EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY

SPRÁVA SÍŤOVÝCH ZAŘÍZENÍ MIKROTIK – MTCNA

URČENO PRO VZDĚLÁVÁNÍ V AKREDITOVANÝCH STUDIJNÍCH PROGRAMECH

JIŘÍ BALEJ

KONKURENCESCHOPNÝ ABSOLVENT
MENDELOVY UNIVERZITY V BRNĚ

REGISTRAČNÍ ČÍSLO PROJEKTU:
CZ.02.2.69/0.0/0.0/16_015/0002365

BRNO 2018

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

Název:	Správa síťových zařízení MikroTik – MTCNA
Autor:	Jiří Balej
Vydání:	první, 2018
Počet stran:	57

Jazyková korektura nebyla provedena, za jazykovou stránku odpovídá autor.

Obsah

Anotace

Předkládaná výuková opora je určena pro předmět Správa síťových zařízení MikroTik – MTCNA, který studentům poskytuje úvod ke správě zařízení od firmy MikroTik a připravuje je na složení certifikace MTCNA (MikroTik Certified Network Associate). V této opoře jsou zahrnuta následující témata:

- Úvod do síťových zařízení MikroTik:
  - O MikroTiku.
  - Připojení k RouterOS.
  - Výchozí konfigurace RouterOS.
- Základy správy síťových zařízení MikroTik:
  - Aktualizace RouterOS.
  - Správa balíčků
  - Základní správa zařízení.
  - Záloha a obnovení konfigurace.
  - Licencování.
- Protokoly DHCP a ARP:
  - Protokol DHCP.
  - Protokol DNS.
  - Protokol ARP.
- Přepínaní rámců na RouterOS:
  - Nastavení logických rozhraní – bridge.
  - Přepínání rámců dle hardwarové architektury.
  - Bridge u bezdrátového rozhraní.
- Směrování na RouterOS:
  - Směrování a směrovací tabulka.
  - Statické směrování.
  - Dynamické směrování – OSPF.
- Bezdrátové připojení:
  - Bezdrátové standardy a omezení na jejich použití.

Úvod

Předkládaná výuková opora, která se Vám dostává do ruky, byla vytvořena v rámci projektu „Konkurenceschopný absolvent Mendelovy univerzity v Brně“, reg. číslo CZ.02.2.69/0.0/0.0/16_015/0002365.

Výuková opora plně pokrývá požadavky učebních osnov povinného předmětu Správa síťových zařízení MikroTik pro posluchače kombinované formy studia ve studijním programu Administrace IS/ICT na Provozně ekonomické fakultě Mendelovy univerzity v Brně. Tato opora může být samozřejmě použita jako vhodný studijní materiál i pro studenty prezenční formy studia v rámci stejnojmenného předmětu.

Cíle předmětu:
Po prostudování tohoto předmětu:

- naučíte se ovládat a konfigurovat síťová zařízení s RouterOS,
- dozvíte se jak aktualizovat RouterOS a zprovoznit či vypnout různé služby,
- budete umět provést konfiguraci protokolů pro lokální sítě,
- budete schopni propojit několik fyzických rozhraní pro práci v lokální síti,
- naučíte se, nakonfigurovat statické i dynamické směrování,
- dozvíte se, jak správně nastavit zabezpečenou bezdrátovou síť,
- pochopíte, jak funguje firewall a jak zprovoznit překlad adres,
- budete schopni nastavit fronty, pro aplikaci QoS i omezení rychlosti,
- naučíte se různé tunelovací mechanismy včetně VPN,
- a budete umět používat diagnostické a monitorovací nástroje.

Výuková opora je členěna do následujících kapitol:

1. Úvod do síťových zařízení MikroTik.
2. Základy správy síťových zařízení MikroTik.
3. Protokoly DHCP a ARP.
4. Přepínaní rámců na RouterOS.
5. Směrování na RouterOS.
6. Bezdrátové připojení.
7. Firewall.

8. QoS a mechanismy front.
9. Tunelové mechanismy a VPN.
10. Další nástroje a monitoring.

Jednotlivé kapitoly zpravidla obsahují:

- formulaci cílů kapitoly (tedy toho, co by měl student po jejím prostudování umět, znát, pochopit),
- klíčová slova,
- průvodce studiem,
- vlastní výklad učiva,
- kontrolní otázky k procvičení učiva,
- příklady,
- úkoly k zamyšlení,
- korespondenční úkol,
- pojmy k zapamatování
- a shrnutí.

Zařazené korespondenční úkoly mají charakter individuální seminární práce, která je určena k ověření Vašich schopností aplikovat získané teoretické znalosti na analýzu konkrétní problematiky. Povinnou součástí Vašich studijních povinností je vypracování dvou lektorem vybraných korespondenčních úkolů. Jejich bodová hodnocení budou započtena do celkového hodnocení předmětu.

V každé kapitole je uvedeno vše potřebné pro samostatné studium, počínaje definicemi základních pojmů a konče využitím teoretických poznatků v praxi. Vše je doplněno informacemi, jak danou funkcionalitu nakonfigurovat. V těchto místech je čtenář odkazován na oficiální dokumentaci k RouterOS, která umožní studentům dostudovat všechny dílčí vlastnosti. Pro úspěšné studium doporučujeme v průběhu studia zkoušet si jednotlivá nastavení na lokální instalaci RouterOS a vlastní experimentování pro úplné pochopení probírané látky.
Čas potřebný k prostudování jednotlivých lekcí explicitně neuvádíme, neboť z našich zkušeností vyplývá, že rychlost studia závisí na Vašich schopnostech a studijních návycích.

Předpokládáme, že si mnozí z Vás budou chtít doplnit a rozšířit poznatky studiem dalších literárních pramenů a elektronických zdrojů. Oficiální studijní materiál ke kurzu MTCNA (MirkoTik Certified Network Associate) je prezentace [1], jejíž kopii Vám dá vyučující k dispozici. Vzhledem k tomu, že RouterOS je neustále se vyvíjející systém, je dalším vhodným a aktuálním zdrojem elektronická dokumentace v podobě MikroTik Wikipedie [2]. Také je možné využít vydaných knižních zdrojů např. [3], [4] a [5], kde však informace postupně zastarávají, ale základní principy by měly být platné stále.

platné. V případě, že na své otázky nenaleznete odpovědi nebo Vás budou zajímat další detaily a novinky, je vhodné se podívat na prezentace z pravidelných setkání uživatelů MikroTik [6] a také na oficiální fórum [7].

Věříme, že Vám předkládaný studijní materiál pomůže pochopit základní principy fungování zařízení postavených na RouterOS, a přejeme Vám hodně úspěchů ve studiu.

Kapitola 1

Úvod do síťových zařízení MikroTik

V této kapitole se dozvíte

- Čím se zabývá firma MikroTik?
- Co je to RouterOS a na jakém systému je postaven?
- Jakými způsoby je možné se připojit zařízení s RouterOS?
- Pomocí jakého SW je možné konfigurovat RouterOS?
- Co obsahuje výchozí konfigurace zařízení s RouterOS?
- Jakým způsobem je možné aktuální konfiguraci vyresetovat?

Po jejím prostudování byste měli být schopni

- Vědět na jaká zařízení je možné nainstalovat RouterOS.
- Identifikovat typ a počet rozhraní dle označení RouterBoardu.
- Orientovat se v konfiguračním programu WinBox a ovládat konfiguraci pomocí příkazového řádku.
- Vědět, který způsob pro konfiguraci zařízení MikroTik je bezpečný.
- Vybrat vhodnou výchozí konfiguraci (Quick Set).
- Umět vyresetovat různými způsoby aktuální konfiguraci a vynutit tzv. prázdnou konfiguraci.

Klíčová slova: MikroTik, RouterOS, RouterBoard, Winbox, WebFig, CLI, console, telnet, SSH, null kabel.

Průvodce studiem kapitoly

V této kapitole jsou popsány základní informace o firmě MikroTik a zařízeních, která vyrábí a o operačním systému RouterOS, který je na nich naistalován. Dozvíte se, jakým způsobem je možné provádět konfiguraci zařízení s RouterOS a jak je možné spustit automatickou konfiguraci. Velice důležité je znát obsah výchozí konfigurace a umět tuto konfiguraci obnovit, případně úplně vymazat.

1.1 O MikroTiku

MikroTik je Lotyšská společnost, která se od roku 1996 zabývá vývojem operačního systému RouterOS, který je postaven na Linuxovém jádře a umožňuje vytvořit z počítače router s pokročilými funkcemi. Jakými vlastnostmi RouterOS disponuje se můžete dočíst na wikistránce Manual:RouterOS_features a bude o nich řeč dále v textu tohoto materiálu. Samotný operační systém je zkompilován nejen na produkty z produkce MikroTiku (viz mikrotik.com/download), ale také na obyčejné PC (x86) a je připraven i image pro různé virtualizace (tzv. CHR – Cloud Hosted Router).

Kromě operačního systému produkuje MikroTik také hardwarová zařízení (RouterBoard) – routery, switche, základní desky, bezdrátové přístupové i point-to-point zařízení, rozhraní a různé příslušenství. Více o aktuálně dostupném hardwaru a jeho vlastnostech, je možné najít na stránce mikrotik.com/products. K orientaci v názvech MikroTik produktů a jejich číslování doporučujeme pročíst wikistránku Manual:Product_Naming.

1.2 Připojení k RouterOS

Pro správu a konfiguraci zařízení s operačním systémem RouterOS je možné využít několika cest. První z nich je možnost připojit přímo klávesnici a monitor, což můžeme udělat v případě nainstalovaní na PC nebo VM. Druhou možností je konfigurace z jiného PC pomocí připojení na konzoli přes sériový nebo USB port pomocí tzv. null kabelu (u jiných výrobců známý jako konzolový kabel) – viz Manual:Console. Poslední a zároveň nejčastěji používaným způsobem je připojení přes datový port (drátový i bezdrátový) a to přes IP adresu pomocí standardních protokolů telnet, SSH, HTTP(S) nebo pomocí programu WinBox (Manual:Winbox). WinBox může být využit i pro objevení[1] zařízení s RouterOS, které jsou přímo připojeny na přenosové médium (Ethernet) a následné připojení k nim i přes MAC adresu, což je výhodné především, když zařízení nemá (správnou) konfiguraci IP protokolu.

Po úspěšném připojení k zařízení je možné provést konfiguraci třemi různými způsoby viz Manual:First_time_startup. Za první pomocí příkazového řádku pomocí připojené klávesnice a monitoru, přes konzoli nebo protokol Telnet či SSH. Přestože tento způsob může být na první pohled složitý a nepřehledný, je velice často využívat pro

[1] Objevování sousedů se děje pomocí proprietárního protokolu MNDP, o kterém se můžete více dozvědět na Manual:IP/Neighbor_discovery.

jeho efektivnost při aplikaci více stejných příkazů. Ovládání RouterOS pomocí konzole je popsáno na wikistránce Manual:Console a doporučujeme se s ní velmi dobře seznámit. Druhým způsobem je využít ke konfiguraci webový prohlížeč a nástroj nazvaný WebFig, který je grafický a dovoluje relativně snadno provádět jednoduché změny, více konfiguraci přes webový prohlížeč najdete na Manual:Webfig. Třetím a zároveň nejčastěji používaným způsobem je program WinBox, který představuje GUI aplikaci umožňující otevřít více oken s různými částmi nastavení. Výhodou je taktéž varianta připojení přes MAC i IP adresu a také možnost ve svém okně spustit také konzoli. Ovládání systému RouterOS pomocí WinBoxu je důkladně popsáno na stránce Manual:Winbox a je nezbytné jej dobře znát.

Ve všech případech konfigurace je silně doporučeno používat zabezpečenou variantu – tedy SSH místo Telnet, HTTPS (port 443) místo HTTP (port 80) a ve WinBox zapnout tzv. Secure Mode.

1.3 Výchozí konfigurace RouterOS

Ve výchozím stavu je na zařízení s RouterOS tzv. výchozí konfigurace (default configuration), která se liší dle typu samotného zařízení a je připravena tak, aby umožnila uživateli co nejsnadnější použití – ve spoustě případů není potřeba téměř nic měnit. Popis jednotlivých typů výchozích konfigurací je možné najít na wikistránce Manual:Default_Configurations a tyto výchozí konfigurace jsou nabízeny v menu `Quick Set`, kde je možné jednoduše nastavit vlastnosti předpřipravené „výchozí“ konfigurace.

Pro restart do výchozí konfigurace je možné v menu WinBoxu vybrat možnost `System` → `Reset Configuration`, v případě nedostupnosti konfiguračního rozhraní je možné reset provést podržením resetovacího tlačítka na RouterBoardu po dobu 5 sekund (Manual:Reset_button) v průběhu spouštění – viz Manual:Reset#Button_reset.

Když chceme operační systém nastavit dle vlastních představ je nejvhodnější začít z prázdné konfigurace, kterou je možné vynutit při resetování z konfiguračního menu, kde u volby `System` → `Reset Configuration` je třeba zaškrtnout `No Default Configuration`.

1.4 Shrnutí kapitoly a úkoly k procvičení

1.4.1 Kontrolní otázky

1. Čím se zabývá společnost MikroTik a kde sídlí?
2. Jak se nazývají fyzická zařízení od firmy MikroTik.
3. Kolik portů (ethernetových, bezdrátových, popř. jiných) mají následující zařízení a jaké další vlastnosti tato zařízení mají:
   (a) RB951Ui-2HnD
   (b) RB433AH

(c) RB921GS-5HPacD-15S

(d) CCR1036-8G-2S+EM

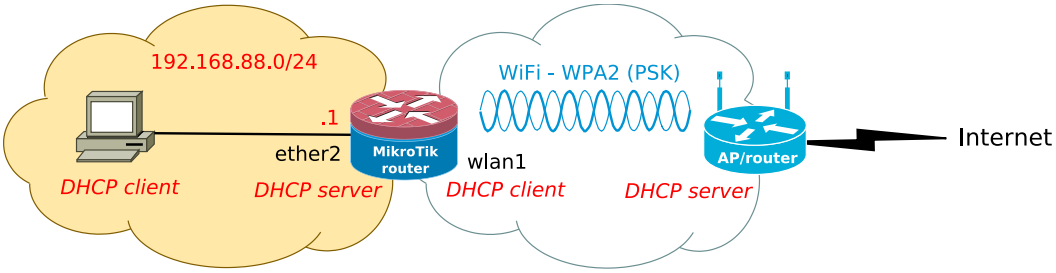
4. Jaké jsou možnosti připojení se k zařízení MikroTik pro provedení konfigurace?
5. Jaké nástroje (programy) lze využít ke konfiguraci zařízení s RouterOS?
6. Které varianty přístupu k zařízení s RouterOS jsou bezpečné (přenášejí informace zabezpečenou cestou)?
7. Co obsahuje výchozí konfigurace domácího Wifi routeru MikroTik?
8. Jakými způsoby je možné vyresetovat konfiguraci RouterOS.

1.4.2 Úkoly k zamyšlení

1. Jaké produktové řady prodává MikroTik a k jakým účelům se jednotlivé řady hodí?
2. Popřemýšlejte, jakým nejjednodušším způsobem je možné zprovoznit MikroTik na osobním počítači (pro testovací účely).
3. Zamyslete se, které způsoby přístupu k zařízení jsou v kterém okamžiku nejvhodnější?
4. Kdy je vhodné využít nějakou z předpřipravených konfigurací (Quick Set) a kdy je vhodné začít konfigurovat z prázdné konfigurace?

1.4.3 Korespondenční úkol

Pro provedení korespondenčního úkolu postupujte podle následujících kroků:



Obrázek 1.1: Topologie zapojení pro korespondenční úkol 1.4.3

1. Připojte si k MikroTik routeru osobní počítač pomocí kabelu a připravte si přístupové údaje k bezdrátovému (např. domácímu) routeru s WPA2 PSK autentizací, který Vás připojí na Internet. Zapojení úlohy je na obrázku 1.1. [2]

[2] Alternativně je možné využít VM routeru MikroTik (virtualizovanou pomocí Oracle VirtualBox) se síťovou kartou ether1 (místo wlan1) připojenou k NAT a kartou ether2 připojenou do Sítě pouze s hostem. V tom případě vynechejte kroky 7, 9, 10 a v krocích 8 a 11 použijte jako rozhraní `ether1`.

2. Vyresetujte MikroTik router – stiskněte tlačítko pro reset a držte jej stisknuté prvních 5 sekund zapínání (více viz Manual:Reset#Button_reset). Pokud máte na zařízení přístup např. přímo na monitor (VM ve VirtualBox) nebo přes CLI je možné provést reset pomocí příkazu: `/system reset-configuration`.
3. Po vyresetování by měla být v routeru přítomna tzv. výchozí konfigurace obsahující na rozhraní ehter2 DHCP server.
4. Získejte/Obnovte IP konfiguraci na počítači, tak aby příslušné rozhraní získalo IP adresu z DHCP serveru na MikroTik routeru.
5. Vyzkoušejte různé způsoby připojení na IP adresu MikroTik routeru (`192.168.88.1`) – telnet a SSH (např. pomocí programu PuTTY), WebFig (pomocí webového prohlížeče) a Winbox (program stáhnete ze stránky mikrotik.com/download). Výchozí uživatelské jméno je `admin` bez žádného hesla.
6. Vyzkoušejte objevení MikroTik routeru a připojení se na něj pomocí MAC adresy. Ve Winbox, přejděte na záložku Neighbors a počkejte až se Vám objeví MikroTik router. Kliknutím na MAC adresu routeru se Vám vyplní do pole `Connect To:` a tlačítkem `Connect` se připojíte. Výhodou MAC Winboxu je možnost připojení i v případě výpadku IP adresy, což můžete vyzkoušet, když zneaktivníte (`disable`) IP adresu na bridge rozhraní (`IP` → `Address`, vybrat příslušný řádek a `disable` nebo z CLI pomocí příkazu `/ip address disable` *číslo řádku*).
7. V nabídce `Bridge` → `Ports` odeberte rozhraní `wlan1` nebo z CLI: `/interface bridge port remove` *číslo řádku*.
8. Nastavte DHCP client na `wlan1` rozhraní – `IP` → `DHCP Clinet` → `Add` nebo z CLI: `/ip dhcp-client add interface=`*název rozhraní* `disabled=no`.
9. Nastavte nový security profil (`Wireless` → `Security Profiles`), kde vyplňte WPA2 PSK (pre-shared key) nebo z CLI: `/interface wireless security-profiles add name=`*jméno* `mode=dynamic-keys authentication-types=wpa2-psk wpa2-pre-shared-key=`*heslo*.
10. Následně nastavte tento security profil k WiFi rozhraní (`Wireless` → `Interfaces`) a nastavte mód rozhraní na `station` nebo z CLI: `/interface wireless set mode=station security-profile=`*název profilu* `numbers=`*číslo řádku*.
11. V menu `IP` → `Firewall` → `NAT` přidejte pravidlo v řetězci `srcnat`, které při odchodu rozhraním `wlan1` provede akci (`Action`) `masquerade` nebo z CLI: `/ip firewall nat add chain=srcnat out-interface=wlan1 action=masquerade`.
12. Vyzkoušejte funkčnost řešení, pomocí příkazu `ping` na adresu v Internetu (např. `www.mikrotik.com`) z počítače, z WinBoxu (`Tools` → `Ping`) i z CLI: `/ping` *adresa*.

1.4.4 Pojmy k zapamatování

- RouterOS,
- RouterBoard,
- CHR – Cloud Hosted Router,

- null kabel,
- Winbox,
- WebFix,
- Default Configuration,
- Quick Set.

1.4.5 Příkazy vysvětlené v této kapitole

- `/system reset-configuration`
- `/ip address disable` *číslo řádku*
- `/interface bridge port remove` *číslo řádku*
- `/ip dhcp-client add interface=`*název rozhraní* `disabled=no`
- `/interface wireless security-profiles add name=`*jméno* `mode=dynamic-keys authentication-types=wpa2-psk wpa2-pre-shared-key=`*heslo*
- `/interface wireless set mode=station security-profile=`*název profilu* `numbers=`*číslo řádku*
- `/ip firewall nat add chain=srcnat out-interface=wlan1 action=masquerade`
- `/ping` *adresa*

1.4.6 Shrnutí

Lotyšská firma MikroTik se zabývá vývojem operačního systému RouterOS, který umožňuje snadno konfigurovat obyčejné PC či jiné zařízení jakou síťové zařízení. Firma MikroTik vyrábí mnoho rozličných produktů (pod názvem RouterBoard) – např. pro bezdrátové propojení dvou míst, realizaci interní bezdrátové sítě, vysokorychlostní směrování či přepínání a mnoho dalšího.
Pro přístup k zařízení s RouterOS je nejvhodnější použít specializovaný program WinBox, případně je možné provádět konfiguraci přes CLI a připojit se na zařízení pomocí SSH, Telnetu nebo konzolovým kabelem a v neposlední řadě je možné také použít obyčejný webový prohlížeč.
Po instalaci OS nebo vybalení zařízení z krabice, toto obsahuje výchozí konfigurace, která je postavena tak, aby co nejlépe plnila obvyklou roli zařízení. Mimo to je však možné tuto výchozí konfiguraci změnit v menu `Quick Set` a nebo zařízení úplně vymazat, aby neobsahovalo žádnou konfiguraci. Pokud fyzické zařízení nereaguje a není možné se k němu jinak připojit, lze vyresetovat konfiguraci podržením zabudovaného tlačítka v průběhu startu OS.

Kapitola 2

Základy správy síťových zařízení MikroTik

V této kapitole se dozvíte

- Jakým způsobem je možné provést aktualizaci systému RouterOS?
- Jaké větve RouterOS v současné době MikroTik vytváří?
- Jak zprovoznit či vypnout určitou funkcionalitu RouerOS?
- Jakou konfiguraci je vhodné aplikovat do nového zařízení?
- Jak provést zálohu konfigurace a její obnovení?
- Jak je licencován operační systém RouterOS a jak je možné získat vhodnou licenci?

Po jejím prostudování byste měli být schopni

- Aktualizovat online i offline systém RouterOS.
- Zjistit vhodnou verzi RouterOS dle architektury CPU zařízení.
- Pracovat s balíčky (packages) na RouterOS.
- Nastavit název zařízení, upravit uživatelské účty a jejich oprávnění.
- Určit, kterými protokoly je možné k zařízení s RouterOS přistupovat.
- Získat zálohu zařízení s RouterOS v binární i textové podobě.
- Obnovit konfiguraci na stejném zařízení i na jiném zařízení.
- Vybrat vhodnou licenci a nainstalovat ji.

Klíčová slova: Aktualizace, upgrade, Bugfix only, Current, Release candidate, balíčky, uživatelské účty, záloha konfigurace, obnovení konfigurace, licence.

Průvodce studiem kapitoly

Tato kapitola se věnuje úplným základům nutným pro správu zařízení s RouterOS. V prvé řadě je třeba znát způsoby aktualizace operačního systém RouterOS a správu balíčků, které zprostředkovávají jednotlivé funkcionality. Velmi důležité je u nového zařízení nastavit jeho správný název, změnit přístupové údaje a případně omezit způsoby přihlášení na zařízení. V této kapitole se také dozvíte, jak je možné provádět zálohu konfigurace a její obnovení. Poslední část této kapitole je věnována problematice licencí pro použití operačního systému RouterOS.

2.1 Aktualizace RouterOS

Systém RouterOS je neustále vyvíjen, a proto vývojáři rozlišují odzkoušené verze od těch, kde jsou nejnovější, ale neodladěné funkcionality. Proto se balíčky v současné době dělí do větví: Bugfix only, Current, Release candidate – podrobnosti o vlastnostech jednotlivých větví najdete na Manual:Upgrading_RouterOS#RouterOS_version_release_chain

Pro aktualizaci routeru připojeného k síti Internet je možné použít přímo nabídku v menu: `System` → `Packages` → `Check For Updates`, kde je možné si vybrat příslušnou větev, přečíst si aktuální změny a případně verzi stáhnout a nainstalovat (podrobněji viz Manual:Upgrading_RouterOS#Automatic_upgrade). Po samotné instalaci je však potřeba restartovat systém.

Druhou možností jak aktualizovat RouterOS je stáhnout Main package pro správnou architekturu CPU[1] ze stránek mikrotik.com/download, nahrát jej na zařízení a následně jej restartovat (`System` → `Reboot`). Podrobněji je tento postup popsán na wikistránce Manual:Upgrading_RouterOS#Upgrade_process.

Po aktualizaci zařízení RouterBoard je vhodné také aktualizovat verzi firmwaru, která se spolu s aktualizací stáhla. Vynutit aktualizaci firmwaru je možné v menu `System` → `Routerboard` → `Upgrade` a následně restartovat zařízení. Detaily k upgradu firmware najdete na Manual:Upgrading#RouterBOARD_Firmware_Upgrade.

2.2 Správa balíčků

Jednotlivé funkcionality RouterOS jsou řešeny pomocí balíčků, tak aby mohly být samostatně zapínány dle potřeby, podrobnosti o typech balíčků a zpřístupněných funkcionalitách najdete na Manual:System/Packages#RouterOS_packages. Po spuštění systému si v menu `System` → `Packages` můžeme všimnout, že ne všechny balíčky jsou aktivované a ne všechny existující jsou nainstalované. Nainstalované balíčky je možné jednoduše zapínat a vypínat, pouze je vždy restartovat systém. Pro doinstalaci dalších balíčků – např. `multicast`, `ntp`, `user-manager` a další je nutné stáhnout balíček pro stejnou verzi instalovaného sytému ze stránek mikrotik.com/download, nahrát do zařízení a restartovat.

[1] Architekturu CPU je možné vyčíst v horní liště okna Winbox nebo v menu `System` → `Resources` v políčku `Architecture Name`.

Stejně jako je možné balíčky upgradovat, je možné nainstalovat i starší verzi, např. z důvodu kompatibility. Downgrade zařízení je možné provést dle popisu v Manual:System/Packages#Downgrade.

2.3 Základní správa zařízení

Mezi úplné první kroky při konfiguraci nového zařízení patří jeho pojmenování, které se provede v nabídce `System` → `Identity` (Manual:System/identity).

Dále je vhodné změnit výchozí heslo a i název superuživatele nebo nejlépe přidat nové uživatele a superuživatele (admin) deaktivovat (`System` → `Users`), podrobnější informace najdete na Manual:Router_AAA#Router_Users. Jednotlivým uživatelům je zadávat povolení pomocí skupin oprávnění, které je možné dále definovat (`System` → `Users` → `Groups`) více o skupinových oprávněních na Manual:Router_AAA#User_Groups.

V neposlední řadě je vhodné určit, jakými způsoby je možné se k zařízení s RouterOS připojit. Povolení a konfiguraci jednotlivých způsobů přístupu přes IP adresu (telnet, SSH, HTTP, HTTPS, Winbox a další) je možné najít v menu `IP` → `Services`, podrobnější vysvětlení jednotlivých služeb a nastavení najdete na Manual:IP/Services#Properties.

2.4 Záloha a obnovení konfigurace

Schopnost provést zálohu konfigurace a její obnovení patří mezi to nejdůležitější u produkčních prvků. U zařízení s RouterOS rozlišujeme dva různé typy záloh: tzv. `.backup` soubor a `export` (`.rsc`) soubor.

Backup soubor je možné použít pouze na tom stejném routeru a umožní jeho obnovení do zazálohovaného stavu. Jedná se o binární soubor obsahující kompletní konfiguraci (včetně hesel, klíčů atd.), který ale bohužel není čitelný ani dále editovatelný či přenositelný. Vytvoření zálohy i její obnovení je možné z nabídky `Files` ve Winboxu nebo z CLI dle Manual:Configuration_Management#System_Backup.

Export konfigurace je souhrn příkazů v textové podobně pro nakonfigurovaní routeru do aktuálního stavu, a proto je tento typ zálohy vhodný pro migraci konfigurace na jiný router. Dále je vhodný k uložení konfigurace pro dokumentační účely. Nevýhodou je chybějící export uživatelských hesel a klíčů a to, že jeho aplikování nezpůsobí odebrání dříve zadaných nastavení. Vytvoření souboru se zálohou konfigurace je možné provést z CLI pomocí příkazu `export`, který exportuje všechny příkazy vztahující se k aktuální úrovni zanoření. Postup jakým exportovat i importovat (příkaz `import`) textovovou zálohu najdete na Manual:Configuration_Management#Exporting_Configuration.

Pro přenos souboru se zálohou je možné použít protokolu SCP, FTP nebo při použití programu Winbox jednoduchým Drag&Drop příslušného souboru z menu `Files`.

V případě problémů s konfigurací či operačním systémem je možné k přístupu na zařízení použít program Netinstall, který je možné stáhnout ze stránek mikrotik.com/download. Podrobnosti k použití programu Netinstall najdete na Manual:Netinstall.

2.5 Licencování

K použití operačního systému RouterOS je nutná licence, kterou je možné získat koupí zařízení od firmy MikroTik nebo pořízením samostatné licence. V případě potřeba RouterOS pouze vyzkoušet je možné zvolit Trial licenci na 24 hodin nebo po registraci na stránce MikroTik tzv. Free Demo licenci, která má omezení na 1 rozhraní a tunel. Podrobnosti o rozdílech mezi jednotlivými typy licencí najdete na Manual:License.

Pro použití jako virtualizovaný stroj je možné pořídit licenci pro CHR, kde Free licence má rychlost rozhraní omezenu na 1 Mbit/s. Po registraci na stránce MikroTik je možné získat volnou licenci na 60 dní. Detaily o licencování CHR zařízení jsou uvedeny na Manual:CHR#CHR_Licencing.

2.6 Shrnutí kapitoly a úkoly k procvičení

2.6.1 Kontrolní otázky

1. Jak se odlišují jednotlivé větve RouterOS?
2. Jakými způsoby je možné provést aktualizaci RouterOS (online i offline)?
3. Jaké funkcionality zpřístupňují následující balíčky:
   (a) routing,
   (b) advanced-tools,
   (c) IPv6,
   (d) ntp.
4. Jaké nastavení je vhodné provést v prázdné konfiguraci RouterOS.
5. Jak zapnout nebo vypnout způsoby přístupu k zařízení?
6. Jak se liší záloha konfigurace (`File` → `Backup`) a export konfigurace (`export file=`*nazev_souboru*)?
7. K čemu slouží program Netinstall?
8. Jak se liší jednotlivé licence?

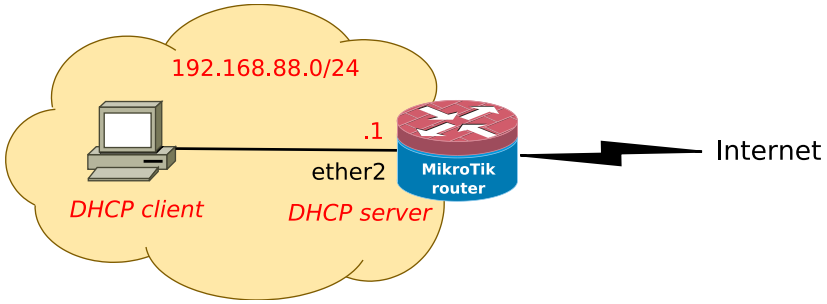
2.6.2 Úkoly k zamyšlení

1. Proč MikroTik vytváří RouterOS v různých větvích?
2. Co znamená upgrade firmware fyzického zařízení a kdy je vhodné jej provést?
3. Proč je vhodné vypnout nepoužívané balíčky funkcionalit?
4. V jakém případě je vhodné provést tzv. downgrade zařízení s RouterOS?
5. Proč je vhodné používat pro každého uživatele separátní účet s vhodně nastavenými oprávněními?

6. Které služby pro přístup k zařízení RouterOS je vhodné vypnout?
7. Jakým způsobem je možné si připravit/opravit konfiguraci zařízení offline?

2.6.3 Korespondenční úkol

Pro provedení korespondenčního úkolu postupujte podle následujících kroků:



Obrázek 2.1: Topologie zapojení pro korespondenční úkol 2.6.3

1. Připojte si k MikroTik routeru osobní počítač pomocí kabelu a zajistěte, aby zařízení mělo přístup na Internet (např. můžete navázat na korespondenční úkol 1.4.3). Zapojení úlohy je na obrázku 2.1. [2]
2. V menu `System` → `Packages` → `Check For Updates` zkontrolujte, jaká je nainstalovaná verze a jaká je nejnovější dostupná verze. Podívejte se na jednotlivé vývojové větve (`Channel:`) a prohlédněte si changelog této verze. Vyberte nějaký kanál, který bude novější než aktuální verze a proveďte aktualizaci (`Dowload & Install`). Alternativně lze aktualizaci provést z CLI pomocí příkazů v menu: `/system package update`.
3. Vyzkoušejte si práci s balíčky (`System` → `Packages` nebo z CLI `/system package`):
   (a) Proveďte deaktivaci vybraného balíčku (např. `advanced-tools`) pomocí `disable`.
   (b) Restartujte router – `System` → `Reboot` nebo z CLI `/system reboot`.
   (c) Zkontrolujte změny v menu Packages a také chybějící funkcionality (menu `Tools`).
   (d) Obdobným způsobem proveďte aktivaci balíčku.
   (e) Nainstalujte nový balíček (např. `ntp`), který si stáhněte ze stránek mikrotik.com/download v části `extra packages`. Důležité je vybrat stejnou verzi systému jako je aktuálně nainstalovaná.
   (f) Stažený balíček rozbalte (.zip) a nahrajte na router (např. pomocí Drag & Drop).

[2] Alternativně je možné využít VM routeru MikroTik (virtualizovanou pomocí Oracle VirtualBox) se síťovou kartou ether1 připojenou k NAT a kartou ether2 připojenou do Sítě pouze s hostem.

(g) Následně restartujte router a zkontrolujte přítomnost balíčku a nové funkcionality.

4. Proveďte základní nastavení RouterOS:
   (a) Nastavte název zařízení (`System` → `Identity` nebo z CLI `/system identity`) a pozorujte, kde se změna projeví.
   (b) Vytvořte nového uživatele, nastavte mu heslo a udělte mu plný přístup. Práce s uživateli se provádí v menu `System` → `Users` nebo z CLI `/user`.
   (c) Změňte uživateli `admin` heslo a nastavte jeho oprávnění pouze pro čtení.
   (d) Odhlaste se od RouterOS a přihlaste se pod novým účtem a poté pod účtem admin. Zkontrolujte nastavení – admin právo pouze pro čtení.
   (e) Prozkoumejte možnosti nastavení skupin a vytvořte novou skupinu umožňující čtení konfigurace pouze přes web (v menu `System` → `Users` → `Groups` nebo z CLI `/user group`).
   (f) Zakažte použití přístupu nezabezpečené protokoly (telnet, ftp, www atd.). Úprava této konfigurace je možná z menu `IP` → `Services` nebo z CLI `/ip service`.
5. Proveďte zálohu konfigurace a její obnovení:
   (a) Binární zálohu je možné získat z menu `Files` → `Backup` nebo z CLI `/system backup save`. Podívejte se na výchozí označení zálohy a také zkuste provést zálohu pojmenovanou dle sebe. Soubor se zálohou zkopírujte na Váš počítač a pokuste se jej otevřít textovým editorem.
   (b) Textová záloha může být vytvořena pouze z CLI a to pomocí příkazu: `/export file=`*nazev_souboru*. Opět tento soubor zkopírujte na Váš počítač a pokuste se jej otevřít textovým editorem.
   (c) Proveďte změny v textové verzi, soubor s textovou verzí nahrajte zpět a importujte (možné pouze z CLI) pomocí `/import file-name=`*nazev_souboru*.
   (d) Proveďte obnovení konfigurace z binárního souboru – pomocí `Files` → `Restore` nebo z CLI `/system backup load`.
6. Volitelný úkol: stáhněte si program Netinstall (ze stránek mikrotik.com/download) a dle pokynů na Manual:Netinstall#How_to_use_Netinstall aktualizujte (opravte) RouterOS.

2.6.4 Pojmy k zapamatování

- Aktualizace,
- Bugfix only,
- Current,
- Release candidate,
- package,

- downgrade,
- identity,
- export konfigurace,
- Netinstall,
- licence,
- CHR.

2.6.5 Příkazy vysvětlené v této kapitole

- `/system package update`
- `/system package`
- `/system reboot`
- `/system identity`
- `/user`
- `/user group`
- `/ip service`
- `/system backup save`
- `/system backup load`
- `/export file=`*nazev_souboru*
- `/import file-name=`*nazev_souboru*

2.6.6 Shrnutí

V této kapitole byly popsány důležité kroky, které by měl odpovědný správce zařízení provést při prvotní konfiguraci. Konkrétně jakým způsobem vybrat správnou větev a verzi operačního systému RouterOS a jak zařízení aktualizovat. Dále je vhodné aktivovat pouze ty balíčky, jež budou používány a jak je možné doinstalovat další funkcionality. U nového zařízení je v prvé řadě důležité nastavit jeho název, upravit oprávnění a především hesla uživatelských účtů a také vhodně nastavit přístup k zařízení.
Samotnou konfiguraci zařízení je možné zazálohovat dvěma způsoby, přičemž pro pozdější úpravy nebo převod na jiné zařízení je nejvhodnější export konfigurace ve formě textových příkazů. Poslední část kapitoly se věnuje různým druhům licencí operačního systému RouterOS.

Kapitola 3

Protokoly DHCP a ARP

V této kapitole se dozvíte

- Jaké protokoly jsou potřebné pro automatickou funkci koncového zařízení v síti.
- K čemu slouží protokol DHCP?
- Jaké parametry je možné pomocí DHCP přidělit klientské stanici?
- Kdy je nutný překlad doménových jmen?
- K čemu slouží protokol APR?

Po jejím prostudování byste měli být schopni

- Nastavit DHCP klienta na RouterOS.
- Nastavit DHCP server na RouterOS, určit rozsah přidělovaných adres a nastavit další parametry.
- Zprovoznik na RouterOS DNS server ve funkci resolveru.
- Znát fungování ARP protokolu.
- Umět si zobrazit ARP tabulku a vložit do ní statický záznam.

Klíčová slova: DHCP, IP adresa, výchozí brána, DNS, doménové jméno, ARP, MAC adresa.

Průvodce studiem kapitoly

V této kapitole jsou popsány protokoly důležité k fungování připojení pro uživatelská koncová zařízení. V prvé řadě se jedná o protokol DHCP, který automaticky přidělí koncovému zařízení IP konfiguraci. Pro používání doménových jmen je nezbytné poskytovat přístup na DNS server, který tato jména dokáže přeložit na IP adresu. Posledním protokolem je ARP, který slouží k mapování MAC adresy k IP adrese zařízení.

3.1 Protokol DHCP

DHCP (Dynamic Host Configuration Protocol) slouží k automatickému přidělení IP adresy a dalších parametrů (maska, výchozí brána, DNS server, atd.) pro L3 rozhraní. V základní verzi pracuje v rámci broadcastové domény, ale při použití tzv. DHCP relay (ip helper) je možné oslovit i DHCP server mimo broadcastovou doménu (více o DHCP relay najdete na Manual:IP/DHCP_Relay). Protokol DHCP by měl být používán pouze v důvěryhodných sítích, jinak může být příčinou získání útočníkem podvržené konfigurace.

Stanice, které je IP konfigurace dynamicky přidělována, se nazývá DHCP klient a je možné ji na MikroTik nastavit na kterékoliv L3 rozhraní (fyzické i bridge). Konfigurace se provádí z menu `IP → DHCP Client`. Podrobné informace jak nastavit DHCP clienta najdete na Manual:IP/DHCP_Client.

Zařízení, které má za úkol přidělovat IP konfiguraci DHCP klientům, se nazývá DHCP server. Na jednom MikroTik routeru může existovat několik DHCP serverů i klientů zároveň, každý však musí pracovat na jiném L3 rozhraní. Pro nastavení DHCP serveru je možné použít průvodce v menu `IP → DHCP Server → DHCP Setup` nebo vše nastavit manuálně. V tom případě je třeba připravit IP rozsah přidělovaných adres (`IP → Pool`), konfiguraci IP sítě (`IP → DHCP Server → Networks`) a následně DHCP server (`IP → DHCP Server`). Pro klienty je na straně serveru možné připravit rezervaci konkrétní IP adresy ve vazbě na konkrétní MAC adresu, tyto statické zápůjčky je možné konfigurovat v menu `IP → DHCP Server → Leases`. Podrobné informace k nastavení DHCP serveru a jeho funkci najdete na stránce Manual:IP/DHCP_Server.

3.2 Protokol DNS

K překladu doménových jmen na IP adresy (a případně i zpět) je nezbytné poskytovat možnost dotázat se na DNS (Domain Name System) server. MikroTik router v menších sítích slouží především jako DNS resolver, který vyhledává dotazovaná doménová jména klientům a získané výsledky si dočasně ukládá (cache). Konfigurace DNS serveru je v menu `IP → DNS` a podrobný popis možností konfigurace najdete na Manual:IP/DNS.

3.3 Protokol ARP

Protokol ARP (Address Resolution Protocol) slouží k vytvoření vazby mezi logickou IP adresou (L3) a fyzickou MAC adresou (L2). Tento protokol zpravidla pracuje dynamicky a to tak, že v případě hledání MAC adresy k určité IP adrese je odeslán v rámci lokální sítě (broadcastové domény) všesměrový dotaz hledající vlastníka dané IP adresy. Odpověď obsahuje jak hledanou MAC adresu, tak i IP adresu k ní příslušející. Tento pár adres (IP a MAC) je zpravidla po určitou dobu udržován na zařízení, aby nebylo nutné dotaz stále opakovat. ARP tabulku na MikroTik routeru je možné zobrazit v menu `IP → ARP`.

Vzhledem k charakteru komunikace ARP protokolu, může být tento relativně snadno zneužit k útoku Man-in-the-middle, kdy se útočník bude pomocí ARP protokolu vydávat za cílovou stanici. Proto je v některých případech vhodné přepnout ARP protokol konkrétního rozhraní do módu pouze odpovědí na dotazy (reply-only) nebo jej úplně vypnout (disabled). V obou případech zařízení bere v úvahu pouze staticky nastavené páry adres IP a MAC. Více o jednotlivých módech ARP protokolu a dalších nastaveních nadejte na Manual:IP/ARP.

V případě, že máme nakonfigurovaný DHCP server, je možné jej nastavit tak, aby pro každou novou zápůjčku IP adresy vytvořil i záznam do ARP tabulky.

3.4 Shrnutí kapitoly a úkoly k procvičení

3.4.1 Kontrolní otázky

1. K čemu slouží DHCP server?
2. Jaké parametry je možné nastavit klientovi z DHCP serveru?
3. K čemu slouží DNS server?
4. Jaké adresy k sobě mapuje protokol ARP?
5. Jaké módy ARP je možné nastavit na rozhraní?

3.4.2 Úkoly k zamyšlení

1. Kdy je vhodné na routeru nastavit DHCP klienta?
2. Jakým způsobem je možné provozovat DHCP server mimo lokální síť?
3. Zamyslete se, jak by fungoval Internet bez DNS serverů a doménových jmen?
4. Zamyslete, proč je ARP protokol potřebný?
5. Zamyslete se, jaká bezpečnostní rizika mohou nastat, pokud útočník odpoví na zprávu s dotazem o MAC adresu dříve než skutečný vlastník IP adresy?

3.4.3 Pojmy k zapamatování

- DHCP server,
- DHCP klient,
- výchozí brána,
- doménové jméno,
- DNS resolver,
- DNS cache,
- ARP tabulka,

- Man-in-the-middle.

3.4.4 Shrnutí

V této kapitole jste se dozvěděli především jak nastavit DHCP protokol v roli klienta i serveru. Tento protokol je velice důležitý neboť poskytne koncovému zaířzení správnou IP konfiguraci (IP adresa, maska, výchozí brána, DNS server, …) bez aktivní součinnosti uživatele. Druhým dnes podstatným protokolem je DNS, který zpřístupňuje svět IP adres lidskému mozku. Po prostudování této kapitoly byste měli být schopni nastavit DNS resolver. Posledním automaticky fungujícím protokolem v lokální síti je ARP, který zjišťuje k IP adrese MAC adresu zařízení.

Kapitola 4

Přepínaní rámců na RouterOS

V této kapitole se dozvíte

- Co je to bridge (most)?
- Jaký je rozdíl mezi L2 a L3 rozhraním?
- K čemu slouží Spanning Tree Protocol (STP)?
- Jak je možné zajistit přepínání rámců přímo v HW čipu switche?
- Jak je možné udělat bridge z bezdrátových rozhraní?

Po jejím prostudování byste měli být schopni

- Nakonfigurovat bridge rozhraní a přidat do něj žádaná fyzická rozhraní.
- Nastavit vlastnosti bridge rozhraní jako je STP, VLAN a ARP.
- Vědět, jakým způsobem filtrovat L2 provoz.
- Umět najít HW architekturu konkrétního zařízení MikroTik a vědět, jak nastavit přepínání rámců přímo v HW switchi.
- Vědět, jaký mód bezdrátového rozhraní použít pro jeho zařazení do bridge.

Klíčová slova: Bridge, most, STP, rozhraní, VLAN, master-port, hardware offload, WDS.

Průvodce studiem kapitoly

Tato kapitola poskytuje úvod do problematiky propojení rozhraní do jednoho logického. V rámci takového rozhraní sestávajícího se s více fyzických rozhraní dochází k přepínání rámců (L2). Při komunikaci mimo toto rozhraní jde o směrování (L3). Dozvíte se, jak funguje přepínání rámců na RouterOS a jakým způsobem je možné provést přepnutí rámci v rámci hardwaru. V neposlední řadě se budeme věnovat přepínání u bezdrátových rozhraní.

4.1 Nastavení logických rozhraní – bridge

Historicky bridge (most) sloužil k propojení dvou (popř. více) síťových segmentů a rozdělení kolizní domény. V operačním systému RouterOS je termín bridge používán k propojení několika fyzických (popř. i tunelových) rozhraní do jednoho logického. Výhodou toho je možnost propojit tyto rozhraní transparentně v rámci L2 a případně na L3 tomuto společnému rozhraní přidělit L3 konfiguraci (zpravidla IP adresa). Díky tomu je například u SOHO (Small Office Home Office) routeru možné spojit do jedné L2 sítě několik Ethernetových portů a bezdrátovou kartu/y. Zároveň, ale umožňuje vyčlenit některá rozhraní jako samostatná L3 rozhraní – ve výchozí konfiguraci jde o `ether1`, který je připraven pro připojení k ISP (Internet Service Provider).

Konfigurace bridge rozraní zahrnuje jednak jeho vytvoření, zahrnutí příslušných fyzických rozhraní a také nastavení ARP, Spanning Tree protokolu (STP) a u nových verzí (od 6.41), také navázání na VLAN (jde vlastně o vytvoření SVI, tak jak je chápáno na zařízeních Cisco). Konfigurace bridge rozhraní se provádí v menu `Bridge` a podrobnosti ohledně možností nastavení se dočtete na Manual:Interface/Bridge. Příklady jak nakonfigurovat RouterOS pro použití VLAN najdete na Manual:Interface/VLAN a podrobnosti o implementaci STP je na Manual:Spanning_Tree_Protocol.

Přestože datové jednotky (rámce) v rámci bridge rozhraní neprochází L3 firewallem, je možné jejich chování ovlivnit tzv. bridge firewallem, který bere v úvahu informace z L2 vrstvy. Nastavení bridge firewallu se provádí z menu `Bridge` → `Filters` a podrobnosti o jeho možnostech se dozvíte na Manual:Interface/Bridge#Bridge_Firewall.

4.2 Přepínání rámců dle hardwarové architektury

Vzhledem k tomu, že každý RouterBoard má jinou fyzickou architekturu, je nutné toto zvážit při vytváření konfigurace. Základem víceportových zařízení je často tzv. hardwarový switch modul, který umožňuje ulehčit softwaru (RouterOS) a některé L2 funkcionality řešit přímo v rámci hardwaru. Jaký switch module je u zařízení použitý najdete v jeho produktovém listu a následně je pak možné si vlastnosti a funkcionality příslušného switch modulu najít na Manual:Switch_Chip_Features.

Do verze RouterOS 6.40 bylo možné nastavení switch modulu řešit v menu `Switch` a nastavení přepínání pouze v rámci hardwarového modulu provádět nastavení pomocí `master-port` v menu `Interfaces` a konfigurace příslušného rozhraní. Od verze 6.41 bylo toto nastavení zjednodušeno a stačí zapnout v `Bridge` → `Ports` u příslušného rozhraní možnost `Hardware Offload`. Podrobnější informace o této problematice najdete na Manual:Switch_Chip_Features#Bridge_Hardware_Offloading.

4.3 Bridge u bezdrátového rozhraní

Vzhledem k omezení standardu 802.11, není možné provést bridge bezdrátového rozhraní v módu klienta. RouterOS obsahuje několik módů, které toto omezení obcházejí. Konkrétně módy: `station bridge` (mezi RouterOS zařízeními), `station pseudobridge` (mezi RouterOS a jinými zařízeními) a `station wds` (proprietární RouterOS protokol pro „bezdrátový Ethernet“. V případě `station bridge` je nutné zapnout volbu

`bridge` v nastavení bezdrátového rozhraní. Podrobnosti o možnostech použití jednotlivých typů bezdrátových rozhraní najdete na Manual:Wireless_Station_Modes.

4.4 Shrnutí kapitoly a úkoly k procvičení

4.4.1 Kontrolní otázky

1. Co je to bridge (most) z historického hlediska?
2. K čemu slouží bridge na RouterOS?
3. Jaké varianty STP podporuje RouterOS?
4. Jak je možné přenechat zpracování L2 provozu přepínacím čipem?
5. Jaké módy bezdrátového rozraní umožňují jeho použití v bridge?

4.4.2 Úkoly k zamyšlení

1. V jakých případech je třeba spojit několik rozhraní do jednoho bridge?
2. Zamyslete se, proč jsou v bridge rozhraní z jedné VLAN?
3. Kdy je vhodné filtrovat provoz procházející L2 rozraním?
4. Jaké výhody a nevýhody plynou zpracováním provozu HW chipem oproti SW?
5. Zamyslete se, proč není standardizováno klientské bezdrátové rozhraní pro použití jako součást bridge?

4.4.3 Pojmy k zapamatování

- Bridge,
- most,
- STP,
- VLAN,
- master-port,
- hardware offload,
- station bridge.

4.4.4 Shrnutí

V této kapitole jste se dozvěděli, že bridge je spojení fyzických L2 rozhraní a vytvořením bridge na RouterOS vytvoříme jedno logické rozhraní (L3). Toto rozhraní může být i navázáno na VLAN a vytvořit obdobu SVI. Mezi rozhraními uvnitř bridge dochází k přepínání rámců, které je možné v některých případech nechat na hardwaru přepínacího čipu. Závěr kapitoly byl věnován propojení bezdrátových rozhraní do bridge a možností, které nám RouterOS k tomu dává.

Kapitola 5

Směrování na RouterOS

V této kapitole se dozvíte

- Jak funguje a vypadá směrovací tabulka na RouterOS?
- Jakými způsoby se dostane záznam do směrovací tabulky?
- K čemu slouží výchozí cesta ve směrovací tabulce a jak zajistit její automatické přidání?
- Kdy je vhodné použít dynamický směrovací protokol?
- Jak funguje protokol OSPF?

Po jejím prostudování byste měli být schopni

- Rozeznat význam písmenek před záznamem ve směrovací tabulce.
- Určit, který směrovací záznam bude použit pro určitou cílovou adresu.
- Přidat statický směrovací záznam a zapnout automatickou kontrolu dostupnosti brány.
- Nastavit dynamický směrovací protokol OSPF.

Klíčová slova: Směrování, routing, connected, static, dynamic, brána, OSPF.

Průvodce studiem kapitoly

Směrování je klíčovým jádrem fungování Internetu a zajišťuje doručení datové jednotky k cílovému zařízení. V této kapitole se dozvíte, jak vypadá směrovací tabulka na RouterOS a jakým způsobem je vybrána nejvhodnější cesta pro paket. Dále je zde popsán staticky definovaný záznam ve směrovací tabulce a jak je možné jej vytvořit. Mimo to bude ukázán i dynamický směrovací protokol OSPF a popsány rozdíly mezi statickou a dynamickou cestou plnění směrovací tabulky.

5.1 Směrování a směrovací tabulka

Směrování se týká 3. vrstvy OSI modelu a je zpravidla prováděno dle cílové IP adresy v paketu. Na jaké rozhraní bude paket s danou cílovou IP adresou směrován, závisí na směrovací tabulce (na RouterOS v menu `IP` → `Routes`). Ta ve výchozím stavu obsahuje cesty k přímo připojeným sítím (pro něž je nakonfigurovaná IP adresa na některém z rozhraní), které jsou označeny písmeny `DAC` (dynamic, active, connected). Podrobnosti, jak funguje směrování na zařízení s RouterOS se dočtete na Manual:IP/Route.

5.2 Statické směrování

K zajištění směrování do jiných než přímo připojených sítí je třeba tyto doplnit do směrovací tabulky, což je možné manuálně (staticky) nebo automaticky (dynamické směrovací protokoly). Statický směrovací záznam se přidá v menu `IP` → `Routes`, kde je nutné u nové statické cesty definovat cílovou adresu (`dst. address`) a bránu přes kterou je dostupná (`gateway`). Statický záznam je označen písmenem `S` (static) a případně dalšími dle charakteru. Příklad jak je možné nastavit statické směrování najdete na Manual:Simple_Static_Routing.

Pokud k cíli vede více cest, bude vybrána specifičtější cesta. Proto je vhodné nastavit na router takzvanou výchozí cestu – `default route`, která vede k poskytovateli síťového připojení. Konfigurace výchozí cesty se neliší od konfigurace statické cesty, pouze je jako cílová adresa uvedeno `0.0.0.0/0`. Výchozí cesta může být získána také pomocí DHCP klienta, kdy je instalována automaticky (musí být zapnuta volba `add-default-route`).

Pro kontrolu platnosti statického směrování je možné zapnout pravidelnou kontrolu dostupnosti brány – u statického směrovacího záznamu jde o volbu `check-gateway`.

5.3 Dynamické směrování – OSPF

Statické směrování se výborně hodí pro malé sítě a levná zařízení. Především protože u malých sítí je jednoduchá na konfigurace směrování a statické směrování nespotřebovává výpočetní výkon síťového zařízení. Oproti tomu dynamické směrování se hodí především do větších sítí. Často používaným protokolem ve firemním prostředí je protokol OSPF – Open Shortest Path First.

Pro nastavení OSPF na zařízení s RouterOS je třeba mít aktivovaný balíček `routing`. Veškeré nastavení je následně prováděno v menu `Routing` → `OSPF`. V tomto menu je nezbytné nastavit OSPF instanci a přidat sítě (`Networks`), pro které má pracovat. Podrobnosti o dalším nastavení OSPF najdete na Manual:Routing/OSPF a doporučujeme projít případovou studii nasazení OSPF na Manual:OSPF_Case_Studies.

5.4 Shrnutí kapitoly a úkoly k procvičení

5.4.1 Kontrolní otázky

1. Jak je možné zobrazit směrovací tabulku na RouterOS?
2. Jaký význam mají následující písmena před směrovacím záznamem: `D`, `A`, `C`, `S`, `o`?
3. Jak je možné přidat statický směrovací záznam?
4. Jakými způsoby se může automaticky do směrovací tabulky dostat výchozí cesta (default gateway)?
5. Co je třeba nastavit pro zprovoznění dynamického směrovacího protokolu OSPF?

5.4.2 Úkoly k zamyšlení

1. Proč je zásadní pro funkci routeru mít správné záznamy ve směrovací tabulce?
2. Který směrovací záznam je vybrán, pokud existují dva stejné záznamy naučené různými způsoby (např. staticky a OSPF)?
3. K čemu může být výhodné použít kontrolu dostupnosti brány pomocí check-gateway?
4. Jaký výhody a nevýhody mají dynamické směrovací protokoly?

5.4.3 Pojmy k zapamatování

- Connected,
- static,
- dynamic,
- active,
- default route,
- výchozí brána,
- check-gateway,
- OSPF.

5.4.4 Shrnutí

V této kapitole jste se dozvěděli, jak vypadá směrovací tabulka na RouterOS a jakým způsobem se rozhoduje o směrování paketu k cíli. Statické záznamy ve směrovací tabulce jsou vhodné pro malé sítě, kde lze snadno určit, jaké cesty by měla obsahovat. U složitějších sítí je velice vhodné aktivovat dynamický směrovací protokol (např. OSPF), který bude plnit směrovací tabulku automaticky.

Kapitola 6

Bezdrátové připojení

V této kapitole se dozvíte

- Jaké standardy se pro bezdrátový přenos signálu používají?
- Jaká jsou omezení na použití bezdrátových přenosových pásem?
- Jaké vlastnosti je nutné nastavit na přístupovém bodu a co na klientské stanici?
- Jakým způsobem zabezpečit bezdrátovou síť?
- Jakými nástroji disponuje RouterOS pro diagnostiku bezdrátového spektra?

Po jejím prostudování byste měli být schopni

- Vědět čím se liší jednotlivé standardy a na čem závisí maximální rychlost.
- Znát hlavní omezení na použití frekvenčních pásem 2,4 GHz a 5 GHz.
- Nastavit bezdrátové rozhraní MikroTik pro použití jako klienta i přístupový bod.
- Vědět, která zabezpečení jsou považovaná za spolehlivá v dnešní době a jak je nastavit.
- Nastavit omezení pro přístup k AP pomocí Access List.
- Umět používat nástroje jaké Wireless Snooper, Scanner a Freq Usage, pro výběr vhodného kanálu a nalezení okolních sítí.

Klíčová slova: Bezdrátový přenos, wireless, 802.11, WiFi, ČTÚ, frekvence, přístupový bod, SSID, WPA2 a WPS.

Průvodce studiem kapitoly

Tato kapitola se věnuje bezdrátovému připojení, kde nejsme omezeni dostupností přenosového média. Dozvíte se, že volné použití bezdrátového přenosu je limitováno lokálními podmínkami a také co omezuje rychlost přenosu volným prostorem. Naučíte se nastavit bezdrátové rozhraní na MikroTik jako klienta nebo přístupový bod. Vzhledem k tomu, že bezdrátový přenos je přístupný všem v jeho dosahu, a proto je velice důležité ji správně zabezpečit, což se dozvíte v poslední části této kapitoly.

6.1 Bezdrátové standardy a omezení na jejich použití

Přenos dat pomocí bezdrátové sítě, označované jako WiFi, je definováno skupinou standardů IEEE 802.11. Nejznámější dílčí standardy definují parametry přenosu a z toho vyplývající maximální přenosové rychlosti, konkrétně jde v současnosti o standardy 802.11a,b,g,n,ac,ad. Tyto standardy se liší především frekvencí přenosového pásma (2,4 GHz, 5 GHz, 60 GHz), šířkou přenosového kanálu (20 MHz, 40 MHz, 80 MHz a 160 MHz), počtem antén (rádií) a dalšími parametry jako je modulace, kódovacím schématem atd.

Přenosové pásmo okolo 2,4 GHz nabízí v Evropě celkem 13 kanálů, z čehož jsou však pouze 3 nepřekrývající se 20 MHz kanály (obvykle používána kombinace 1, 6, 11). Proto je toto pásmo v dnešní době dost zaplněné a pro kvalitní bezdrátový přenos hůře použitelné. Na přenosovém pásmu okolo 5 GHz je hlavní omezení na použití uvnitř/venku a nutnost na vyšších frekvencích implementovat mechanismus předcházení meteorologickým radarům.

Dle lokálního omezení (dané všeobecným oprávněním ČTÚ) je nutné dodržet maximální vysílací výkon 20 dBm (EIRP). Pro splnění všech omezení a národních regulací je vhodné v konfiguraci bezdrátového rozhraní (`Wireless` → `WiFi Interfaces`) zvolit tzv. `Advanced mode`, nastavit `Frequency Mode`: `regulatory-domain` a `Country`: `czech republic` (pro ČR).

6.2 Nastavení bezdrátového rozhraní

Základní nastavení bezdrátového rozhraní (`Wireless` → `WiFi Interfaces` → `Wireless`) spočívá především ve výběru správného módu (`mode`), přenosového pásma a standardu (`Band`), frekvence (`Frequency`), šířky přenosového pásma (`Channel Width`), SSID a zabezpečení (`Security Profile`).

Pro práci v režimu přístupového bodu je nutné zvolit mód `ap bridge` (popř. `bridge` pro dvoubodový spoj) a pro režim klientské stanice je možné vybrat z několika různých módů – `station`, `station bridge` a další popsané v kapitole 4.3. Aktuálně připojené klienty k přístupovému bodu je možné vidět v nabídce `Wireless` → `Registration Table`.

Z dalších nastavení je vhodné zmínit alespoň nastavení jména rádia (`Wireless` → `WiFi Inerfaces` → `Wireless` → `Radio Name`), vysílacího výkonu (`Wireless` → `WiFi Inerfaces` → `Tx Power`) a nastavení MIMO (`Wireless` → `WiFi Interfaces` → `HT`).

Podrobné informace o nastavení bezdrátového rozhraní najdete v manuálu na stránce Manual:Interface/Wireless. Příklad konkrétního nastavení bezdrátového přístupového bodu a klienta najdete na Manual:Wireless_AP_Client.

6.3 Zabezpečení a monitoring bezdrátové sítě

Základním nastavením pro nastavení bezpečnosti je tvorba tzv. bezpečnostního profilu v `Wireless` → `Security Profiles`, kde je možné zvolit vhodný typ zabezpečení – nejčastěji WPA2 PSK (SOHO řešení) nebo EAP (enterprise řešení). Tento bezpečnostní profil jen nutné také nastavit v bezdrátovém rozhraní (`Wireless` → `WiFi Interfaces` → `Wireless`). Podrobnosti jak funguje zabezpečení pomocí profilu najdete na Manual:Interface/Wireless#Security_Profiles.

Pro zjednodušení připojení k zabezpečení síti, je možné použít WPS, které pomocí současného stisku (během 2 minut) tlačítka umožní autentizovat příslušné zařízení. Jakým způsobem je možné WPS u zařízení MikroTik použít najdete na Manual:Interface/Wireless#WPS.

U zařízení fungujícího jako klient bezdrátových sítí je vhodné nastavit tzv. `Connect List`, který umožní automatické připojení ke známým bezdrátovým sítím – více viz Manual:Interface/Wireless#Connect_List.

Zařízení pracující jako přístupový bod umožňuje řídit autentizaci připojovaných zařízení pomocí tzv. `Access List`, který může definovat MAC adresu, sílu signálu, sdílený klíč a další vlastnosti připojované stanice. Pro připojení pouze stanic vyhovujících záznamu v `Access List` je nutné zrušit volbu `Default Authenticate` (v `Wireless` → `WiFi Inerfaces` → `Wireless`). Konkrétní možnosti nastavení `Access List` najdete na Manual:Interface/Wireless#Access_List.

Pro zvýšení bezpečnosti v sítích, kde nejsou klientské stanice pod kontrolou, je vhodné vypnout možnost komunikace mezi stanicemi pomocí vypnutí volbu `Default Forward` (v `Wireless` → `WiFi Interfaces` → `Wireless`).

Ke sledování jiných bezdrátových sítí je vhodný nástroj `Wireless Snooper`, který je přímo v nabídce `Wireless`. Další užitečný nástroj je `Scanner`, který se hodí především k vyhledání vhodné sítě a připojení se k ní. Pro výběr vhodné frekvence se hodí nástroj `Freq. Usage`, který zobrazuje využití jednotlivých frekvencí a umožňuje tak výběr nejméně využité.

6.4 Shrnutí kapitoly a úkoly k procvičení

6.4.1 Kontrolní otázky

1. Jaké dílčí standardy (určující přenosové rychlosti) jsou ve skupině standardu 802.11?
2. Kolik nezávislých (nepřekrývajících) kanálů je v přenosovém pásmu okolo 2,4 GHz?
3. Jaké omezení na použití přenosových pásem existují v ČR?
4. Jakým nejjednodušším způsobem, je možné se z MikroTiku připojit k jiné bezdrátové síti?
5. Co je třeba nastavit pro použití MikroTiku jako přístupového bodu?
6. Jaké znáte nástroje pro monitoring bezdrátových sítí?

6.4.2 Úkoly k zamyšlení

1. Zamyslete se, proč je u bezdrátových pásem (okolo 2,4 GHz a 5 GHz) omezen vysílací výkon?
2. Zamyslete se, čím je způsobena vyšší přenosová rychlost u standardů 802.11n a 802.11ac a je vždy možné ji dosáhnout?
3. Proč není dostatečné zabezpečení bezdrátové sítě pomocí omezení MAC adres, které se mohou přihlásit?
4. Zamyslete se, v jakých případech je výhodné použít připojení k síti pomocí WPS tlačítka?

6.4.3 Pojmy k zapamatování

- IEEE 802.11 (a,b,g,n,ac,ad),
- frekvenční pásmo okolo 2,4 GHz, 5 GHz, 60 GHz,
- ČTÚ – Český Telekomunikační Úřad,
- EIRP,
- SSID,
- přístupový bod,
- MIMO,
- WPA2 PSK/EAP,
- WPS,
- Access List,
- Connect List.

6.4.4 Shrnutí

Pro použití bezdrátového přenosu na volně dostupných pásmech je nutné dodržovat podmínky dané všeobecným oprávněním. V průběhu času vzniklo několik dílčích standardů ze skupiny IEEE 802.11. Starší standardy pracující na frekvenci 2,4 GHz (b, g, n) jsou problematické velkým zarušením přenosového pásma, oproti tomu standardy pracující na 5 GHz (a, n, ac) mají menší dosah a také je nižší podpora ze strany koncových zařízení. Nastavení MikroTik jako klienta, stačí správně nastavit mód, SSID a přístupové údaje, popř. využít Scanner a připojit se k dostupné síti. Nastavení přístupového bodu je složitější – je nutné minimálně vybrat mód, pásmo, SSID, přístupové údaje a nastavit rádio. Pro zabezpečení bezdrátové sítě je nejvhodnější používat WPA2 (personal nebo enterprise).

Kapitola 7

Firewall

V této kapitole se dozvíte

- Jak funguje firewall na RouterOS a na jakém základu je postaven?
- Co je to stavový firewall a jak je možné využít této vlastnosti?
- Na základě jakých informací umožňuje RouterOS filtrovat provoz.
- Jaké akce umožňuje firewall vykonat při shodě s vlastnostmi pravidla?
- Do, kterých řetězců je třeba vložit pravidla pro filtrování průchozího nebo příchozího provozu?
- K čemu slouží překlad adres a kdy je nutné jej použít?

Po jejím prostudování byste měli být schopni

- Vědět, k čemu slouží jednotlivé tabulky (filter, NAT, mangle) firewallu na RouterOS.
- Znát postup vyhodnocování paketu při průchodu RouterOS.
- Nastavit firewall pro ochranu samotného zařízení.
- Sestavit pravidla firewallu tak, aby filtroval provoz mezi důvěryhodnou a nedůvěryhodnou zónou.
- Nastavit překlad privátních adres z vnitřní sítě na veřejné.

Klíčová slova: Firewall, Netfilter, Filter, NAT, Mangle, řetězec, chain, packet flow, input, forward, srcnat a dstnat.

Průvodce studiem kapitoly

Z této kapitoly se naučíte, jak pracuje firewall na operačním systému RouterOS. Důležité je pochopit strukturu firewallu a vědět, do kterých částí vložit příslušná pravidlo, aby mělo patřičný účinek. Dále se dozvíte, jakým způsobem funguje filtrování provozu a jaký je rozdíl mezi vstupujícím a směrovaným provozem. Poslední část této kapitoly je věnována překladu adres (tzv. NAT) a nastavení ve firewallu, která jsou k tomu nezbytná.

7.1 Princip firewallu na RouterOS

Zajištění síťové bezpečnosti především mezi vnitřní a vnější sítí zajišťuje firewall. Na zařízeních s RouterOS je tento firewall založen na linuxovém modulu Netfilter (ovládaný přes `iptables`). Z toho vyplývá i struktura, kdy je celý firewall rozdělen do tabulek – Filter (filtrování), NAT (překlad adres), Mangle (úprava hlavičky paketu a značkování) a Raw. V těchto tabulkách jsou předefinované řetězce (chains), které jsou uplatněny na určité chování (např. řetězec input slouží k práci s příchozím provozem). V těchto řetězcích jsou sekvenčně uvedena pravidla, který mají definovanou akci (např. accept, drop, reject, jump, src-nat, dst-nat). Při shodě vlastností paketu s pravidlem je vykonána definovaná akce a paket se dále nevyhodnocuje. Výjimkou v tomto je akce jump, která posune paket na vyhodnocení jiným řetězcem (může být i definovaný uživatelem).

Způsob jakým je konkrétní paket procházející MikroTikem zpracováván najdete na stránce Manual:Packet_Flow, především si nastudujte postup vyhodnocování řetězců u jednotlivých tabulek. Všimněte si bloku Connection tracking, který zajišťuje uchovávání informace o probíhajícím spojení, díky čemuž je možné rozhodovat dle stavu spojení. Firewall Netfilter i ten na RouterOS je tzv. stavový firewall. Kromě stavu spojení je možné rozhodnout na základě mnoha parametrů, mezi ty důležité patří: vstupní a výstupní rozhraní, zdrojová a cílová adresa, protokol, port, TCP flagy, ICMP kód, DSCP značka, TTL, …Často používané porty můžete najít např. na Manual:IP/Services#Protocols_and_ports.

7.2 Filtrování vstupujícího a směrovaného provozu

K filtrování provozu slouží u firewallu na RouterOS tabulka filter (`IP` → `Firewall` → `Filter Rules`, ve které jsou zabudované tři řetězce – input, output a forward. Pro filtrování provozu, který routerem (firewalem) prochází, slouží řetězec forward, pro provoz mířící přímo na router (např. management) slouží řetězec input a provoz, který vytváří router je filtrován pomocí řetězce output.

Důležité akce, které je možné použít u pravidla v tabulce filter jsou accept (povolit), drop (zahodit), reject (zahodit a odeslat zprávu o nedostupnosti), log (vložit záznam do logu), jump (skočit do jiného řetězce) a return (návrat z vnořeného řetězce). Pro zpřehlednění struktury pravidel je vhodné vytvářet vlastní řetězce a také vytvá-

řet skupiny adres (`IP` → `Firewall` → `Address Lists`). Podrobnosti o možnostech tvorby skupin adres najdete na Manual:IP/Firewall/Address_list.

Důležité je také to, že výchozí akcí zabudovaných tabulek je accept, proto pokud je třeba zahodit vše co nevyhoví předchozím pravidlům, je nutné na konec těchto řetězců umístit pravidlo s akcí drop.

V řetězci input povolujeme přístup určitým zařízením a protokolům na router – obvykle jde o povolení managementu (SSH, Winbox) z určitých adres a také povolení protokolů provozovaných na routeru (např. NTP, OSPF, VPN, …). Obvykle je ukončen pravidlem vše ostatní zakaž (drop).

Řetězec forward kontroluje průchozí provoz a dobrým zvykem je jako jedno z prvních pravidel uvést povolení všech paketů se stavem established a related. Pakety s těmito stavy patří nebo se váží k již existujícímu (povolenému) provozu a tak není obvykle třeba jej znovu kontrolovat. Další pravidla se mohou vztahovat k zónové politice, kdy některé zóny (rozhraní) jsou důvěryhodné a povolujeme téměř veškerý provoz, jiné zóny jsou naopak nedůvěryhodné a povolujeme pouze vybrané protokoly, porty a adresy.

Veškeré informace k tabulce Filter najdete na stránce Manual:IP/Firewall/Filter. Od verze RouterOS 6.29 je možné použít speciální akci Fasttrack, který urychluje zpracování paketu a snižuje zátěž procesoru, jak funguje Fasttrack se můžete dočíst na Manual:IP/Fasttrack.

7.3 Source a destination NAT

Vzhledem k tomu, že si firewall na RouterOS udržuje v tzv. Connection Tracking (více viz Manual:IP/Firewall/Connection_tracking) tabulce informace o spojeních, je možné měnit při průchodu firewallem adresy – provádět tzv. překlad adres (NAT), který řeší tabulka NAT (`IP` → `Firewall` → `NAT`). V tabulce NAT jsou dva zabudované řetězce srcnat (v Netfilter se jmenuje POSTROUTING) a dstnat (PREROUTING), které řeší změnu zdrojové respektive cílové adresy paketu. Detaily o funkci tabulky NAT najdete na Manual:IP/Firewall/NAT#Properties.

Source nat (srcnat) je důležitý především v sítích, kde jsou použity privátní adresy (cca 95 % všech domácích sítí) dle RFC 1918. Tyto adresy je možné opakovaně používat, ale není možné, aby putovaly veřejným Internetem. Proto je nutné na hranici takové sítě provádět změnu zdrojové (privátní) adresy na veřejnou. K tomu je možné použít akci src-nat (změna na určitou adresu) nebo akci masquerade (změna na adresu odchozího rozhraní). Ve většině případů tak dochází ke „zamaskování“ několika zdrojových privátních adres za jednu veřejnou. Příklad jak funguje source nat najdete na Manual:IP/Firewall/NAT#Source_NAT.

Destination nat (dstnat) mění cílovou adresu na jinou např. z důvodu rozdělení služeb směřujících na jednu adresu mezi více strojů. Akce, které je možné použít, jsou redirect (změní cílový port a směruje přímo na router) a dst-nat (může změnit cílovou adresu i port). Ukázku použití destination nat najdete na Manual:IP/Firewall/NAT#Destination_NAT

7.4 Shrnutí kapitoly a úkoly k procvičení

7.4.1 Kontrolní otázky

1. Jaké tabulky obsahuje firewall na RouterOS a k jakému účelu slouží?
2. Jaké parametry je možné nastavit v pravidlech?
3. Do jakých řetězců je třeba vložit pravidla pro filtrování příchozího a směrovaného provozu?
4. Jaké akce je možné použít v tabulce filter a jaké v tabulce nat?
5. Jak je možné změnit zdrojovou privátní adresu paketu na veřejnou?

7.4.2 Úkoly k zamyšlení

1. Z jakého důvodu, je implementace firewallu na RouterOS podobná firewallu Netfilter?
2. Zamyslete se, proč se téměř nevyužívá filtrování odchozího provozu v tabulce output?
3. Proč se častěji využívá akce drop a ne akce reject?
4. Zamyslete se, kdy má význam vytvořit vlastní řetězce a jaká pravidla do nich sdružit.
5. Zamyslete se nad důvody a výhodami použití destination nat?

7.4.3 Pojmy k zapamatování

- Firewall,
- Netfilter,
- filter,
- NAT,
- mangle,
- input,
- forward,
- address list,
- connection tracking,
- privátní adresa.

7.4.4 Shrnutí

Firewall v prvé řadě zajišťuje ochranu mezi vnitřní a vnější sítí a to pomocí filtrování provozu. RouterOS je postaven na Linuxu, a tak i firewall je svoji strukturou velmi podobný linuxovému firewallu Netfilter. Jednotlivé funkcionality zajišťují tzv. tabulky – např. Filter pro filtrování provozu a NAT pro překlad adres. V každé tabulce jsou implicitní a uživatelem definované řetězce, ve kterých jsou organizována pravidla. Pravidla jsou procházena sekvenčně a při shodě parametrů pravidla (např. IP adresa, protokol, port, stav, …) je provedena nastavená akce. U tabulky Filter je třeba pravidla, která mají chránit samotný router umisťovat do řetězce input, ta co mají filtrovat procházející provoz do řetězce forward. V tabulce NAT jsou pouze dva implicitní řetězce a to srcnat a dstnat, přičemž každý slouží k překladu jiné adresy (zdrojové nebo cílové).

Kapitola 8

QoS a mechanismy front

V této kapitole se dozvíte

- K čemu se používají QoS mechanismy?
- Jak omezit přenosovou rychlost zařízením v lokální síti?
- Jaké mechanismy řízení odchozích front obsahuje MikroTik?
- Jak umožnit dočasné využití vyšší přenosové rychlosti?
- Jak nastavit automatické vytvoření více stejných front pro různé provozy?

Po jejím prostudování byste měli být schopni

- Určit, kdy je nezbytné aplikovat QoS.
- Nastavit Simple Queue pro omezení přenosové rychlosti a zaručené minimální rychlosti.
- Nastavit dočasné zvýšení přenosové rychlosti zákazníkům pomocí burst.
- Vytvořit automatické rozdělení provozu do několika front.

Klíčová slova: QoS, rate limiting, frontový mechanismus, simple queue, burst, PCQ.

Průvodce studiem kapitoly

Tato kapitola se věnuje řízení provozu pomocí frontových mechanismů. Dozvíte se, kdy je potřeba nastavit QoS pro priorizaci služeb. Taktéž se dočtete, jak je možné frontové mechanismy využít pro omezení rychlosti zákazníků. V prvé řadě je zde probírána tzv. Simple Queue, která slouží především k omezení přenosu od jednoho zákazníka. Dále se dozvíte, jak funguje tvorba několika front se stejnými parametry pro více zákazníků.

8.1 Principy QoS a omezení přenosové rychlosti

Quality of Service (QoS) je způsob, jakým upřednostnit přenos preferovaných dat před jinými. Mechanismy QoS se uplatní v místě, kde je přenosová rychlost linky nižší než množství příchozích dat. V tu chvíli je možné určit mechanismus, kterým budou odbavovány příchozí pakety – např. paket preferovaného hlasového hovoru bude odbaven před ostatními.

Frontové mechanismy používané u QoS najdou uplatnění i u omezení přenosové rychlosti – např. klientům dle jejich zaplaceného tarifu. K řízení front slouží nabídka `Queues`, kde je možné nastavit různé typy front. Podrobné informace o tom, jak jsou frontové mechanismy implementovány na RouterOS najdete na Manual:Queue.

8.2 Simple Queue

Jednou variantou jak omezit přenosovou rychlost klientských stanic je možnost Simple Queue (`Queues` → `Simple Queues`), která umožňuje omezit rychlost v jednotlivých směrech (download, upload) nebo celkovou rychlost (total). Při tvorbě nové fronty je třeba správně zvolit pro kterou adresu(y) má být uplatněna (`Target`). Maximální rychlost pro klienta pak definujeme v kolonkách `Max. Limit` samostatně pro Upload a Download. Pokud chceme omezit (nebo neomezit) rychlost pouze k některým cílovým adresám je třeba vyplnit položku `Dst`. V případě, že máme více klientů a chceme jim nabídnout maximální dostupnou rychlost, ale ve chvíli kdy budou připojeni zároveň jim garantovat určitou rychlost, je třeba nastavit na záložce `Advanced` možnosti `Limit At`. Další podrobnosti jak nastavit simple queue najdete na stránce Manual:Queue#Simple_Queues

Specialitou MikroTiku je možnost povolit krátkodobé využití vyšší přenosové rychlosti (nad maximum) pomocí tzv. `burst`. V případě burstu se nastavuje přenosová rychlost po dobu burstu (`Burst Limit`), množství dat, které je takto možné přenést rychleji (`Burst Threshold` a doba po kterou je možné burst znovu využít (`Burst Time`). Podrobně popsány bursty jsou na stránce Manual:Queues_-_Burst.

8.3 Frontový mechanismus PCQ

V případě velkého počtu zákazníku se stejnými podmínkami, nebo v případě potřeby vyrovnat přenosovou rychlost různých služeb, je vhodné využít jiného typu fronty. Per Connection Queuing (PCQ) automaticky vytvoří frontu pro každé spojení dle udaných podmínek. Mezi podmínkami může (ale nemusí) být zdrojová nebo cílová IP adres (délka společného prefixu) a zdrojový nebo cílový port. Pro každé spojení, které bude v definovaných parametrech rozdílné, se vytvoří samostatná fronta. Příklad, jakým může být fronta PCQ implementována najdete na Manual:Queues_-_PCQ_Examples.

8.4 Shrnutí kapitoly a úkoly k procvičení

8.4.1 Kontrolní otázky

1. K čemu slouží QoS a jakém místě sítě je třeba jej nastavit?
2. Jak je možné omezit přenosovou rychlost konkrétní stanice?
3. Jak definujeme v Simple Queue cíl omezení, musí se jednat o jednu IP adresu?
4. Jak dosáhneme zaručení minimální přenosové rychlosti pro konkrétní stanici?
5. Na základě kterých parametrů, je možné vytvořit samostatné fronty pomocí PCQ?

8.4.2 Úkoly k zamyšlení

1. Proč není nutné aplikovat QoS v sítích s dostatečnou propustností (přenosovou rychlostí)?
2. Zamyslete se, z jakého důvodu poskytovatelé připojení omezují přenosovou rychlost zákazníkům?
3. V jakých případech může být vhodné povolit, krátkodobé zvýšení přenosové rychlosti (burst)?
4. Jaké výhody přináší mechanismus PCQ, a v jakých případech je vhodné jej použít?

8.4.3 Pojmy k zapamatování

- Quality of Service (QoS),
- Simple Queue,
- max. limit,
- burst,
- limit at,
- PCQ.

8.4.4 Shrnutí

QoS slouží k řízení kvality služeb tak, aby služby (např. hlasový přenos) měli zaručené přenosové parametry (zpoždění, přenosovou rychlost). Rate limiting je naopak mechanismus, který omezuje přenosovou rychlost např. zákazníka tak, aby kvalita (přenosová rychlost) jeho připojení odpovídala jeho smlouvě. Obojí je možné ovlivňovat pomocí frontových mechanismů, které řídí odbavování provozu. RouterOS obsahuje tzv. Simple Queue, která umožňuje jednoduché, ale podrobné nastavení rychlosti a dalších parametrů pro konkrétní adresu. Oproti tomu PCQ vytváří mnoho stejných front pro provozy, které jsou rozlišeny např. dle IP adres, adresního prefixu, portů, ….

Kapitola 9

Tunelové mechanismy a VPN

V této kapitole se dozvíte

- K čemu slouží tzv. Point-to-Point protokoly?
- Jak je možné autentizovat klienta v lokální síti?
- Jak vytvořit zabezpečený tunel mezi dvěma sítěmi?
- Jaké VPN protokoly existují a jak se na RouterOS nastavují?

Po jejím prostudování byste měli být schopni

- Nastavit IP rozsah pro PPP služby.
- Nakonfigurovat autentizační PPPoE server pro použití v lokální síti.
- Nastavit PPPoE klienta na Windows i RouterOS.
- Znát varianty VPN a vědět, které jsou považovány za bezpečné.
- Umět nakonfigurovat PPTP a SSTP server na RouterOS.

Klíčová slova: PPP, VPN, point-to-point, PPPoE, autentizace, PPTP, TLS a SSTP.

Průvodce studiem kapitoly

V této kapitole se dočtete základy Point-to-Point protokolu (PPP), na jehož základě je postaveno mnoho tunelovacích a VPN spojení. Konkrétně bude popsána možnost autentizace klienta v lokální síti pomocí PPP over Ethernet. Jako příklad VPN spojení budou představeny protokoly PPTP a SSTP.

9.1 PPP koncept

Point-to-Point Protocol (PPP) slouží k vytvoření tunelu (přímého propojení) mezi dvěma stanicemi. Mezi stanicemi může poskytovat autentizaci, šifrování a kompresi.

RouterOS poskytuje různé varianty PPP tunelů – např. PPPoE, PPTP a SSTP. Konfigurace PPP probíhá z menu `PPP`, kde je nutné pro většinu účelů připravit PPP profile (`PPP` → `Profiles`) a heslo pro uživatele (`PPP` → `Secrets`). Podrobnosti k nastavení jednotlivých voleb PPP najdete na Manual:PPP_AAA.

Pro přidělení IP adresy klientům je v některých případech nutné připravit IP rozsah (`IP` → `Pools`), ze kterého budou adresy přidělovány. Podrobnosti o IP rozsazích najdete na Manual:IP/Pools.

9.2 Autentizace v lokální síti pomocí PPPoE

PPP over Ethernet (PPPoE) je implementace PPP protokolu přes síť Ethernet a pro jeho použití je nutné, aby klient i server byli v rámci broadcastové domény. S výhodou může být použita pro autentizaci klientů (zákazníků), aby bylo zajištěno připojení pouze validních uživatelů. Zároveň je tímto způsobem poskytnuta uživatelskému zařízení IP adresa a případně může být přeno šifrován. Obecný popis jak funguje PPPoE najdete v kapitole Manual:Interface/PPPoE#PPPoE_Operation.

Na většině běžných operačních systémů (Windows, Linux, MacOS) je PPPoE klient už přímo součástí systému. Pro konfiguraci PPPoE klienta (`PPP` → `Interface` → `add PPPoE client`) na RouterOS je třeba nastavit alespoň uživatelské jméno, heslo a Ethernetové rozhraní, na kterém má pracovat. Velice vhodné je nastavit `service name`, aby se klient nepřipojil ke špatnému PPPoE serveru. Více o nastavení PPPoE klienta se dočtete na Manual:Interface/PPPoE#PPPoE_Client.

PPPoE server je možné na RouterOS nastavit v menu `PPP` → `PPPoE Servers`, kde je nezbytné nastavit rozhraní, na kterém má fungovat (nesmí být součástí bridge). Další nezbytné vlastnosti PPPoE serveru jsou: profil (`Default Profile` a typ autentizace (`Authentication`). V rámci profilu nebo příslušného hesla (secret) musí být nastavena lokální a vzdálená adresa, navíc je vhodné vybrat, zda se má provoz komprimovat a šifrovat. Příklad nastavení PPPoE serveru najdete na Manual:Interface/PPPoE#PPPoE_Serve

9.3 Řešení VPN pomocí PPTP a SSTP

Virtual Private Network (VPN) je způsob jakým zajistit zabezpečené připojení vzdálené stanice nebo sítě. Při připojení vzdálené sítě (site-to-site) je vytvořen zabezpečený tunel mezi okrajovými prvky sítí (routery), kterým je směrován provoz mezi sítěmi. Při připojení vzdálené stanice do sítě (remote access) je vytvořen zabezpečený tunel přímo z koncového zařízení a veškerý provoz zpravidla přichází až na router, který pracuje jako VPN server. RouterOS podporuje různé protokoly, kterými je možné vytvořit VPN. Konkrétně jde o OpenVPN, IPSec (pomocí L2TP nebo IKE), PPTP a SSTP. V tomto kurzu budeme řešit pouze dva poslední jmenované.

Point-to-Point Tunneling Protocol (PPTP) je relativně jednoduchý způsob, jak vytvořit zabezpečenou VPN síť. Protokol je implementován v mnoha operačních systémech a tak je velmi oblíbený. Nevýhodou je, že cca od roku 2012 není považován za bezpečný. PPTP ke komunikaci využívá port TCP 1723 a na nižší vrstvě protokol GRE.

Na zařízení s RouterOS je možné vytvořit jak PPTP server, tak i klienta. Pro nastavení klienta je třeba přidat nové PPTP klientské rozhraní rozhraní `PPP` → `Interface` → `PPTP Client` a na záložce `Dial Out` vyplnit adresu serveru (`Connect To`), uživatelské jméno a heslo. Zaškrtnutím volby `Add Default Route` zajistíme, že veškerý provoz bude směrován na PPTP server. Podrobněji o nastavení PPTP klienta najdete na Manual:Interface/PPTP#PPTP_Client.

Nastavení PPTP serveru se provede tlačítkem `PPTP Server` v nabídce `PPP` → `Interface` a k jejímu zprovoznění je třeba vytvořit profil (`PPP` → `Profiles`), uživatelská jména a hesla (`PPP` → `Secrets`). Více o nastavení PPTP serveru najdete na Manual:Interface/PPTP#PPTP_Server.

Secure Socket Tunneling Protocol (SSTP) je způsob jak vytvořit zabezpečenou síť přes TLS kanál, což je způsob obdobný protokolu HTTPS a využívá i stejný transportní port (TCP 443). Nevýhodou je potřeba certifikátu pro serverovou stranu a také nutnost doinstalovat klientské aplikace na operační systémy (vyjma Windows a Linux). Nastavení protokolu SSTP na zařízení s RouterOS je obdobné nastavení PPTP a detailní popis je možné najít na Manual:Interface/SSTP.

9.4 Shrnutí kapitoly a úkoly k procvičení

9.4.1 Kontrolní otázky

1. Co je to PPP protokol a k čemu slouží?
2. K čemu je výhodné použít PPPoE v lokální síti.
3. Jak nastavit šifrování a komprimaci pro protokoly využívající PPP.
4. Které VPN protokoly nejsou považované za bezpečné?
5. Jaké výhody a nevýhody má VPN protokol SSTP?

9.4.2 Úkoly k zamyšlení

1. Zamyslete se, případně vyhledejte, varianty PPP protokolu používané v sítích bez L2 protokolu Ethernet.
2. Proč poskytovatelé připojení (ISP) používají PPPoE místo DHCP?
3. Proč není v dnešní době často využívána komprimace při vytváření tunelového spojení?
4. Zamyslete se, s jakými VPN protokoly jste se již setkali. Např. jaký VPN protokol je používat pro připojení do školní sítě?

9.4.3 Pojmy k zapamatování

- PPP,

- VPN
- PPPoE,
- PPTP,
- GRE,
- TLS,
- SSTP.

9.4.4 Shrnutí

Protokol PPP se využívá k vytvoření přímého propojení mezi dvěma zařízeními, příkladem takového využití je varianta přes Ethernet (PPPoE), kdy je možné autentizovat připojujícího klienta a přidělit mu také IP konfiguraci.
Pro tvorbu VPN spojení je k dispozici na RouterOS mnoho variant. Jednou z nich je PPTP protokol, který má širokou podporu klientských zařízení, ale v dnešní době není považován za bezpečný. Druhým příkladem je protokol SSTP, který pracuje na TLS vrstvě, kterou využívá např. HTTPS. Z tohoto důvodu není problém s průchodem firewally, ale je nutné vlastnit certifikát pro stranu serveru.

Kapitola 10

Další nástroje a monitoring

V této kapitole se dozvíte

- Jaké jsou základní nástroje pro diagnostiku stavu sítě?
- Jak je možné nastavit automatickou notifikaci (např. na e-mail) v případě problémů?
- Kde zjistit informace o využití systémových prostředků MikroTiku?
- Jak si zobrazit systémové zprávy (log)?
- K čemu slouží protokol SNMP a jak je využít pro sledování stavu sítě?
- Jakým způsobem je možné kontaktovat podporu z MikroTik?

Po jejím prostudování byste měli být schopni

- Používat nástroje ping a traceroute pro diagnostiku stavu sítě.
- Nastavit notifikace na e-mail v případě nedostupnosti IP adresy.
- Zobrazit si procesy, které vytěžují procesor.
- Nastavit generování grafů provozu.
- Nakonfigurovat SNMP a odesílání logů na externí server.
- Vygenerovat soubor se stavem zařízení a zobrazit si jeho obsah.

Klíčová slova: Tools, e-mail, ping, traceroute, profile, log, traffic monitor, The Dude, SNMP, supout.rif a Watchdog.

Průvodce studiem kapitoly

Tato kapitola obsahuje popis nejrůznějších nástrojů, které správci sítě mohou usnadnit práci. Za prvé se jedná o nástroje pro diagnostiku stavu sítě – ping, traceroute a Netwatch, pro sledování dostupnosti vzdálené stanice. Dočtete se také o nástrojích, které umožňují hlídání vytížení procesoru a přenosových linek samotného routeru. Popsán je zde i protokol SNMP pro vzdálené sledování zařízení a způsob jakým se konfiguruje úroveň logování. Poslední část popisuje, jakým, způsobem je možné řešit problémy s operačním systémem RouterOS a jak je možné kontaktovat podporu.

10.1 Nástroje pro diagnostiku sítě

RouterOS poskytuje různé nástroje, které správcům sítí usnadňují práci a pomáhají diagnostikovat stav sítě. Jednotlivé nástroje je možné najít v menu `Tools` a pro funkci některých z nich je třeba mít nainstalovaný balíček `advanced-tools`.

V případě, že je MikroTik napojen na síť Internet je možné při určitých událostech odesílat e-mailovou zprávu. K tomu je nutné zadat správnou konfiguraci SMTP serveru a e-mailového účtu v menu `Tools` → `Email`. Odesílání e-mailové zprávy je poté možno nastavit například při výpadku rozhraní. Více o natavení e-mailu najdete na Manual:Tools/email.

Nástroj na sledování stavu sítě je například Netwatch, který pravidelně testuje dostupnost dané adresy pomocí ICMP a v případě nedostupnosti spustí definovaný skript (např. odeslání e-mailu). Nastavení Netwatch se provádí v `Tools` → `Netwatch` a podrobnosti k jeho nastavení najdete na Manual:Tools/Netwatch.

Hlavními nástroji pro diagnostiku sítě jsou `ping` a `traceroute`, jejichž grafická podoba (včetně dalších voleb) je k dispozici z menu `Tools`. Ping pomocí ICMP zprávy Echo Request (alternativně i ARP Request) zjišťuje dostupnost cílové stanice. Traceroute oproti tomu zobrazuje celou cestu (L3 prvky) mezi zdrojem a cílem, čímž se hodí pro diagnostiku místa, kde dochází k problémům. U traceroute na RouterOS je možné zvolit protokol ICMP nebo UDP. Více o nástroji ping najdete na Manual:Tools/Ping.

10.2 Hlídání stavu zařízení

Jádrem zařízení s RouterOS je procesor, popř. procesory, u kterých je vhodné sledovat jejich zatížení a nejvíce vytěžující procesy. Zobrazení aktuálně běžících procesů je možné provést pomocí `Tools` → `Profile`, více o významu zobrazených hodnot najdete na Manual:Tools/Profiler.

Dále vhodné vědět nakolik je saturovaná přenosová rychlost jednotlivých rozhraní. Aktuální přenosová rychlost rozhraní je vidět v záložce `Traffic` konkrétního fyzického rozhraní. Pro zobrazení historie zatížení je nutné nastavit tzv. `Traffic Monitor` (nástroj ze skupiny `Tools`), více o jeho použití najdete na Manual:Tools/Traffic_Monitor.

Informace o jednotlivých síťových tocích lze zjistit pomocí nástroje `Torch`, který zobrazí aktuálně probíhající spojení dle zadaných kritérií.

Pro přehledné zobrazení vývoje zatížení CPU, paměti a disku je možné nastavit generování grafu na webovou stránku routeru. Stejným způsobem je možné nechat generovat přenosovou rychlost jednotlivých rozhraní nebo front. Nastavení generování grafů je v menu `Tools` → `Graphing`, kde lze i nastavit omezení přístupu k danému grafu. Detaily k nastavení grafů můžete najít na Manual:Tools/Graphing.

Podstatným zdrojem informací o stavu zařízení jsou systémové logy obsahující zprávy informující o různých událostech. Standardně jsou logy ukládány do paměti, která je po restartu zařízení vymazána. Proto je vhodné nastavit jejich ukládání na disk a nejlépe jejich odesílání na Syslog server, kde mohou být takto uchovány informace z různých zařízení. Zobrazení aktuálních logů je možné z nabídky `Log`, samotné nastavení logování se prování z menu `System` → `Logging`. V nastavení je třeba správně připravit akci (`Actions`), která se má provést při výskytu zprávy k zalogování a následně samotná pravidla (`Rules`) určující při jakém kontextu se má akce provést. Více o prohlížení logovacích zpráv a nastavení sbíraných zpráv najdete na Manual:System/Log.

10.3 Monitoring stavu sítě

K monitoringu stavu síťových zařízení se často používá protokol SNMP (Simple Network Management Protocol), který umožňuje pomocí OID identifikátoru prvku odečítat jeho aktuální hodnotu a v některých případech ji i měnit. V praxi se setkáme především s kontrolou stavu rozhraní a jiných systémových vlastností pomocí automatizovaných dohledových systémů (např. The Dude, Nagios, Zabbix, Cacti, …). Nastavení SNMP na RouterOS se provádí v `IP` → `SNMP`, kde je třeba jej povolit a vyplnit správnou komunitu (`Communities`). Podrobné informace o možnostech nastavení SNMP najdete na Manual:SNMP.

The Dude je dohledový systém vyvinutý firmou MikroTik a poskytovaný zdarma (od verze 6.34 jako balíček do RouterOS). Tento systém dokáže pojmout celou topologii sítě, monitorovat běžící služby a přenosové linky a především notifikovat různými způsoby vzniklé problémy. Se zařízením MikroTik funguje relativně automaticky a se zařízeními jiných firem umí komunikovat např. pomocí SNMP. Ke sledování stavu sítě je nutné si nainstalovat klientský program, který je k dispozici pouze pro OS Windows. Více informací o monitorovacím systému The Dude najdete na Manual:The_Dude.

10.4 Řešení problémů

V případě, že vznikne s operačním systémem RouterOS problém a je nutné kontaktovat podporu, je vhodné vygenerovat tzv. support output file (`supout.rif`). Vygenerování takového souboru lze provést přes položku `Make Supout.rif` a tento soubor následně stáhnout do počítače. Kromě odeslání `supout.rif` na podporu, je možné si po přihlášení na stránce mikrotik.com/client/supout zobrazit detaily aktuálního stavu zařízení. Více o výstupu pro support se dozvíte na Manual:Support_Output_File.

Pro zajištění supout.rif souboru krátce před vznikem problému, je možné využít nástroj Watchdog, který při vzniku problému (nebo nedostupnosti zadané adresy) vygeneruje výstup pro support a umožní jej i odeslat e-mailem. Nástroj Watchdog

je možné nastavit z menu `System` → `Watchdog` a podrobnosti o něm se dozvíte na Manual:System/Watchdog.

Úplný popis dostupných nástrojů pro řešení problémů (tzv. troubleshooting) najdete na Manual:Troubleshooting_tools.

10.5 Shrnutí kapitoly a úkoly k procvičení

10.5.1 Kontrolní otázky

1. Jaký balíček je třeba mít aktivovaný pro použití většiny diagnostických a managementových nástrojů?
2. Jak nastavit generování grafů systémových prostředků a přenosových linek a jak omezit přístup k těmto informacím?
3. Co je to OID a co může identifikovat?
4. Jaké znáte dohledové systémy?
5. Na jakých místech je možné hledat podporu při řešení problémů?

10.5.2 Úkoly k zamyšlení

1. Zamyslete se nad rozdíly mezi nástroji ping a traceroute a určete, na co se který hodí.
2. Popřemýšlejte, proč je důležité sledovat stav zařízení a co lze vyčíst z procesů vytěžujících procesor?
3. Zamyslete se, k jakým účelům by měl dohledový systém sloužit a co by měl hlídat?
4. Porovnejte obsah ze souboru supout.rif s exportem konfigurace a zálohou pomocí tlačítka Backup.

10.5.3 Pojmy k zapamatování

- SMTP server,
- ICMP,
- ping,
- traceroute,
- Netwatch,
- Profiler,
- Graphing,
- log,

- SNMP,
- The Dude,
- supout.rif,
- Watchdog.

10.5.4 Shrnutí

Pro usnadnění správy je důležité efektivně používat správné nástroje. V prvé řadě je nezbytné ovládat nástroje ping a traceroute. Kromě toho MikroTik nabízí nástroj Netwatch, který pravidelně sleduje dostupnost daného zařízení a v případě chyby dokáže například odeslat e-mail o nedostupnosti. Stav samotného routeru je možné hlídat pomocí nástroje Profiler (vytížení procesoru), vytížení fyzických rozhraní pomocí Traffic Monitor. Ke sledování stavu sítě je výhodné využít protokol SNMP a dohledový systém – např. The Dude od MikroTiku. K řešení problémů se samotným operačním systémem RouterOS je možné vygenerovat soubor s výstupem pro support (podporu) – supout.rif, který obsahuje veškeré detaily o konfiguraci a stavu zařízení.

Literatura

[1] MikroTik. *MTCNA training materials (2016-03)*. MikroTik Academy, 2016.

[2] MikroTik. *MikroTik Wiki: Documentation* [online]. 2018 [cit. 2018-08-25]. Dostupné z `https://wiki.mikrotik.com`.

[3] HART, Tyler. *Networking with MikroTik: MTCNA Study Guide*. Independently published, 2017. 360 s. ISBN 978-1973206354.

[4] DISCHER, Stephen R. W. *RouterOS by Example*. Second edition. ISP Services, Inc., 2016. 426 s. ISBN 978-0692777909.

[5] BURGESS, Dennis. *Learn RouterOS*. Second edition. Link Technologies, Inc. 2011. 448 s. ISBN 978-1105069598.

[6] MikroTik. *MUM – MikroTik User Meeting* [online]. 2018 [cit. 2018-08-25]. Dostupné z `https://mum.mikrotik.com/archive`.

[7] MikroTik. *MikroTik – Forum* [online]. 2018 [cit. 2018-08-25]. Dostupné z `https://forum.mikrotik.com/`.