

MikroTik RouterOS Семинар

QoS Лучшая практика

(перевод на русский язык white_crow 2010 г. от P.X)

Прага,
MUM Чехия2009

Вопросы и ответы

- *Вопрос:* Это возможно – приоритезация трафика по типу для каждого отдельного клиента и строгие ограничения на том же маршрутизаторе?
- *Ответ:* Да!

- *Вопрос:* Что для этого нужно?
- *Ответ:* Вам понадобятся:
 - 1)Packet Flow Diagram
 - 2)HTB (queue tree)
 - 3)Mangle
 - 4)PCQ
 - 5)Address List

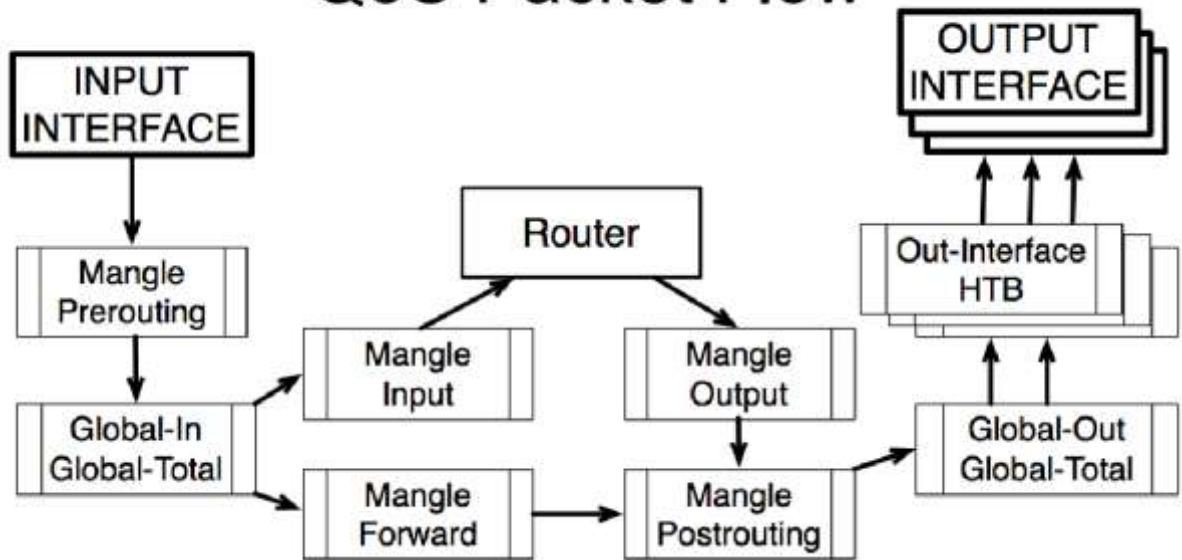
Mangle

- Mangle позволяет вам маркировать IP пакеты специальными метками.
- Эти метки используются другими средствами маршрутизатора, такими как маршрутизация и управление полосой пропускания для идентификации пакетов.
- В добавок, средствами mangle можно модифицировать некоторые поля в IP заголовке, такие как TOS (DSCP) и TTL поля.

Hierarchical Token Bucket

- Вся реализация управления пропускной способностью в RouterOS основана на иерархии - Hierarchical Token Bucket (HTB)
- HTB позволяет вам создавать иерархические структуры очередей и определять отношения между очередями
- RouterOS поддерживает 3 виртуальных HTB (global-in, global-total, global-out) и еще один прямо перед каждым выходным интерфейсом.

QoS Packet Flow



http://wiki.mikrotik.com/wiki/Packet_Flow

Двойной QoS

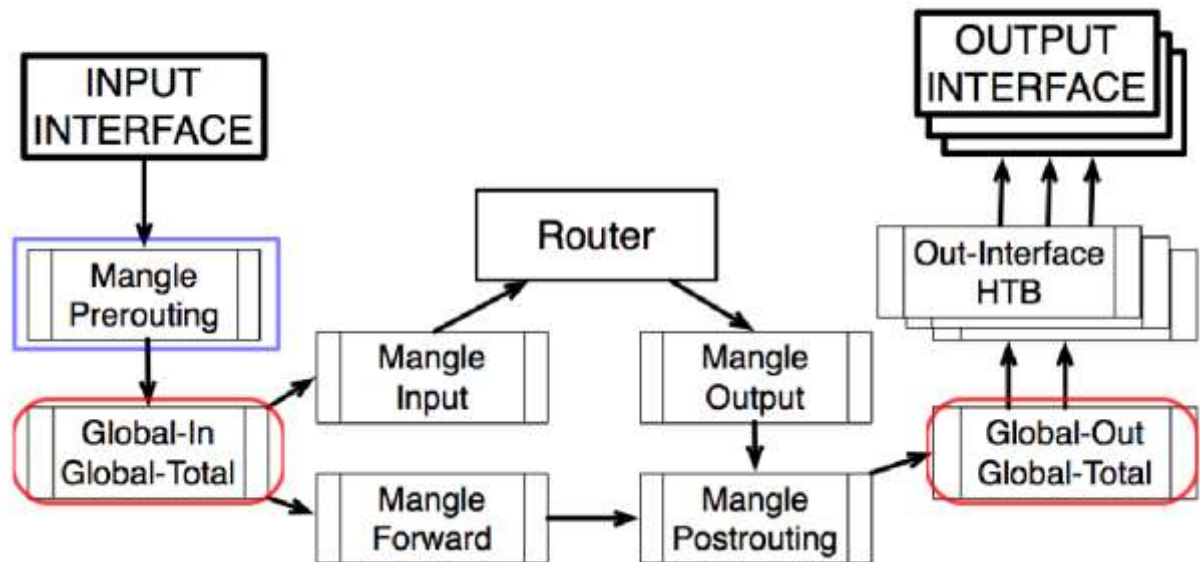
- Возможно маркировать и шейпить трафик дважды на одном роутере:
 - Prerouting в цепочке Mangle – для первой маркировки
 - Global-in HTB – для первого шейпинга
 - Forward или Postrouting в цепочке Mangle - для второй маркировки.
 - Global-out или Out-interface HTB для второй маркировки
- Двойной QoS возможен только с помощью Queue Tree.

Почему не Simple Queues?

- Simple queues (простые очереди) отсортированы – по аналогии с правилами фаервола
 - Для того, чтобы добраться до 999-ой очереди, пакет должны быть проверен на соответствие всем 998-ми предыдущим очередям.
- Каждая простая очередь **может** стоять в 3 отдельных очередях:
 - One in Global-in (“direct” part)
 - One in Global-out (“reverse” part)
 - One in Global-total (“total” part)

Simple Queues and Mangle

(простые очереди и Mangle)



Queue Tree

(дерево очередей)

- Дерево очередей является только однонаправленным и может быть расположено в любом из доступных НТВ.
- Очереди **Queue Tree** обрабатываются не по порядку – весь трафик обрабатывается одновременно.
- Все дочерние очереди должны иметь пакеты, маркированные с помощью средств “/ip firewall mangle” , назначенных для них.
- Простая очередь (Simple queue) помещенная в тот же НТВ, будет «принимать» весь трафик от Queue Tree очереди.

Global-Out или Interface НТВ?

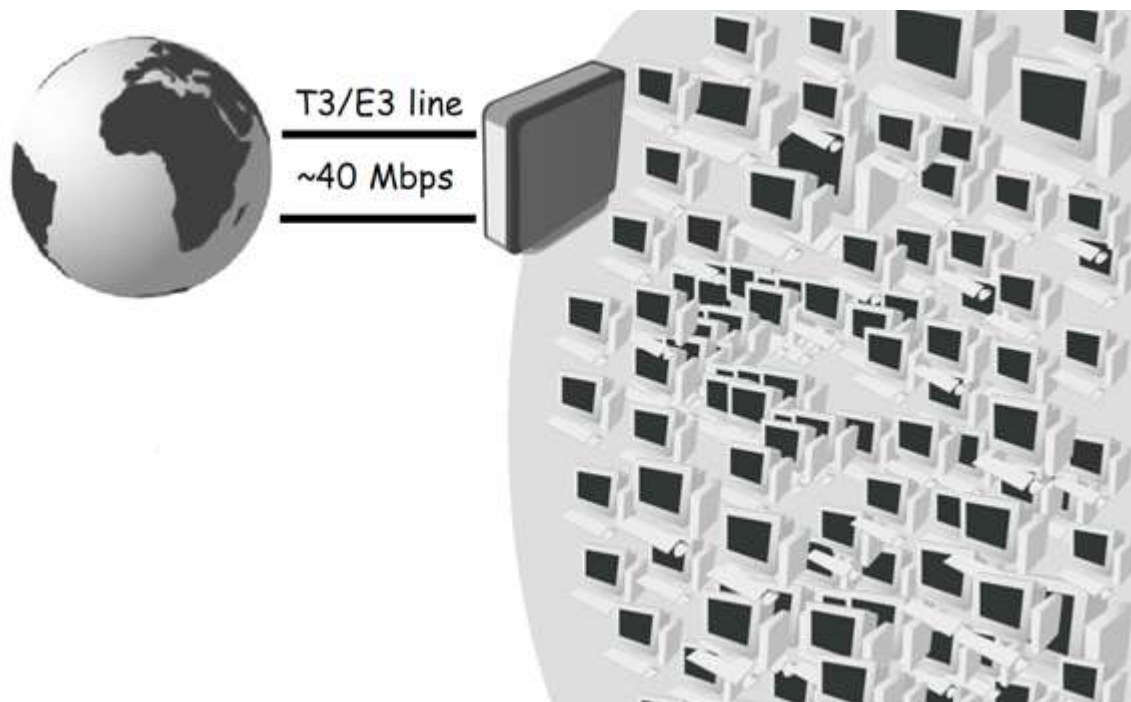
Существует два основных отличия

- В случае SRC-NAT (masquerade) - Global-Out будет знать о частных адресах клиента, но Интерфейс НТВ не будет - интерфейс НТВ находится после SRC-NAT.
- Каждый интерфейс НТВ получает только трафик, который будет отправится через определенный интерфейс - нет необходимости в разделении upload и download в mangle

Выводы

- Мы будем использовать mangle и queue tree:
 - Маркировать трафик по типу в mangle цепочке Prerouting
 - Приоритезация и ограничение трафика по типу в Global-in HTB
 - Перемаркировка трафика по клиентам в mangle цепочке Forward
 - Ограничение трафика по клиентам в Interface HTB
- Необходимо свести количество правил mangle и очередей к минимуму, чтобы увеличить производительность этой конфигурации.

Ограничение клиентов



●Вы имеете более чем 400 клиентов и 3 разных тарифа для подключений:

- «Бизнес» (4Mbps/1Mbps)
- «Стандарт» (750kbps/250kbps)
- «Базовый» (375kbps/125kbps)

PCQ

- Очередь по подключению (Per Connection Queue – PCQ) – это тип очереди, способная делить трафик на под-потoki (sub-streams), на основе выбранных классификаторов.
- Каждый под-поток будет проходить FIFO очередь, с размером очереди, указанным в опции “pcq-limit” и с максимальной скоростью, указанной в опции “pcq-rate”.

New Queue Type

Type Name:

Kind: ▼

Rate:

Limit:

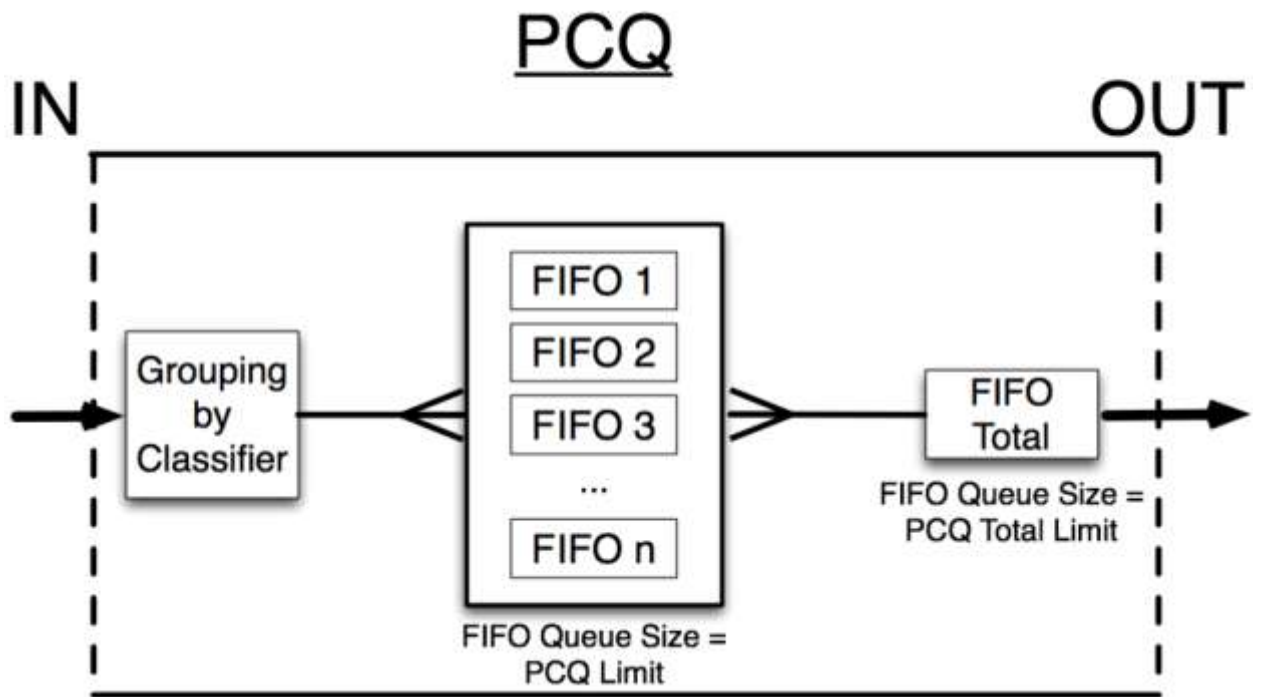
Total Limit:

– Classifier –

☐ Src. Address ☒ Dst. Address

☐ Src. Port ☐ Dst. Port

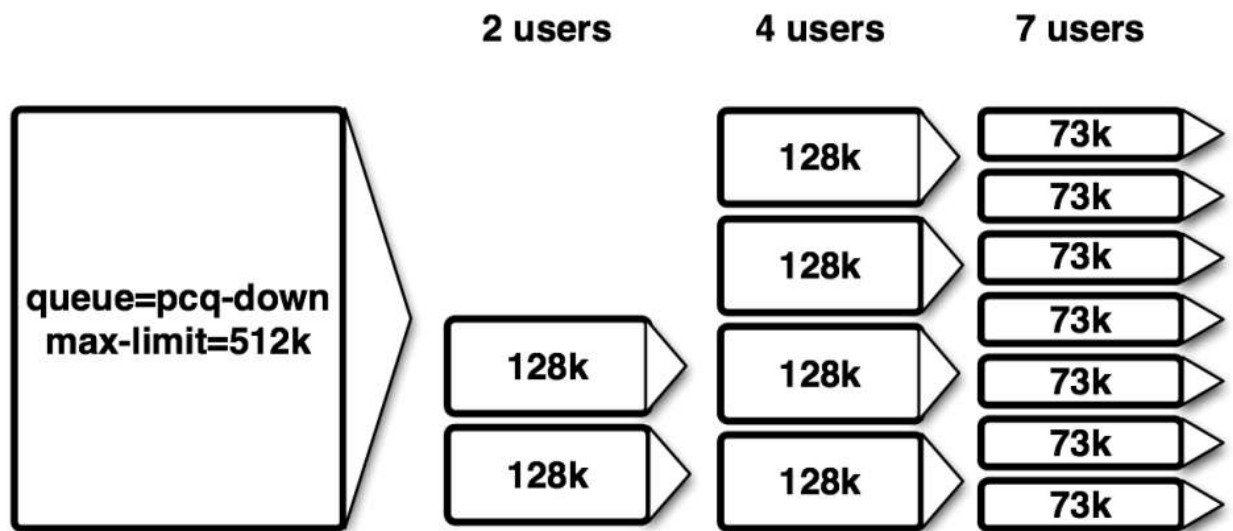
OK
Cancel
Apply
Copy
Remove



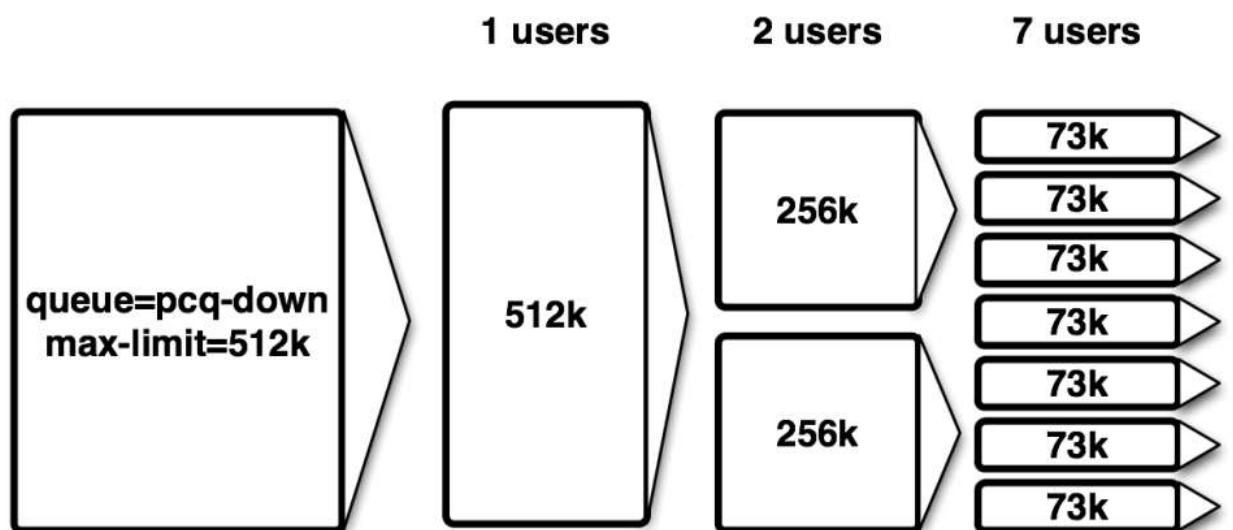
PCQ Part 2

- Для того, чтобы гарантировать, что каждый PCQ под-поток представляет собой одного конкретного клиента , мы должны создать 2 разных PCQ типа:
 - PCQ_upload – в качестве классификатора – адрес источника (source address)
 - PCQ_download - в качестве классификатора – адрес назначения (destination address)
- PCQ будет распределять имеющийся трафик равномерно между под-очередями, пока скорость pcq-rate доступна (если она указана)

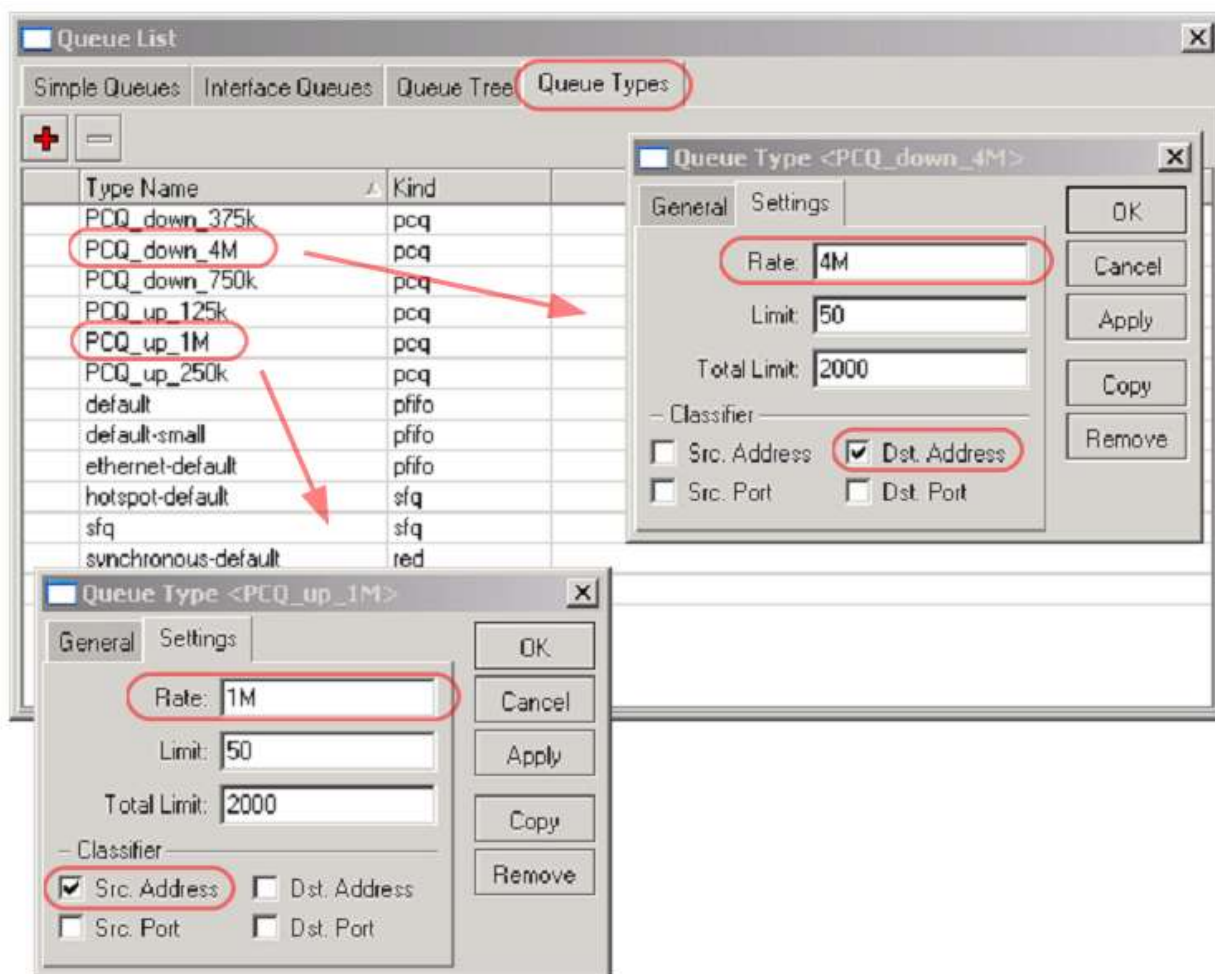
pcq-rate=128000



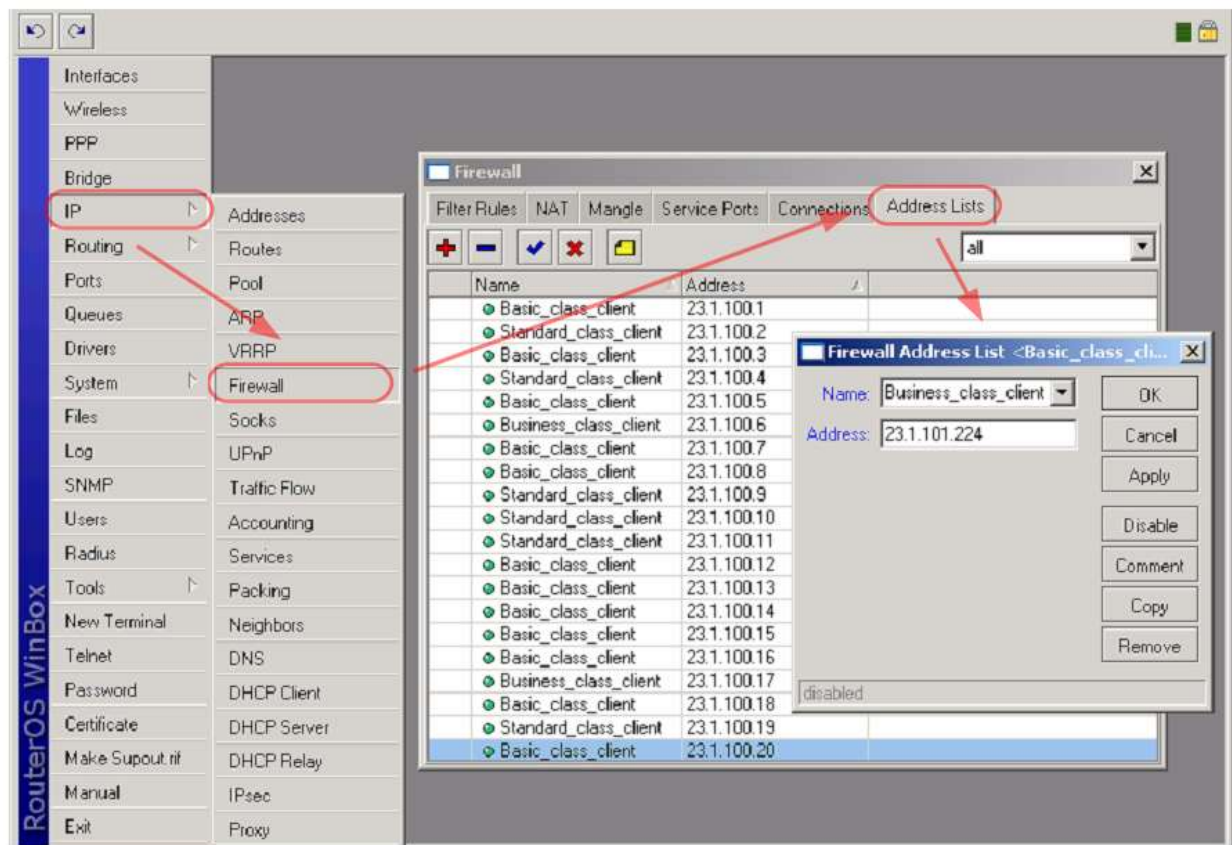
pcq-rate=0



Обзор PCQ Тип: Winbox

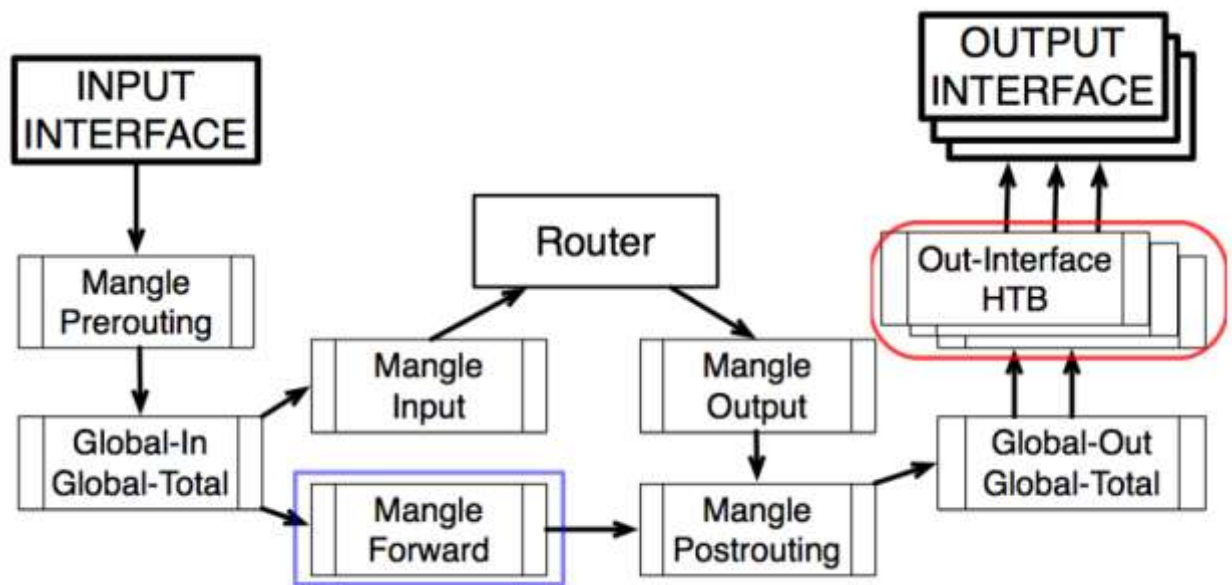


Address Lists



- Адрес листы (Address lists) были введены для того, чтобы определить множество IP адресов в одно и тоже правило фаервола, таким образом сокращается общее число правил фаервола и повышается производительность роутера.
- Адресные листы могут быть созданы:
 - Вручную
 - Автоматически из PPP профиля – просто укажите опцию address-list и как только клиент соединиться, он будет добавлен в надлежащий адрес-лист.
 - Автоматически через RADIUS-атрибут: "Mikrotik:19" (Mikrotik-Address-List).

Где ?



Маркировка пакетов

- Используйте действие (action) - “connection-mark”, чтобы классифицировать все соединения, основанные на клиентских адресных листах.
- Используйте действие - “packet-mark”, чтобы классифицировать весь трафик, основанный на маркировке соединений
- Вопросы для размышления:
 - Какая скорость должна быть доступна для клиентов, с тарифом «бизнес», если осуществляется загрузка (downloading) с клиентом тарифа «Базовый»?
 - У вас есть еще немаркированный трафик?

Правило «Connection-mark»

The image displays two screenshots of the Mikrotik WinBox 'Mangle Rule' configuration window, illustrating the setup for a 'Connection-mark' rule.

Left Screenshot (Advanced Tab):

- General:** Chain: forward
- Advanced:** Src. Address List: Basic_class_client (selected)
- Action:** Disabled
- Statistics:** Disabled

Right Screenshot (Action Tab):

- General:** Chain: forward
- Advanced:** Src. Address List: Basic_class_client (selected)
- Action:** mark connection (selected)
- New Connection Mark:** basic_client_conn (selected)
- Passthrough:** Checked
- Statistics:** Disabled

Правило «Packet-mark»

The image displays two screenshots of the Mikrotik WinBox 'Mangle Rule' configuration window, illustrating the setup for a 'Packet-mark' rule.

Left Screenshot (General Tab):

- General:** Chain: forward (selected)
- Advanced:** Src. Address: , Dst. Address: , Protocol: , Src. Port: , Dst. Port: , P2P: , In. Interface: , Out. Interface: , Packet Mark: , Connection Mark: basic_client_conn (selected), Routing Mark: , Connection State: , Connection Type:
- Action:** Disabled
- Statistics:** Disabled

Right Screenshot (Action Tab):

- General:** Chain: forward
- Advanced:** Src. Address: , Dst. Address: , Protocol: , Src. Port: , Dst. Port: , P2P: , In. Interface: , Out. Interface: , Packet Mark: , Connection Mark: basic_client_conn (selected), Routing Mark: , Connection State: , Connection Type:
- Action:** mark packet (selected)
- New Packet Mark:** basic_client_traffic (selected)
- Passthrough:** Unchecked
- Statistics:** Disabled

Обзор Mangle: Winbox

Firewall

Filter Rules

NAT

Mangle

Service Ports

Connections

Address Lists

+

-

✓

✗

📁

00 Reset Counters

00 Reset All Counters

forward

#	Action	Chain	Priority	New Packet Mark	New Connection Mark	Bytes	Packets
::: mark basic client traffic							
	mark connection	forward			basic_client_conn	9893.1 MiB	18 599 504
	mark packet	forward		basic_client_traffic		22575.4 MiB	35 292 323
::: mark standard client traffic							
	mark connection	forward			standard_client_conn	825.4 MiB	2 747 515
	mark packet	forward		standard_client_traffic		6396.7 MiB	7 248 925
::: mark business client traffic							
	mark connection	forward			business_client_conn	190.2 MiB	912 903
	mark packet	forward		business_client_traffic		1324.9 MiB	1 929 206
::: Check for unmarked traffic							
	log	forward				2062.0 KiB	9 014

Обзор Mangle: Export

```

/ ip firewall mangle
add chain=forward src-address-list=Basic_class_client action=mark-connection \
    new-connection-mark=basic_client_conn passthrough=yes comment="mark basic \
    client traffic" disabled=no
add chain=forward connection-mark=basic_client_conn action=mark-packet \
    new-packet-mark=basic_client_traffic passthrough=no comment="" disabled=no
add chain=forward src-address-list=Standard_class_client \
    action=mark-connection new-connection-mark=standard_client_conn \
    passthrough=yes comment="mark standard client traffic" disabled=no
add chain=forward connection-mark=standard_client_conn action=mark-packet \
    new-packet-mark=standard_client_traffic passthrough=no comment="" \
    disabled=no
add chain=forward src-address-list=Business_class_client \
    action=mark-connection new-connection-mark=business_client_conn \
    passthrough=yes comment="mark bussiness client traffic" disabled=no
add chain=forward connection-mark=business_client_conn action=mark-packet \
    new-packet-mark=business_client_traffic passthrough=no comment="" \
    disabled=no
add chain=forward action=log log-prefix="" comment="Check for unmarked \
    traffic" disabled=no

```

Обзор Queue Tree: Winbox

Queue List					
<div> <div>Simple Queues</div> <div>Interface Queues</div> <div>Queue Tree</div> <div>Queue Types</div> </div> <div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>00 Reset Counters</div> <div>00 Reset All Counters</div> </div>					
	Name	Parent	Packet Mark	Limit At	Max Limit
	Total_download	local_ether1		0	0
	basic_client_download	Total_download	basic_client_traffic	0	0
	business_client_download	Total_download	business_client_traffic	0	0
	standard_client_download	Total_download	standard_client_traffic	0	0
	Total_upload	public_ether3		0	0
	basic_client_upload	Total_upload	basic_client_traffic	0	0
	business_client_upload	Total_upload	business_client_traffic	0	0
	standard_client_upload	Total_upload	standard_client_traffic	0	0
<div>0 B queued</div> <div>0 packets queued</div>					

Обзор Queue Tree: Export

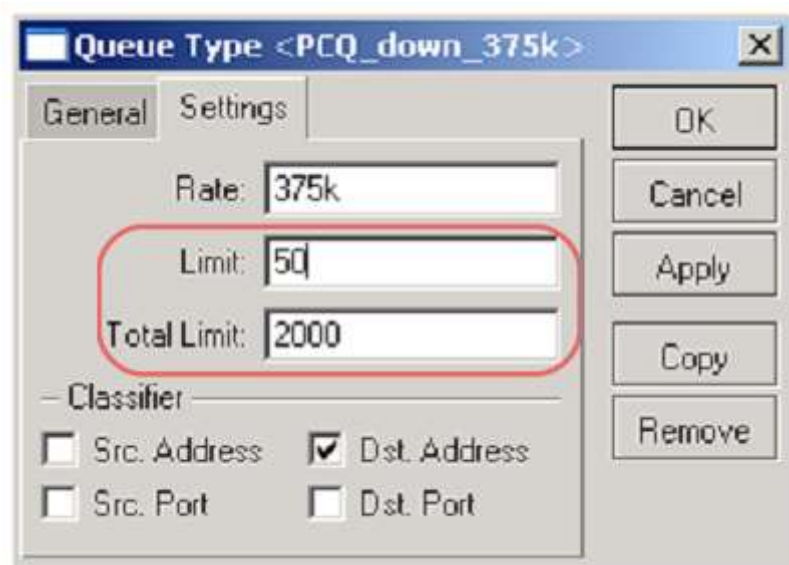
```

/ queue tree
add name="Total_download" parent=local_ether1 packet-mark="" limit-at=0 \
    queue=default priority=1 max-limit=0 burst-limit=0 burst-threshold=0 \
    burst-time=0s disabled=no
add name="basic_client_download" parent=Total_download \
    packet-mark=basic_client_traffic limit-at=0 queue=PCQ_down_375k priority=8 \
    max-limit=0 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
add name="standard_client_download" parent=Total_download \
    packet-mark=standard_client_traffic limit-at=0 queue=PCQ_down_750k \
    priority=4 max-limit=0 burst-limit=0 burst-threshold=0 burst-time=0s \
    disabled=no
add name="business_client_download" parent=Total_download \
    packet-mark=business_client_traffic limit-at=0 queue=default priority=1 \
    max-limit=0 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
add name="Total_upload" parent=public_ether3 packet-mark="" limit-at=0 \
    queue=default priority=8 max-limit=0 burst-limit=0 burst-threshold=0 \
    burst-time=0s disabled=no
add name="basic_client_upload" parent=Total_upload \
    packet-mark=basic_client_traffic limit-at=0 queue=PCQ_up_125k priority=8 \
    max-limit=0 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no
add name="standard_client_upload" parent=Total_upload \
    packet-mark=standard_client_traffic limit-at=0 queue=PCQ_up_250k \
    priority=4 max-limit=0 burst-limit=0 burst-threshold=0 burst-time=0s \
    disabled=no
add name="business_client_upload" parent=Total_upload \
    packet-mark=business_client_traffic limit-at=0 queue=PCQ_up_1M priority=1 \
    max-limit=0 burst-limit=0 burst-threshold=0 burst-time=0s disabled=no

```

PCQ Queue Size

(Размер очереди PCQ)



Total_limit = X может занять до $X \cdot (2000 \text{ bytes} + 200 \text{ bytes})$ of RAM

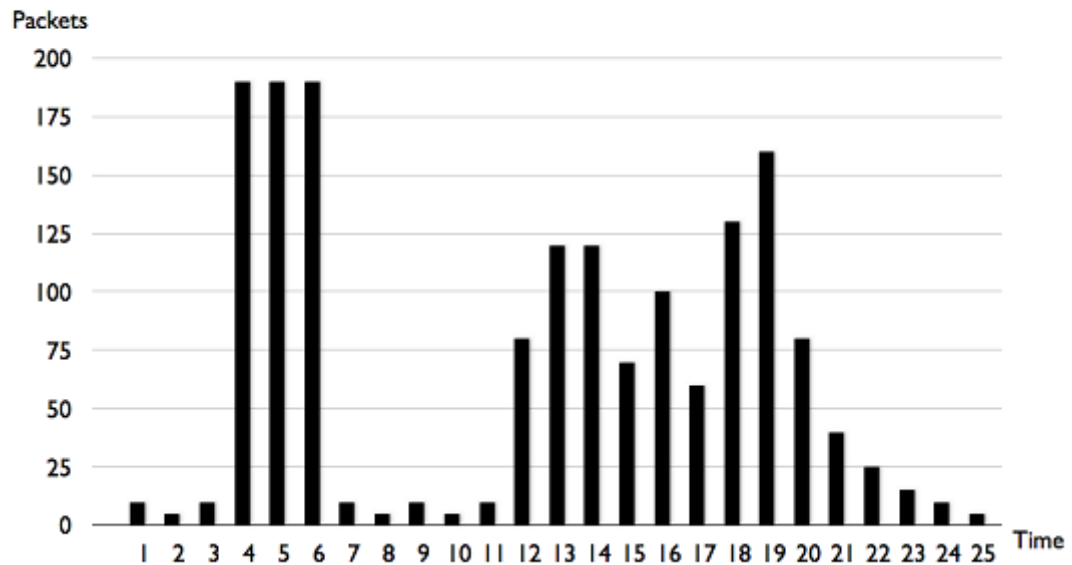
2000 bytes – buffer for 1 packet
200 bytes – service data for 1 packet

total_limit = 2000 =< 4,2MB RAM
total_limit = 5000 =< 10,5MB RAM

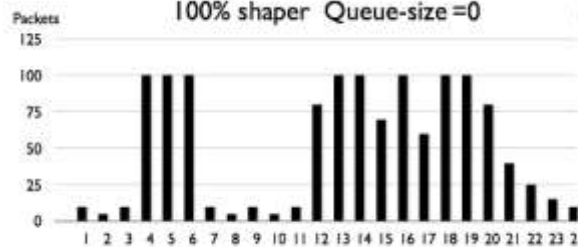
- Это может занять только 40 пользователей для заполнения очереди. (because $\text{total_limit}/\text{limit} = 2000/50 = 40$).
- Это необходимо для повышения "total_limit" и/или уменьшения значения "limit".
- Там должно быть не менее 10-20 пакетов в очереди, доступных для каждого пользователя

Размер очереди

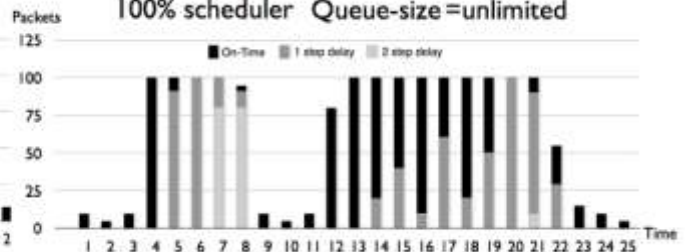
Queue Size



100% shaper Queue-size =0



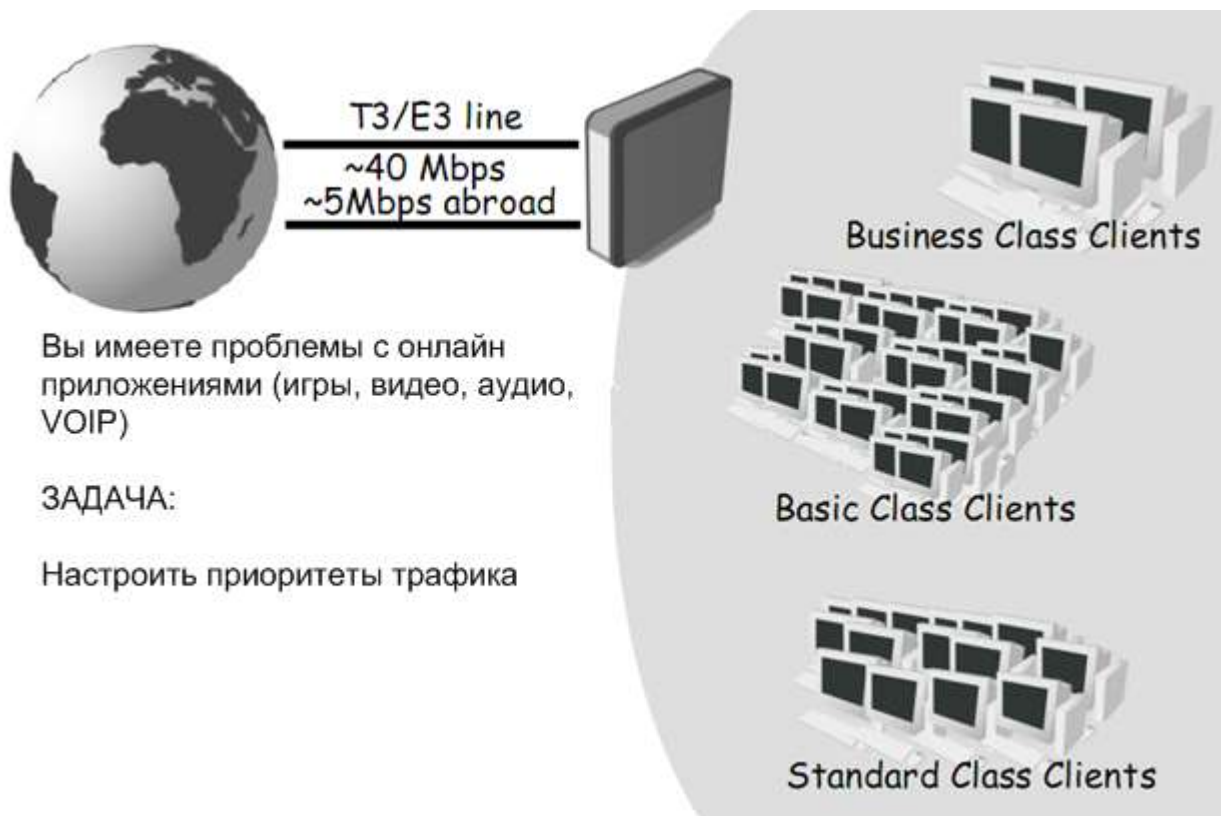
100% scheduler Queue-size =unlimited



Настройка PCQ

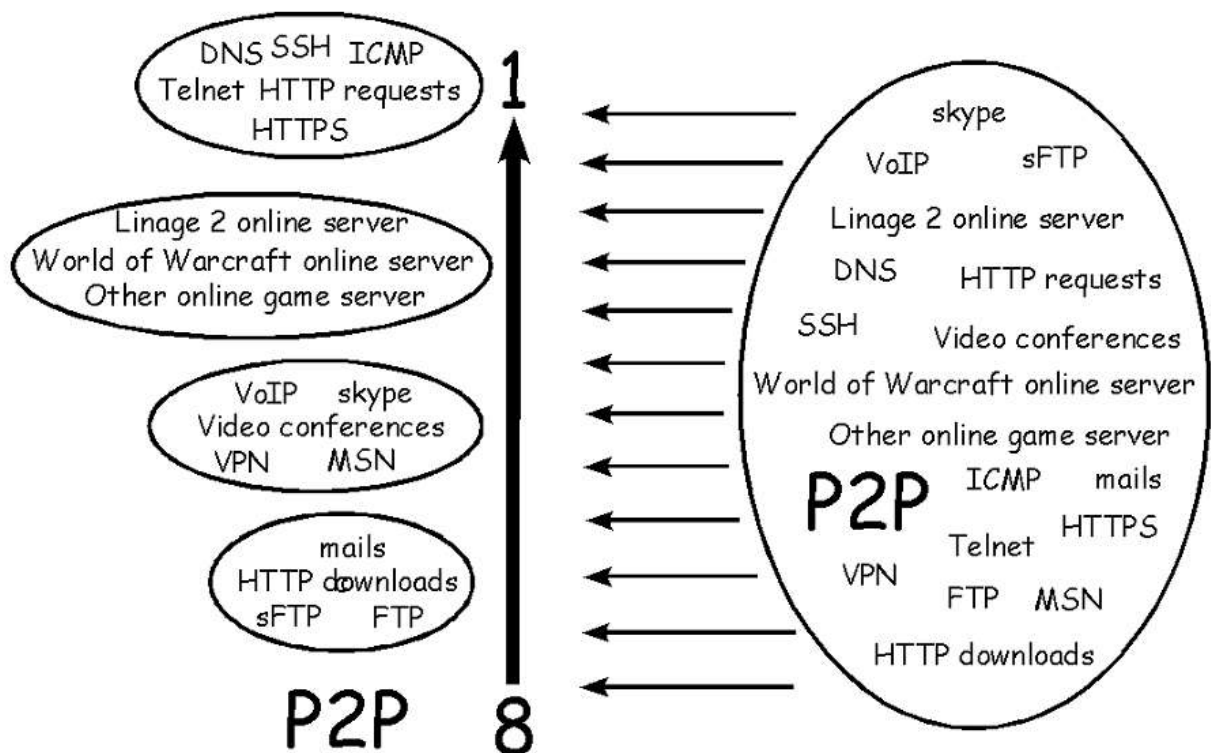
- Есть ~340 клиентов, с тарифом «Базовый», то :
 - `pcq_limit = 40`
 - `pcq_total_limit = 7000` ($\sim 20 \cdot 340$) ($\sim 15\text{MB}$)
- Есть ~40 клиентов, с тарифом «Стандарт», то :
 - `pcq_limit = 30`
 - `pcq_total_limit = 1000` ($\sim 20 \cdot 40$) ($\sim 2\text{MB}$)
- Есть ~20 клиентов, с тарифом «Бизнес», то :
 - `pcq_limit = 20` (!!!)
 - `pcq_total_limit = 500` ($\sim 20 \cdot 20$) ($\sim 1\text{MB}$)

Приоритезация трафика

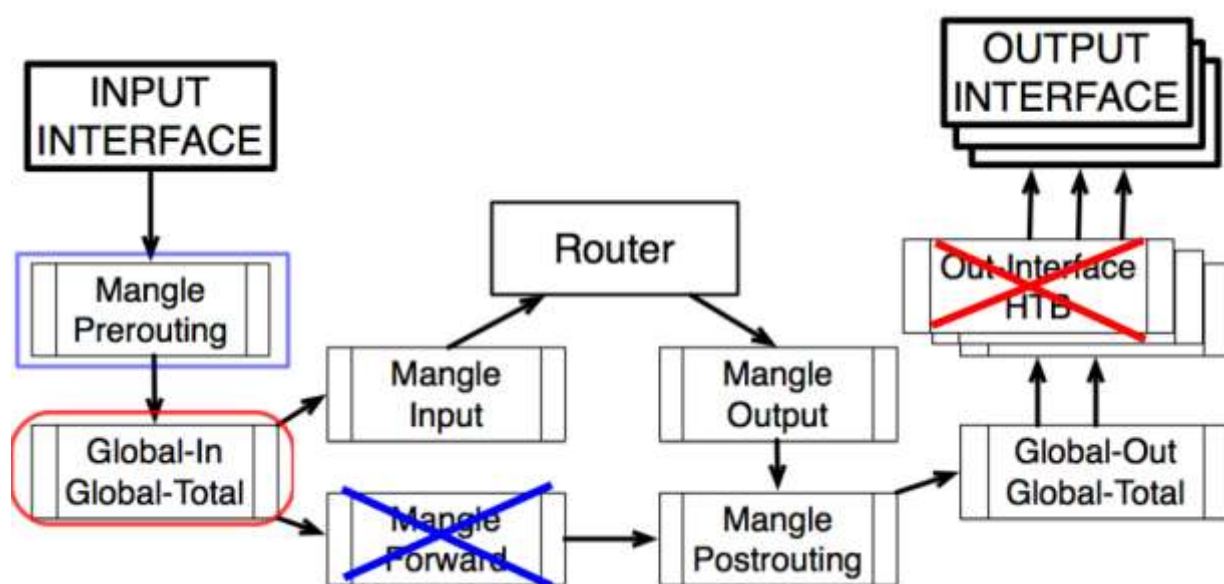


План приоритетов

Prioritization Plan



Где?



Как?

Group	Service	Protocol	Dst-Port	Other conditions
P2P_services	P2P			p2p=all-p2p
Download_services	Mails	TCP	110	
		TCP	995	
		TCP	143	
		TCP	993	
		TCP	25	
	HTTP downloads	TCP	80	Connection-bytes=500000-0
Ensign_services	FTP	TCP	20	
		TCP	21	
	SFTP	TCP	22	Packet-size=1400-1500
	DNS	TCP	53	
		UDP	53	
	ICMP	ICMP	-	
User_requests	HTTPS	TCP	443	
	Telnet	TCP	23	
	SSH	TCP	22	Packet-size=0-1400
	HTTP requests	TCP	80	Connection-bytes=0-500000
Communication_services	Online game servers			Dst-address-list=user_requests
	VoIP			
	Skype			
	Video conferences			
	VPN			
	MSN			

Приоритеты

- Создайте маркировку пакетов в mangle цепочке “Prerouting” для приоритезации трафика в global-in очереди
 - Флагманские сервисы (Priority=1)
 - Пользовательские запросы (Priority=3)
 - Коммуникационные сервисы (Priority=5)
 - Сервисы загрузок (Priority=7)
 - Сервисы P2P (Priority=8)