



Балансировка каналов доступа в сеть
интернет для средних и малых предприятий
на примере PCC (Per Connection Classifier)



О себе (нас)

Павел Нагобидянс
Компания «SUPCORE»
Системный администратор

MTCNA
MTCRE
dCAA

mail.: npg@supcore.ru
mob.: +7 (914) 707 23 32



Зачем это?

- 1 - Работа 90% компаний зависит от доступа в сеть интернет
- 2 - Ни один провайдер не гарантирует 100% доступность канала
- 3 - Не рационально когда второй канал простаивает
- 4 - Иногда одного канала не достаточно для нужд компании

Почему MikroTik и PCC?

MikroTik:

- 1 - Доступность оборудования
- 2 - Ассортимент
- 3 - Русско говорящая техподдержка
- 4 - Гибкая настройка

PCC (Per Connection Classifier):

- 1 - Простота настройки
- 2 - Понятность работы
- 3 - Отсутствие скриптов
- 4 - Масштабируемость

Как можно реализовать на оборудовании MikroTik?

~~1 - Distance~~

2 - ECMP (Equal cost multi-path routing)

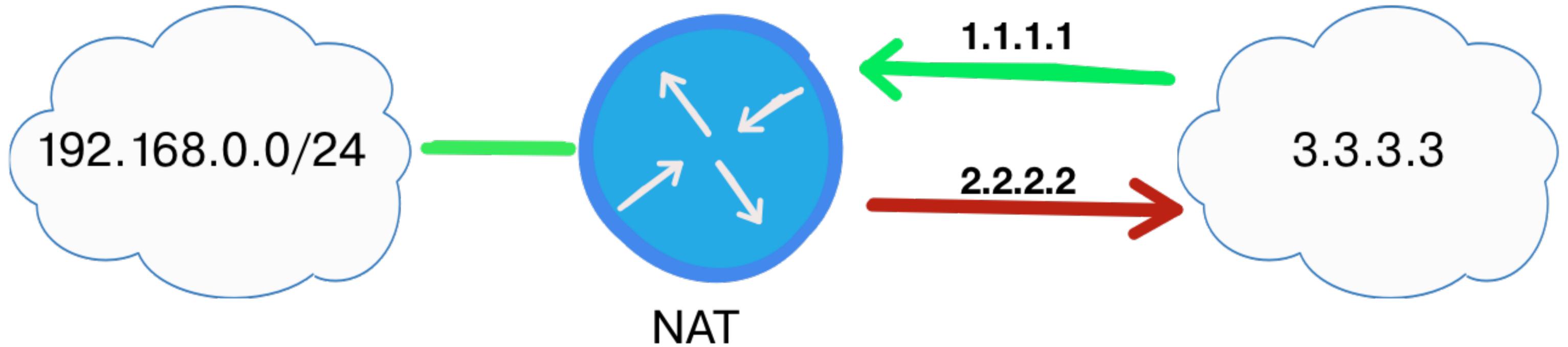
3 - PBR (Policy Based Routing)

4 - PCC (Per Connection Classifier)

Прежде чем начать

- 1 - Мы распределяем соединения, а не пакеты
- 2 - Нам не стоит использовать DNS провайдера
- 3 - Мы должны учитывать наличие NAT

NAT и несколько внешних каналов



Для работы с маршрутизатором извне

1 - Маркируем входящее подключение (connection-mark) в цепочке input

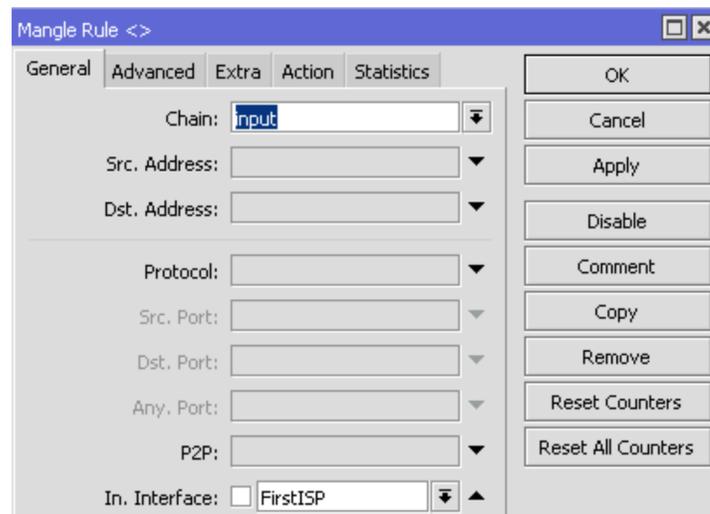
2 - На основании connection-mark маркируем маршрут (mark-routing) в цепочке output

Пример маркировки

CLI:

```
[admin@MUM] /ip firewall mangle> print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=input action=mark-connection new-connection-mark=connections-FirstISP passthrough=yes in-interface=FirstISP log=no log-prefix=""
1 chain=output action=mark-routing new-routing-mark=route-FirstISP passthrough=no connection-mark=connections-FirstISP log=no log-prefix=""
```

WinBox:



Mangle Rule <>

General | Advanced | Extra | Action | Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

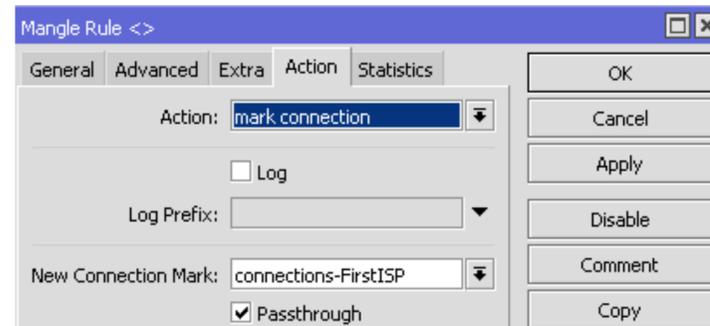
Dst. Port:

Any. Port:

P2P:

In. Interface: FirstISP

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters



Mangle Rule <>

General | Advanced | Extra | Action | Statistics

Action:

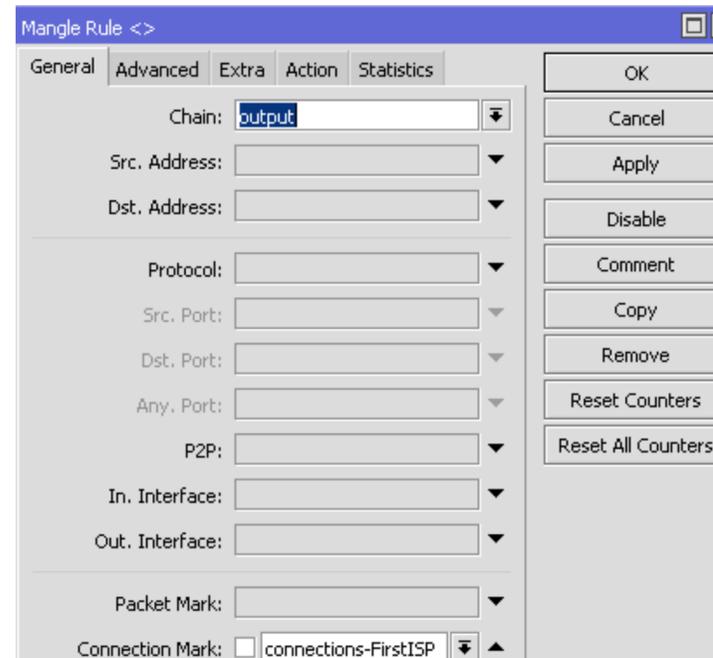
Log

Log Prefix:

New Connection Mark:

Passthrough

Buttons: OK, Cancel, Apply, Disable, Comment, Copy



Mangle Rule <>

General | Advanced | Extra | Action | Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

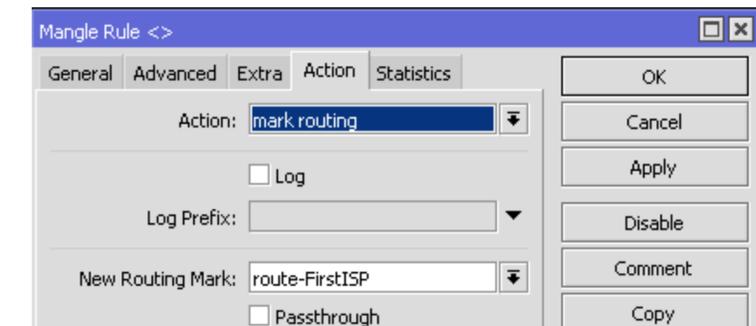
In. Interface:

Out. Interface:

Packet Mark:

Connection Mark: connections-FirstISP

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters



Mangle Rule <>

General | Advanced | Extra | Action | Statistics

Action:

Log

Log Prefix:

New Routing Mark:

Passthrough

Buttons: OK, Cancel, Apply, Disable, Comment, Copy

Что такое PCC

PCC (Per connection classifier) - это классификация по соединениям которая работает следующим образом:

Каждый IP-пакет имеет заголовок, в котором есть два поля адрес:порт источника и адрес:порт назначения

С помощью алгоритма хеширования данные из выбранных полей преобразуется в уникальное 32-битное значение

Использование данных хеширования позволяет отсортировать соединения на основе адреса источника, порта источника, адреса назначения, порта назначения или их различной комбинации

С помощью маркировки соединений формируются правила маршрутизации, которые направляют пакеты в соответствии с таблицей маршрутизации по указанному интерфейсу

На основании каких данных можно сортировать трафик

Per Connection Classifier:	<input type="checkbox"/>	src address	▼	:	1	/	0	▲
Src. MAC Address:	<input type="checkbox"/>	both addresses both addresses and ports both ports						▼
Out. Bridge Port:	<input type="checkbox"/>	dst address dst address and port						▼
In. Bridge Port:	<input type="checkbox"/>	dst port src address src address and port						▼
IPsec Policy:	<input type="checkbox"/>	src port						▼

Математика распределения

$$2-0=2$$

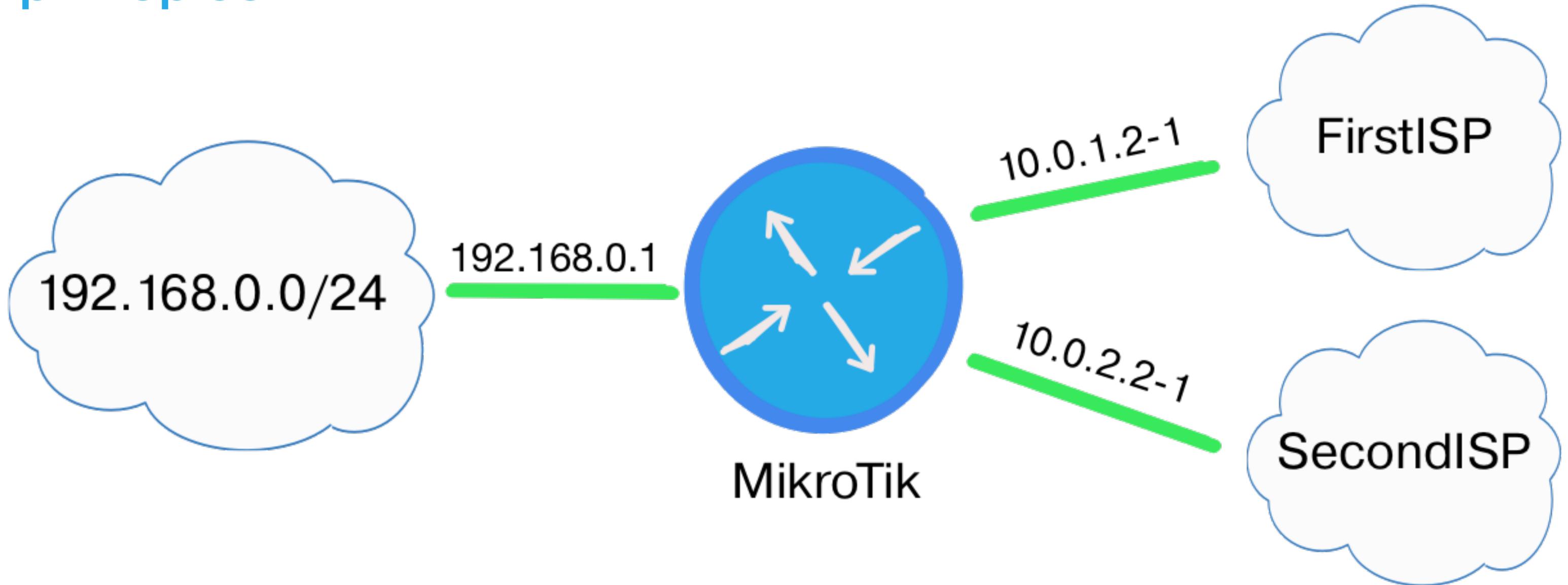
Per Connection Classifier: src address : 2 / 0

$$2-1=1$$

Per Connection Classifier: src address : 2 / 1

$$2-2=0$$

Пример сети



План настройки маршрутизатора

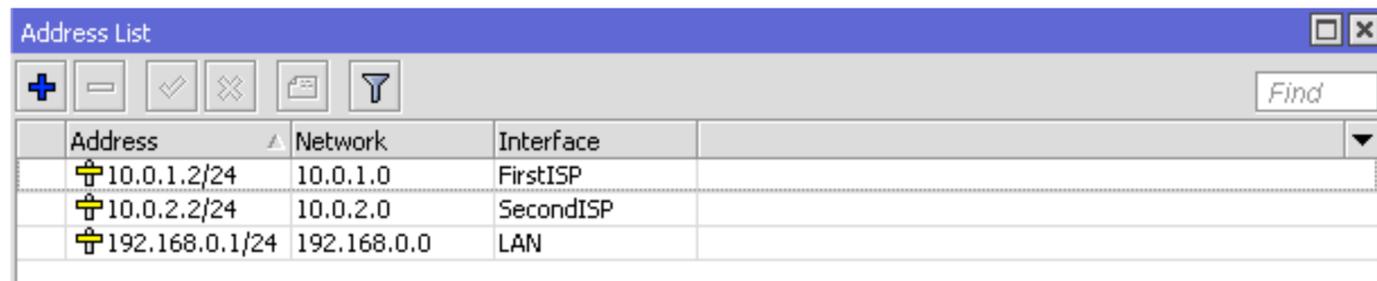
- 1 - Прописать адреса на интерфейсах маршрутизатора
- 2 - Настроить NAT на внешние каналы
- 3 - Настроить маркировку соединений которые предназначены непосредственно маршрутизатору
- 4 - Настроить маркировку и распределение соединений средствами PCC для обоих каналов
- 5 - Настроить маркировку маршрутов
- 6 - Прописать маршруты
- 7 - Предусмотреть прохождение трафика в случае отказа одного из каналов

Пропишем адреса и настройки NAT

```
[admin@MUM] /ip address> print
```

```
Flags: X - disabled, I - invalid, D - dynamic
```

#	ADDRESS	NETWORK	INTERFACE
0	10.0.1.2/24	10.0.1.0	FirstISP
1	10.0.2.2/24	10.0.2.0	SecondISP
2	192.168.0.1/24	192.168.0.0	LAN



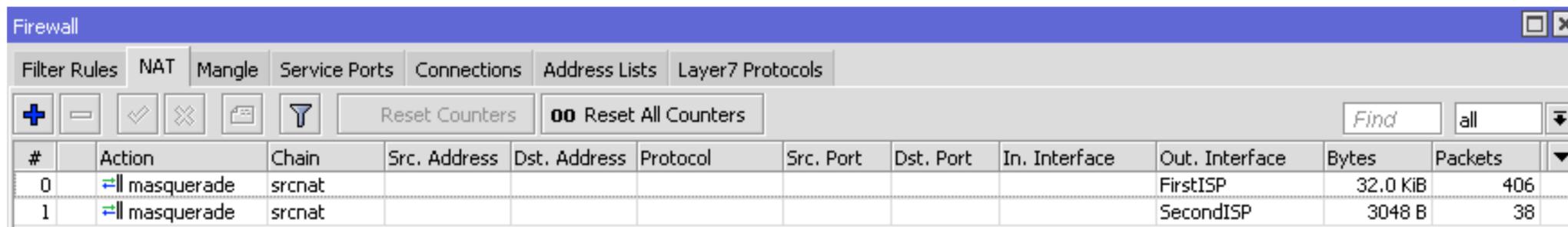
Address	Network	Interface
10.0.1.2/24	10.0.1.0	FirstISP
10.0.2.2/24	10.0.2.0	SecondISP
192.168.0.1/24	192.168.0.0	LAN

```
[admin@MUM] /ip firewall nat> print
```

```
Flags: X - disabled, I - invalid, D - dynamic
```

```
0 chain=srcnat action=masquerade out-interface=FirstISP log=no log-prefix=""
```

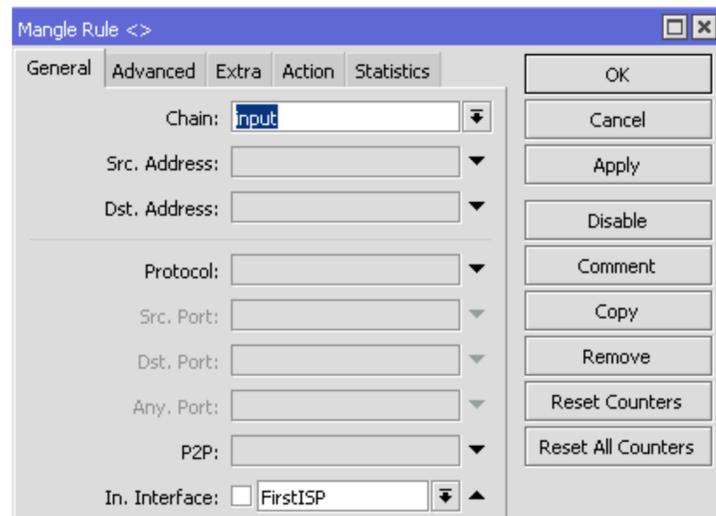
```
1 chain=srcnat action=masquerade out-interface=SecondISP log=no log-prefix=""
```



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Bytes	Packets
0	masquerade	srcnat							FirstISP	32.0 KiB	406
1	masquerade	srcnat							SecondISP	3048 B	38

Промаркируем соединения для роутера

```
[admin@MUM] /ip firewall mangle> print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=input action=mark-connection new-connection-mark=connections-FirstISP passthrough=yes in-interface=FirstISP log=no log-prefix=""
1 chain=output action=mark-routing new-routing-mark=route-FirstISP passthrough=no connection-mark=connections-FirstISP log=no log-prefix=""
```



Mangle Rule <>

General | Advanced | Extra | Action | Statistics

Chain: input

Src. Address: []

Dst. Address: []

Protocol: []

Src. Port: []

Dst. Port: []

Any. Port: []

P2P: []

In. Interface: FirstISP

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters



Mangle Rule <>

General | Advanced | Extra | Action | Statistics

Action: mark connection

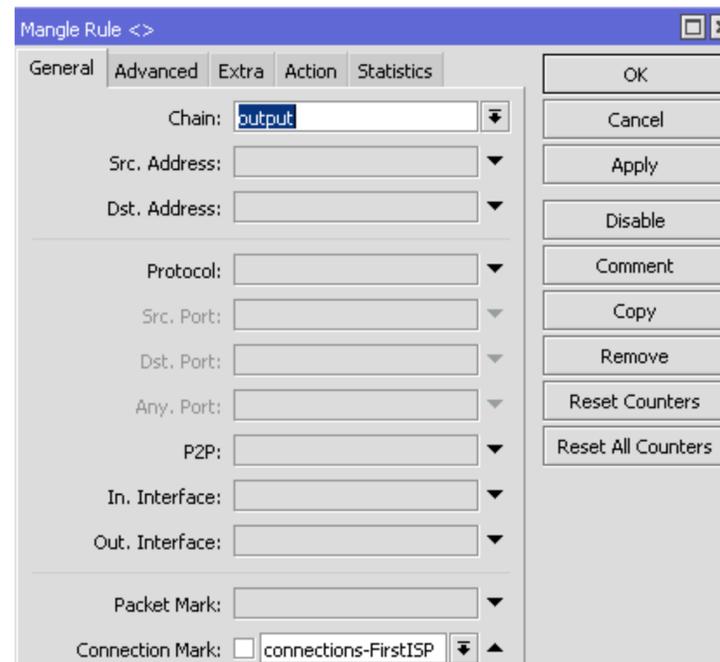
Log

Log Prefix: []

New Connection Mark: connections-FirstISP

Passthrough

Buttons: OK, Cancel, Apply, Disable, Comment, Copy



Mangle Rule <>

General | Advanced | Extra | Action | Statistics

Chain: output

Src. Address: []

Dst. Address: []

Protocol: []

Src. Port: []

Dst. Port: []

Any. Port: []

P2P: []

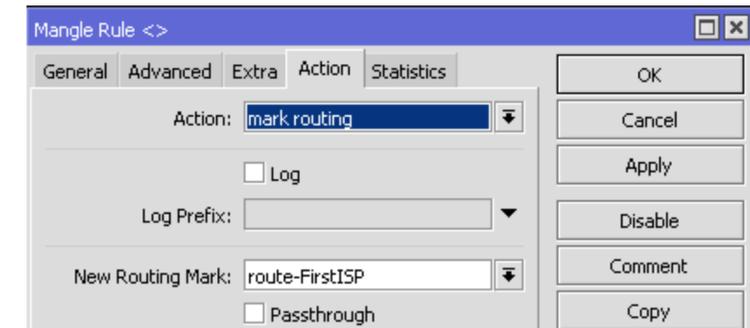
In. Interface: []

Out. Interface: []

Packet Mark: []

Connection Mark: connections-FirstISP

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters



Mangle Rule <>

General | Advanced | Extra | Action | Statistics

Action: mark routing

Log

Log Prefix: []

New Routing Mark: route-FirstISP

Passthrough

Buttons: OK, Cancel, Apply, Disable, Comment, Copy

Настроим балансировку трафика средствами РСС

```
[admin@MUM] /ip firewall mangle> print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=prerouting action=mark-connection new-connection-mark=connections-FirstISP passthrough=yes dst-address-type=!local in-interface=LAN
  per-connection-classifier=both-addresses:2/0 log=no log-prefix=""
```

Mangle Rule <>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface: LAN

Mangle Rule <>

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier: both addresses : 2 / 0

Mangle Rule <>

General Advanced Extra Action Statistics

Connection Limit

Limit

Dst. Limit

Nth

Time

Src. Address Type

Dst. Address Type

Address Type:

Invert

Mangle Rule <>

General Advanced Extra Action Statistics

Action:

Log

Log Prefix:

New Connection Mark:

Passthrough

Сделаем марки для маршрутов

```
1 chain=prerouting action=mark-routing new-routing-mark=route-FirstISP passthrough=no dst-address-type=!local connection-mark=connections-FirstISP log=no log-prefix=""
```

Mangle Rule <>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark: connections-FirstISP

Mangle Rule <>

General Advanced Extra Action Statistics

Connection Limit

Limit

Dst. Limit

Nth

Time

Src. Address Type

Dst. Address Type

Address Type:

Invert

Mangle Rule <>

General Advanced Extra Action Statistics

Action:

Log

Log Prefix:

New Routing Mark:

Passthrough

С mangle закончили

```

/ip firewall mangle
add action=mark-connection chain=prerouting dst-address-type=!local in-interface=LAN new-connection-mark=connections-FirstISP per-connection-classifier=\
both-addresses:2/0
add action=mark-routing chain=prerouting connection-mark=connections-FirstISP dst-address-type=!local new-routing-mark=route-FirstISP passthrough=no
add action=mark-connection chain=prerouting dst-address-type=!local in-interface=LAN new-connection-mark=connections-SecondISP per-connection-classifier=\
both-addresses:2/1
add action=mark-routing chain=prerouting connection-mark=connections-SecondISP dst-address-type=!local new-routing-mark=route-SecondISP passthrough=no
add action=mark-connection chain=input in-interface=FirstISP new-connection-mark=connections-FirstISP
add action=mark-routing chain=output connection-mark=connections-FirstISP new-routing-mark=route-FirstISP passthrough=no
add action=mark-connection chain=input in-interface=SecondISP new-connection-mark=connections-SecondISP
add action=mark-routing chain=output connection-mark=connections-SecondISP new-routing-mark=route-SecondISP passthrough=no

```

Firewall								
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols								
+ - [check] [x] [info] [filter] Reset Counters 00 Reset All Counters								
#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Interface
0	mark connection	prerouting						LAN
1	mark routing	prerouting						
2	mark connection	prerouting						LAN
2	mark routing	prerouting						
2	mark connection	input						FirstISP
2	mark routing	output						
2	mark connection	input						SecondISP
2	mark routing	output						

Создадим маршруты

```

/ip route
add check-gateway=ping distance=1 gateway=10.0.1.1 routing-mark=route-FirstISP
add check-gateway=ping distance=2 gateway=10.0.2.1 routing-mark=route-FirstISP
add check-gateway=ping distance=1 gateway=10.0.2.1 routing-mark=route-SecondISP
add check-gateway=ping distance=2 gateway=10.0.1.1 routing-mark=route-SecondISP
add check-gateway=ping distance=1 gateway=10.0.1.1
add check-gateway=ping distance=2 gateway=10.0.2.1

```

Route <0.0.0.0/0>

General | Attributes

Dst. Address:

Gateway: reachable FirstISP

Check Gateway: Type:

Distance: Scope: Target Scope:

Routing Mark:

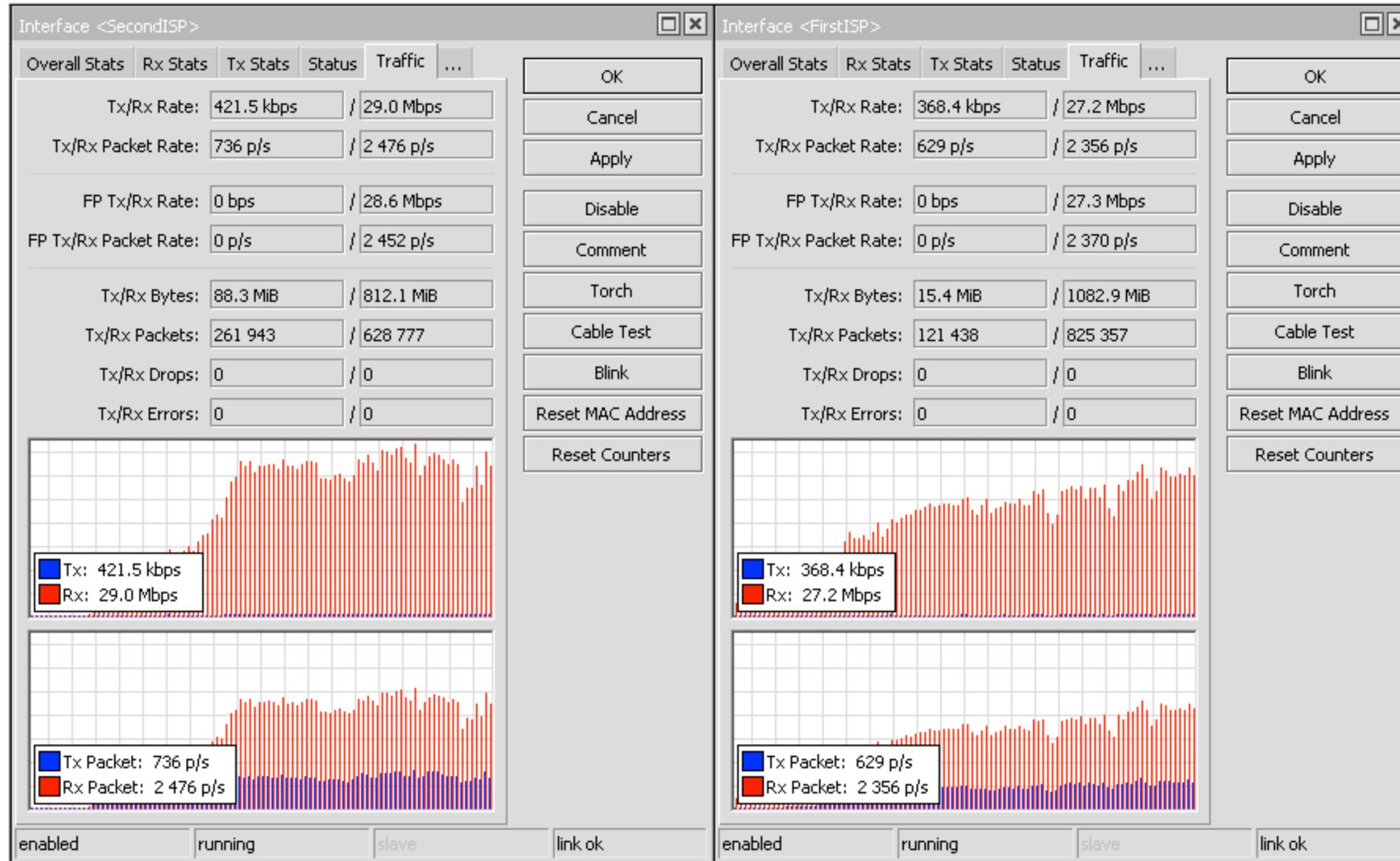
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	10.0.1.1 reachable FirstISP	1	route-FirstISP	
AS	0.0.0.0/0	10.0.2.1 reachable SecondISP	1	route-SecondISP	
AS	0.0.0.0/0	10.0.1.1 reachable FirstISP	1		
S	0.0.0.0/0	10.0.2.1 reachable SecondISP	2		
S	0.0.0.0/0	10.0.2.1 reachable SecondISP	2	route-FirstISP	
S	0.0.0.0/0	10.0.1.1 reachable FirstISP	2	route-SecondISP	
DAC	10.0.1.0/24	FirstISP reachable	0		10.0.1.2
DAC	10.0.2.0/24	SecondISP reachable	0		10.0.2.2
DAC	192.168.0.0/24	LAN reachable	0		192.168.0.1

- all
- main
- route-FirstISP
- route-SecondISP

Итого

```
/ip address
add address=10.0.1.2/24 interface=FirstISP network=10.0.1.0
add address=10.0.2.2/24 interface=SecondISP network=10.0.2.0
add address=192.168.0.1/24 interface=LAN network=192.168.0.0
/ip dns
set allow-remote-requests=yes servers=8.8.8.8,8.8.4.4
/ip firewall mangle
add action=mark-connection chain=prerouting dst-address-type=!local in-interface=LAN new-connection-mark=connections-FirstISP per-connection-classifier=\
  both-addresses:2/0
add action=mark-routing chain=prerouting connection-mark=connections-FirstISP dst-address-type=!local new-routing-mark=route-FirstISP passthrough=no
add action=mark-connection chain=prerouting dst-address-type=!local in-interface=LAN new-connection-mark=connections-SecondISP per-connection-classifier=\
  both-addresses:2/1
add action=mark-routing chain=prerouting connection-mark=connections-SecondISP dst-address-type=!local new-routing-mark=route-SecondISP passthrough=no
add action=mark-connection chain=input in-interface=FirstISP new-connection-mark=connections-FirstISP
add action=mark-routing chain=output connection-mark=connections-FirstISP new-routing-mark=route-FirstISP passthrough=no
add action=mark-connection chain=input in-interface=SecondISP new-connection-mark=connections-SecondISP
add action=mark-routing chain=output connection-mark=connections-SecondISP new-routing-mark=route-SecondISP passthrough=no
/ip firewall nat
add action=masquerade chain=srcnat out-interface=FirstISP
add action=masquerade chain=srcnat out-interface=SecondISP
/ip route
add check-gateway=ping distance=1 gateway=10.0.1.1 routing-mark=route-FirstISP
add check-gateway=ping distance=2 gateway=10.0.2.1 routing-mark=route-FirstISP
add check-gateway=ping distance=1 gateway=10.0.2.1 routing-mark=route-SecondISP
add check-gateway=ping distance=2 gateway=10.0.1.1 routing-mark=route-SecondISP
add check-gateway=ping distance=1 gateway=10.0.1.1
add check-gateway=ping distance=2 gateway=10.0.2.1
```

Тест/результат



Вопросы?

Павел Нагобидиянс
Компания «SUPCORE»
Системный администратор

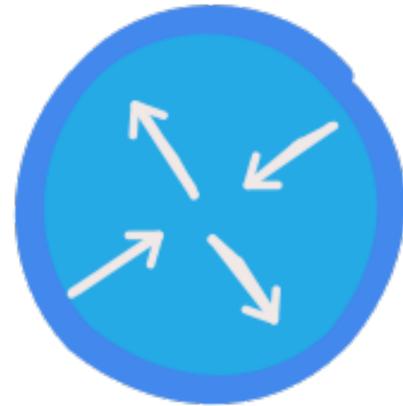
MTCNA
MTCRE
dCAA

mail.: npg@supcore.ru
mob.: +7 (914) 707 23 32



MikroTik
Certified Consultant

Спасибо за внимание!



**KEEP CALM
I'M AN
ENGINEER**