

MikroTik RouterOS Workshop

QoS Best Practice

Dallas/Fort Worth
MUM USA 2009

Questions and Answers

- Q: Is it possible to prioritize traffic by type for every single client while having strict per-user limitations on the same router?
- A: Yes!

- Q: What will I need to achieve that?
- A: You will need:
 - 1) Packet Flow Diagram
 - 2) HTB (queue tree),
 - 3) Mangle,
 - 4) PCQ,
 - 5) Address List

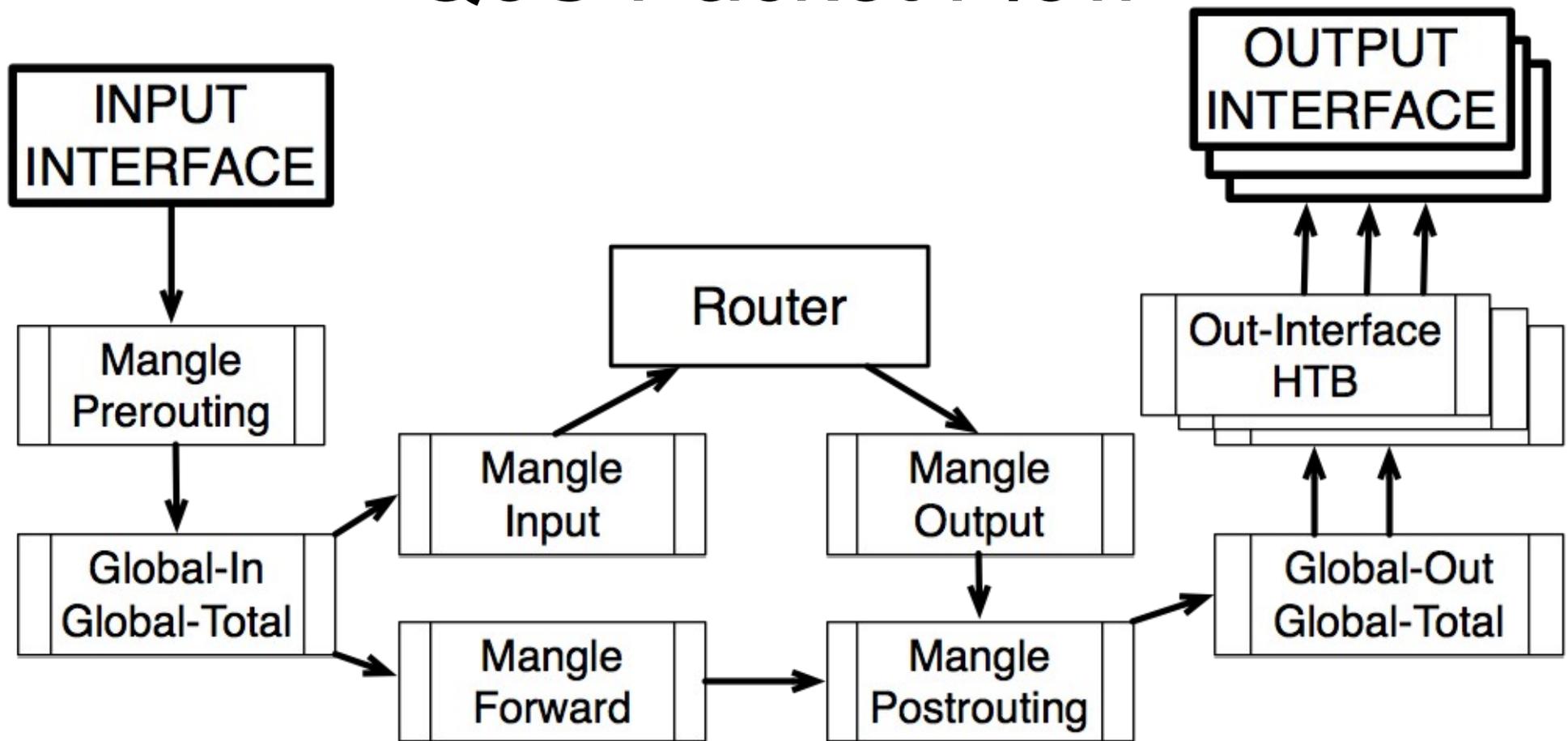
Mangle

- The mangle facility allows you to mark IP packets with special marks.
- These marks are used by other router facilities like routing and bandwidth management to identify the packets.
- Additionally, the mangle facility is used to modify some fields in the IP header, like TOS (DSCP) and TTL fields.

Hierarchical Token Bucket

- All bandwidth management implementation in RouterOS is based on Hierarchical Token Bucket (HTB)
- HTB allows you to create hierarchical queue structure and determine relations between queues
- RouterOS supports 3 virtual HTBs (global-in, global-total, global-out) and one more just before every output interface

QoS Packet Flow



- This diagram is created from RouterOS Packet Flow diagram.

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

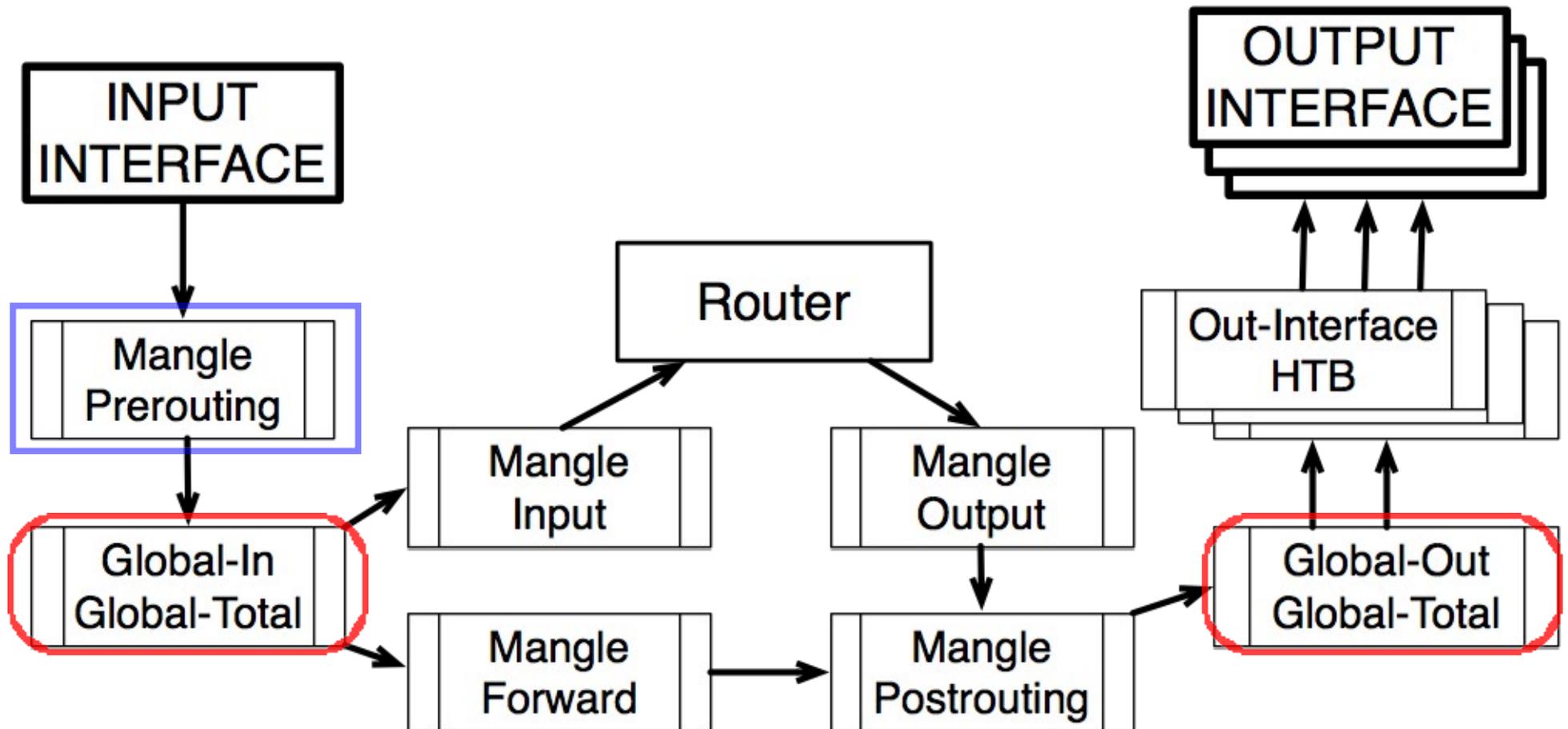
Double QoS

- It is possible to mark and shape traffic twice in the same router:
 - ◆ Mangle chain Prerouting – for first marking
 - ◆ Global-in HTB – for first shaping
 - ◆ Mangle chain Forward or Postrouting for second marking
 - ◆ Global-out or Out-interface HTB for second marking
- Double QoS is only possible with Queue Tree

Why not Simple Queues?

- Simple queues are ordered - similar to firewall rules
 - ◆ In order to get to 999th queue packet will have to be checked for match to all 998 previous queues
- Each simple queue **might** stand for 3 separate queues:
 - ◆ One in Global-in (“direct” part)
 - ◆ One in Global-out (“reverse” part)
 - ◆ One in Global-total (“total” part)

Simple Queues and Mangle



Queue Tree

- Tree queue is one directional only and can be placed in any of the available HTBs
- Queue Tree queues don't have any order – all traffic is processed simultaneously
- All child queues must have packet marks from “/ip firewall mangle” facility assigned to them
- If placed in the same HTB, Simple queue will take all the traffic away from the Queue Tree queue

Global-Out or Interface HTB?

There are two fundamental differences

- In case of SRC-NAT (masquerade) Global-Out will be aware of private client addresses, but Interface HTB will not – Interface HTB is after SRC-NAT
- Each Interface HTB only receives traffic that will be leaving through a particular interface – there is no need for to separate upload and download in mangle

Conclusions

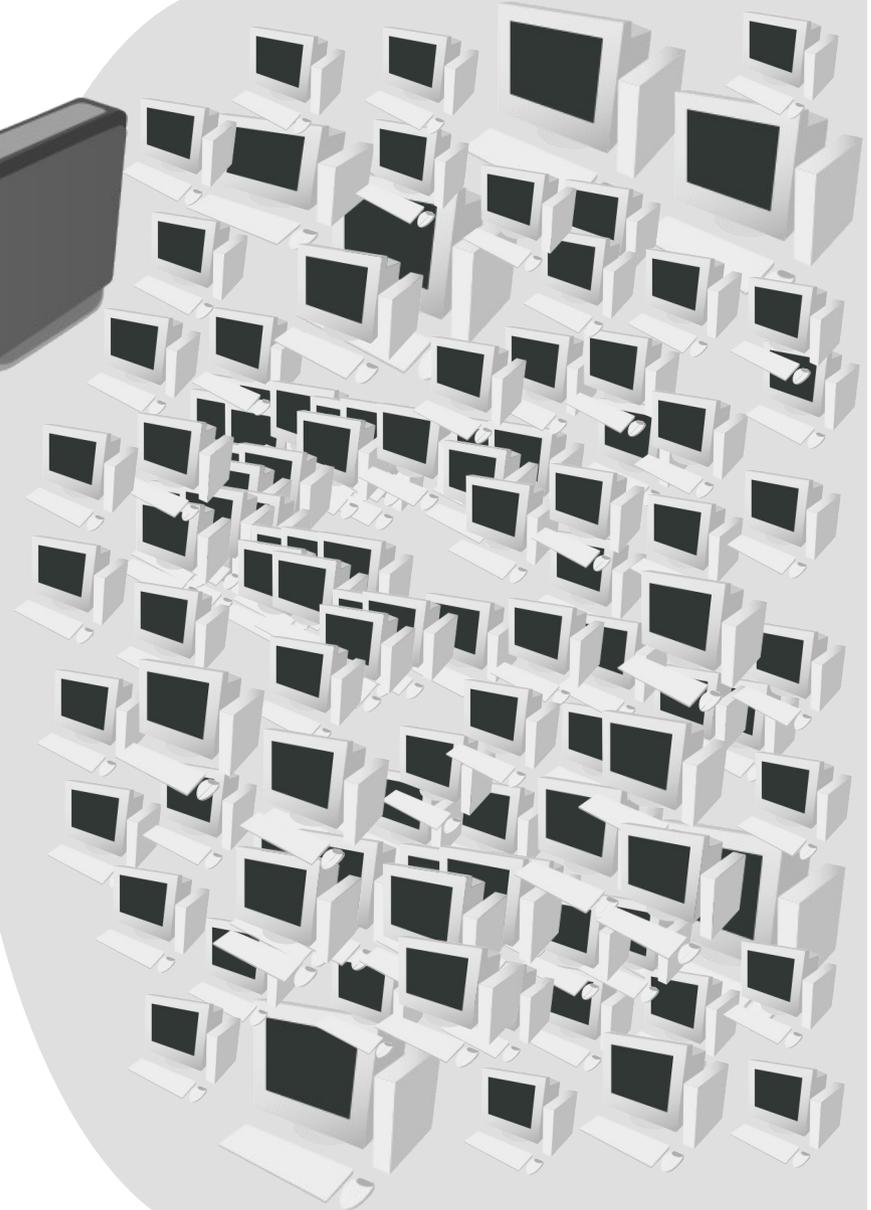
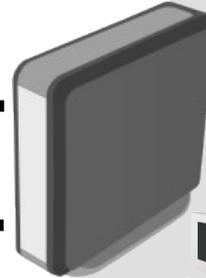
- We will use mangle and queue tree:
 - ◆ Mark traffic by traffic type in mangle chain Prerouting
 - ◆ Prioritize and limit traffic by type in Global-in HTB
 - ◆ Re-Mark traffic by clients in mangle chain Forward
 - ◆ Limit traffic per client in Interface HTB
- It is necessary to keep the amount of mangle rules and queues to a minimum to increase the performance of this configuration.

Client Limitation



T3/E3 line

~40 Mbps



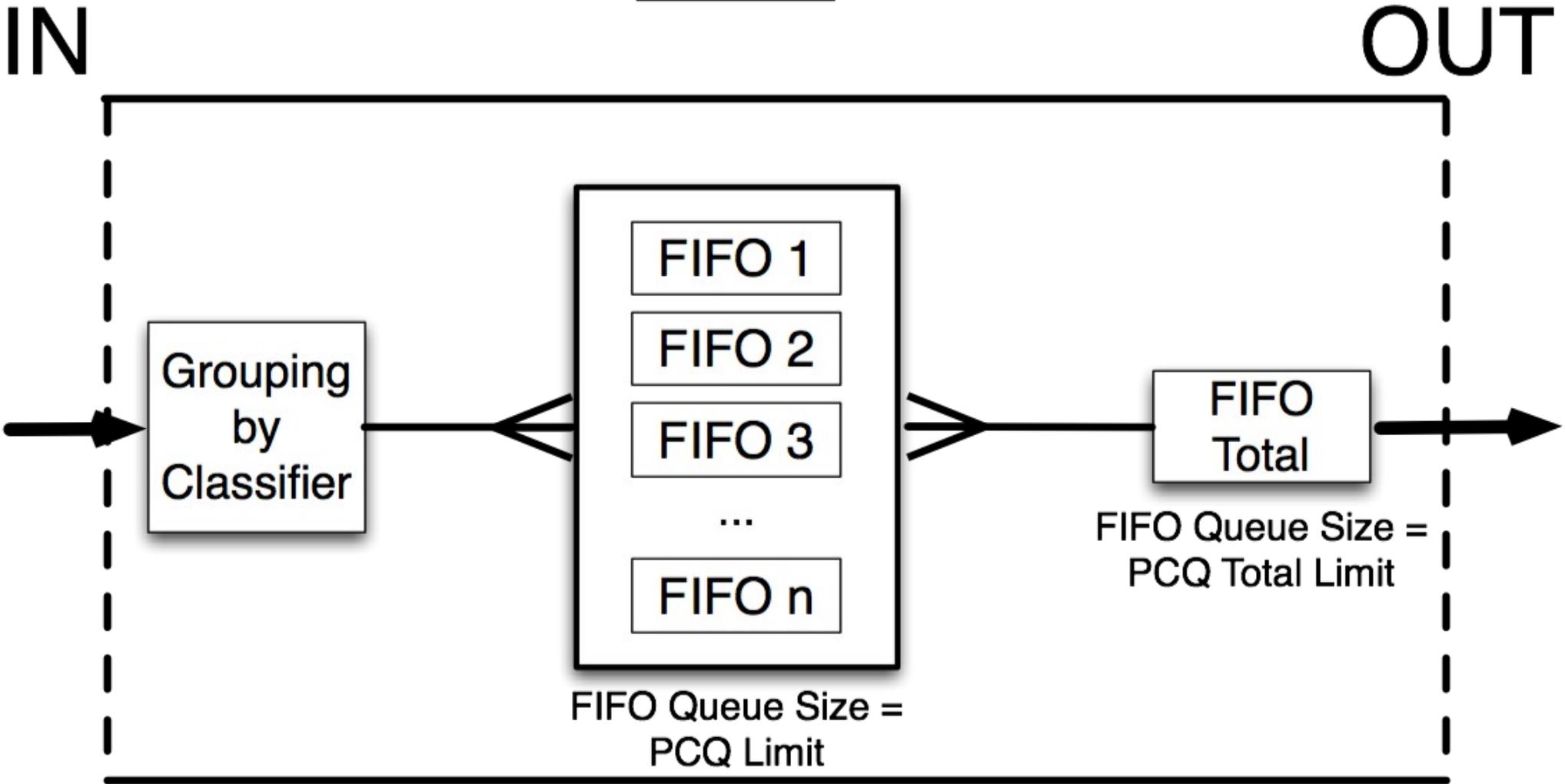
- You have more than 400 clients and 3 different connection types:
 - Business (4Mbps/1Mbps) connection
 - Standard (750kbps/250kbps) connection
 - Basic (375kbps/125kbps) connection

PCQ

- Per Connection Queue is a queue type capable of dividing traffic into sub-streams based on selected classifiers
- Each sub-stream will then go through FIFO queue with queue size specified by “pcq-limit” option and maximal rate specified by “pcq-rate” option

The screenshot shows the 'New Queue Type' configuration window. The 'Type Name' is 'queue1', the 'Kind' is 'pcq', the 'Rate' is '0', the 'Limit' is '50', and the 'Total Limit' is '2000'. Under the 'Classifier' section, the 'Dst. Address' checkbox is checked, while 'Src. Address', 'Src. Port', and 'Dst. Port' are unchecked.

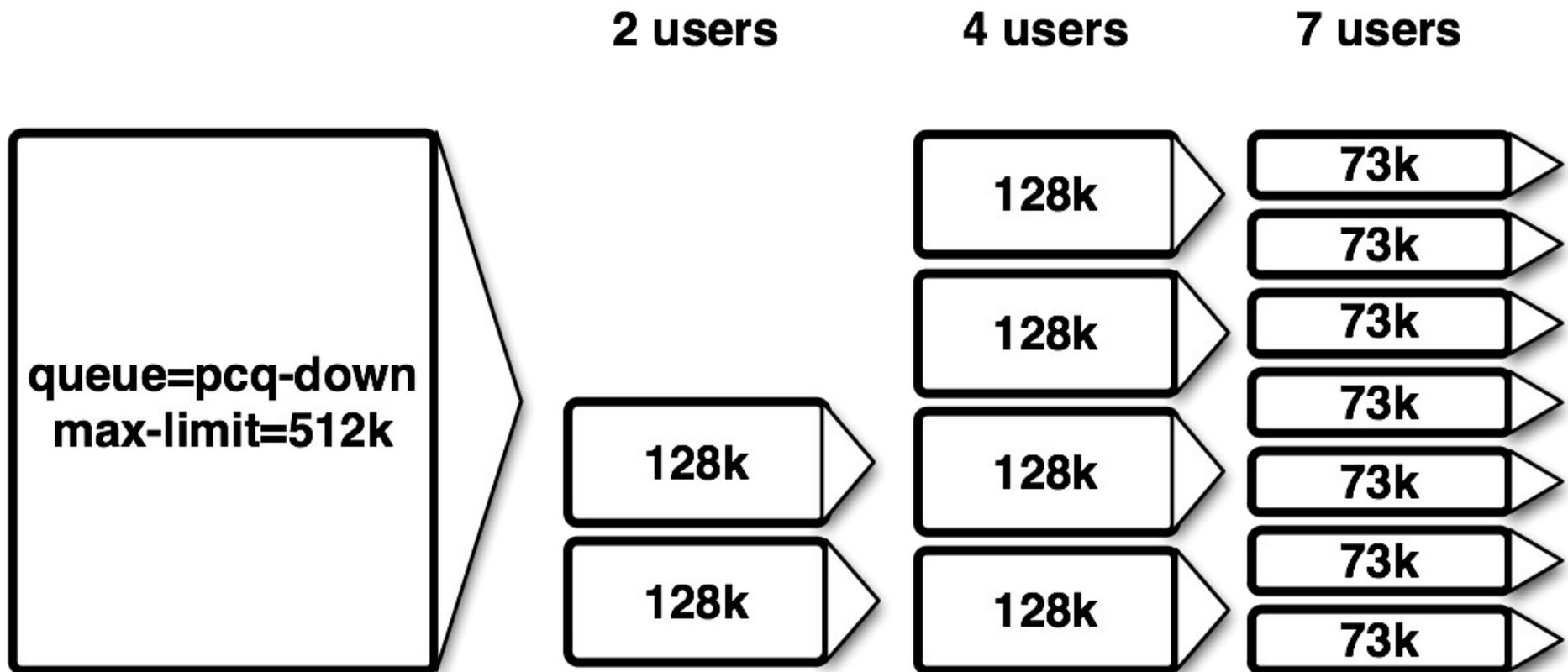
PCQ



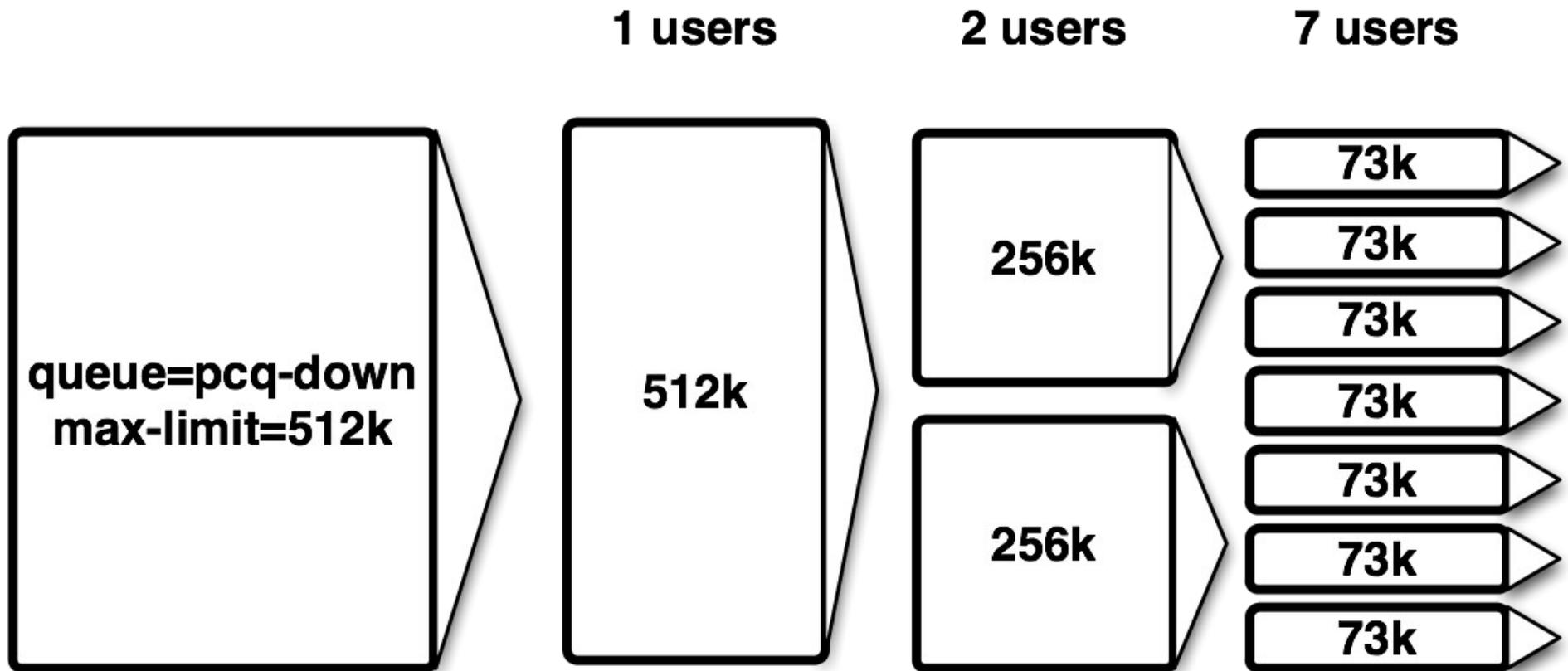
PCQ Part 2

- In order to ensure that each PCQ sub-stream represents one particular client we need to create 2 different PCQ types:
 - ◆ PCQ_upload – source address as classifier
 - ◆ PCQ_download - destination address as classifier
- PCQ will distribute available traffic equally between sub-queues until the pcq-rate is reached (if it is specified)

pcq-rate=128000



pcq-rate=0



PCQ Types – Winbox View

The image shows the Mikrotik Winbox interface for configuring PCQ types. The main window is titled "Queue List" and has four tabs: "Simple Queues", "Interface Queues", "Queue Tree", and "Queue Types". The "Queue Types" tab is active and contains a table of queue types. Two entries, "PCQ_down_4M" and "PCQ_up_1M", are circled in red. Red arrows point from these entries to two separate "Queue Type" configuration dialog boxes. The top dialog box is for "PCQ_down_4M" and the bottom one is for "PCQ_up_1M". Both dialog boxes have "General" and "Settings" tabs. The "Settings" tab is active in both. In the "PCQ_down_4M" dialog, the "Rate" field is set to "4M" and the "Dst. Address" checkbox is checked. In the "PCQ_up_1M" dialog, the "Rate" field is set to "1M" and the "Src. Address" checkbox is checked. Other fields include "Limit" (50) and "Total Limit" (2000). The "Classifier" section has checkboxes for "Src. Address", "Dst. Address", "Src. Port", and "Dst. Port".

Type Name	Kind
PCQ_down_375k	pcq
PCQ_down_4M	pcq
PCQ_down_750k	pcq
PCQ_up_125k	pcq
PCQ_up_1M	pcq
PCQ_up_250k	pcq
default	pfifo
default-small	pfifo
ethernet-default	pfifo
hotspot-default	sfq
sfq	sfq
synchronous-default	red

Queue Type <PCQ_down_4M> Settings

- Rate: 4M
- Limit: 50
- Total Limit: 2000
- Classifier:
 - Src. Address
 - Dst. Address
 - Src. Port
 - Dst. Port

Queue Type <PCQ_up_1M> Settings

- Rate: 1M
- Limit: 50
- Total Limit: 2000
- Classifier:
 - Src. Address
 - Dst. Address
 - Src. Port
 - Dst. Port

Address Lists

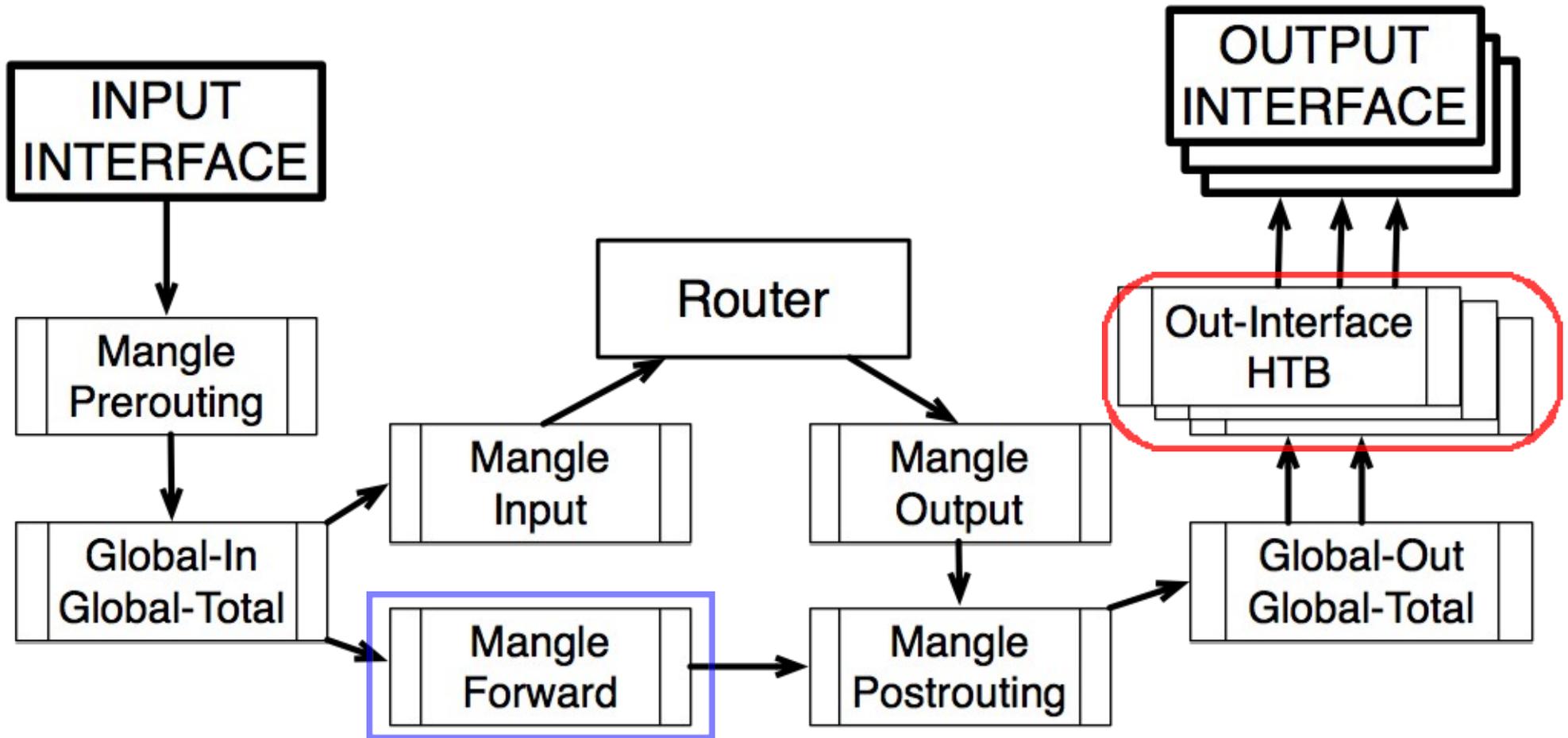
- Address lists was introduced to assign multiple IP addresses/ranges to the same firewall rule, in this way reducing the total number of firewall rules and increasing router performance
- Address lists can be created:
 - ◆ Manually
 - ◆ Automatically from PPP profile – just specify address-list option and as soon as the client connects it will be added to the proper address list
 - ◆ Automatically from RADIUS – attribute “Mikrotik:19”

Address Lists

The screenshot shows the Mikrotik WinBox interface. On the left is a vertical menu with 'RouterOS WinBox' written vertically. The 'IP' menu item is highlighted with a red box, and its sub-menu 'Firewall' is also highlighted with a red box. A red arrow points from the 'Firewall' sub-menu to the 'Firewall' configuration window. The 'Firewall' window has several tabs: 'Filter Rules', 'NAT', 'Mangle', 'Service Ports', 'Connections', and 'Address Lists'. The 'Address Lists' tab is selected and highlighted with a red box. Below the tabs is a table of address lists. A red arrow points from the 'Address Lists' tab to the table. Another red arrow points from the 'Address Lists' tab to a 'Firewall Address List' dialog box. The dialog box has a 'Name' field set to 'Business_class_client' and an 'Address' field set to '23.1.101.224'. The dialog box also has buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. The table in the 'Firewall' window contains the following data:

Name	Address
Basic_class_client	23.1.100.1
Standard_class_client	23.1.100.2
Basic_class_client	23.1.100.3
Standard_class_client	23.1.100.4
Basic_class_client	23.1.100.5
Business_class_client	23.1.100.6
Basic_class_client	23.1.100.7
Basic_class_client	23.1.100.8
Standard_class_client	23.1.100.9
Standard_class_client	23.1.100.10
Standard_class_client	23.1.100.11
Basic_class_client	23.1.100.12
Basic_class_client	23.1.100.13
Basic_class_client	23.1.100.14
Basic_class_client	23.1.100.15
Basic_class_client	23.1.100.16
Business_class_client	23.1.100.17
Basic_class_client	23.1.100.18
Standard_class_client	23.1.100.19
Basic_class_client	23.1.100.20

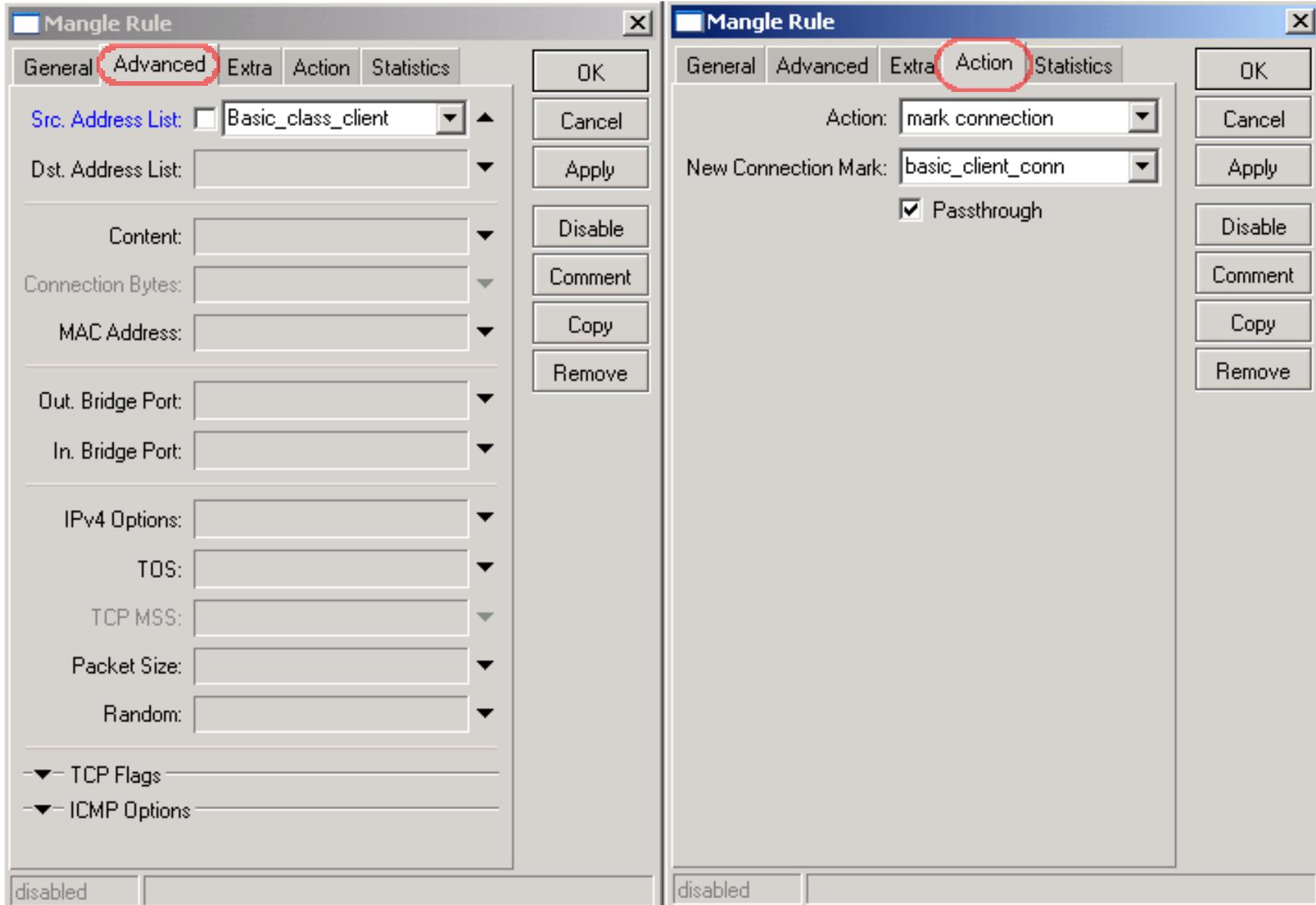
Where?



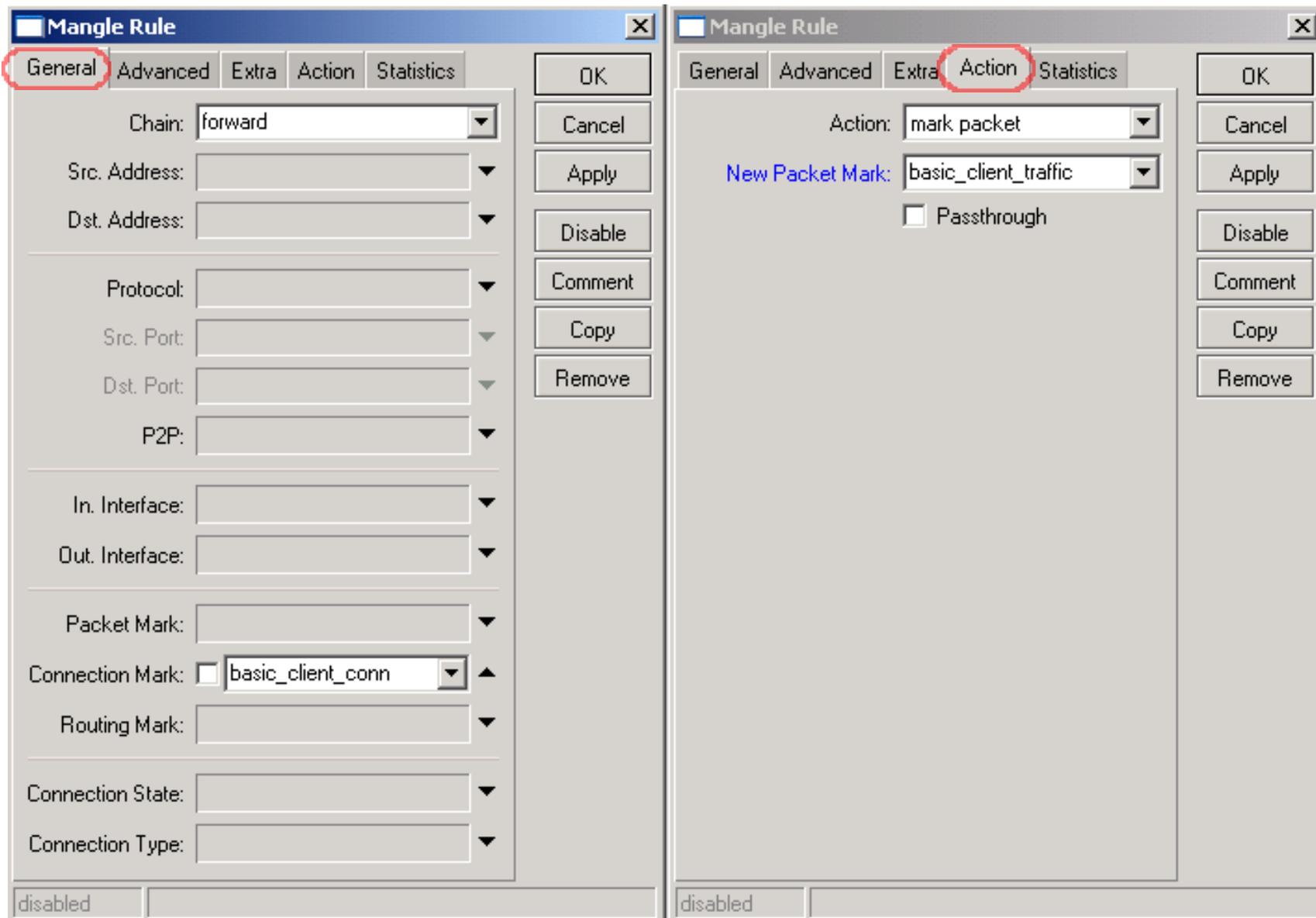
Packet Marking

- Use “connection-mark” action to classify all connections based on client address list
- Use “packet-mark” action to classify all traffic based on connection marks
- Questions to think about:
 - ◆ What speed should be available for Business client if downloading from basic client?
 - ◆ Do you still have unmarked traffic?

Connection-mark rule



Packet-mark rule



Working Mangle- Winbox view

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists

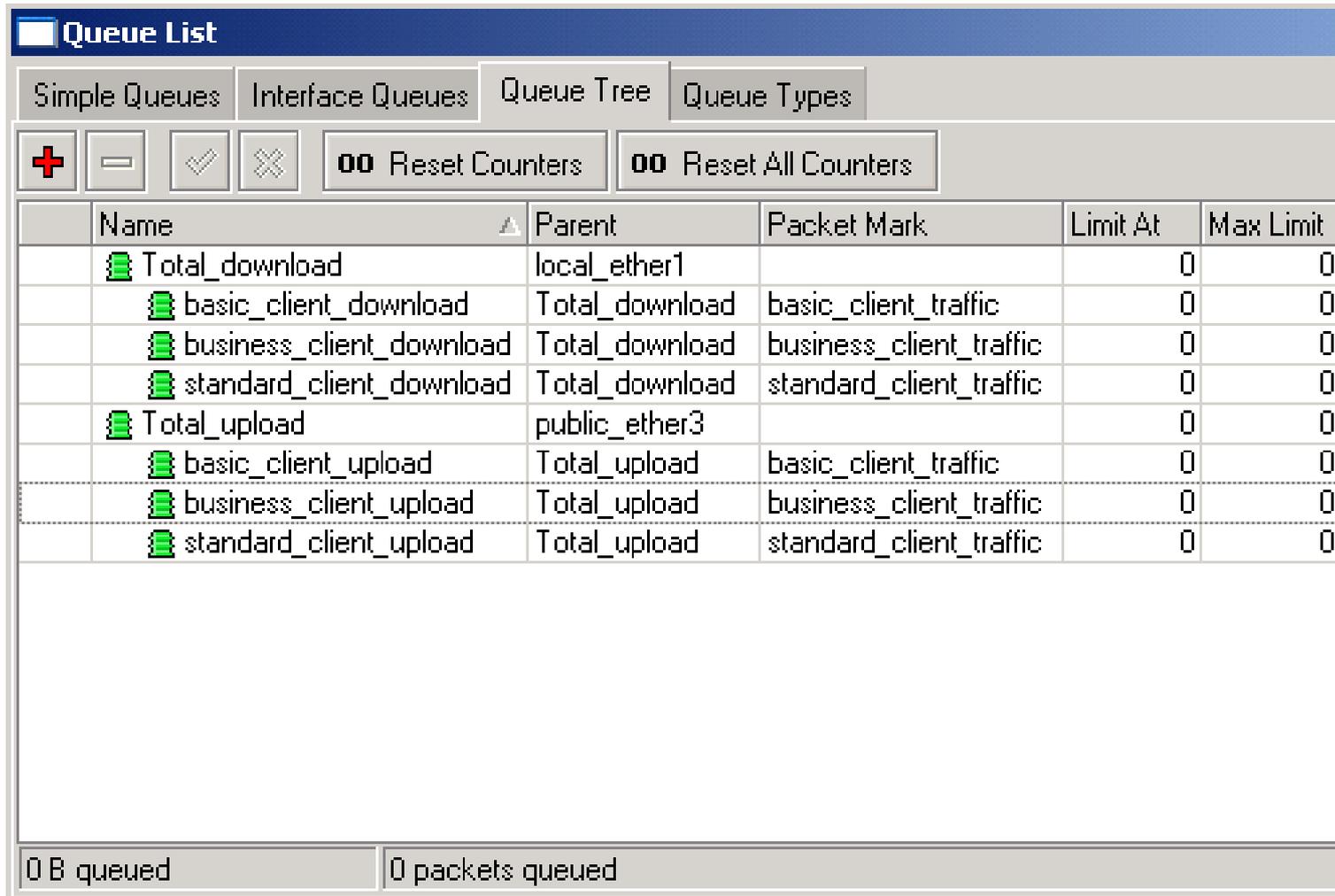
forward ▾

#	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 bussiness 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

Working Mangle- Export view

```
/ 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
```

Queue Tree – Winbox View



The screenshot shows the 'Queue List' window in Winbox. The window has a title bar 'Queue List' and a menu bar with 'Simple Queues', 'Interface Queues', 'Queue Tree', and 'Queue Types'. Below the menu bar are several buttons: a red plus sign, a minus sign, a checkmark, a cross, 'Reset Counters', and 'Reset All Counters'. The main area contains a table with the following columns: Name, Parent, Packet Mark, Limit At, and Max Limit. The table lists several queues, including 'Total_download' and 'Total_upload', each with its own sub-queues. At the bottom of the window, there are two status boxes: '0 B queued' and '0 packets queued'.

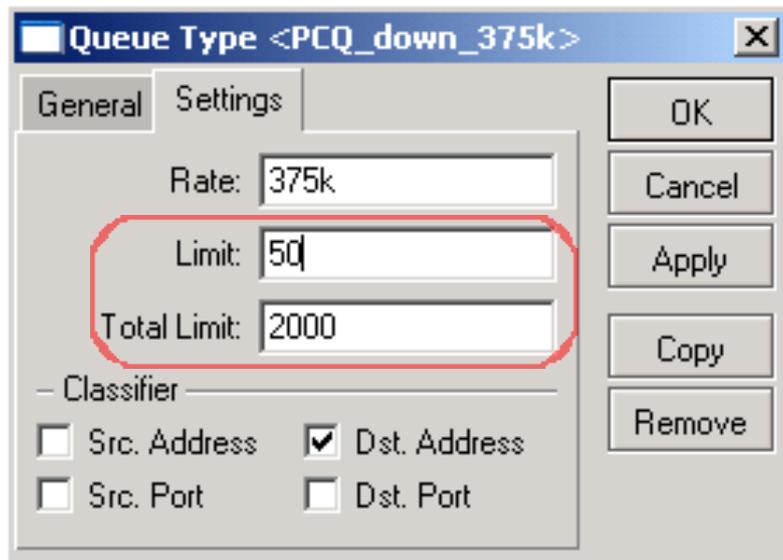
Name	Parent	Packet Mark	Limit At	Max Limit
Total_download	local_ether1		0	0
basic_client_download	Total_download	basic_client_traffic	0	0
business_client_download	Total_download	business_client_traffic	0	0
standard_client_download	Total_download	standard_client_traffic	0	0
Total_upload	public_ether3		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

0 B queued 0 packets queued

Queue Tree – Export View

```
/ 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



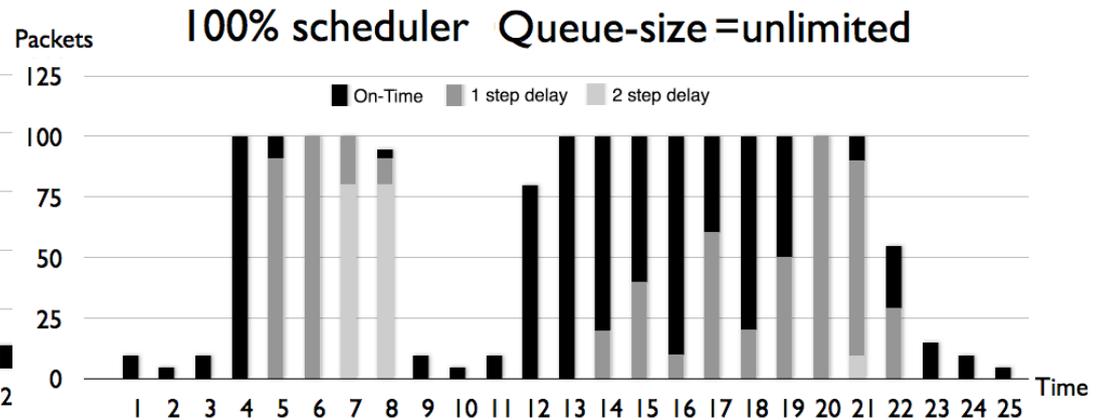
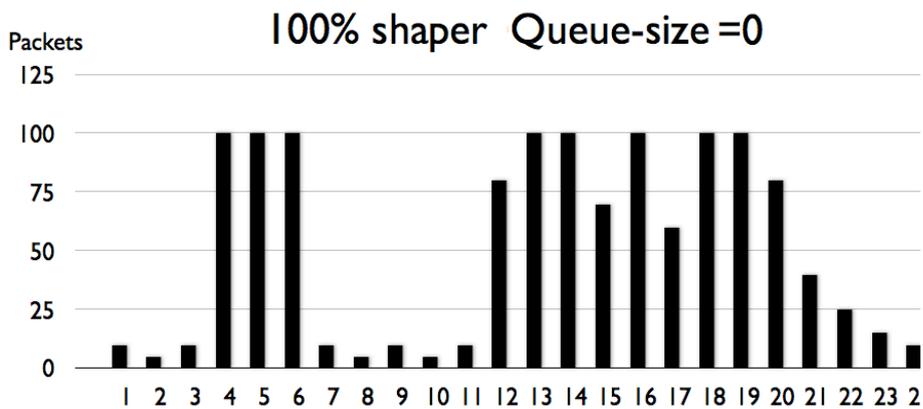
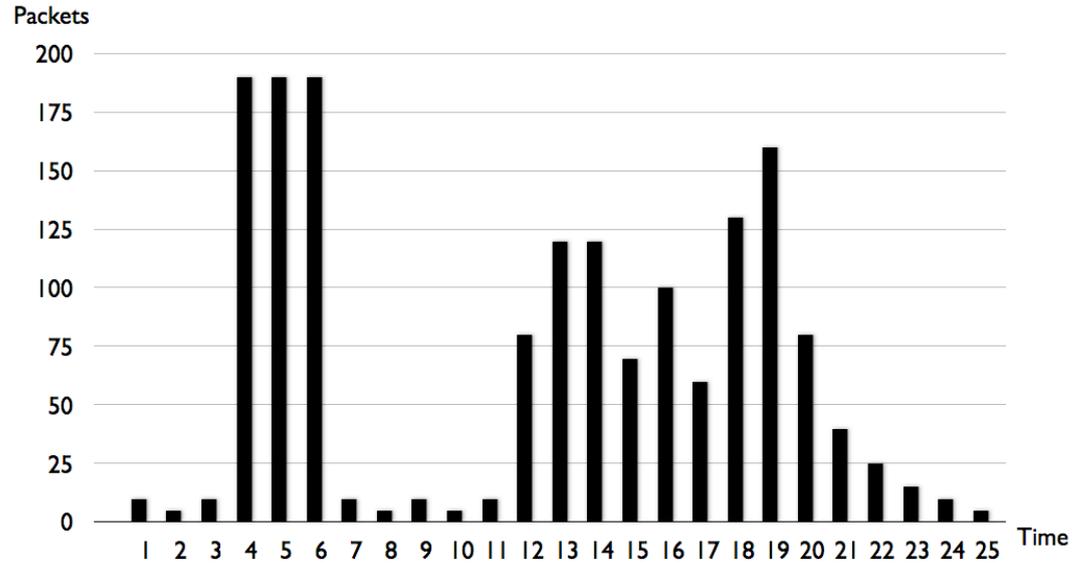
Total_limit = X can take up to
 $X \times (2000 \text{ bytes} + 200 \text{ bytes})$ of RAM

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

- It can take only 40 users to fill the queue
(because $\text{total_limit}/\text{limit} = 2000/50 = 40$)
- It is necessary to increase “total_limit” and/or decrease the “limit” value
- There should be at least 10-20 packet places in queue available per user

Queue Size



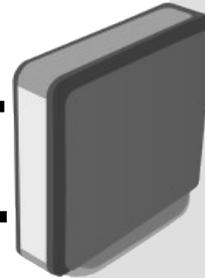
PCQ Adjustments

- There are ~340 Basic class clients so:
 - ➔ $pcq_limit = 40$
 - ➔ $pcq_total_limit = 7000$ ($\sim 20 * 340$) (~15MB)
- There are ~40 Standard class clients so:
 - ➔ $pcq_limit = 30$
 - ➔ $pcq_total_limit = 1000$ ($\sim 20 * 40$) (~2MB)
- There are ~20 Business class clients so:
 - ➔ $pcq_limit = 20$ (!!!)
 - ➔ $pcq_total_limit = 500$ ($\sim 20 * 20$) (~1MB)

Traffic Prioritization



T3/E3 line
~40 Mbps
~5Mbps abroad



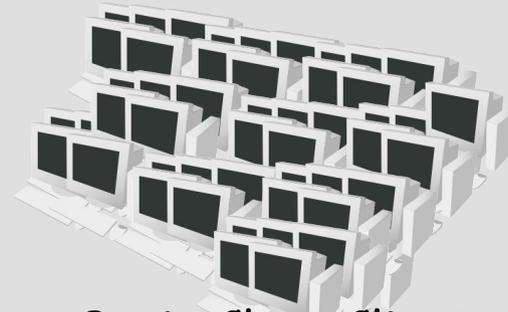
You have problems with on-line communications (video, audio, VOIP, games)

Task:

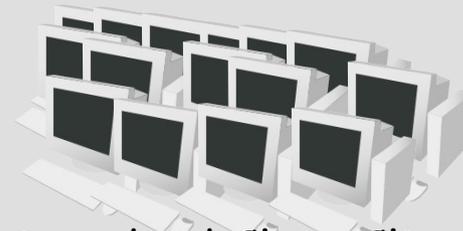
Prioritize the traffic



Business Class Clients

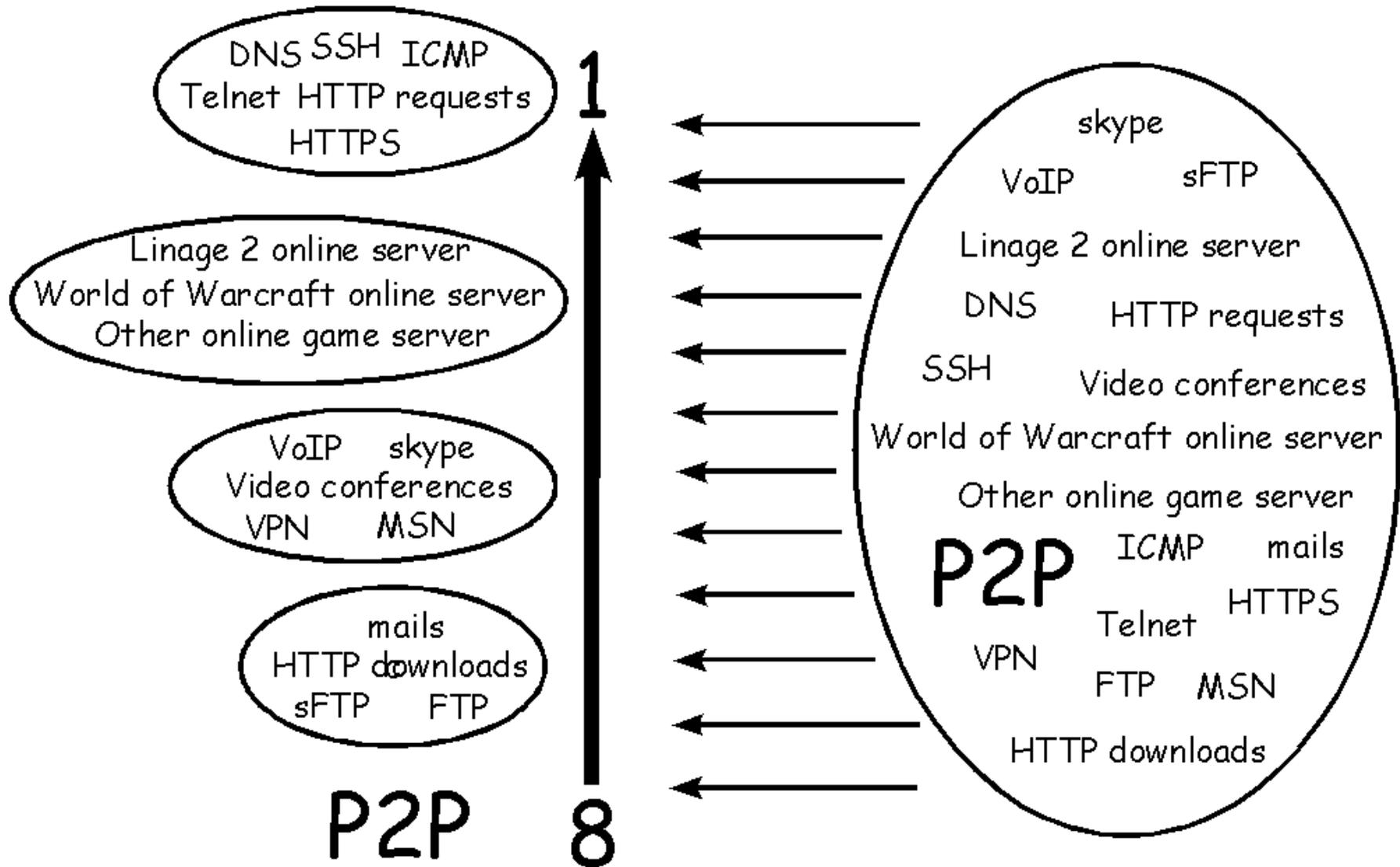


Basic Class Clients

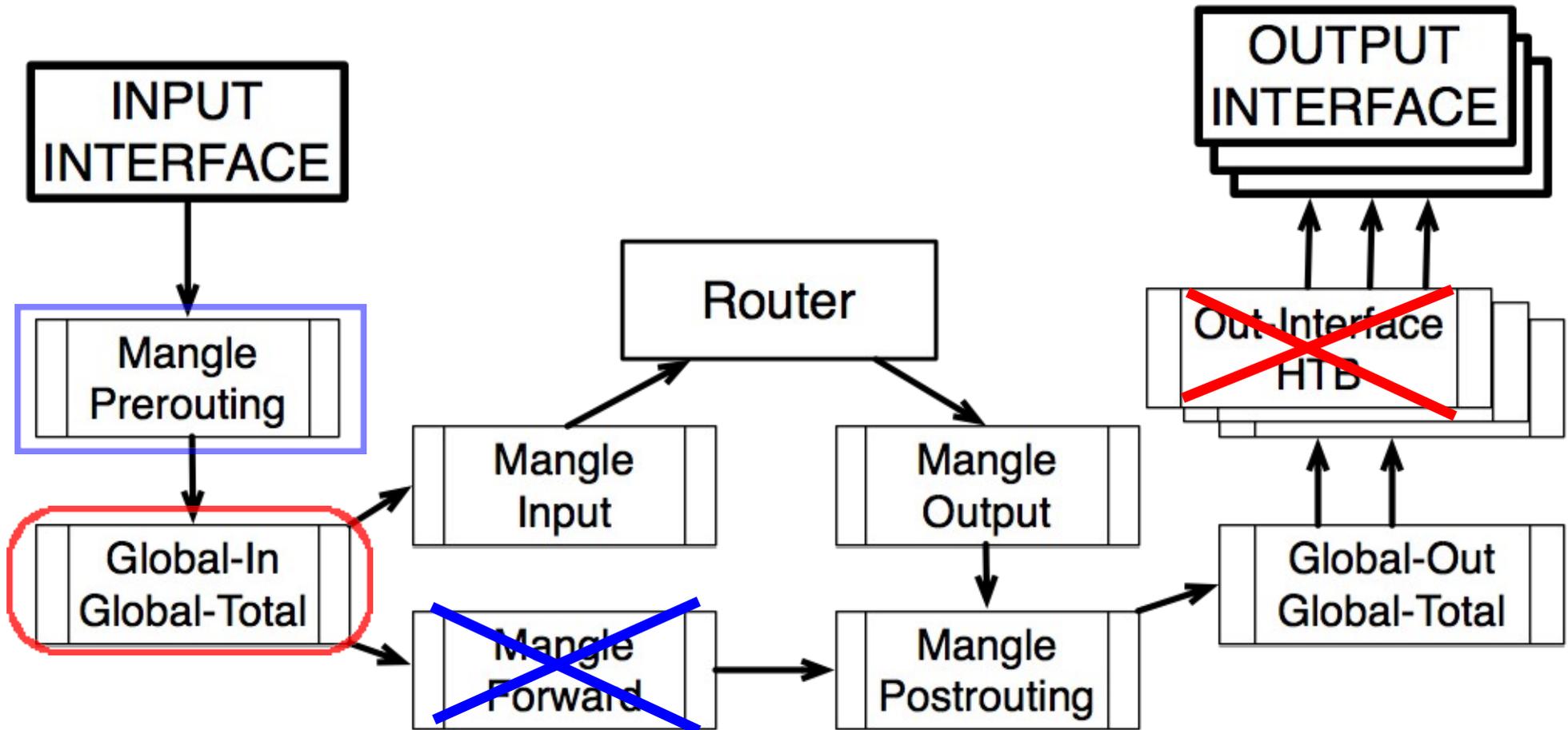


Standard Class Clients

Prioritization Plan



Where?



How?

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
	FTP	TCP	20	
		TCP	21	
	SFTP	TCP	22	Packet-size=1400-1500
Ensign_services	DNS	TCP	53	
		UDP	53	
	ICMP	ICMP	-	
	HTTPS	TCP	443	
	Telnet	TCP	23	
	SSH	TCP	22	Packet-size=0-1400
	HTTP requests	TCP	80	Connection-bytes=0-500000
User_requests	Online game servers			Dst-address-list=user_requests
Communication_services	VoIP			
	Skype			
	Video conferences			
	VPN			
	MSN			

Priorities

- Create packet marks in the mangle chain “Prerouting” for traffic prioritization in the global-in queue
 - ◆ Ensign_services (Priority=1)
 - ◆ User_requests (Priority=3)
 - ◆ Communication_services (Priority=5)
 - ◆ Download_services (Priority=7)
 - ◆ P2P_services (Priority=8)