

Мikrotik и несколько провайдеров. Резервирование каналов

 interface31.ru/tech_it/2023/03/mikrotik-i-neskol-ko-provayderov-rezervirovanie-kanalov.html

Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Mikrotik и несколько провайдеров. Резервирование каналов

Зависимость нормальной работы предприятия от доступа в сеть интернет сегодня приобретает критический характер и перебои в работе провайдера могут привести к реальным убыткам или просто рабочих процессов, поэтому многие подключают резервные каналы других поставщиков услуг, чтобы использовать их для резервирования или балансировки нагрузки. В данном цикле статей мы рассмотрим работу с несколькими провайдерами на оборудование Mikrotik и сегодня расскажем про различные способы резервирования, а также их достоинства и недостатки.



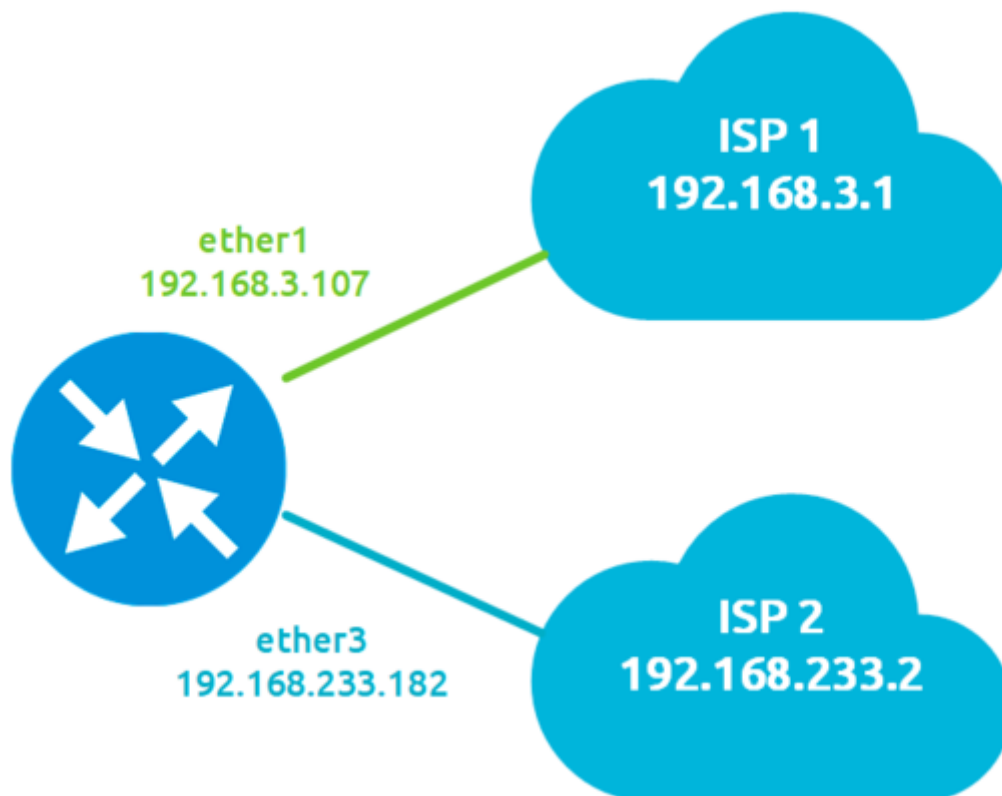
Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

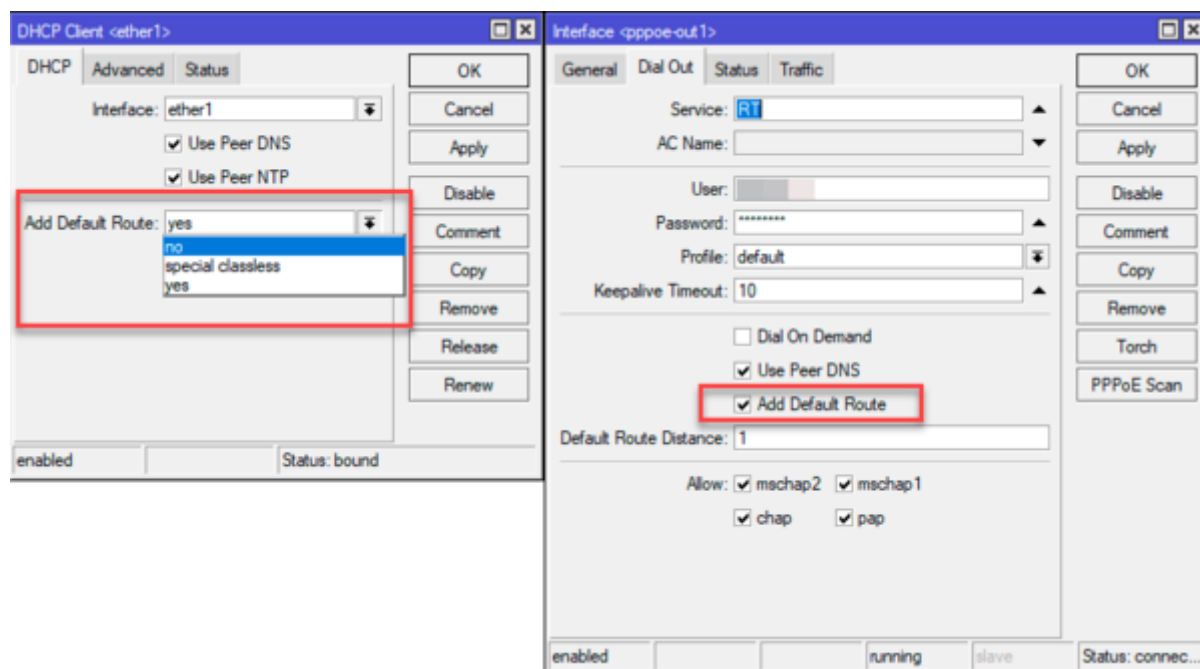
В данной статье мы не будем рассматривать базовую настройку роутера: выход в интернет, правила брандмауэра и т.п., будем считать, что читатель владеет этими вещами и уделим внимание только обеспечению резервирования внешних каналов.

Данная статья предназначена для **RouterOS 6.x**

Ниже показана схема, реализованная в нашей лаборатории с указанием адресов и интерфейсов, подключенных к двум условным провайдерам, а также их шлюзы.



Для правильной работы всех описанных ниже способов вам потребуется отключить динамическое добавление маршрутов, которое может быть включено если вы получаете сетевые настройки от провайдера по DHCP или используете PPPoE:



Важно! Во время выполнения операций с настройкой маршрутов у вас кратковременно пропадет доступ в интернет. Поэтому все указанные действия следует выполнять **имея физический доступ** к устройству.

Хотя можно обойтись и без этого, просто перед настройкой создайте дополнительный нулевой маршрут через основной шлюз и укажите ему самую меньшую административную дистанцию. Но помните, что любое неверное ваше действие грозит потерей сетевого доступа к устройству из внешней сети.

Резервирование на основе дистанции маршрута

Самый простой, можно даже сказать примитивный способ, в этом случае мы добавляем два маршрута с разной административной дистанцией и включаем проверку доступности шлюза для них.

Для этого перейдем в **IP - Routes** и добавим маршрут к первому провайдеру: **Dst. Address** - оставляем по умолчанию - **0.0.0.0/0**, **Gateway** - указываем шлюз первого провайдера, в нашем случае **192.168.3.1**, включаем механизм проверки доступности шлюза - **Check Gateway - ping**, и устанавливаем административную дистанцию маршрута - **Distance - 1**.

The screenshot shows the 'New Route' dialog box with the following configuration:

- Dst. Address:** 0.0.0.0/0
- Gateway:** 192.168.3.1
- Check Gateway:** ping
- Type:** unicast
- Distance:** 1
- Scope:** 30
- Target Scope:** 10
- Routing Mark:** (empty)
- Pref. Source:** (empty)

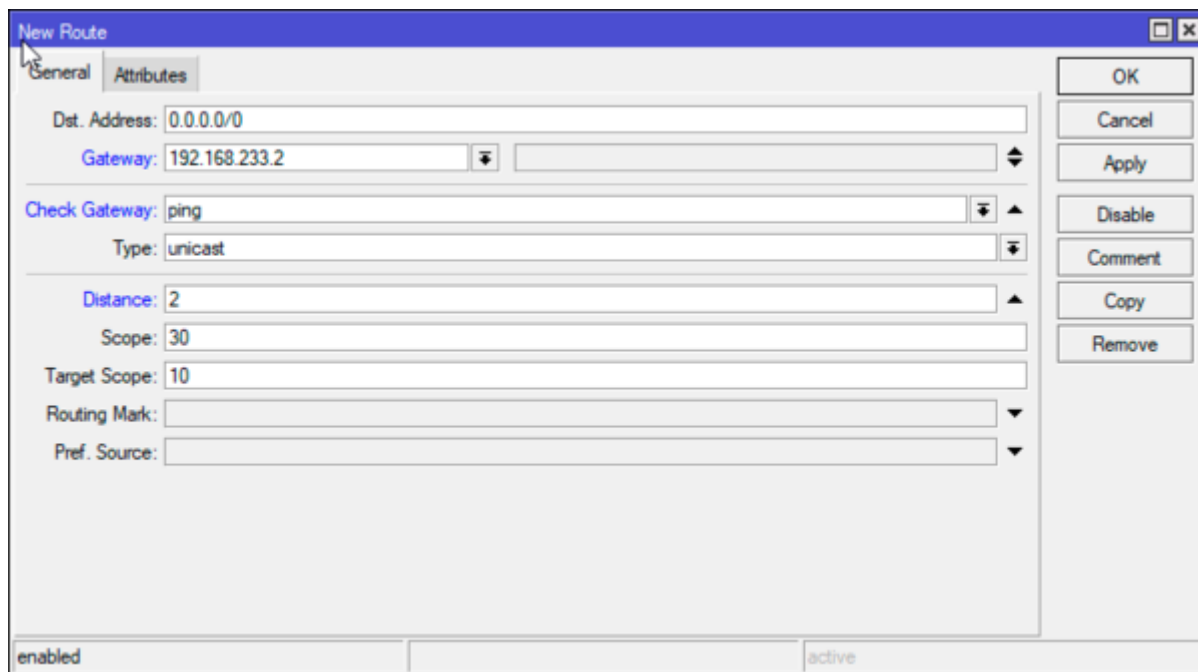
Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove.

At the bottom: ☒ enabled, ☒ active

Эти же действия в терминале:

```
/ip route  
add check-gateway=ping distance=1 gateway=192.168.3.1
```

Аналогичным образом добавляем маршрут ко второму провайдеру, только указываем административную дистанцию **Distance - 2**. В данном случае абсолютные цифры не так важны, при наличии нескольких маршрутов к одному адресу назначения работать будет тот, у которого административная дистанция меньше.

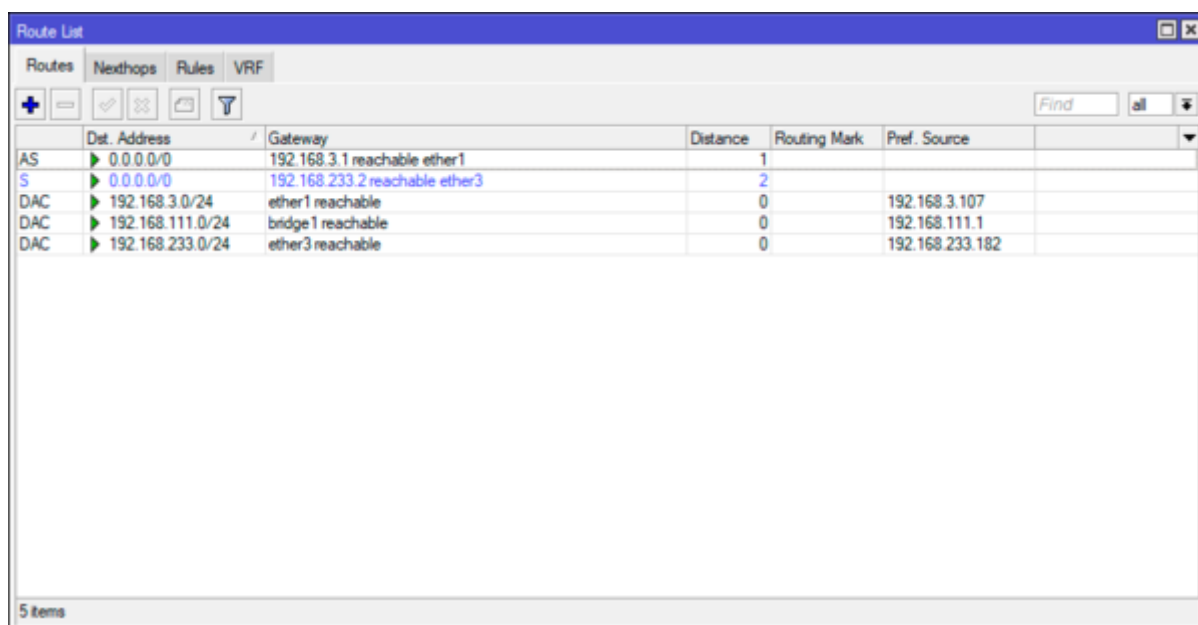


The 'New Route' window shows the configuration for a new route. The 'General' tab is active. The 'Dst. Address' is set to '0.0.0.0/0'. The 'Gateway' is set to '192.168.233.2'. The 'Check Gateway' is set to 'ping'. The 'Type' is set to 'unicast'. The 'Distance' is set to '2'. The 'Scope' is set to '30'. The 'Target Scope' is set to '10'. The 'Routing Mark' and 'Pref. Source' are empty. The 'enabled' checkbox is checked, and the 'active' checkbox is also checked. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'.

Или в терминале:

```
/ip route
add check-gateway=ping distance=2 gateway=192.168.233.2
```

После этого у вас появится интернет и будет активен маршрут через первого провайдера:



The 'Route List' window shows a table of routes. The 'Routes' tab is active. The table has columns for 'Dst. Address', 'Gateway', 'Distance', 'Routing Mark', and 'Pref. Source'. The routes are listed as follows:

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	192.168.3.1 reachable ether1	1		
S	0.0.0.0/0	192.168.233.2 reachable ether3	2		
DAC	192.168.3.0/24	ether1 reachable	0		192.168.3.107
DAC	192.168.111.0/24	bridge1 reachable	0		192.168.111.1
DAC	192.168.233.0/24	ether3 reachable	0		192.168.233.182

At the bottom of the window, it says '5 items'.

Теперь имитируем аварию, в нашем случае мы просто отключим патч-корд от интерфейса **ether1**, через небольшое время роутер обнаружит недоступность шлюза и сделает маршрут не активным, после чего автоматически заработает маршрут через второго провайдера и трафик пойдет туда.

	Dst. Address	Gateway	Distance	Routing Mark	Pref.	Source
S	0.0.0.0/0	192.168.3.1 unreachable	1			
AS	0.0.0.0/0	192.168.233.2 reachable ether3	2			
DAC	192.168.3.0/24	ether1 reachable	0		192.168.3.107	
DAC	192.168.111.0/24	bridge1 reachable	0		192.168.111.1	
DAC	192.168.233.0/24	ether3 reachable	0		192.168.233.182	

После восстановления доступности шлюза провайдера обратное переключение произойдет автоматически.

Резервирование при помощи рекурсивной маршрутизации

Преыдуший способ имеет один серьезный недостаток, он проверяет доступность шлюза провайдера, но не проверяет наличие интернета за этим шлюзом, и вы можете оказаться в ситуации, когда интернет отсутствует, но переключения на резервный канал не произошло. Чтобы избежать такой ситуации следует проверять доступность не шлюза провайдера, а внешних высокодоступных узлов.

Один из методов, позволяющих это сделать, называется рекурсивной маршрутизацией, мы подробно рассматривали ее в отдельной статье, поэтому здесь просто покажем последовательность настройки, не вдаваясь в подробности.

Резервирование каналов в Mikrotik при помощи рекурсивной маршрутизации

Прежде всего выберем два высокодоступных узла, в нашем случае это будут **8.8.8.8** и **9.9.9.9** и пропишем к каждому из них маршрут через шлюзы первого и второго провайдеров.

Переходим в **IP - Routes** и создаем маршрут: **Dst. Address** - **8.8.8.8** - узел для проверки первого провайдера, **Gateway** - **192.168.3.1** - шлюз первого провайдера, **Distance** - **1**, **Scope** - **10**. Обратите внимание на значение **области (Scope)**, если вы оставите там значение по умолчанию - 30, то рекурсивная маршрутизация работать не будет! Затем добавим второй аналогичный маршрут, но уже к узлу **9.9.9.9** через шлюз второго провайдера.

Тоже самое быстро в терминале:

```
/ip route
add distance=1 dst-address=8.8.8.8/32 gateway=192.168.3.1 scope=10
add distance=1 dst-address=9.9.9.9/32 gateway=192.168.233.2 scope=10
```

Теперь добавим рекурсивные маршруты для каждого из провайдеров со следующими настройками: **Dst. Address** оставляем по умолчанию - **0.0.0.0/0**, **Gateway** - **8.8.8.8** - высокодоступный узел для первого провайдера, **Check Gateway** - **ping** - указываем проверку доступности шлюза, **Distance** - **1**. Для второго провайдера все тоже самое, но **Gateway** - **9.9.9.9** и **Distance** - **2**.

В терминале воспользуйтесь командами:

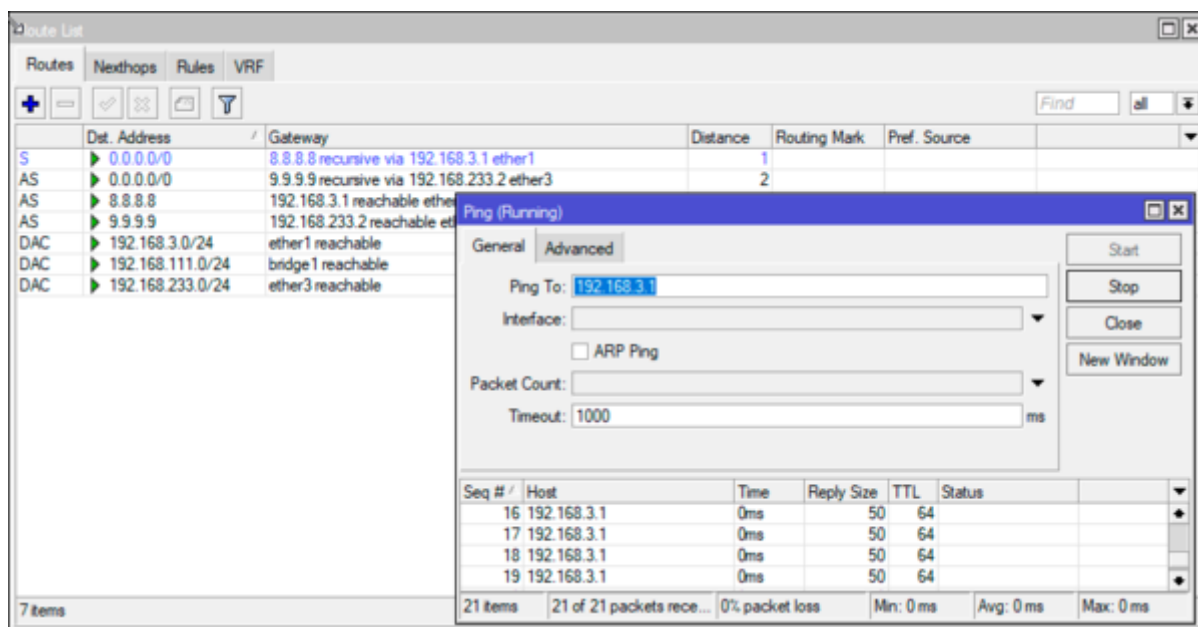
```

/ip route
add check-gateway=ping distance=1 gateway=8.8.8.8
add check-gateway=ping distance=2 gateway=9.9.9.9

```

Мы сейчас не будем вдаваться в подробности как это работает, для этого есть отдельная статья, но общий смысл заключается в том, что рекурсивные маршруты в итоге работают через реальные шлюзы провайдеров, но проверяют доступность не провайдерского шлюза, а высокодоступного узла за ним. Если связь пропала - маршрут деактивируется и начинает работать следующий, с большей дистанцией.

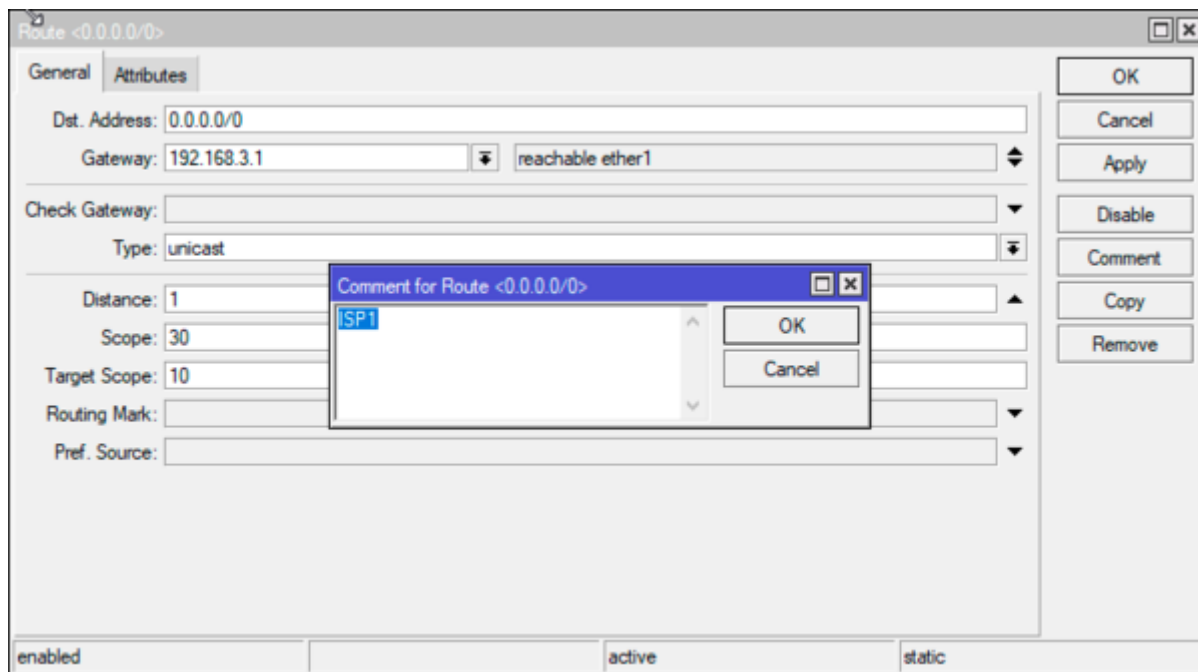
На рисунке ниже мы можем видеть, что активный маршрут переключился на резервный канал несмотря на то, что шлюз основного провайдера доступен:



При восстановлении работы первого провайдера обратное переключение произойдет автоматически.

Резервирование при помощи Netwatch

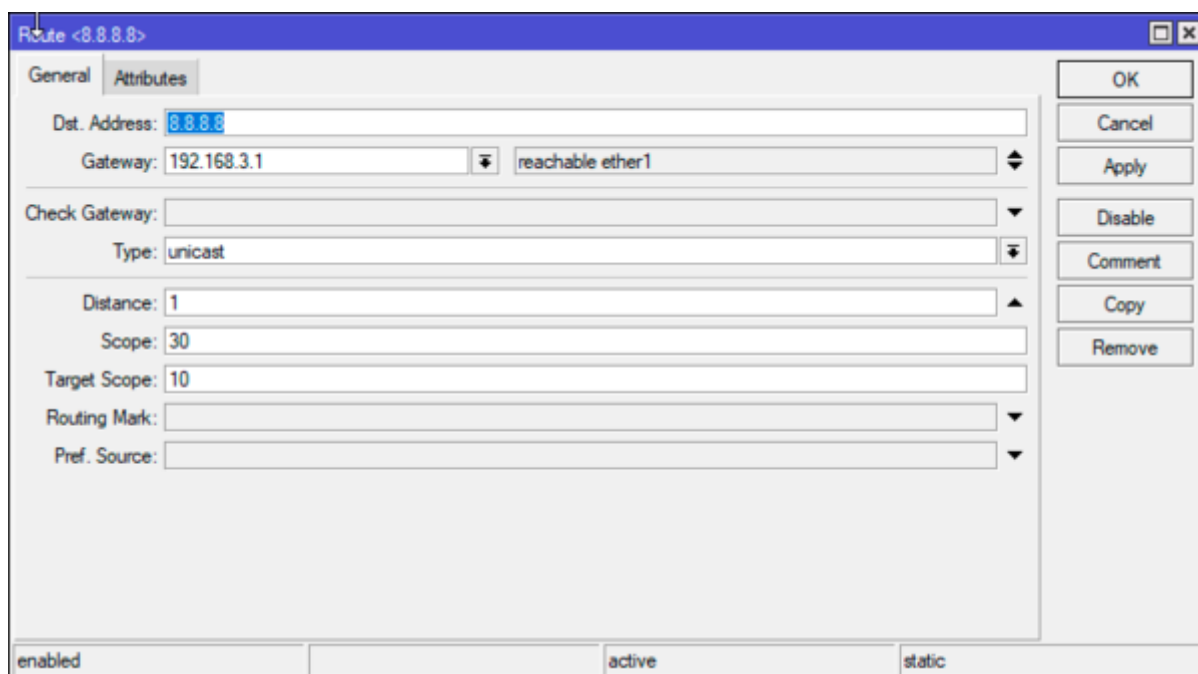
Прежде всего добавим маршруты к каждому из провайдеров с разными дистанциями, никаких проверок включать не надо, но обязательно следует добавить к каждому маршруту комментарий, в нашем случае это будут "ISP1" и "ISP2".



В терминале:

```
/ip route
add comment=ISP1 distance=1 gateway=192.168.3.1
add comment=ISP2 distance=2 gateway=192.168.233.2
```

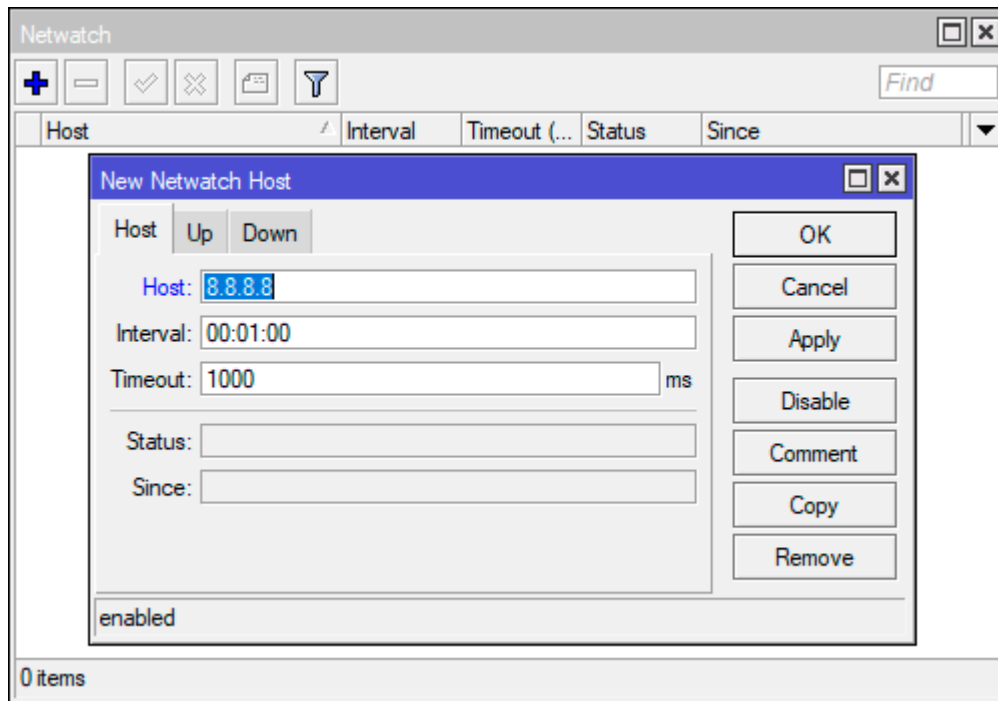
Затем выбираем высокодоступный хост и добавляем к нему маршрут через первого провайдера:



Эти же действия в терминале:

```
/ip route
add distance=1 dst-address=8.8.8.8/32 gateway=192.168.3.1
```


Затем переходим в **Tools - Netwatch** и добавляем там новый узел, на закладке **Host** указываем адрес выбранного высокодоступного узла, при необходимости меняем интервал опроса.



На закладке **Up** вводим следующий скрипт:

```
/ip route set [find comment="ISP1"] disabled=no  
/ip route set [find comment="ISP2"] disabled=yes
```

Затем на закладке **Down**:

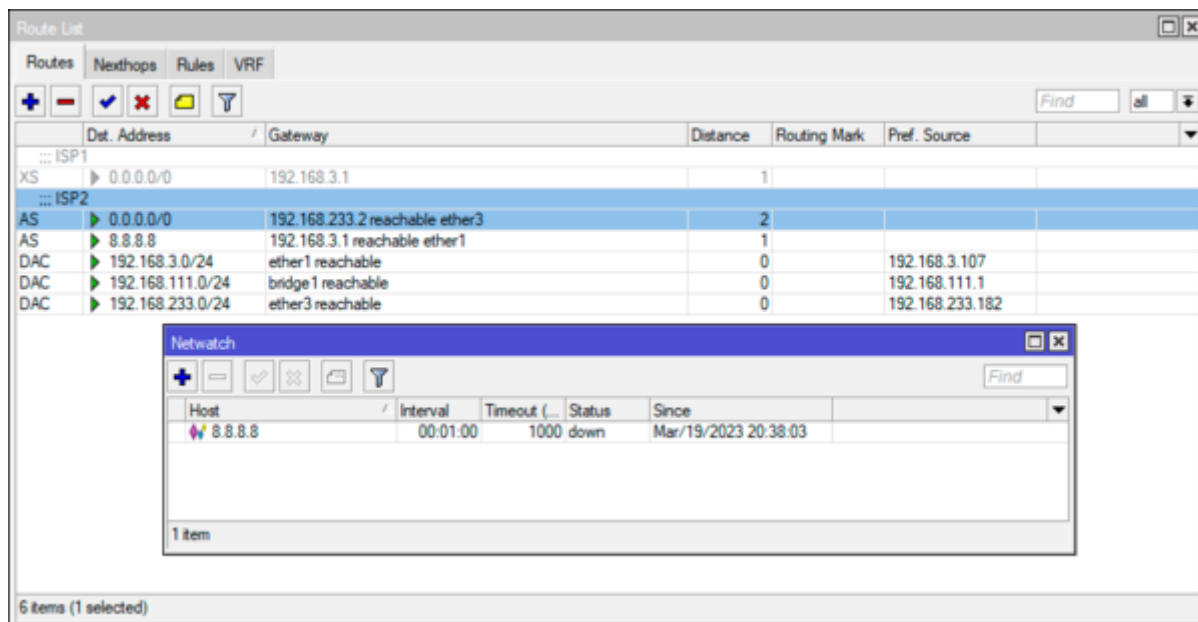
```
/ip route set [find comment="ISP1"] disabled=yes  
/ip route set [find comment="ISP2"] disabled=no
```

Их смысл предельно прост, если узел через первого провайдера доступен, то включаем маршрут с меткой ISP1, а маршрут с меткой ISP2 выключаем, если недоступен - то делаем ровно наоборот.

В терминале все это можно быстро сделать при помощи "заклинания":

```
/tool netwatch  
add down-script="/ip route set [find comment=\"ISP1\"] disabled=yes\r\  
  \n/ip route set [find comment=\"ISP2\"] disabled=no" host=8.8.8.8 \  
  up-script="/ip route set [find comment=\"ISP1\"] disabled=no\r\  
  \n/ip route set [find comment=\"ISP2\"] disabled=yes"
```

Для проверки блокируем доступ через первого провайдера и убеждаемся, что переключение происходит:



Обратное переключение произойдет автоматически после восстановления связи с высокодоступным узлом.

Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.