

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 byt 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 skrini prostě prestava fungovat pod naporem MikroTiku, který chtej adresy i když jim je nemůže dát, protože jsou v subnetu, ve kterém není v hosts zanesený 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 má mikrotik více než 1 uplink - např. u zákazníka s SLA, je nutné nakonfigurovat OSPF následujícím způsobem:

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 vždy IP adresu routeru v ethernetovém rozsahu zákazníka. Nikdy NE IP adresu některého z uplinků !
- **redistribute-static, redistribute-connected** - nůto nastavit na as-type-1 (defaultně vypnuto). Toto způsobí, že jakýkoliv další připojený rozsah se do site naroutuje pouze přidáním IP adresy na interface, pokud je přímo připojen k routeru (connected) nebo přidáním rozsahu do routovací tabulky s uvedením IP adresy brány, kudy má být směřován (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** - rozhraní uplinku na mikrotiku
- **COST** - cena linky - čím menší cena, tím má větší prioritu. Na obou stranách spoje musí být cena stejná !
- **AUTHENTICATION-KEY** - libovolný klíč pro zabezpečení spoje - musí být na obou stranách spoje stejný !

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 případě vypadku tohoto spoje a preroutování na druhý spoj by ten nat nefungoval !!!



Uvedená nastavení OSPF platí i pro menší AP, kde vše routuje také Mikrotik !

Pokud potřebujeme BGP

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:

Propojovací adresa	2001:67c:2190:3b00:10:11:104:13/64
Defaultní brána	2001:67c:2190:3b00::1
Vnitřní rozsah	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 vyjmujeme 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
```

První pravidlo obsahuje veřejnou IP adresu, přidělenou od druhého ISP (za tuto adresu je potřeba nastavit NAT, pro pakety co budou odcházet na interface druhého ISP)

- přidáme default routu do nové 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
```

Druhé pravidlo zadáme v případě, že chceme privátní adresy routovat vždy přes primární uplink

- A nyní definujeme samotné rozsahy, které chceme primárně směřovat přes záložního ISP. Je možné napsat skript, který zadaná pravidla zapne nebo vypne v případě nedostupnosti primární konektivity nebo preroutuje všechny site na záložní konektivitu, to už záleží na konkrétní úpravě

```
/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 dále v budoucnosti využívat i pro hromadné změny nastavení v mikrotiku apod., proto prosím provádějte nahrávání klíče na každý mikrotik !

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

Reinstalace RouterOS na havarovanem mikrotiku pres NetInstall

V případě, může se nepodaří zavést RouterOS, snaží se Mikrotik bootovat ze sítě. To lze využít pro reinstalaci firmwaru přes netboot pomocí nástroje **NetInstall**. Na síťovce, kterou si propojíme se síťovkou na mikrotiku nastavíme IP např. 192.168.88.100/24, stáhneme balíček příslušné verze RouterOS a můžeme začít:

```
netinstall# ./netinstall -r -i enp60s0 -a 192.168.88.3 routeros-7.18.2-
arm.npk
bash: ./netinstall: Adresář nebo soubor neexistuje
root@regulus:/home/gandalf/winapp/netinstall# ./netinstall-cli -r -i enp60s0
-a 192.168.88.3 routeros-7.18.2-arm.npk
Version: 7.18.2(2025-03-11 13:07:03)
Will reset to default config
Waiting for Link-UP on enp60s0
Waiting for RouterBOARD...
Assigned 192.168.88.3 to F4:1E:57:CD:50:CA
Booting device F4:1E:57:CD:50:CA into setup mode
Formatting device F4:1E:57:CD:50:CA
Sending packages to device F4:1E:57:CD:50:CA
Packages sent to device F4:1E:57:CD:50:CA
Rebooting device F4:1E:57:CD:50:CA
Successfully finished installing the device with MAC address
F4:1E:57:CD:50:CA
```

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

Permanent link:
https://wiki.spoje.net/doku.php/howto/network/mikrotik_klient

Last update: **2025/04/29 19:40**

