	10.0.1.0/24							14.6 KiB	293
4		mark packet	forward		10.0.1.0/24						60.8 MiB	285 845
5		mark packet	forward	10.0.1.0/24							5.7 MiB	29 748
6		mark routing	prerouting	10.0.1.0/24							1060.2 ...	15 859
7		mark routing	prerouting	10.0.1.0/24							68.6 MiB	284 069

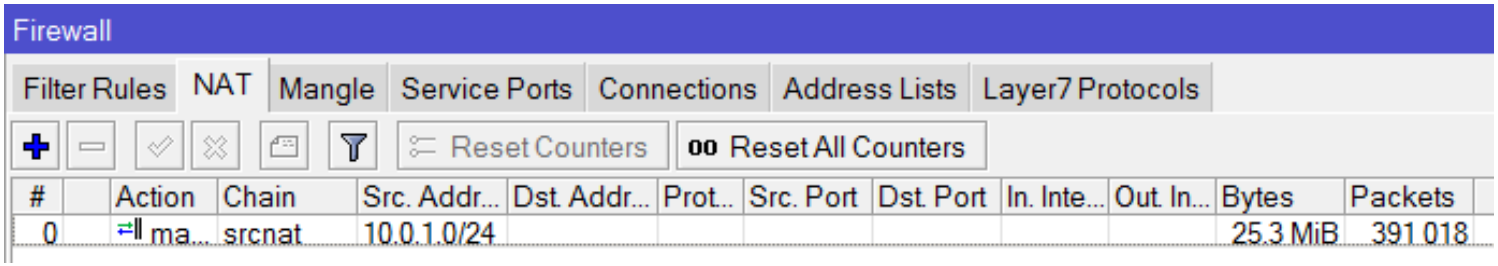
/ip firewall mangle add chain=forward action=mark-packet new-packet-mark=world passthrough=yes dst-address=10.0.1.0/24 src-address-list=!KGNET
/ip firewall mangle add chain=forward action=mark-packet new-packet-mark=world passthrough=yes src-address=10.0.1.0/24 dst-address-list=!KGNET
/ip firewall mangle add chain=forward action=mark-packet new-packet-mark=kg passthrough=yes dst-address=10.0.1.0/24 src-address-list=KGNET
/ip firewall mangle add chain=forward action=mark-packet new-packet-mark=kg passthrough=yes src-address=10.0.1.0/24 dst-address-list=KGNET
/ip firewall mangle add chain=prerouting action=mark-routing new-routing-mark=world-route passthrough=yes src-address=10.0.1.0/24 dst-address-list=!KGNET
/ip firewall mangle add chain=prerouting action=mark-routing new-routing-mark=kg-route passthrough=yes src-address=10.0.1.0/24 dst-address-list=KGNET

4) В связи с тем, что множество пользователей используют локальную зону KG для работы торрент-клиентов, а раздача через ADSL модем негативно влияет на скорость входящего трафика, создадим правила маршрутизации,
где трафик по зоне KG будет идти через PPPoE и только в случае недоступности PPPoE соединения, пойдет через ADSL.
Доступ к зарубежной сети будет идти через ADSL, и только при его неработоспособности будет направлен через PPPoE
Обязательно необходимо для каждого маршрута необходимо установить проверку доступности шлюза (arp или ping)



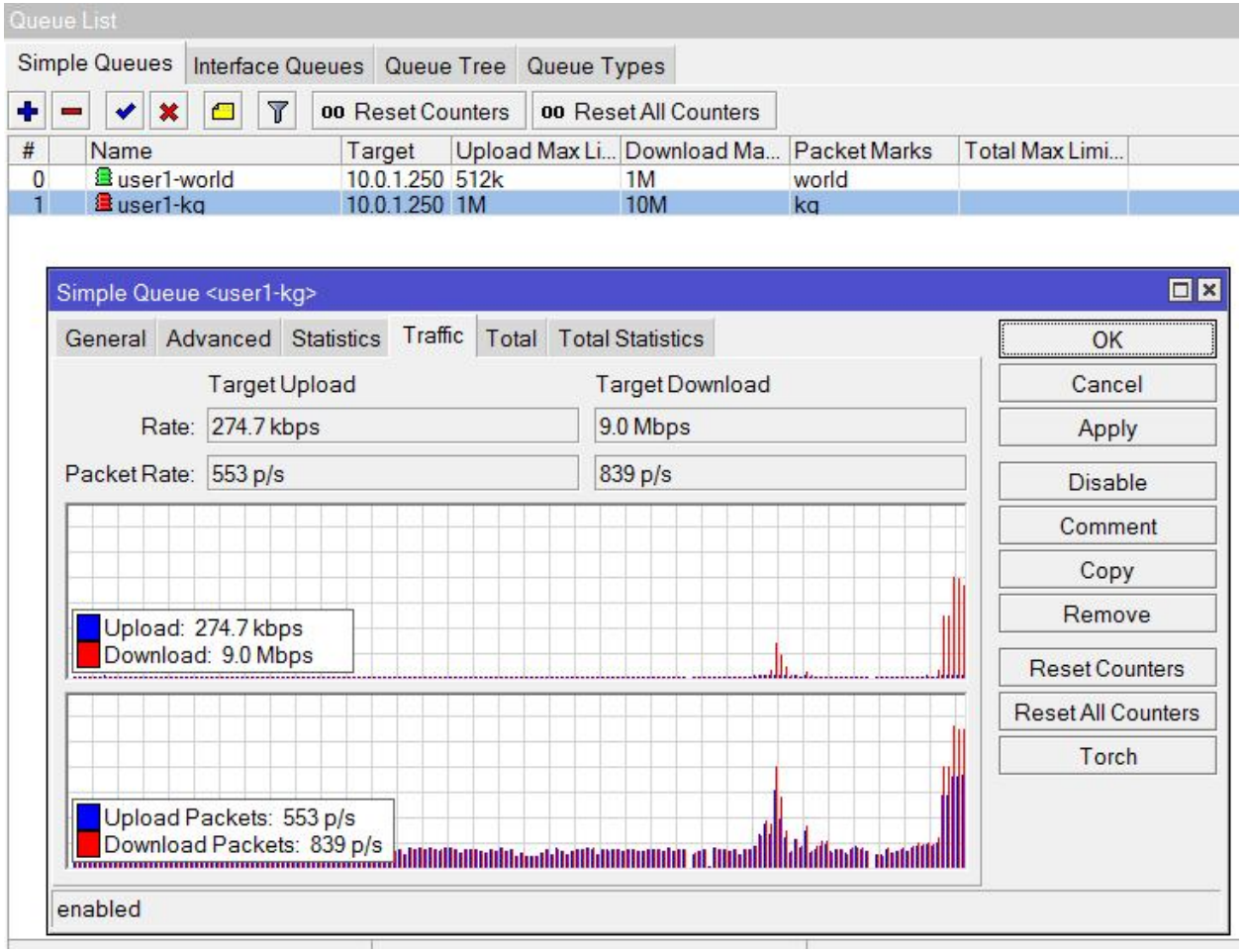
/ip route add dst-address=0.0.0.0/0 gateway=pppoe check-gateway=ping distance=1 routing-mark=kg-route
/ip route add dst-address=0.0.0.0/0 gateway=192.168.0.1 check-gateway=ping distance=2 routing-mark=kg-route
/ip route add dst-address=0.0.0.0/0 gateway=192.168.0.1 check-gateway=ping distance=1 routing-mark=world-route
/ip route add dst-address=0.0.0.0/0 gateway=pppoe check-gateway=ping distance=2 routing-mark=world-route

Создадим правило трансляции адресов локальных пользователей в сеть интернет (NAT)



/ip firewall nat add chain=srcnat action=masquerade to-addresses=0.0.0.0 src-address=10.0.1.0/24

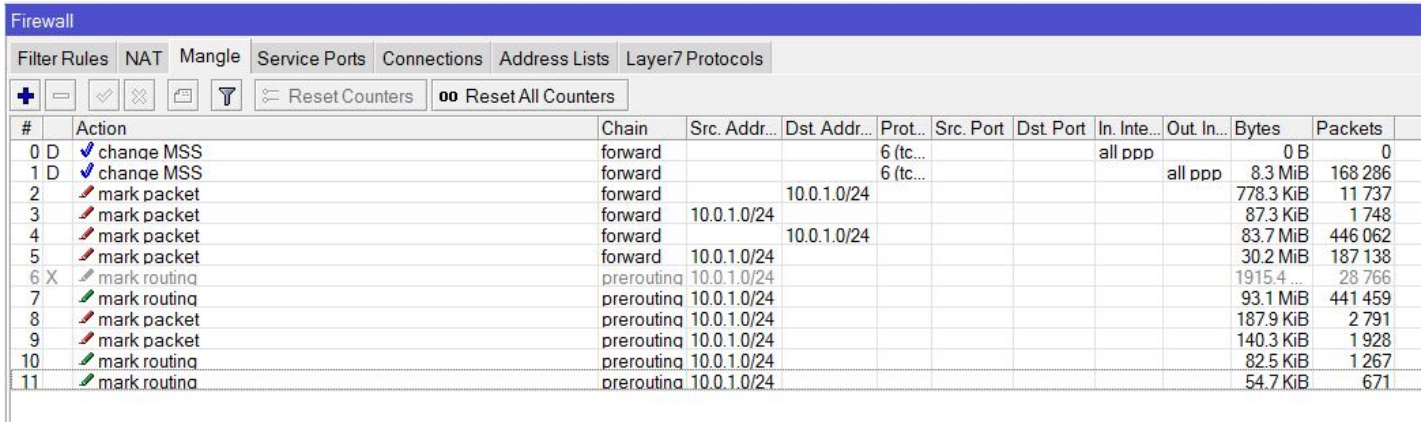
5) Создадим правило, например, для пользователя с адресом 10.0.1.250
Скорость доступа к зарубежной сети интернет ограничим входящую на 1Мбит/, а исходящую на 512кбит/с.
Для доступа к зоне KG входящая пусть будет ограничена на 10Мбит/с, а исходящая на 1Мбит/с.



/queue simple add name="user1-world" target=10.0.1.250/32 packet-marks=world max-limit=512k/1M
/queue simple add name="user1-kg" target=10.0.1.250/32 packet-marks=kg max-limit=1M/10M

6) Скорость доступ к зарубежной сети намного меньше, чем к Кыргызстанскому сегменту сети.
Модернизируем наши подключения так, чтобы для доступа к зарубежным сайтам использовались подключения как ADSL, так и PPPoE.

Стоит также учитывать специфику объединения, соединения имеют разные ip адреса, и чтобы корректно работали сайты с аутентификацией и шифрованием:
Проведем некоторые изменения



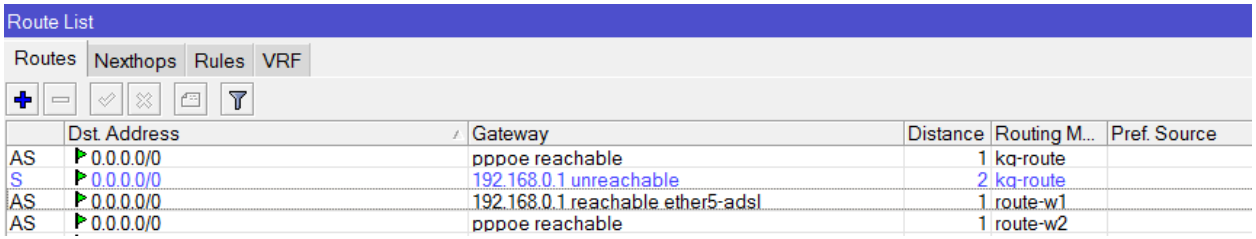
#		Action	Chain	Src. Addr...	Dst. Addr...	Prot...	Src. Port	Dst. Port	In. Inte...	Out. In...	Bytes	Packets
0	D	change MSS	forward			6 (tc...			all ppp		0 B	0
1	D	change MSS	forward			6 (tc...				all ppp	8.3 MiB	168 286
2		mark packet	forward		10.0.1.0/24						778.3 KiB	11 737
3		mark packet	forward	10.0.1.0/24							87.3 KiB	1 748
4		mark packet	forward		10.0.1.0/24						83.7 MiB	446 062
5		mark packet	forward	10.0.1.0/24							30.2 MiB	187 138
6	X	mark routing	prerouting	10.0.1.0/24							1915.4 ...	28 766
7		mark routing	prerouting	10.0.1.0/24							93.1 MiB	441 459
8		mark packet	prerouting	10.0.1.0/24							187.9 KiB	2 791
9		mark packet	prerouting	10.0.1.0/24							140.3 KiB	1 928
10		mark routing	prerouting	10.0.1.0/24							82.5 KiB	1 267
11		mark routing	prerouting	10.0.1.0/24							54.7 KiB	671

Правила наметки пакетов для ограничителя
/ip firewall mangle add chain=forward action=mark-packet new-packet-mark=world passthrough=yes dst-address=10.0.1.0/24 src-address-list=!KGNET
/ip firewall mangle add chain=forward action=mark-packet new-packet-mark=world passthrough=yes src-address=10.0.1.0/24 dst-address-list=!KGNET
/ip firewall mangle add chain=forward action=mark-packet new-packet-mark=kg passthrough=yes dst-address=10.0.1.0/24 src-address-list=KGNET
/ip firewall mangle add chain=forward action=mark-packet new-packet-mark=kg passthrough=yes src-address=10.0.1.0/24 dst-address-list=KGNET

Правила наметки для маршрутизации KG зоны
/ip firewall mangle add chain=prerouting action=mark-routing new-routing-mark=kg-route passthrough=yes src-address=10.0.1.0/24 dst-address-list=KGNET

Правила наметки и распределения пакетов для зарубежной зоны
/ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=w1 passthrough=yes src-address=10.0.1.0/24 dst-address-list=!KGNET per-connection-classifier=dst-address:2/0
/ip firewall mangle add chain=prerouting action=mark-packet new-packet-mark=w2 passthrough=yes src-address=10.0.1.0/24 dst-address-list=!KGNET per-connection-classifier=dst-address:2/1
/ip firewall mangle add chain=prerouting action=mark-routing new-routing-mark=route-w1 passthrough=yes src-address=10.0.1.0/24 dst-address-list=!KGNET packet-mark=w1
/ip firewall mangle add chain=prerouting action=mark-routing new-routing-mark=route-w2 passthrough=yes src-address=10.0.1.0/24 dst-address-list=!KGNET packet-mark=w2

7) Внесем полученные изменения в таблицу маршрутизации

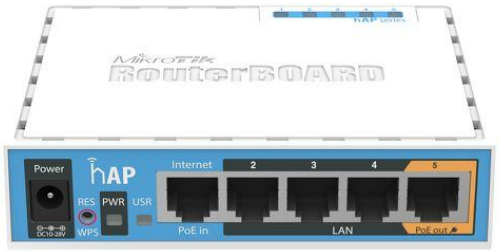


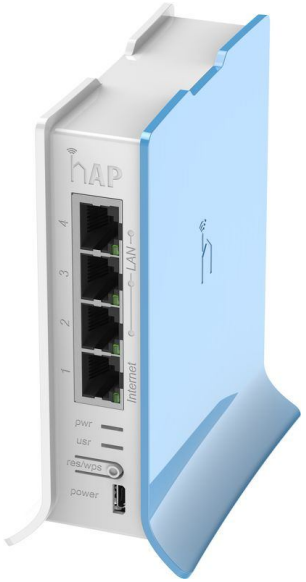
Направим трафик в KG зону через PPPoE, и резервирование через ADSL
/ip route add dst-address=0.0.0.0/0 gateway=pppoe check-gateway=ping distance=1 routing-mark=kg-route
/ip route add dst-address=0.0.0.0/0 gateway=192.168.0.1 check-gateway=ping distance=2 routing-mark=kg-route

Направим трафик намеченных пакетов route-w1 и route-w2 направим в зарубежную зону через шлюзы ADSL и PPPoE
/ip route add dst-address=0.0.0.0/0 gateway=192.168.0.1 check-gateway=ping distance=1 routing-mark=route-w1
*/ip route add dst-address=0.0.0.0/0 gateway=pppoe check-gateway=ping distance=1 routing-mark=route-*w2

Результаты работы MikroTik RouterBOARD

- *Запущена система обеспечения офиса круглосуточным доступом к сети интернет*
- *Распределена нагрузка между подключениями ADSL и PPPoE*
- *Настроена система резервирования интернет доступа (backup)*
- *Ограничена скорость для каждого пользователя, как по направлениями (KG и зарубежный интернет), так и входящая и исходящая*
- *Синхронное объединение доступа к зарубежной сети интернет через двух провайдеров*
- *Подключение роутера к сети электропитания без прокладки силового кабеля (питание через PoE)*





Заключение

В настоящее время роутеры MikroTik RouterBOARD с вышеописанной настройкой установлены в различных офисных и гостиничных зданиях.

Дополнительные возможности настройки MikroTik RouterBOARD позволили также осуществлять следующее:

- перезагрузка ADSL модема по ssh с помощью Mikrotik RouterBOAD при ухудшении качества связи

- оповещение о проблемах интернет соединений посредством сервиса sms2email

- еженедельный автоматический backup настроек с отправкой на электронную почту

- сетевое хранилище данных SMB (внешний HDD подключенный к USB порту Mikrotik RouterBOAD)

Спасибо за внимание