Obsah:

Úvod do RouterOS

Dokument jsme nazvali Seznámení s RouterOS a obsah je mu poplatný. Jeho smyslem není suplovat originální dokumentaci dostupnou na www.mikrotik.com či specializované české how-to dostupné na www.routeros.cz, nýbrž poskytnout nezbytný odrazový můstek pro všechny začínající české a slovenské uživatele.

Základem sítě Internet je protokol TCP/IP. K němu dále patří nespojový protokol UDP a protokol pro diagnostiku ICMP. V souvislosti se svým rozšířením pak Internet vytlačil protokoly, dříve hojně používané v lokálních sítích, jako je NetBEUI či IPX/SPX. Z nichž první jmenovaný neměl ani možnost pracovat ve směrovaných (routovaných) sítích. A právě routování sítí je hlavním posláním Mikrotik RouterOS.

Abychom mohli obsluhovat RouterOS, je nutné mít alespoň základní znalost sítí, síťového modelu ISO/OSI a TCP/IP. Pokud zmíněnými znalostmi nevládnete, je třeba to co nejdříve napravit.

Výborným a snad až příliš podrobným zdrojem informací jsou články p. Peterky, které jsou zdarma dostupné na adrese http://earchiv.isdn.cz/i_coje.php3.

Dalším skvělým zdrojem informací je server www.svetsiti.cz, kde v menu Tutorialy – Základy počítačových sítí, naleznete množství článků věnovaných určité problematice počítačových sítí.

MikroTik RouterOS používá až na výjimky zkrácený zápis masky sítě (např. 192.168.1.50/24), uvádím jednoduchou tabulku pro rozsah, kterou byste měli mít v hlavě. Šikovným pomocníkem Vám především v začátcích může být IP kalkulátor. Jeden z takových si můžete stáhnout například na http://www.studna.cz/go/detail.php/fid/1622.

255.255.0.0	/16	
255.255.255.0	/24	(prostor "C“ – 256 IP adres)
255.255.255.128	/25	
255.255.255.192	/26	
255.255.255.224	/27	
255.255.255.240	/28	
255.255.255.248	/29	
255.255.255.252	/30	
255.255.255.255	/32	(1 IP adresa)

Inicializace RouterOS

Ve chvíli, kdy se vám RouterOS dostane do rukou, je v defaultním nastavení. Při každém startu systému je provedena inicializace a každý podporovaný hardware je okamžitě připraven k použití. V defaultním nastavení jsou všechny zařízení zakázány. Prvotní nastavení je nutné provést přes příkazovou řádku. K té můžete přistupovat přes sériové rozhraní nebo přímo přes konzoli (monitor+klávesnice).

Příkazová řádka umožňuje kompletní administraci RouterOS. Ovládání je velmi intuitivní (nedá se mu upřít podobnost s konzolí produktů Cisco) a je vybavena bohatou nápovědou, která se dá kdykoliv vyvolat napsáním otazníku „?“. Přesto předpokládáme, že většině začínajících uživatelů bude bližší grafické rozhraní WinBox. Abyste ho mohli použít, musíte nastavit IP adresu a povolit síťové rozhraní (interface), přes který se k RouterOS

připojujete. Pro tyto účely je RouterOS vybaven jednoduchým průvodcem, který spustíte po přilogování k systému (jméno „admin“, prázdné heslo) příkazem `/ setup`.

Příkaz `/ setup` dává na výběr menu nastavení základních parametrů. Stisknutím „a“ zvolíte submenu nastavení IP adresy a brány. Opětovným stisknutím „a“ zvolíte nastavení IP adresy. V následujícím dotazu zvolíte interface, který chcete aktivovat. Pokud ho smažete a stisknete „?“, dostanete nápovědu všech dostupných interface. Po zvolení interface můžete zadat IP adresu ve tvaru např.: 192.168.1.50/24. Dvojím stisknutím „x“ potvrdíte změny. Funkčnost nastavení můžete ihned vyzkoušet příkazem `/ ping`. Pokud nastavení nefunguje, zkuste zapojit síťový kabel do ostatních síťových karet. Pokud vše funguje, můžete použít WinBox.

POZOR: Z bezpečnostních důvodů neponechávejte zapnutou konzoli. Vždy se odlogujte příkazem `/ quit`. Zabráníte tak případným „zvědavcům“ v nekalé činnosti, kteří by mohli mít přístup k lokální konzoli.

Aplikaci WinBox si stáhnete ze stránky, kterou zobrazíte v prohlížeči internetu, kam zadáte http://ip_adresa_RouterOS. Soubor winbox.exe uložte v počítači a spusťte. Vyplňte IP adresu, přihlašovací jméno a heslo a připojte se. Při prvním přihlášení se vám stáhnou pluginy nutné pro běh WinBoxu. Pluginy jsou rozdílné pro jednotlivé verze RouterOS, v případě upgrade se vám stáhnou nové.

Nastavení interfaces

V menu `interfaces` najdete všechny rozpoznané síťové adaptéry (metalické i bezdrátové). Také jsou zde zobrazeny virtuální adaptéry (bridge, IP tunely, virtuální AP). Můžete nastavit vlastní názvy interface, které se poté budou zobrazovat ve všech ostatních nastaveních, velikost MTU, režim ARP, u ethernetových karet rychlost a duplex (10/100 Mbps, full/half duplex, autodetekce), u bezdrátových karet parametry bezdrátové sítě (SSID, frekvenci, zabezpečení, rychlost atd..).

Pod tlačítkem `Settings` naleznete volbu `Wireless Tables`, což je tabulka autorizovaných MAC adres pro bezdrátové sítě.

Statické routování

Routování slouží k určování cest paketů v sítích TCP/IP. V menu `ip – routes` můžete zadávat statické routy. Kromě toho zde vidíte dynamické routy, které se automaticky tvoří ze zadaných IP adres. Jednou ze základních položek je defaultní brána (gateway), kterou vytvoříte přidáním statické routy s `Destination` 0.0.0.0/0 a vyplněním políčka `gateway`.

Nastavení DNS

Mikrotik RouterOS pro svou práci DNS nepotřebuje. Má ovšem zabudován interní DNS server, který je schopen odpovídat na požadavky překladu doménových názvů. K tomu potřebuje mít nastaven nadřazený doménový server. Zodpovězené dotazy si uchovává ve vyrovnávací paměti, čímž zrychluje vyřizování požadavků. Nastavení naleznete v `ip – dns – settings`.

Můžete zde dále zadat statické záznamy, které nebudou překládány, ale přesměrovány dle nastavení statického záznamu.

Synchronizace času pres NTP

Přestože na samotný chod směrovače to nemá vliv, je vhodné na něm zajistit aktuální čas. Co například s logovacími soubory, pokud mají zaznamenávané události špatný čas? Pokud používáme funkci `system – scheduler`, nemá ani smysl o správně nastaveném systémovém čase polemizovat.

Ruční nastavení systémové času můžeme provést přes menu `system – time`. Abychom však pokaždé nemuseli správný čas korigovat ručně, využijeme k tomu automatickou synchronizaci času přes protokol NTP (Network Time Protocol).

RouterOS umí s NTP pracovat jako klient i jako server pro ostatní stanice v síti. Veškeré volby naleznete v `system – ntp client` a `system – ntp server`. Pro nastavení NTP klienta potřebujeme znát IP adresu serveru, podle kterého provádíme synchronizace. Seznam volně dostupných serverů naleznete na adresách:

http://www.eecis.udel.edu/~mills/ntp/clock1a.html
http://www.eecis.udel.edu/~mills/ntp/clock2a.html

Nastavení DHCP (klient i server)

Mikrotik RouterOS může obsluhovat dynamické přidělování IP adres. Konfigurace DHCP serveru sestává z několika kroků:

Nejprve je třeba definovat rozsah přidělovaných adres, který lze nastavit v `ip – pool`. Po přidání položky zvolte název a rozsah požadovaných adres, který můžete zadat ve tvaru např. 192.168.1.100-192.168.1.150, popř. pomocí tlačítka `[…]` můžete přidat jednotlivé IP adresy či více rozsahů.

Ostatní nastavení se provádí v `ip – dhcp server`. Na záložce DHCP definujete nastavení serveru, který adresy přiděluje. Po přidání položky zvolte název, interface, na kterém mají být adresy přidělovány, expirační dobu a rozsah IP adres, který jste definovali v `ip – pool`.

Pokud nechcete přidělovat dynamické IP adresy ale pouze statické, můžete zvolit `static-only`. DHCP server bude přidělovat pouze adresy definované na záložce `Leases`. Na záložce `Networks` nastavíte údaje přidělované DHCP serverem – gateway, maska sítě, DNS servery, doménu a servery WINS. Pomocí položky `Address` nastavíte, jakým IP adresám se mají údaje přidělovat.

Na záložce `Leases` vidíte přidělené IP adresy, popř. jak bylo řečeno výše, můžete zde nastavit statické záznamy i mimo rozsah adres definovaných v `ip – pool`.

Mikrotik RouterOS může pracovat i jako DHCP klient. Nastavení naleznete v `ip – dhcp client`. Nastavení je jednoduché, klienta pouze zapnete a nastavíte interface, na kterém má být DHCP klient aktivní.

Nastavení source NAT

Pokud používáte privátní IP adresy, musíte pro jejich přístup do vnější sítě nastavit překlad adres neboli NAT (network address translation). Nastavení se provádí v `ip – firewal - source nat`. Pro překlad adres stačí pouze přidat nový záznam, kde v `Src. Address` zvolíte skupinu IP adres, většinou celý rozsah privátních adres (např. 192.168.1.0/24), v `Out. interface` zvolíte interface, kterým pakety opouští směrovač (můžete ponechat all) a na záložce `Action` nastavíte `Action` na `Masquerade`.

Nastavení destination NAT

Ve chvíli, kdy jste zprovoznili směrovač pro privátní síť a vnitřní počítače mohou na Internet, většinou potřebujete namapovat některé vnější porty na vnitřní počítače. Mimo jiných případů i tento pokrývá `destination NAT`. Naleznete ho, podobně jako `source NAT`, v `ip – firewall – destination nat`.

Nastavení není složité. Po přidání stačí nastavit následující položky:

Na záložce general:

`Src. address` – zdrojová adresa, zde můžete nastavit, že se na daný mapovaný port půjde přihlásit pouze z jedné IP adresy, popř. rozsahu
`In. Interface` – příchozí interface, můžete ponechat all
`Dst. Address` – cílová adresa, jedná se o VNĚJŠÍ adresu směrovače, tedy adresu, na kterou se budou hlásit vnější uživatelé. Pokud se jedná pouze o jednu adresu, musí mít masku /32.
`Dst. Port` – port, na kterém budou požadavky přijímány, může být odlišný od portu vnitřní IP adresy, na kterou se budou požadavky směrovat
`Protocol` – protokol, na který se má pravidlo aplikovat. Pokud chcete definovat jednotlivé porty, musíte zvolit protokol tcp

Na záložce action:

`Action` – typ akce, v našem případě to bude `nat`
`To Dst. Addresses` – cílové adresy ve vnitřní síti, zadejte do obou políček cílovou adresu
`To Dst. Ports` – cílový port vnitřní IP adresy

Základní práce s paketovým firewallem

Mikrotik RouterOS disponuje pokročilým firewallem, který umožňuje pracovat s pakety procházející směrovačem. Pravidla pro práci s pakety můžete nastavit v `ip – firewall`, záložka `Filter Rules`.

Pravidla ve `Filter Rules`, jsou rozdělena do tří základních skupin, tzv. `Filter Chains`:

`Input` – pravidla aplikující se na pakety, které přichází některým rozhranním a končí na směrovači. Mohou to být např. pingy, administrační pakety (WinBox, ssh) atd…

`Forward` – pravidla pro pakety, které prochází směrovačem, na tyto pakety se neuplatňují pravidla uvedené v `Input` či `Output`
`Output` – pravidla pro pakety, které vznikly na směrovači a odcházejí některým rozhranním. Mohou to být odpovědi na pingy, komunikace s WinBoxem, ssh atd…

Můžete si (např z důvodu přehlednosti) definovat vlastní `Filter Chain`. Pokud budete chtít jejich aplikaci, musíte v některém z defaultních `Filter Chains` definovat pravidlo, které přesměruje datový tok do vašeho `Filter Chain`. Nastavení takového pravidla naleznete níže.

Každé pravidlo ve firewallu se skládá z podmínek definující pakety, s nimiž chcete pracovat, a akce, která má být s těmito pakety provedena. Pravidlo může být aplikováno na základě následujících podmínek:

`Src. address` – zdrojová adresa
`Src. port` – zdrojový port
`In. Interface` – příchozí rozhraní paketu
`Dst. Address` – cílová adresa
`Dst. Port` – cílový port
`Out. interface` – odchozí rozhraní paketu
`Protocol` – protokol, na jehož pakety bude pravidlo aplikováno
`Content` – textový řetězec, který musí paket obsahovat
`Flow` – značka, kterou paket obdržel při značkování paketů (mangling), značkování paketů je popsané v sekci Bandwidth management
`Connection` – stejně jako flow
`P2P` – zahrnutí paketů některého (všech) z výměnných systémů P2P
`Src. MAC Address` – zdrojová MAC adresa
`TOS` – Type of service, typ služby
`Limit count, Limit burst, Limit time` – omezení funkčnosti pravidla na určitý počet hitů za stanovený čas

S paketem vybraným dle podmínek můžete provést následující akce:

`Accept` – paket je akceptován a puštěn dál
`Drop` – paket je zahozen, není generováno chybové hlášení
`Reject` – paket je odmítnut, směrovač vygeneruje chybové hlášení ICMP
`Passthrough` – není aplikována žádná akce, pravidlo se chová, jako by bylo vypnuto. Může být použito pro počítání paketů
`Jump` – provede skok do určeného Chainu
`Return` – vrátí se do předchozího Chainu

Na záložce `Statistics` vidíte počet bytů a paketů, na které bylo toto pravidlo aplikováno. Rovněž si můžete nechat aktivitu pravidla nechat logovat. Je vhodné (pro případ časté aplikace pravidla) zkontrolovat nastavení loggingu (viz sekce **Lokální a vzdálené logování událostí)**

Bandwidth management

Problematika nastavení omezování rychlostí je popsána v samostatném How-to RouterOS – Řízení datových toků
http://www.routeros.cz/data/routeros_rizeni_datovych_toku.pdf
Zde zmíním jen základní nastavení.

MikroTik RouterOS disponuje širokými možnostmi omezování a řízení datových toků. Od omezování jednotlivých IP adres po upřednostňování jednotlivých protokolů, portů, omezování skupin IP adres (sdílené linky).

Omezování se provádí pomocí Queues. Mikrotik rozeznává dva typy Queues: `Simple queues` a `Queue tree`. `Simple queues` se používají pro jednoduché a rychlé nastavení omezení. Jdou použít pouze pro omezení jednotlivých IP adres, popřípadě skupin definovaných síťovou maskou. `Queue tree` se dají použít pro pokročilé řízení provozu. Základem jejich fungování je označování paketů, tzv. mangling, který se nastavuje v `ip – firewall – mangle`. Označování paketů je podobné jako zadávání pravidel ve firewallu. Paket se označí na základě daných podmínek. Značkou (`flow`, `connection`) se rozumí textový řetězec, kterým je paket označen v rámci směrovače. Pomocí značky můžete s paketem pracovat v různých nastaveních (např. firewall, routování) včetně `Queue tree`. Můžete označit všechny pakety které mají cílový port 80 (http) a upřednostnit před ostatními pakety. Konfiguraci označování paketů, `Simple queues` a `Queue tree` naleznete ve výše uvedeném How-to.

Jak na hotspot

Hotspot je systém pro ověřování a účtování uživatelů, připojujících se jak přes bezdrátové, tak přes metalické připojení. Zastřešuje ověřování a připojování klientů pomocí jména a hesla prostřednictvím vestavěného web serveru. Příklad použití je připojení hotelových hostů, stavba veřejných přístupových bodů k Internetu atd. Pro připojování zákazníků pomocí bezdrátových karet nebo PPPoE není hotspot zapotřebí.

Diagnostické utility

RouterOS Vám nabízí řadu utilit pro diagnostiku sítě. Všechny naleznete v menu `tools`:

`Ping`	Základní utilita pro ověření dostupnosti vzdálené IP adresy
`Ping MAC`	Ověření vzdáleného síťového zařízení na základě MAC adresy, funguje pouze mezi systémy Mikrotik
`Traceroute`	Na základě zadané IP adresy zobrazí směrovače po cestě k ní
`Bandwidth test`	Měření propustnosti k jinému RouterOS nebo Windows stanici s běžícím programem Bandwidth tester, ke stažení: http://www.mikrotik.com/download/BandwidthTest.zip
`Btest server`	Zapíná bandwidth server pro vzdálené klienty, opačný případ předchozí utility
`Packet Sniffer`	Utilita pro odchytávání paketů, možnost zobrazení ve WinBoxu nebo přesměrování na jiný stroj
`Torch`	Monitorování aktuálního provozu s možnostmi zobrazování dle kritérií (zdrojová IP adresa, port, protokol, cílová adresa)
`Mac Server`	Nastavení služby `mac telnet`, obdoba klasického telnetu bežícího na základě mac adres, pouze pro mikrotik, k dispozici klient pro windows http://www.mikrotik.com/download/neighbour.zip
`Ping Speed`	Orientační výpočet rychlosti linky na základě příkazu ping
`Flood ping`	Odeslání velkého počtu pingů o dané velikosti
`Netwatch`	Monitoring dostupnosti IP adres v síti, možnost spuštění libovolného skriptu při událostech UP/DOWN

Lokální a vzdálené logování událostí

Seznam událostí, které RouterOS dovoluje logovat naleznete pod menu `system – logging`. U každé z událostí máte možnost nastavit čtyři druhy zacházení se vzniklým záznamem:

`None`	Ignoruje jakoukoliv událost
`Memory`	Zaznamená událost do paměti, která je pak přístupná přes menu `Log`. Záznam událostí je při každém rebootu smazán.
`Disk`	Zaznamenává události na CF. Tuto možnost strikně nedoporučujeme vzhledem k omezenému množství zápisů na CF. Snižujete tak její životnost.
`Remote`	Logování událostí na vzdálený Syslog server. Tím může být například Linuxový Syslog (spuštěný s volbou „-r“) nebo některá z Windows alternativ. Na adrese http://www.mikrotik.com/download.html#syslog můžete stáhnout Windows Syslog server přímo od Mikrotiku.

Lehký úvod do skriptování

Mikrotik RouterOS disponuje skriptovacím jazykem, který umožňuje základní práci se smyčkami, podmínkami a proměnnými. Psaní skriptů již vyžaduje určitou znalost systému a technické angličtiny, zkušenější uživatel by si s tím měl být schopen poradit. Skripty jsou uloženy v `/system scripts`. Je možné je psát ve WinBoxu, nebo přímo v příkazové řádce, kde je implementován multiřádkový editor, který můžete vyvolat příkazem `/system script edit <název_skriptu> source`.

Příklad “ručního“ netwatche (výhodou je, že pošle 5 pingů, než označí stroj za nedostupný):

```
:if ([/ping 192.168.1.199 count=5] = 0) \
do= {
    :log message "Can't ping 192.168.1.199"
    } \
else={   :log message "192.168.1.199 is running"    }
```

Anglickou příručku skriptovacího jazyka pro RouterOS naleznete zde http://www.mikrotik.com/docs/ros/2.8/system/scripting.content.
Příklady skriptů zde http://www.mikrotik.com/docs/ros/2.8/appex/scripting1.content.

Export, import a zálohování konfigurace

Konfigurace routeru může být kompletně zazálohována pomocí funkce `/system backup save name <název_souboru>`. Pokud není zadán název souboru, RouterOS vygeneruje název z data a času vytvoření zálohy. Záloha může být také vytvořena ve WinBoxu ve `files – backup`. Obnova se může provést buď `/system backup load name <název_souboru>`, nebo opět z WinBoxu `files – restore` poté co kliknete na příslušný soubor zálohy. RouterOS poté vyžaduje restart. Pokud provádíte obnovu zálohy na stejném stroji, obnova se provede v plném rozsahu. Pokud obnovu provádíte na jiném stroji, s největší pravděpodobností se neobnoví správně interfaces, které pak musíte dokonfigurovat ručně.

Kromě kompletní zálohy je možné exportovat a importovat jednotlivé části konfigurace pomocí příkazu `export`, který spustíte v dané sekci, např. `/interface ethernet`

`export` vypíše na obrazovku kompletní konfiguraci ethernetových rozhranní tak, jak byste ji museli zadat přes příkazovou řádku. Příkaz export můžete použít s parametrem `file <název_souboru>`, kterým můžete exportní skript uložit do souboru.

Importování konfigurace se provádí přes příkaz `/system import <název_souboru>`.
Pozor, u pravidel firewallu, queues apod. nedojde importem k přepsání konfigurace, ale k přidání nových pravidel ke stávajícím. Je proto nutné stará pravidla smazat, aby nedošlo k duplicitám.

Pro přenos souborů z/do směrovače lze použít ftp nebo scp klienta. Je však vhodné řídit se doporučeními uvedenými v sekci Základy bezpečnosti.

Základy bezpečnosti

Bezpečností směrovače rozumíme zajištění bezpečné komunikace a administrace se směrovačem. Zabezpečení RouterOS je rozebráno v how-to http://www.routeros.cz/data/routeros_zakladni_zabezpeceni.pdf .
V případě RouterOS tuto bezpečnost ovlivňuje z největší části správce.

Upgrade firmware

Mikrotik RouterOS je možné (v případě, že vám to umožňuje licence) upgradovat či downgradovat na libovolnou minoritní verzi. Downgrade doporučujeme používat pouze v případě, kdy jste si jisti, že daná vyšší verze obsahuje chybu, která v nižší verzi nebyla. Z důvodu změny licenčních pravidel není možné přejít z verze 2.8.x na 2.7.x. Ve verzi 2.9.x by licenční pravidla neměla být změněna.

Upgrade i downgrade se provádí podobně nakopírováním příslušných balíčků na směrovač. V případě upgrade stačí pouze provést reboot, buď pomocí příkazu, nebo zapomocí Ctrl+Alt+Delete na konzoli. Downgrade se musí provést ručně příkazem `/system package downgrade`.

V obou případech zůstane na směrovači zachována konfigurace. Avšak i přes vysokou spolehlivost tohoto procesu doporučujeme provést zálohu konfigurace.

Seznam balíčků

Název	Obsah	Závislost	License
advanced-tools	**email klient, pingers, netwatch a další utility**	**none**	**none**
arlan	**Podpora pro DSSS 2.4GHz 2mbps Aironet ISA karty**	**none**	**2.4GHz/5GHz Wireless Client**
dhcp	**Podpora DHCP serveru a klienta**	**none**	**none**
gps	**Podpora pro GPS zařízení**	**none**	**none**
hotspot	**HotSpot gateway**	**none**	**any additional license**

isdn	**Podpora ISDN zařízení**	**ppp**	**none**
lcd	**Podpora pro informační LCD display**	**none**	**none**
ntp	**Podpora network time protocol**	**none**	**none**
ppp	**Podpora pro PPP, PPTP, L2TP, PPPoE a ISDN PPP**	**none**	**none**
radiolan	**Poskytuje podporu pro 5.8GHz RadioLAN cards**	**none**	**2.4GHz/5GHz Wireless Client**
routerboard	**Podpora pro specifické funkce a nástroje RouterBoard**	**none**	**none**
routing	**Dynamické routování RIP, OSPF a BGP4**	**none**	**none**
security	**Silně doporučujeme! Podpora pro IPSEC, SSH a kryptované spojení WinBox**	**none**	**none**
synchronous	**Podpora pro Frame Relay a Moxa C101, Moxa C502, Farsync, Cyclades PC300, LMC SBE a XPeed synchronní karty**	**none**	**Synchronous**
system	**Základní systém**	**none**	
telephony	**Podpora IP telefonie (H.323)**	**none**	**none**
ups	**Podpora monitoringu záložních zdrojů APC Smart Mode UPS**	**none**	**none**
web-proxy	**Podpora HTTP Web proxy**	**none**	**none**
wireless	**Podpora pro bezdrátové karty Cisco Aironet, PrismII, Atheros. V režimech stanice i AP.**	**none**	**2.4GHz/5GHz Wireless Client / 2.4GHz/5GHz Wireless AP**
wireless-legacy	**Starší verze balíčku wireless bez podpory protokolu nstreme**	**none**	**2.4GHz/5GHz Wireless Client / 2.4GHz/5GHz Wireless AP**

Reset do defaultního nastavení

Reset provede výmaz všech nastavení a uvedení RouterOS do defaultního stavu, kdy nejsou zaktivovány ani žádné síťové rozhraní. Proto jej provádějte, pokud máte přístup k lokální administraci, tedy přes klávesnici nebo seriové rozhraní.

```
/ system reset
```