

MikroTik Router OS

Обзор Command Line Interface (CLI)

RouterOS може да се управлява от командния ред (CLI). Има различни команди, всяка със собствен синтаксис и възможни опции. CLI може да бъде достъпен по множество начини: чрез директна връзка със сериен порт, през мрежата чрез **telnet** или **SSH**, чрез екран на конзолата в помощната програма GUI **Winbox** или чрез вашия уеб браузър. Конзолата се използва и за писане на скриптове. Тъй като има много налични команди, те са разделени на групи, организирани в йерархия. За щастие не е нужно да помните всяка възможна команда или дори пълния списък с команди. RouterOS има няколко функции, които да ви помогнат при въвеждането на команди.

Съкратени команди: За всяка команда трябва да въведете само толкова букви, колкото са необходими, за да направите тази команда уникална. Например, помислете за `ping 10.0.0.1 count 3 size 100`. Същата команда може да бъде въведена като `pi 10.1 c 3 si 100`, което е много по-кратко! В допълнение, командите могат да се дописват автоматично, чрез използване на клавиша **[TAB]**. Например `interface mt` **[TAB]** се довършва като `interface monitor-traffic`, което е пълната команда.

HotLock Mode: Когато режимът HotLock е активиран, командите ще бъдат автоматично завършени. За да включите/изключите режим HotLock, натиснете **[CTRL]+[V]**. Двойният `>>` е индикация, че режимът HotLock е активиран. Например, ако въведете `pi`, то ще бъде автоматично завършено до `ping`.

Онлайн помощ: Всеки път, когато не знаете, натиснете **?** и CLI ще покаже синтаксиса и структурата на командата, която сте въвели. Например `ping ?` ще покаже синтаксиса на командата `ping`.

Безопасен режим: Когато за първи път се свържете с рутера и влезете (потребителско име по подразбиране: `admin`, без парола), командният ред ще ви покаже: `[admin@MikroTik]>`. Понякога е възможно да промените конфигурацията на рутера по начин, който ще направи рутера недостъпен през мрежата и достъпен само от локалната конзола. Ако възникне такъв вид грешка от администратора, може да няма начин да отмените последната промяна, тъй като връзката с рутера вече е прекъсната. Безопасният режим може да се използва за минимизиране на този риск. В безопасен режим се влиза чрез натискане на **[CTRL]+[X]**. За да запазите промените и да излезете от безопасен режим, трябва да натиснете **[CTRL]+[X]** отново. За да излезете, без да запазвате промените, натиснете **[CTRL]+[D]**.

За да избегнете проблеми с конфигурацията, се препоръчва винаги да влизате в безопасния режим в началото на всяка лабораторна работа чрез **[CTRL]+[X]** и никога да не излизате от този режим до края на лабораторията, когато излизате с **[CTRL]+[D]**. Показва се съобщението **Safe Mode taken** и командният ред се променя, за да отрази, че сесията вече е в безопасен режим (`<SAFE>`). Всички промени в конфигурацията, направени, докато рутерът е в безопасен режим, се отменят автоматично, ако сесията в безопасен режим приключи необичайно, т.е. чрез **[CTRL]+[D]**. Имайте предвид, че „quit“ се счита за нормално прекратяване и по този начин ще запази промените в конфигурацията.

Reset Configuration

Желателно е да стартирате всяка лаборатория с конфигурацията по подразбиране и да се уверите, че нищо не е запазено в конфигурацията на рутера от предишна работа:

```
system reset-configuration
```

Съвет: Използвайте клавиша Tab, за да завършите автоматично тази команда!

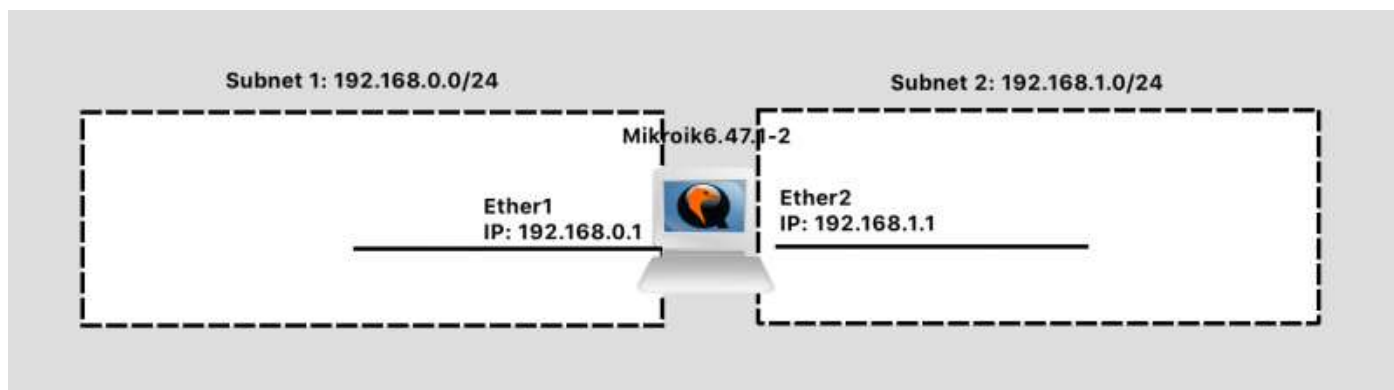
Рутерът ще ви помоли да потвърдите, че искате да нулирате конфигурацията. Въведете „y“ като отговор. Командата връща рутера към неговата конфигурация по подразбиране, включително потребителското име и парола по подразбиране („admin“ и без парола). IP адресите и други конфигурации се изтриват, а интерфейсите ще бъдат деактивирани. След командата за нулиране рутерът ще се рестартира и ще трябва да се свържете отново.

Ако се интересувате от конфигурацията по подразбиране, можете да я отпечатате чрез:

```
system default-configuration print
```

Примерна конфигурация на рутера

Този пример показва как да конфигурирате обикновен рутер с два интерфейса, свързващи две подмрежи в командния ред:



Ако не сте в безопасен режим, преминете към този режим чрез **[CTRL]+[X]**. Командният ред ще се промени от **[admin@MikroTik] >** на **[admin@MikroTik] > <SAFE>**

Проверете списъка с интерфейси на вашия рутер:

```
<SAFE> interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#   NAME      TYPE      ACTUAL-MTU  L2MTU  MAX-L2MTU  MAC-ADDRESS
0   R ether1   ether      1500       1500      1500      0C:46:BE:AE:E1:00
1   R ether2   ether      1500       1500      1500      0C:46:BE:AE:E1:01
2   R ether3   ether      1500       1500      1500      0C:46:BE:AE:E1:02
3   R ether4   ether      1500       1500      1500      0C:46:BE:AE:E1:03
```

Проверете списъка с IP адреси, присвоени на интерфейсите:

```
<SAFE> ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS      NETWORK      INTERFACE
```

Задайте IP адрес 192.168.0.1 с маска на подмрежа 255.255.255.0 на интерфейса ether1:

```
<SAFE> ip address add address=192.168.0.1 netmask=255.255.255.0 interface=ether1
```

Задайте IP адрес 192.168.1.1 с маска на подмрежа 255.255.255.0 на интерфейса ether2:

```
<SAFE> ip address add address=192.168.1.1 netmask=255.255.255.0 interface=ether2
```

Проверете дали IP адресите са присвоени на интерфейсите ether1 и ether2:

```
<SAFE> ip address print
[admin@MikroTik] <SAFE> ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS      NETWORK      INTERFACE
0   192.168.0.1/24  192.168.0.0   ether1
1   192.168.1.1/24  192.168.1.0   ether2
```

Свет: ако направите грешка при въвеждане на IP адрес, можете да го премахнете чрез следния процес:

1. Първо въведете `ip address print` и отбележете номера на реда (#), на който се появява неправилният запис
2. След това въведете `ip address remove numbers=X`, където X е номерът на записа, който искате да премахнете.
3. Потвърдете, че неправилният запис е премахнат, като повторите отпечатването на `ip address print`.

За тази проста мрежа не е необходимо да дефинираме маршрути. И двете подмрежи са директно свързани към рутера и записите в таблицата за маршрутизиране ще бъдат добавени автоматично. Но ако искаме да добавим тези статично (ръчно), командите ще изглеждат така:

Маршрутизирайте трафика, насочен към мрежата 192.168.0.0/24 през интерфейс ether1 и трафика, предназначен към мрежата 192.168.1.0/24 през интерфейс ether2

```
<SAFE> ip route add dst-address=192.168.0.0/24 gateway=ether1
<SAFE> ip route add dst-address=192.168.1.0/24 gateway=ether2
```

Проверете зададените статични маршрути, за да проверите конфигурацията на мрежата:

```
<SAFE> ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#   DST-ADDRESS    PREF-SRC    GATEWAY      DISTANCE
0   ADC  192.168.0.0/24    192.168.0.1   ether1         0
1   ADC  192.168.1.0/24    192.168.1.1   ether2         0
```

Накрая деактивирайте DHCP клиента на рутера. Освен ако не сте стартирали Wireshark на връзката, няма да забележите, че новия рутер по подразбиране активира DHCP клиент на Ether1, опитвайки се да конфигурира автоматично този мрежов порт, така че администратор да има достъп до рутера през мрежата. Това не е полезно за нас в симулирана мрежа.

```
ip dhcp-client print      # Observe the running DHCP client and its configuration number
ip dhcp-client remove numbers=0    #Remove it
```

Натиснете `[CTRL] + [D]`, за да излезете от безопасен режим и да оставите конфигурацията на рутера непроменена.