

# Klientské Mikrotiky - Instalační checklist

## Nastavení DHCP



Pokud neplanujeme přidělovat IP adresu na WANu Mikrotiku dynamicky, je nutné vypnout DHCP klienta. Pokud DHCP klienta necháme zapnutého, je nutné zaevidovat jeho MAC adresu do hosts = viz. následující Harviho mail.

Pokud nekam davate novyho mikrotiku, tak prosim udelejte 2 nasledujici veci:

- 1.) Nastavte mu spravne hostname (identity)
- 2.) Vypnete mu DHCP klienta!!!

Mikrotiky maj defaultne zaplyho DHCP klienta a ted, kdy jsem nasadil DHCP do cely site, to muze bejt problem jak pro ten MikroTik (pokud neni vas zamer, aby mel adresu z DHCP - treba na zaklade macovky co napisete do hosts), tak pro centralni DHCP server. Obzvlast v pripade, kdy takovej mikrotik pripojite do subnetu, kterej nema DHCP pool.

Pak nam zadelavate na problemy s pretizenim DHCP serveru, protoze MikroTikovskej DHCP klient je pomerne agresivni a kdyz nedostane IP adresu, tak je dost neodbytnej. Mam vyzkouseny, ze kdyz je takovejch zarizeni v siti 20, tak DHCP server ve skrinu prostu prestava fungovat pod naporem MikroTiku, který chtej adresy i kdyz jim je nemuze dat, protoze jsou v subnetu, ve kterym neni v hosts zanesenej DHCP pool.

## Vypnutí DHCP

Zakázat všechny DHCP klienty:

```
/ip dhcp-client disable [/ip dhcp-client find]
```

## Nastavení IP

- Rozsah s maskou /31 se zadává jako maska /32, akorát do "network" uvedete IP protistrany !

```
add address=10.11.10.42 interface=ether1 network=10.11.10.43
```

## Nastavení routingu

Pokud ma mikrotik vice nez 1 uplink - napr. u zakaznika s SLA, je nutne nakonfigurovat OSPF nasledujicim zpusobem:

Nastavení instance OSPF

```
[[admin@ros10]] > routing ospf instance print
Flags: X - disabled, * - default
 0 * name="ros10" router-id=10.11.82.249 distribute-default=never
    redistribute-connected=as-type-1 redistribute-
static=as-type-1
    redistribute-rip=no redistribute-bgp=no redistribute-
other-ospf=no
    metric-default=1 metric-connected=20 metric-static=20
metric-rip=20
    metric-bgp=auto metric-other-ospf=auto in-
filter=ospf-in out-filter=ospf-out
```

- **router-id** - nastavujeme vzdy IP adresu routeru v ethernetovem rozsahu zakaznika. Nikdy NE IP adresu nektoreho z uplinku !
- **redistribute-static, redistribute-connected** - nunto nastavit na as-type-1 (defaultne vypnuto). Toto zpusobi, ze jakykoliv dalsi pripojeny rozsah se do site naroutuje pouze pridanim ip adresy na interface, pokud je primo pripojen k routeru (connected) nebo pridanim rozsahu do routovaci tabulky s uvedenim IP adresy brany, kudy ma byt smerovan (static).

Nastavení interfacu, na kterých má OSPF poslouchat a vysílat pakety

```
[[admin@ros10]] > routing ospf interface print
Flags: X - disabled, I - inactive, D - dynamic, P - passive
#   INTERFACE          COST PRIORITY NETWORK-TYPE AUTHENTICATION
AUTHENTICATION-KEY
0   wlan2              500   1   broadcast   none
abcd1234
1   wlan1              2000  1   broadcast   none
abcd1234
```

- **INTERFACE** - rozhrani uplinku na mikrotiku
- **COST** - cena linky - cim mensi cena, tim ma vetsi prioritu. Na obou stranach spoje musi byt cena stejna !
- **AUTHENTICATION-KEY** - libovovolny klic pro zabezpeceni spoje - musi byt na obouch stranach spoje stejny !

Nastavení propojovacích subnetů, na kterých běží OSPF - nastavují se rozsahy na příslušném interfacu (bez nastavení networku OSPF nepoběží)

```
[[admin@ros10]] > routing ospf network print
```

Flags: X - disabled, I - invalid

#	NETWORK	AREA
0	10.11.42.128/26	backbone
1	10.11.104.0/26	backbone

- **NETWORK** - přidáváme rozsahy, které jsou na rozhraních, definovaných v záložce interfaces - tímto se finálně zapíná OSPF proces

POZOR: Při zapnutí ospf je nutné přidat ještě ospf filter, aby se nepropagovali jiné než naše routy, např. 192.168. atp. Upravujeme podle toho, jestli je routerborad v síti 10.11, 10.34 nebo 10.18

Nastavení filtru, aby se do sítě nešířili lokální rozsahy, např. natované subnety, tunelované IP adresy atp.



```
[[admin@ros10]] > routing filter print
```

Flags: X - disabled

0	chain=ospf-out	prefix=10.11.0.0/16	prefix-length=16-32	invert-match=no	action=accept	set-bgp-prepend-path=""
1	chain=ospf-out	prefix=77.87.240.0/21	prefix-length=21-32	invert-match=no	action=accept	set-bgp-prepend-path=""
2	chain=ospf-out			invert-match=no	action=reject	set-bgp-prepend-path=""

## Pokud zákazník na routeru s OSPF chce mít NAT

- nutno přidělit nějaký malý rozsah např. /29 na ethernet rozsah mikrotiku, kde je i natovaná síť
- nastavit rychlost na jednu z přidělených desítkových adres
- nastavit nat na tuto IP adresu

```
[[admin@ros10]] > ip address print
```

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

#	ADDRESS	NETWORK	INTERFACE
0	X **192.168.88.1/24**	192.168.88.0	bridge1
1	10.11.104.30/26	10.11.104.0	wlan2
2	10.11.42.130/26	10.11.42.128	wlan1
3	10.11.82.249/29	10.11.82.248	bridge1
4	**10.11.82.250/29**	10.11.82.248	bridge1
5	X 10.11.82.251/29	10.11.82.248	bridge1
6	10.11.106.1/27	10.11.106.0	wlan3

```
7 10.11.106.33/28 10.11.106.32 vlan2
```

```
[[admin@ros10]] > ip firewall nat print  
Flags: X - disabled, I - invalid, D - dynamic  
0 chain=srcnat action=src-nat to-addresses=10.11.82.250 src-  
address=192.168.88.0/24
```



POZOR: NIKDY nenastavujte nat za IP adresu jednoho z uplinku. V prípade vypadku tohoto spoje a preroutovani na druhy spoj by ten nat nefungoval !!!



Uvedena nastaveni OSPF plati i pro mensi AP, kde vse routuje take Mikrotik !

## Pokud potrebujeme BGP

[http://www.isp-servis.cz/config\\_mikrotik.html](http://www.isp-servis.cz/config_mikrotik.html)

## Statické nastavení IPv6

- Nejprve zapnout balíček ipv6, pokud ještě není: `system package enable ipv6` a potom `reboot`

Typický setup IPv6 na klientském mikrotiku vypadá takhle:

- Na uplink (wan) interfacu nastavíme propojovací adresu včetně délky prefixu a bez `advertise!`
- Přidáme adresu výchozí brány (defaultní routa je označována jako `::/0`)
- Na interface/bridge s pracovními stanicemi (lan) nastavíme přidělený prefix (typicky `/64`) a zaškrtneme "advertise"

### Příklad

Od správce jsme dostali tyto informace:

<b>Propojovací adresa</b>	2001:67c:2190:3b00:10:11:104:13/64
<b>Defaultní brána</b>	2001:67c:2190:3b00::1
<b>Vnitřní rozsah</b>	2001:67c:2190:3b01::/64

```
ipv6 address add address=2001:67c:2190:3b00:10:11:104:13/64 interface=wlan  
advertise=no  
ipv6 address add address=2001:67c:2190:3b01::/64 interface=ether  
advertise=yes
```

```
ipv6 route dst-address=::/0 gateway=2001:67c:2190:3b00::1
```

- Nezapomente vyjmenovat všechny interfacery na routeru v ospf3 s parametrem passive=yes, pouze interfacery, kde ma bezet dynamicky routing vyjmenujeme bez passive !

```
/routing ospf-v3 interface add area=backbone interface=vlan1451
```



screenshoty

## Řešení s více konektivitou od různých poskytovatelů

- Pro další konektivitu musím vytvořit novou routovací tabulku, kterou označíme např. BACKUP

```
/ip route rule add src-address=100.90.0.2/28 table=to_BACKUP  
/ip route rule add routing-mark=to_BACKUP table=to_BACKUP
```

*Prvni pravidlo obsahuje verejnou IP adresu, pridelenou od druhého ISP (za tuto adresu je potreba nastavit NAT, pro pakety co budou odchazet na interface druhého ISP)*

- pridame default routu do nove tabulky

```
ip route add check-gateway=ping distance=1 gateway=100.90.0.1 routing-  
mark=to_BACKUP  
ip route add distance=1 dst-address=10.0.0.0/8 gateway=10.34.1.65 routing-  
mark=to_BACKUP
```

*Druhe pravidlo zadame v pripade, ze chceme privatni adresy routovat vzdy pres primarni uplink*

- A nyní definujeme samotne rozsahy, ktere chceme primarne smerovat pres zalozniho ISP. Je mozne naspat skript, ktery zadana pravidla zapne nebo vypne v pripade nedostupnosti primarni konektivity nebo preroutuje vsechny site na zalozni konektivitu, to uz zalezi na konkretni uprave

```
/ip firewall mangle add action=mark-routing chain=prerouting dst-  
address=!10.0.0.0/8 log=yes new-routing-mark=to_BACKUP src-  
address=10.34.10.0/24  
/ip firewall mangle add action=mark-routing chain=prerouting dst-  
address=!10.0.0.0/8 log=yes new-routing-mark=to_BACKUP src-  
address=10.34.11.0/24
```

## Zálohování konfigurace

Nezapomente nahrát ssh klic pro zálohování. Tento systém bude dale v budoucnosti využívat i pro hromadné změny nastavení v mikrotiku apod., proto prosím provádejte nahrávání klíče na každý mikrotik !

Podrobnosti o zálohování konfigurace naleznete v následujícím dokumentu [Zálohování siti Spojе.Net](#)

From:

<https://wiki.spoje.net/> - **SPOJE.NET**

Permanent link:

[https://wiki.spoje.net/doku.php/howto/network/mikrotik\\_klient?rev=1548260293](https://wiki.spoje.net/doku.php/howto/network/mikrotik_klient?rev=1548260293)

Last update: **2019/01/23 17:18**

