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 $999^{th}$ 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

INPUT INTERFACE

Mangle Prerouting

Global-In
Global-Total

Mangle Input
Mangle Forward

Router

Mangle Output
Mangle Postrouting

Out-Interface
HTB

OUTPUT INTERFACE

Global-Out
Global-Total

© MikroTik 2009
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

- 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.
PCQ

IN

Grouping by Classifier

FIFO 1
FIFO 2
FIFO 3
...
FIFO n

FIFO Queue Size = PCQ Total Limit

FIFO Total

FIFO Queue Size = PCQ Limit

OUT
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

queue=pcq-down
max-limit=512k

2 users
128k
128k

4 users
128k
128k
128k
128k

7 users
128k
128k
128k
73k
73k
73k
73k
73k
73k
73k
73k
pcq-rate=0

queue=pcq-down
max-limit=512k

1 users
256k

2 users
256k

7 users
73k
73k
73k
73k
73k
73k
PCQ Types – Winbox View
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

[Diagram of a network configuration interface highlighting the 'Address Lists' section and a list of addresses with names and corresponding IP addresses]
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

<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Chain</th>
<th>New Packet Mark</th>
<th>New Connection Mark</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>mark basic client traffic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mark connection</td>
<td>forward</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mark packet</td>
<td>forward</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>mark standard client traffic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mark connection</td>
<td>forward</td>
<td></td>
<td></td>
<td>825.4 MiB</td>
<td>2 747 515</td>
</tr>
<tr>
<td></td>
<td>mark packet</td>
<td>forward</td>
<td>standard_client_traffic</td>
<td></td>
<td>6396.7 MiB</td>
<td>7 248 925</td>
</tr>
<tr>
<td>...</td>
<td>mark business client traffic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mark connection</td>
<td>forward</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mark packet</td>
<td>forward</td>
<td>business_client_traffic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>Check for unmarked traffic</td>
<td></td>
<td></td>
<td></td>
<td>2062.0 KiB</td>
<td>9 014</td>
</tr>
</tbody>
</table>
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 business 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Parent</th>
<th>Packet Mark</th>
<th>Limit At</th>
<th>Max Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total_download</td>
<td>local_ether1</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>basic_client_download</td>
<td>Total_download</td>
<td>basic_client_traffic</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>business_client_download</td>
<td>Total_download</td>
<td>business_client_traffic</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>standard_client_download</td>
<td>Total_download</td>
<td>standard_client_traffic</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total_upload</td>
<td>public_ether3</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>basic_client_upload</td>
<td>Total_upload</td>
<td>basic_client_traffic</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>business_client_upload</td>
<td>Total_upload</td>
<td>business_client_traffic</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>standard_client_upload</td>
<td>Total_upload</td>
<td>standard_client_traffic</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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*(2000 bytes + 200 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 total_limit/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

100% shaper   Queue-size = 0

100% scheduler   Queue-size = unlimited
PCQ Adjustments

- There are ~340 Basic class clients so:
  - pcq_limit = 40
  - pcq_total_limit = 7000 (~20*340) (~15MB)

- There are ~40 Standard class clients so:
  - pcq_limit = 30
  - pcq_total_limit = 1000 (~20*40) (~2MB)

- There are ~20 Business class clients so:
  - pcq_limit = 20 (!!!)
  - pcq_total_limit = 500 (~20*20) (~1MB)
Traffic Prioritization

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

**Task:** Prioritize the traffic
Prioritization Plan

DNS SSH ICMP
Telnet HTTP requests
HTTPS

Linage 2 online server
World of Warcraft online server
Other online game server

Voice over IP (VoIP) skype
Video conferences
VPN MSN

mails
HTTP downloads
sFTP FTP

Peer-to-Peer (P2P)

skype
VoIP sFTP
Linage 2 online server
DNS HTTP requests
SSH Video conferences
World of Warcraft online server
Other online game server

ICMP mails
VPN Telnet HTTPS
FTP MSN
HTTP downloads

© MikroTik 2009
Where?
## How?

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