Využití zařízení MikroTik pro zřízení a zabezpečení malých a středních počítačových sítí

Robert Pastyřík

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Robert Pastyřík**
Osobní číslo:	**A16098**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Využití zařízení MikroTik pro zřízení a zabezpečení malých a středních počítačových sítí**
Téma anglicky:	**The Use of MikroTik for Setting up and Securing Small and Medium-sized Computer Networks**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Popište produkty MikroTik a jejich značení.**
3. **Popište vlastnosti RouterOS.**
4. **Popište Firewall RouterOS.**
5. **Navrhněte malou síť se zařízením MikroTik.**
6. **Vyřešte propojení malých sítí.**
7. **Realizujte uvedený návrh sítě.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5. aktualizované vydání. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.**
2. **DISCHER, Stephen. RouterOS by Example. 1. vydání. USA, 2011. ISBN 978-0-615-54704-6.**
3. **BURGESS, Dennis. Learn RouterOS. 2. vydání. Lulu.com, 2011. ISBN 978-1-105-06959-8.**
4. **MikroTik. MikroTik [online]. [cit. 2018-11-23]. Dostupné z: www.mikrotik.com**
5. **MikroTik. MikroTik Documentation [online]. 2017 [cit. 2018-11-23]. Dostupné z: https://wiki.mikrotik.com/wiki /Main_Page**

Vedoucí bakalářské práce:	**Ing. Miroslav Matýsek, Ph.D.** Ústav počítačových a komunikačních systémů
Datum zadání bakalářské práce:	**21. prosince 2018**
Termín odevzdání bakalářské práce:	**15. května 2019**

Ve Zlíně dne 21. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo - diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 13.5.2019

Robert Pastyřík, v.r.
……
podpis diplomanta

ABSTRAKT

Tato práce se věnuje využití zařízení MikroTik pro realizaci počítačových sítí v malých a středních firmách. Pojednává o základních typech zařízení, které v těchto případech připadají v úvahu a o jejich operačním systému, základním nastavení, propojení firemních sítí a především o zabezpečení těchto zařízení před možnými útoky. V práci jsou uvedeny postupy, jak takovou síť pomocí těchto zařízení krok po kroku realizovat, nastavit, zabezpečit a propojit mezi sebou.

Klíčová slova: MikroTik, Firewall, RouterOS, počítačová síť, WinBox

ABSTRACT

This thesis pursues using MikroTik system for implementing computer networks in small and medium-sized companies. It deals with basic types of equipment possible in these cases and also their operational system, essential setting-up, interconnecting company networks and primarily protecting these devices against all kinds of attacks. Step-by-step instructions how to create, set up, secure and interconnect such a network using this system are mentioned in this work.

Keywords: MikroTik, Firewall, RouterOS, Computer Network, WinBox

OBSAH

ÚVOD

V důsledku snahy o úsporu finančních prostředků a současně zvyšující se potřeby malých a středních firem být neustále připojen k Internetu dnes velmi často dochází k tomu, že mnoho těchto firem si pořizuje pro připojení a následně i realizaci vnitřní sítě levná zařízení, která zdaleka nesplňují zvyšující se nároky na bezpečnost a variabilitu nasazení.

Jiným případem je zcela opačný přístup, kdy se z různých důvodů pořizují zbytečně drahá zařízení a prvky. Dochází tak paradoxně k tomu, že tato zařízení jsou vytížena pouze z několika procent a mohla by být nasazena někde jinde, kde by byl více využit jejich potenciál a výkon.

Vzhledem k výše uvedenému vznikla potřeba vytvořit pokud možno jednoduchý postup na základní zprovoznění počítačové sítě při použití jediného zařízení, s minimálními náklady na jeho pořízení a správu, s důrazem na zabezpečení takto vytvořené sítě.

Práce je tedy reakcí na to, že na trhu sice existují zařízení, která jsou schopna splnit ekonomické a bezpečnostní požadavky, chybí však dokumentace v českém jazyce a zřejmě z toho důvodu jsou tato zařízení neprávem opomíjena.

Úkolem bylo seznámení s cenově dostupnými zařízeními firmy MikroTik, s jejich nastavením, ovládáním a zabezpečením. Dále popis druhů zařízení a způsob jejich nastavení tak, aby byla s minimálními náklady schopna splnit požadavky na počítačovou síť a to včetně možnosti propojení sítí, odpovídajícího zabezpečení a mobility.

Práce bude sloužit jako návod, především pro IT pracovníky menších organizací.

I. TEORETICKÁ ČÁST

1 POČÍTAČOVÁ SÍŤ

Počítačová síť je propojení více počítačů mezi sebou tak, aby mohly vzájemně komunikovat. Používá se z mnoha důvodů, nejčastějším z nich je možnost sdílení dat a dalších prostředků, do sítě zapojených, ať už jsou to servery nebo sdílené tiskárny. Výhody tohoto propojení jsou zřejmé - není nutné přenášet soubory na externím zařízení při každé úpravě, tisk na společnou tiskárnu uspoří čas a náklady a nutností je dnes už sdílení připojení k Internetu.

Je jasné, že nároky na rozsáhlost, vybavení a správu se budou lišit podle rozlehlosti sítě, počtu zaměstnanců, množství používaných síťových prostředků atd. Podle toho je také nutné vybírat síťová zařízení, která se k zprovoznění sítě použijí.

Při zřizování sítě je snahou se soustředit na maximální jednoduchost, pokud možno co nejnižší náklady nejen na pořízení, ale i na správu a to vše s důrazem na zabezpečení a možnost případného dalšího rozšíření.

1.1 Druhy počítačových sítí

LAN (Local Area Network) - lokální počítačová síť, zpravidla spojuje firemní nebo domácí zařízení v jednom objektu, budově nebo místnosti.

MAN (Metropolitan Area Network) - metropolitní síť, propojuje různá místa v městské síti.

WAN (Wide Area Network) **-** rozlehlá síť, která propojuje velmi vzdálená místa, například města mezi sebou.

GAN (Global Area Network) - rozlehlé, globální sítě. Zde je možno zařadit celosvětovou síť Internet [1].

Jsou ještě i jiné druhy sítí, dělící se podle rozlehlosti, ale pro účely této práce plně postačují uvedené tři. V podstatě bylo cílem vytvořit síť LAN (případně několik takovýchto sítí) a ty následně propojit mezi sebou tak, že vznikne síť metropolitní, případně síť WAN, pokud budou kanceláře firmy rozmístěny daleko od sebe.

1.2 Pasivní prvky

Metalické kabely - kroucená dvojlinka. Na jejím provedení záleží, jak rychlá síť bude. Kabely se rozdělují do několika kategorií, které jsou označovány čísly a od nich se odvíjí maximální rychlost přenášených dat a odolnost proti rušení. Pro rychlost 100 Mb/s je použito

značení 5, pro vyšší rychlosti do 1 Gb/s se používá značení 5e. Značení 6 a 7 se používá pro rychlosti ještě vyšší, zpravidla kolem 10 Gb/s [1].

Optické kabely - základním prvkem těchto kabelů je optické vlákno, které je uloženo v plášti. Optická vlákna se dělají jednovidová nebo mnohovidová a liší se konstrukcí a hlavně zakončením. Je několik typů konektorů pro optická vlákna, proto je vždy důležité vědět, jaké typy jsou použity v síti, do které bude připojeno naše zařízení [2].

Rozvodné panely - jinými slovy svorkovnice, bývají součástí rozvodných skříní. Jsou v nich zakončeny kabely vedoucí od jednotlivých zásuvek. Propojení zásuvek se potom děje kabelem mezi patch panelem a switchem.

Zásuvky - poslední koncový bod směrem k uživateli. Zásuvkami jsou ukončeny síťové rozvody a do nich se připojují jednotlivá koncová zařízení, tedy počítače, tiskárny atd.

Strukturovaná kabeláž - tímto pojmem je označován způsob vytvoření rozvodů slaboproudých signálů v budově. Základem strukturované kabeláže je hvězdicová topologie, tedy každý prvek sítě je připojen vlastním kabelem. Tyto kabely vedou do rozvodného panelu a odtud jsou pak připojeny například do switche [1].

Jak bylo zmíněno v úvodu, tato práce předpokládá, že firma má již vytvořeny rozvody strukturované kabeláže, tedy že koncová zařízení (počítače a tiskárny) je možné zapojit do zásuvek.

1.3 Aktivní prvky

Switch - slouží pro připojení zařízení k síti. Zprostředkovává propojení mezi jednotlivými prvky a směruje mezi nimi komunikaci. Obsahuje větší počet ethernetových portů, je do něj tedy možné zapojit více zařízení a v případě potřeby jej stohovat. Dnes má již většina switchů management, díky kterému je možné např. sledovat síťový provoz nebo vytvářet virtuální sítě, tzv. VLANy, které mají velký význam při zabezpečení sítě [3].

Router - spojuje dvě (nebo několik) sítí a posílá mezi nimi data. Používá se i pro oddělení těchto sítí, typicky pro oddělení firemní sítě a sítě poskytovatele Internetu [4].

Gateway - slouží pro propojení sítí s odlišnými protokoly. V praxi funguje jako router, odděluje sítě a přeposílá mezi nimi data.

Pro zprovoznění sítě v malé nebo střední firmě v podstatě výše uvedená zařízení postačují. Všechny typy těchto zařízení v sobě sdružuje MikroTik, a to i ta nejlevnější varianta. Záleží jenom na tom, jak bude nakonfigurován.

1.4 Protokoly

V praxi při realizaci sítě, zejména při nastavování firewallu, se setkáme se skupinou protokolů, nazývaných TCP/IP. Je to nejrozšířenější skupina protokolů, o jejímž fungování je popsáno mnoho odborné literatury. Pro účely této práce je důležité hlavně to, že z pohledu funkčního je možné rozdělit TCP/IP protokol na několik základních částí:

Aplikační protokoly - sem se řadí protokoly, pracující s určitou aplikací, např. FTP (File Transfer Protocol), používaný pro přenos souborů, HTTP (Hypertext Transfer Protocol) pro přenos webových stránek, SMTP (Simple Mail Transfer Protocol) zajišťující přenos zpráv mezi poštovními servery a další.

Protokol IP (Internet Protocol) - je to základní protokol, na kterém funguje přenos dat mezi zařízeními. Je nespolehlivý a nenavazuje spojení.

IP protokol existuje ve verzi IPv4 a IPv6. Tyto protokoly jsou používány pro komunikaci v síti Internet. IPv6 postupně nahrazuje starší protokol verze 4, který přestal stačit adresním prostorem [4].

Protokol TCP (Transmission Control Protocol) - stará se o spolehlivý přenos dat mezi zařízeními. Funguje tak, že navazuje spojení, má tedy fázi navázání, přenosu a ukončení spojení.

Protokol UDP (User Datagram Protocol) - funguje v podstatě stejně, jako protokol TCP, nenavazuje však spojení. Je tedy jednodušší, ale zase méně spolehlivý. Někdy je využíván různými aplikacemi pro navázání rychlého spojení i za cenu menší spolehlivosti.

Protokol ICMP (Internet Control Message Protocol) - tento protokol se používá pro přenos hlášení o chybových stavech. Nejčastější použití je společně s příkazem *ping*, pomocí kterého je možno zjišťovat dostupnost jiných zařízení v síti a ověřit si, jestli jsou správně zapojena a funkční.

1.5 Adresace IPv4

Na síti musí mít každé zařízení svoji nezaměnitelnou adresu, prezentovanou čtveřicí čísel, oddělených tečkami. Pro účely této práce je nutné znát hlavně 2 adresy, a to adresu, kterou přidělil poskytovatel Internetu a pak adresu, respektive adresní rozsah vlastní sítě. Zatímco poskytovatelem přidělenou adresu nelze změnit, adresní rozsah vlastní sítě je možné si za určitých podmínek zvolit.

Adresy se dělí do tříd a v každé třídě jsou vymezeny rozsahy neveřejných adres pro lokální sítě, tedy ty, které si můžeme zvolit sami. Jsou to:

Třída A: 10.0.0.0 až 10.255.255.255

Třída B: 172.16.0.0 až 172.31.255.255

Třída C: 192.168.0.0 až 192.168.255.255

Tyto neveřejné rozsahy neprochází z neveřejné sítě směrem ven.

Dále je ještě důležitá síťová maska, která slouží k určení adresy sítě z IP adresy.

A nakonec je důležitá adresa brány, tedy kudy půjdou data z naší sítě ven, což nejčastěji bude IP adresa routeru, tedy našeho vlastního zařízení [3].

1.6 Routing

Routing je technika, která označuje propojení různých sítí. Data jsou routována z jedné sítě do druhé na základě pravidel, která mohou být přednastavena staticky, tedy zápisem do tzv. routovací tabulky nebo jsou vytvářena dynamicky routovacím protokolem podle síťového provozu.

Router je tedy zařízení, které shromažďuje informace o připojených sítích a pak vybírá nejvýhodnější cestu pro směrovaný paket [1].

Při routování je důležitá brána (Gateway), která zajišťuje propojení neveřejné sítě s veřejnou, tedy bod, kudy se počítače z lokální sítě dostávají na Internet. Bývá označována jako Default gateway, tedy výchozí brána.

1.7 DHCP

DHCP (Dynamic Host Configuration Protocol) je protokol, který automaticky přiděluje IP adresy, zajišťuje tedy to, že každý počítač po svém spuštění dostane jedinečnou adresu,

kterou je reprezentován na síti. Toto přidělování zajišťuje DHCP server, který adresy přiděluje na základě požadavku počítače z tzv. poolu, tedy vytvořeného adresního prostoru.

1.8 DNS

Jedná se o protokol a službu, která zajišťuje překlad názvů počítačů v Internetu. I tam má každý počítač svoji adresu, která je reprezentována čísly, bohužel se však těžko pamatuje. Tato služba zajišťuje překlad těchto čísel na jména, která si už lze lépe zapamatovat a zadávat je např. do adresních řádků v prohlížečích. DNS (Domain Name System) navíc rozděluje počítače do zón, tzv. domén, například cz, sk, com, ru atd. [1].

1.9 NTP

NTP (Network Time Protocol) je protokol, který provádí synchronizaci hodin a zajišťuje, že všechny počítače na síti a v ostatních zařízeních mají stejný čas a datum. V praxi protokol funguje tak, že počítače na Internetu (časové servery) na dotaz zasílají odpověď s přesným časem [4].

1.10 NAT

NAT (Network Address Translation) představuje překlad síťových adres. V praxi slouží k tomu, aby překládal adresy neveřejných počítačů na adresu veřejnou, to znamená, že neveřejné adresy zůstanou pro okolní svět skryty. Princip je ten, že zařízení, na kterém provozujeme NAT (ve většině případů router) přijme pakety z neveřejné sítě, zachytí je a změní v nich IP adresu z neveřejné na veřejnou. Do Internetu tedy odchází jenom jedna vnější adresa a to i v případě, že máme rozsáhlou vnitřní síť. Při příchodu paketů zpět zvenčí router podle údajů, které si uložil, zjistí, jestli jsou určené jemu a pokud ano, provede akci s adresami v opačném pořadí, tedy zamění veřejnou s neveřejnou. Tento postup výrazně přispívá k bezpečnosti vnitřní sítě [5].

1.11 Bridge

Bridge, česky také nazýván most, má podobné funkce jako switch a používá se pro oddělení sítí. Bridge má v paměti uloženo, do které části sítě jsou datové rámce určeny a propustí je pouze tam, kam patří. Výhodou je menší zatížení sítě [1].

1.12 Firewall

Firewall slouží v počítačové síti pro blokaci příchozího, případně odchozího provozu. Může být provozován samostatně, ale mnohem častěji je součástí jiného zařízení, zpravidla routeru. Blokaci nebo povolení provozu provádí na základě předem definovaných pravidel a politik. Standardně je instalován do jediného vstupního místa, kudy prochází veškerá komunikace směrem do Internetu a lze jím poměrně efektivně tento provoz kontrolovat a zabezpečit.

1.13 Bezdrátová síť

U bezdrátových sítí se signál přenáší elektromagnetickým vlněním, které nahrazuje zpravidla metalické kabely. Pro přenos se používají nelicencovaná pásma 2,4 GHz a 5 GHz.

Bezdrátová zařízení spolu mohou komunikovat několika způsoby, nejrozšířenější je přístupový bod, tzv. AP (Access Point). Tento bod je připojen k Internetu a zprostředkovává připojení klientským počítačům, je tedy možné na tomto bodě kontrolovat provoz, protože veškerá komunikace prochází přes něj.

Rychlost bezdrátových sítí je obecně nižší než sítí metalických, je totiž závislá na mnoha okolnostech, jako je přímá viditelnost mezi zařízeními, jejich vzdálenost a v neposlední řadě také standard, podle kterého jsou zařízení schopna komunikovat [1].

2 MIKROTIK

MikroTik je společnost z Lotyšska, která byla založena roku 1996 za účelem vývoje routerů a bezdrátových ISP (Internet Service Provider) systémů. V současnosti je to stále se rozrůstající společnost s plně funkčním operačním systémem RouterOS. Mezi produkty společnosti patří také výroba vlastního hardwaru pod názvem RouterBOARD, která se stále vyvíjí s přihlédnutím na požadavky firem a poskytovatelů internetového připojení [5].

U produktů této značky se nikdy nepočítalo s jednoduchou konfigurací, kterou zvládne naprosto každý na pár kliknutí, hlavně proto, že mají větší možnosti nastavení. To je ale zase odlišuje od jednoúčelových zařízení, která plní jenom několik málo funkcí. MikroTik je možné nastavit přesně podle požadavků na funkcionalitu sítě a při změně těchto požadavků jej lze opět relativně rychle a jednoduše přenastavit. Je tak možné změnou konfigurace udělat z routeru přístupový bod, firewall, hotspot nebo jenom obyčejný switch.

V současnosti má firma MikroTik přes 500 distributorů a 145 obchodních zastoupení v mnoha zemích. Pořádá také pravidelné konference s názvem MUM (MikroTik User Meetings), které se týkají jak hardwaru, tak operačního systému RouterOS. Tady je možné nejen shlédnout prezentace, ale také aktivně klást dotazy a seznámit se s technologickými novinkami. Do současnosti už bylo těchto konferencí uspořádáno více než 150.

Kromě toho provozuje i MikroTik Academy, tedy vzdělávací program, který má za úkol výuku ve vzdělávacích střediscích a na technických školách, s cílem přiblížit a vysvětlit problematiku RouterOS co nejširšímu okruhu zájemců a studentů. Kurzy je možno zakončit zkouškou a získat několik typů certifikátů, podle dosažené úrovně vzdělání [6].

3 PRODUKTY MIKROTIK

Společnost MikroTik vyrábí svůj vlastní hardware potřebný pro běh RouterOS. Dříve to byly pouze zařízení s názvem RouterBOARD, s postupem doby se však nabídka rozšířila a dnes je možné vybírat z velkého množství zařízení, jejichž hlavní součástí je však stále jedna základní deska, která je instalována v boxu, podle následného využití. Můžeme se tak na trhu setkat s různými typy produktů:

Ethernetové routery - tato zařízení neobsahují wifi, jsou tedy vhodná pro stavbu malé sítě, kde není potřeba pokrytí bezdrátovým signálem.

Switche - zpravidla opět bez wifi, slouží zejména pro účely rozšiřování sítě. Jejich výhodou je, že běží na stejném operačním systému jako ostatní zařízení MikroTik.

Bezdrátové systémy - antény, které slouží jak pro příjem, tak pro vysílání signálu. Vyrábějí se v mnoha různých typech a tvarech tak, aby co nejlépe splnily požadavky zákazníka, jak na vyzářený výkon, tak na napájení a umístění v prostoru. Uvnitř těchto antén je opět základní deska, obsahující licenci a RouterOS.

Bezdrátové systémy pro firmy a domácnost - tato zařízení jsou svým designem a funkcemi přímo předurčené pro použití buď v domácnosti, nebo v malé, případně středně velké firmě. Většinou mají rovnou vestavěné vnitřní antény pro pokrytí signálem wifi, 3-5 síťových portů pro připojení PC a napájecí zdroj.

RouterBOARD - tento hardware sestává pouze ze základní desky, kterou je možné umístit do vlastního boxu a vytvořit si tak zařízení na míru [7].

3.1 Značení produktů MikroTik

MikroTik vyrábí mnoho produktů se společným značením a přehledným pojmenováním. Například označení modelu RB 751U-2HnD znamená:

RB - jedná se RouterBOARD:

- 7 - je číslo produktové řady s ohledem na design systému.
- 5 - udává počet ethernetových portů.
- 1 - znamená, že deska má 1 rozšiřovací slot (např. pro další wifi rádio).
- U - na desce je k dispozici USB slot.
- 2Hn - deska je vybavena wifi rozhraním s frekvencí 2,4 GHz.

- D - výrobek obsahuje 2 dvoukanálové antény.

Dále možnosti těchto produktů zahrnují písmena:

- A - větší paměť oproti základní verzi.
- H - znamená vyšší výkon vysílací části.
- G - označuje desku osazenou gigabitovými porty.

Portfolio produktů společnosti MikroTik v současnosti obsahuje více než 40 různých druhů zařízení a rozšiřujících karet, které podporují široký výběr aplikací. Výhodou těchto produktů je zejména to, že jsou všestranné a výkonné a vhodným výběrem nám pro účely vytvoření počítačové sítě bude dostačovat jeden produkt. Tím se ušetří dodatečné náklady na nákup dalších, jednoúčelových zařízení [5].

Zatímco dříve byly RB v podstatě jediné produkty, které společnost MikroTik vyráběla, s postupujícím časem a rozšiřováním portfolia se rozšiřovalo i označování produktů. Dnes je tedy možné se setkat ještě s dalším značením, jedná se zejména o písmena v názvech produktů:

hEX - portfolio malých ethernetových routerů, určených převážně pro domácí použití, zejména tam, kde není potřeba pokrytí wifi signálem. Tomu odpovídá i cena, kdy se tento router dá pořídit od 40 USD.

hAP, mAP - opět levná zařízení, jejichž ceny začínají dokonce na 22 USD. Obsahují vše potřebné pro domácí použití, včetně wifi modulu a integrovaných antén.

wAP - bezdrátový přístupový bod, tedy zařízení vhodné jako vysílač wifi signálu. Tato zařízení obsahují zpravidla pouze jeden ethernetový port pro připojení k síti.

SXT - řada kompaktních antén pro bezdrátový provoz. Je možné je použít jak pro příjem signálu od poskytovatele internetu, tak třeba pro připojení point-to-point, tedy například pro vzájemné bezdrátové propojení sítí.

CRS - Cloud Router Switch – jedná se o nejvyšší řadu ethernetových switchů, většinou jednoprocesorových zařízení s možností montáže do racku.

CCR - Cloud Core Router - opět nejvyšší řada, tentokrát routerů, určená pro montáž do racku, která obsahuje několikajádrové procesory, možnost připojení optiky a je určena především pro hodně vytížené provozy [7].

Všechna tato zařízení mají svá produktová označení, která nám podají informace o tom, jaký hardware obsahují. Vzhledem k původnímu značení RB a čísly s písmeny je tak možné se podívat například na model hAP mini, který je na stránkách výrobce dostupný za necelých 20 USD a k vytvoření zabezpečené domácí nebo malé firemní sítě postačí. Jeho produktové označení je RB931-2nD, je tedy jasné, že obsahuje RouterBOARD designové řady 9, 3 ethernetové porty a jeden rozšiřující slot a dále má vestavěnou duální anténu, vysílající na frekvenci 2,4 GHz [7].

Samozřejmě firma MikroTik vyrábí také velké množství příslušenství, ať už se jedná o různé konektory, přídavné antény nebo třeba miniPCI rozšiřující karty. Přehled všech produktů ale nebyl záměrem této práce.

3.2 Podporovaný x86 hardware

Operační systém RouterOS může běžet nejen na hardwaru firmy MikroTik, ale je k dispozici i pro systémy s x86 architekturou. Tato architektura je založená na stejném HW jako běžné osobní počítače, není tedy problém spustit tento systém na běžném domácím nebo kancelářském počítači. Většina funkcí je založena na počtu dostupných síťových portů, kterých u běžných počítačů v základu není mnoho, stačí je ale dovybavit dodatečnými síťovými kartami a tak je možné provozovat plnohodnotný systém MikroTik za velmi nízkou cenu.

Další výhodou je to, že se RouterOS chová jinak, než počítače s Windows. Není nutné nahrávat hlavní instalaci a pak do ní hledat ovladače, vše potřebné je už součástí základu a RouterOS obsahuje všechny ovladače, které jsou potřeba. Tyto ovladače vybírá MikroTik na základě použitelnosti, funkčnosti a popularity, podobně jako je to u Linuxu [8].

Z těchto důvodů je zajímavou možností provozování RouterOS na virtuálním stroji. V dnešní době už je výkonnost hardwaru dostatečně vysoká na to, aby větší firmy, které potřebují mít několik serverů, provozovaly tyto na virtualizační platformě. Není tedy většinou problém přidat další virtuální stroj a do něj nainstalovat RouterOS, ve kterém se použijí jen ty funkce, které jsou potřeba, např. vzájemné propojení poboček zabezpečeným IP tunelem nebo VPN (Virtual Private Network) přístupy pro obchodní cestující.

V případě provozování RouterOS na jiném zařízení než originálním RB je nutné zakoupit licenci, která bude odpovídat požadovaným funkcím.

4 ROUTEROS

RouterOS je operační systém na bázi Linuxu, je to tedy software, který běží na hardwarové platformě založené na PC. Pro provoz RouterOS stačí buď běžný počítač, RouterBOARD, nebo virtuální stroj [5].

Na rozdíl od jednoúčelových zařízení má RouterOS velmi mnoho možností konfigurace, je tedy možné jej použít např. jako router, switch, VPN server nebo jako AP přístupový bod. Vždy záleží na tom, jaké ovladače a balíčky se do něj doinstalují, pokud tedy nejsou už součástí hlavní instalace.

RouterOS podporuje širokou škálu ethernetových síťových adaptérů, bezdrátových rozhraní, optických rozhraní a velký počet adaptérů Mini-PCI a PCI, karet 3G nebo mobilních datových karet a systémových desek. Díky tomu je možné si postavit systém na míru [5].

I přes tyto široké možnosti nelze než doporučit koupi hardwaru přímo od firmy MikroTik, protože její HW je řádně odzkoušen a testován pro provoz vlastního operačního systému.

4.1 Licencování RouterOS

Každé zařízení, na kterém běží RouterOS musí mít nainstalovanou licenci. Jednou z vlastností RouterOS je to, že základní sada funkcí je stejná ve všech verzích licencí, liší se pouze tím, kolik připojení nebo instancí služeb je možno využít současně [8].

Na originálních zařízeních MikroTik je již licence předinstalována, je však třeba na to myslet a před pořízením si ověřit, zda vybraný RouterBoard má opravdu licenci, která umožní ho použít tak, jak je zamýšleno. Mohlo by totiž dojít k tomu, že bude zakoupena anténa s vestavěnou deskou RouterBoard a předinstalována bude licence 3, se kterou není možné tuto anténu provozovat jako AP přístupový bod, nepřipojí se k němu tedy počítače, tablety ani mobilní zařízení.

Pro menší firmu, která by mohla vytvářet, spravovat a zabezpečovat vlastní síť na starším počítači bude zcela postačovat licence 4, která zprostředkuje nejen potřebné funkce a moduly pro provoz sítě, ale také možnost propojení jednotlivých firemních poboček tunely, připojení do firmy a pokrytí kanceláře signálem wifi.

V takovém případě je ale nutné vzhledem k ceně licence zvážit, jestli není efektivnější z pohledu nákladů, prostoru, spotřeby elektrické energie a možného hluku zakoupit spíše hotové zařízení MikroTik, které již licenci 4 zahrnuje.

Navázání funkcí a počtu souběžných připojení je ukázáno v následující tabulce:

Tab. 1 - Licencování - upraveno z [9]

Licence level	0	1	3	4	5	6
	Trial mode	**Demo**				
Wireless AP	24h trial	-	-	ano	ano	ano
Wireless Client	24h trial	-	ano	ano	ano	ano
EoIP tunely	24h trial	1	Bez omezení	Bez omezení	Bez omezení	Bez omezení
PPPoE tunely	24h trial	1	200	200	500	Bez omezení
PPTP tunely	24h trial	1	200	200	500	Bez omezení
L2TP tunely	24h trial	1	200	200	500	Bez omezení
OVPN tunely	24h trial	1	200	200	Bez omezení	Bez omezení
VLAN rozhraní	24h trial	1	Bez omezení	Bez omezení	Bez omezení	Bez omezení
HotSpot	24h trial	1	1	200	500	Bez omezení
RADIUS klient	24h trial	-	ano	ano	ano	Bez omezení
Fronty	24h trial	1	Bez omezení	Bez omezení	Bez omezení	Bez omezení
Web proxy	24h trial	-	ano	ano	ano	Bez omezení
Správce uživatelů	24h trial	1	10	20	50	Bez omezení

Jak je z tabulky vidět, všechny možnosti lze vyzkoušet po dobu 24 hodin bez omezení, pokročilejší a složitější funkce jsou omezeny na jednoho uživatele nebo přístup jako Demo, u kterého není omezení časem.

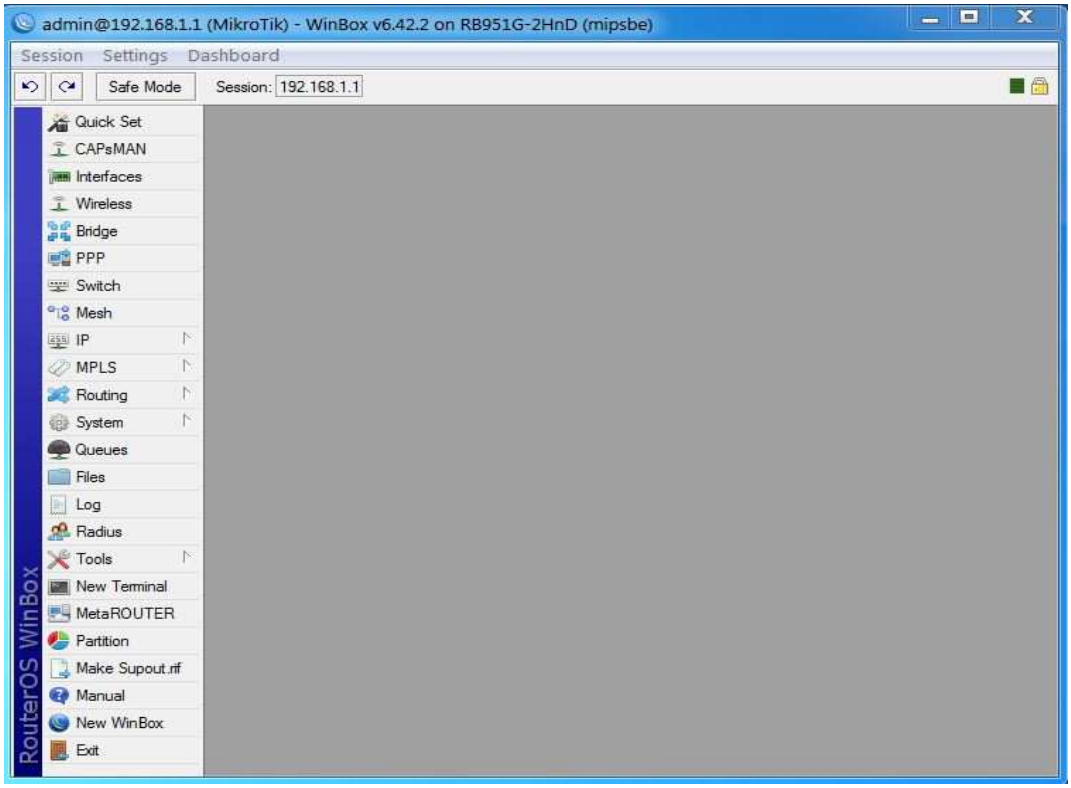
4.2 Ovládání RouterOS

Operační systém je možné ovládat a konfigurovat několika způsoby:

- WinBox.
- WebFig.
- SSH (Secure Shell).
- Telnet (Telecommunication Network).
- Mobilní aplikace.

WinBox je nástroj, který umožňuje správu MikroTik RouterOS pomocí rychlého a jednoduchého grafického rozhraní. Standardně je to aplikace pro Windows, ale může být spuštěna i na Linuxu. WinBox umožňuje konfigurovat všechny funkce MikroTiku z jednoho grafického prostředí při použití standardní klávesnice a myši, což ocení zvláště uživatelé zvyklí na prostředí Windows [10].

Pro připojení k MikroTiku je možné využít buď IP adresu, která je nastavena z výroby a je vždy napsána na krabici nebo je možné použít funkci *Neighbors* (sousedi), kdy WinBox automaticky prohledá síť, zobrazí pouze nalezená zařízení MikroTik podle MAC adres a umožní se k nim připojit [8].

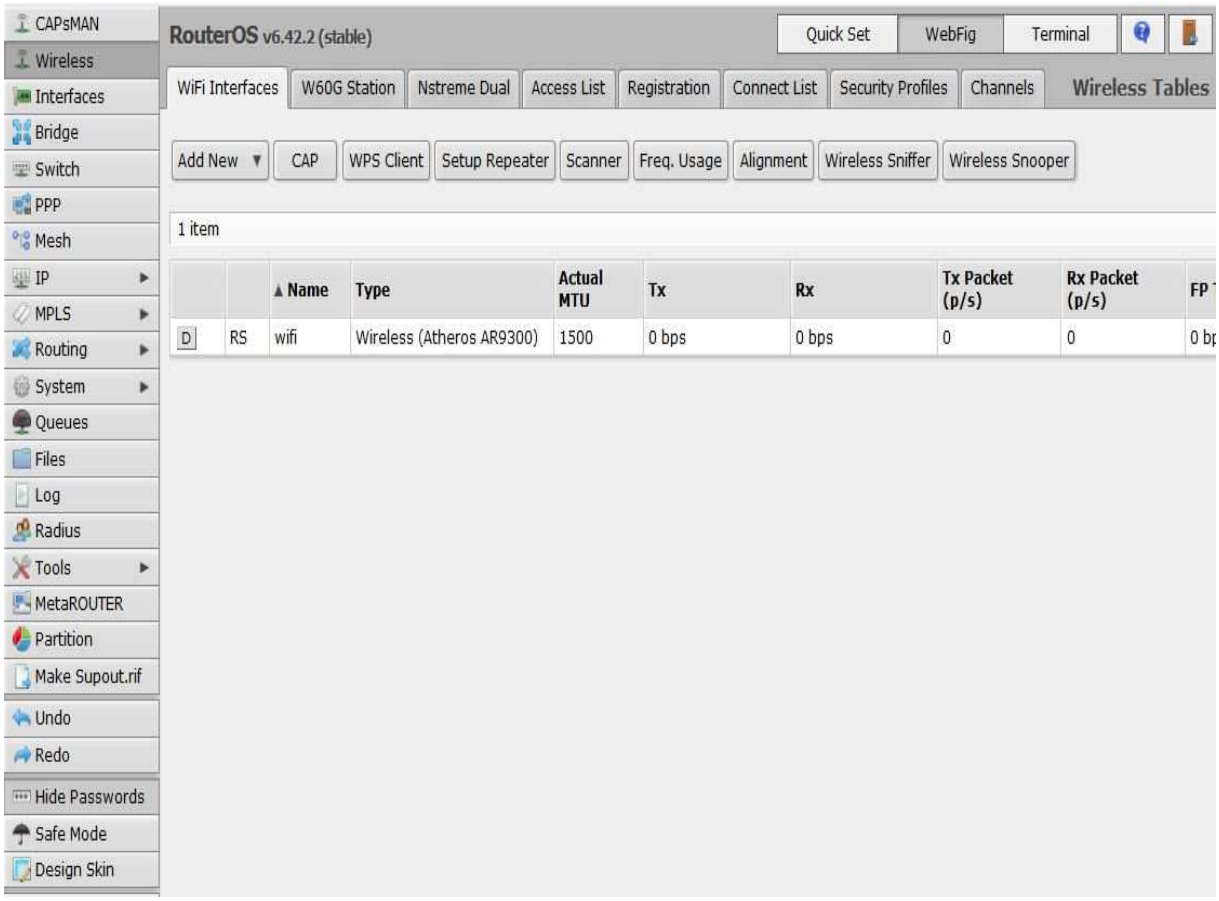


Obr. 1 - WinBox

WebFig je webový nástroj RouterOS, který umožňuje sledovat, konfigurovat a odstraňovat funkce routeru. Je navržen jako alternativa WinBoxu, oba mají podobnou strukturu a oba mají přístup k téměř jakékoli funkci RouterOS. WebFig je přístupný přímo z routeru, což je velkou výhodou, protože není nutné instalovat další software. Další výhodou WebFigu je to, že je to webový nástroj a je tedy nezávislý na platformě a pro jeho použití stačí mít některý z běžně dostupných webových prohlížečů (Internet Explorer, Mozilla, Opera).

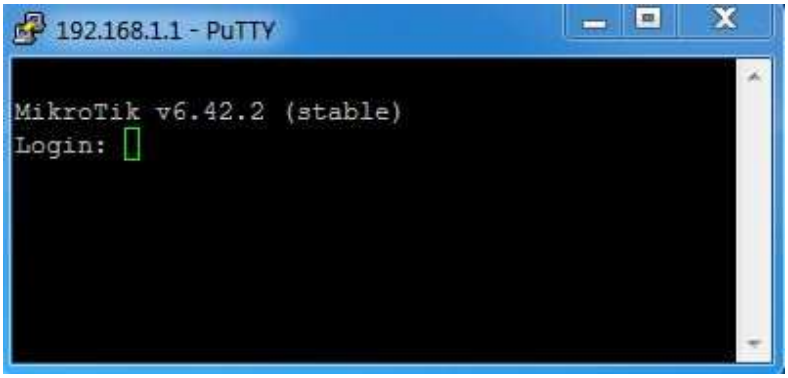
Nejdůležitější úlohy, které je možné provést pomocí aplikace WebFig:

- Konfigurace - umožňuje provádět změny v konfiguraci.
- Monitorování - zobrazuje aktuální stav routeru, statistiky rozhraní, protokoly a další užitečné informace.
- Odstraňování problémů - RouterOS obsahuje velké množství nástrojů pro diagnostiku možných chyb [11].



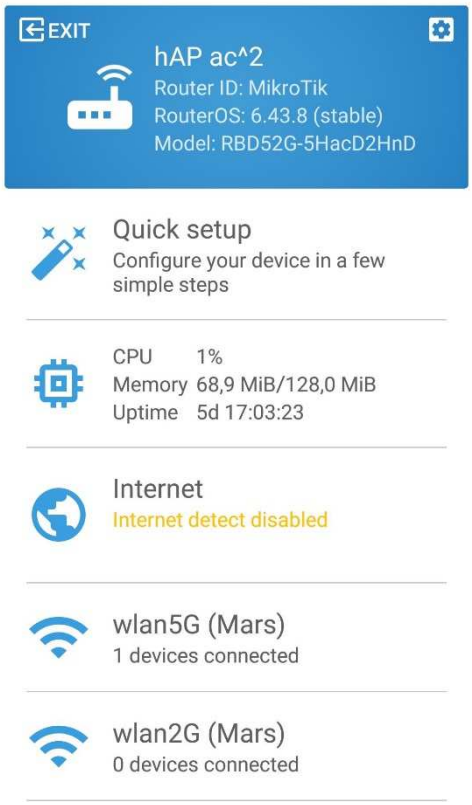
Obr. 2 - WebFig

SSH a Telnet - ovládání přes SSH a Telnet je realizováno pomocí standardní příkazové řádky, která poskytuje dostatečný komfort pro konfiguraci. Jsou podporovány obě verze IP adresování, tedy IPv4 i IPv6.



Obr. 3 - SSH

Mobilní aplikace - společnost MikroTik vyvíjí mobilní aplikaci se stejnojmenným názvem, kterou lze nainstalovat na mobilní telefon nebo tablet s OS Android. Je tak možné se připojit a spravovat všechny důležité funkce v podstatě odkudkoli.



Obr. 4 - Mobilní aplikace

4.3 Vlastnosti RouterOS

Operační systém RouterOS má mnoho zajímavých vlastností, což z něho dělá silný nástroj. Mezi hlavní patří:

Široká podpora hardwaru - jak už bylo zmíněno, podporuje x86 architekturu, několikajádrové procesory, SATA (Serial ATA), USB pevné disky a mnoho síťových karet.

Několik možností instalace - systém je možno instalovat nejen z CD, ale také z USB disku a ze sítě. Zařízení stačí pouze kdekoli v síti připojit kabelem, nastavit adresu a vše pak probíhá zcela automaticky.

Zálohování - celou konfiguraci RouterOS je možno zálohovat do souboru v podstatě jedním kliknutím. Podobně jednoduché je její obnovení v případě havárie, stačí pouze zálohu nakopírovat zpět a zařízení restartovat. Stejně tak se pomocí příkazů v terminálu dá zálohovat jen určitá část konfigurace a ta potom přenést do jiného zařízení MikroTik. Je tak možno zálohovat například nastavení firewallu [13].

Routování - zařízení podporuje několik způsobů routování, a to jak statické tak dynamické, založené na protokolech RIP (Routing Information Protocol) a OSPF (Open Shortest Path First).

VPN - na výběr je mnoho možností připojení vzdálené sítě, založených na protokolu IP, například Point-to-Point tunelování, ať už OVPN (Open VPN), PPTP (Point to Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol), SSTP (Secure Socket Tunneling Protocol), IPSec (IP Security) nebo IPIP (IP in IP) tunel.

Wireless - bezdrátová komunikace - většina zařízení umožňuje zvolit mód, ve kterém budou pracovat. Jedná se zejména o mód Client, AP a Bridge. Dále se jedná o plnou podporu protokolu 802.11n/ac, šifrování WPA2 (Wifi Protected Access) a hlavně možnosti roamingu bezdrátových klientů.

DHCP - router disponuje zajímavou možností nastavit pro každé rozhraní jiný DHCP server, statické a dynamické zapůjčení adres a také DHCP klienta, který umožní zařízení zapojit do cizí sítě a automaticky načíst adresu.

Hotspot - možnost přípojného bodu wifi. Tato funkce podporuje RADIUS protokol pro ověřování uživatelů a také samostatné uživatelské účty s hesly. Na zařízení je možné nastavit i časové omezení přístupu do Internetu, včetně vlastní přihlašovací stránky.

QoS (Quality of Service) - podpora řízení datových toků, která umožňuje dělit vyhrazenou kapacitu připojení na základě různých typů priorit. Je tak možné přidělovat šířku pásma např. do Internetu na jednotlivá rozhraní a tím zamezit zahlcení kapacity linky.

Proxy - proxy server je možné zjednodušeně popsat jako prostředníka mezi počítačem uživatele a cílovým serverem. Nejčastěji se používá se pro oddělení lokální sítě od Internetu.

Nástroje - RouterOS obsahuje celou řadu nástrojů, které správcům umožňují diagnostikovat síť. Jedná se zejména o ping a traceroute, kontrolu vytíženosti provozu (bandwidth control), telnet, ssh, test odesílání emailů a hlavně možnost automatického spouštění skriptů. Skripty mohou provádět automaticky různé naplánované činnosti, např. vzdálené zapnutí počítače na síti.

Firewall - nastavení firewallu v RouterOS je poměrně rozsáhlé, je možné použít několik typů nastavení a ty libovolně kombinovat mezi sebou. To z něj dělá silný nástroj, který je při správném nastavení velmi dobrým pomocníkem při zabezpečení sítě [12].

4.4 Firewall RouterOS

V RouterOS jsou rozlišovány 3 tzv. *chainy* (řetězce), které jsou předinstalovány, a není možné je smazat. Tyto chainy slouží k odlišení a kontrole interního a externího provozu:

a) **Input (vstup)** - slouží k zpracování paketů vstupujících do routeru prostřednictvím jednoho z rozhraní s cílovou adresou IP, která je jednou z adres routeru. V praxi jde tedy o provoz, který přichází jen na MikroTik a není směrován nikam dále, tedy např. připojení přes WinBox.
b) **Forward (skrz)** - slouží k zpracování paketů procházejících routerem. Jedná se tedy o průchozí provoz a to jak směrem dovnitř, tak i směrem ven.
c) **Output (výstup)** - slouží k zpracování paketů pocházejících z routeru a vystupujících ven prostřednictvím některého z rozhraní. V praxi se bude opět jednat o pakety, které jdou přímo z MikroTiku ven a provozu skrze něj se to nijak nedotkne.

Tyto chainy je důležité si uvědomit při nastavování zabezpečení, protože jen jejich správným pochopením lze dosáhnout správného výsledku. Samozřejmě je také možné vytvořit chainy vlastní, definovat vlastní pravidla a tím si nastavit firewall přesně podle vlastních požadavků na míru [8].

Dále se firewall skládá z několika částí:

a) **Stavové filtrování** - v tomto případě firewall udržuje informace o navázaných relacích a propouští pouze ty pakety, které patří do již povolené relace. Zjednodušeně řečeno funguje tak, že co je povoleno směrem ven, má povoleno se i vrátit, např. dotaz na webovou stránku.
b) **Paketové filtry** - pravidla, pomocí kterých definujeme, z jaké adresy a portu na jakou adresu a port povolíme provoz. Tato pravidla umožňují určit, které IP adresy a kam budou mít přístup. V praxi je tak možné např. povolit určitým IP adresám přístup jen do nějakých VLAN nebo jenom na určité IP adresy, typicky na datové úložiště.
c) **Maškaráda** - umožňuje skrýt místní síť za jednu unikátní veřejnou adresu a hromadně přesměrovat IP adresy nebo porty. Je navržena pro specifické použití v situacích, kdy se veřejná IP může náhodně změnit, je-li například přiřazována dynamicky.
d) **Cílový a zdrojový NAT** - jedná se o překlad adres na neveřejnou síť.
e) **Sledování spojení** - firewall sleduje jak interní spojení, tak routování a označování paketů.
f) **Adresní list** - brána firewall umožňuje vytvářet seznamy IP adres pod společným názvem. Filtry pak mohou použít tyto seznamy adres a zjistit, jestli odpovídají povoleným nebo zakázaným paketům.

Existují ještě další možnosti nastavení, ty už jsou však určeny spíše expertům na pokročilé sítě a překračují rámec této práce [14].

Akce, které je možné ve firewallu pro jednotlivá pravidla nastavit:

- **Accept -** povolí provoz, data tedy mohou procházet.
- **Drop** - zakáže provoz, to znamená, že se neprovede žádná akce.
- **Reject** - datový provoz je odmítnut (vrací chybu).
- **Logging** - provádí záznam aktivit, které probíhají na zadaném rozhraní.

Jak je z předchozího vidět, nastavení zabezpečení je v RouterOS na vysoké úrovni, která převyšuje podobná zařízení ve stejné cenové relaci.

II. PRAKTICKÁ ČÁST

5 SÍŤ V MALÉ FIRMĚ

V tomto případě se vychází z obvyklých potřeb malé firmy (do 10 zaměstnanců), kdy je nutné zajistit několik důležitých věcí:

- připojení do Internetu,
- připojení PC po síťovém kabelu,
- přístup notebooků a mobilních telefonů přes wifi,
- zprovoznění tiskáren,
- přístupy na firemní servery, např. NAS (Network Access Storage), případně jakýkoli jiný server.

Síť by měla být koncipována s ohledem na jednoduchost a rozšiřitelnost, snahou tedy je použít co nejméně zařízení, nejlépe jenom jedno, které splní všechny požadavky jak na spolehlivost, tak na bezpečnost. Také je kladen důraz na minimální následnou správu a není tedy zapotřebí mít vlastního správce sítě, což mnohdy celou síť nemálo prodražuje.

Malá firma zpravidla potřebuje propojení kabelem jen pro několik málo počítačů, protože většina dnes používaných zařízení komunikuje prostřednictvím wifi. Má jen omezený počet kanceláří a zaměstnanci používají techniku pouze v rámci těchto kanceláří v jednom sídle. Nepracují z domu, všechnu činnost vykonávají pouze z práce, potřebují ale tisknout, skenovat a ukládat soubory na server.

Mobilní telefony a tablety, které ke své činnosti používají, se také připojují k síti přes wifi. E-maily má taková firma nejčastěji řešeny přes externího dodavatele, typicky pomocí služeb firmy Microsoft Office365, Google Mail nebo podobných.

5.1 Příprava na realizaci sítě

Před realizaci sítě je tedy potřeba si nejprve rozmyslet, kolik počítačů bude připojeno přes kabel, kolik přes wifi, kolik bude tiskáren a případných síťových úložišť.

Na základě této jednoduché analýzy je třeba vybrat zařízení. Předpokládá se připojení do Internetu (ať už pevné nebo bezdrátové), které je zakončeno standardní zásuvkou s konektorem RJ45.

Při výběru je tedy nutno zohlednit několik důležitých věcí:

- počet uživatelů s pevným a mobilním zařízením,

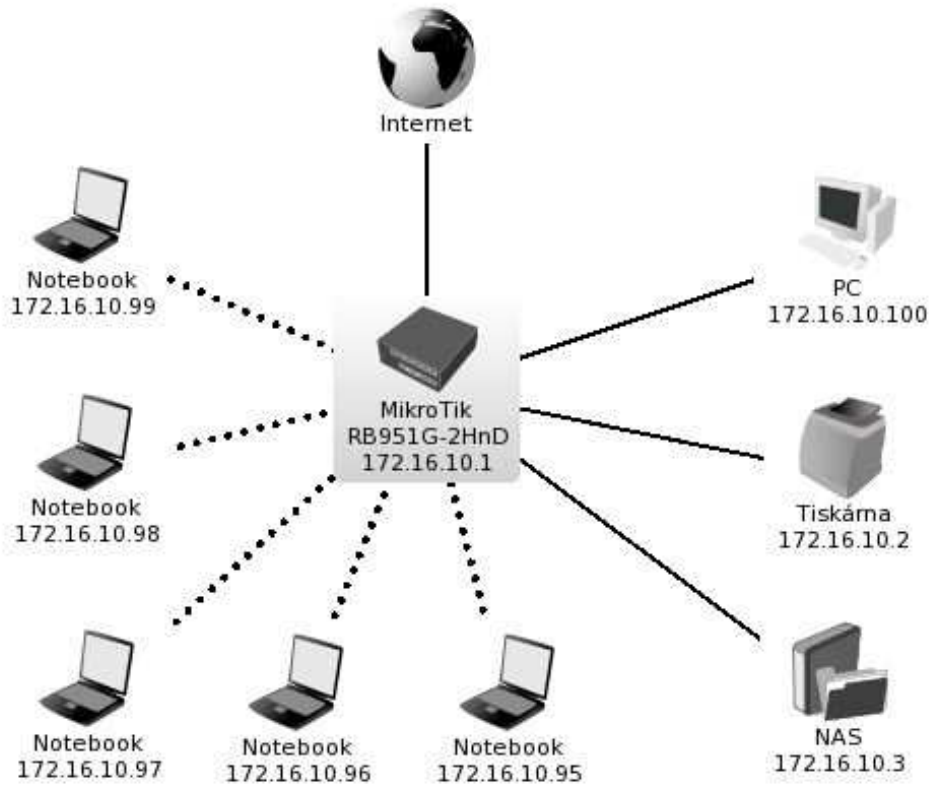
- počet připojených dalších periferních zařízení (tiskárny, NAS),
- rychlost vnitřní sítě, kterou požaduji (100 Mb/s, 1 Gb/s),
- frekvence wifi připojení (2,4 GHz, 5 GHz),
- napájení, možnost připojení napájecího adaptéru do sítě 230V.

V případě malé firmy bylo jednoduchou analýzou zjištěno:

- počet uživatelů: 6,
- počet PC připojených kabelem: 1,
- počet uživatelů s notebooky na wifi: 5,
- počet tiskáren: 1,
- počet úložišť dat: 1,
- rychlost sítě, frekvence wifi: 1 GB a 2,4 GHz.

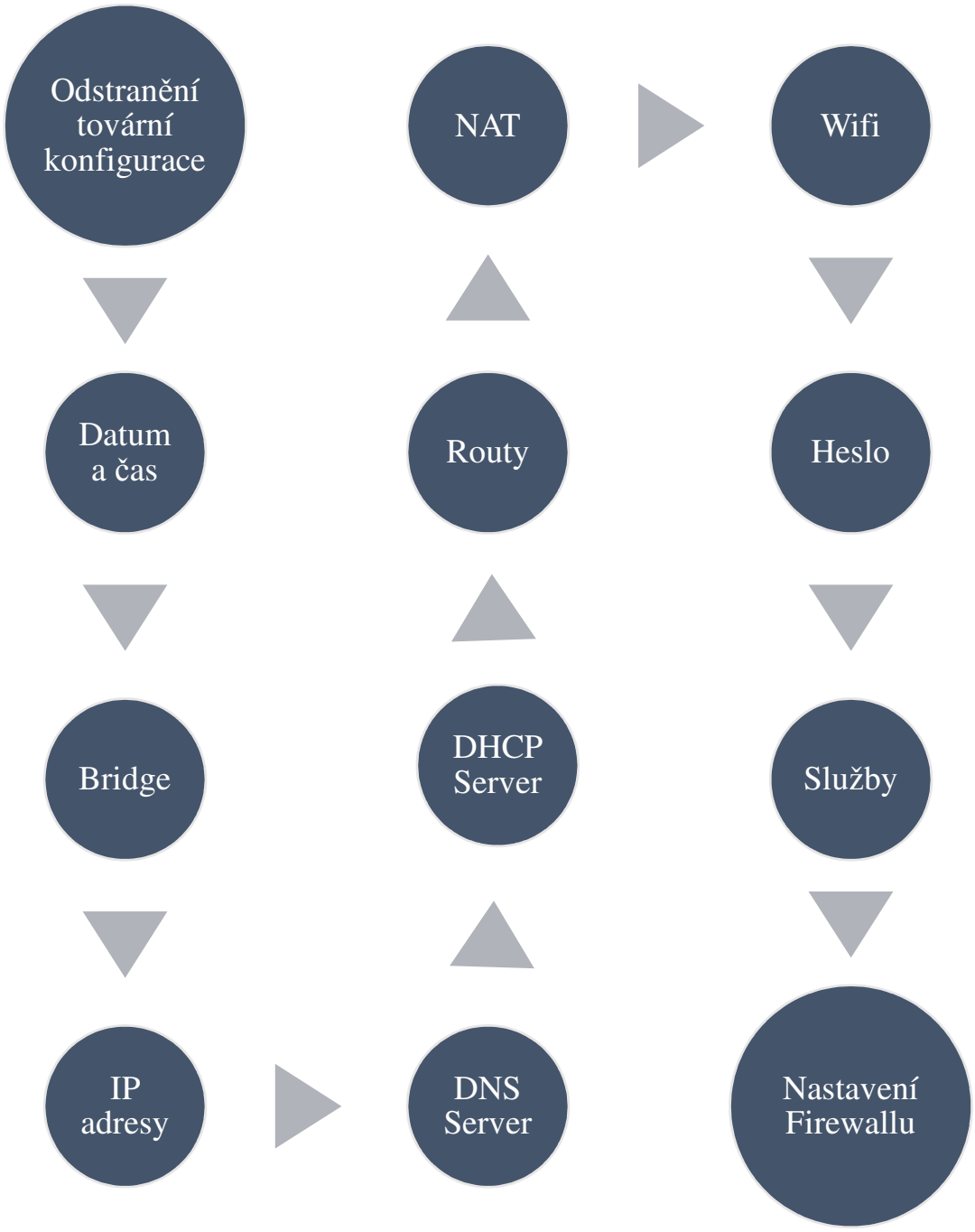
Pro tuto firmu bude tedy postačovat jedno jediné zařízení MikroTik RB951G-2HnD, které svojí konfigurací plně postačuje pro zamýšlené účely. Z výroby obsahuje 5 gigabitových ethernetových portů a má 2 antény MIMO 2,4 GHz.

Cílový stav bude odpovídat obrázku (Obr. 5).



Obr. 5 - Síť v malé firmě

Seznam kroků a nastavení, které je třeba provést, znázorňuje obrázek (Obr. 6).

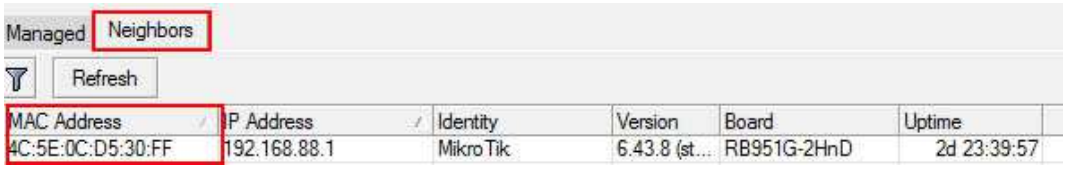


Obr. 6 - Postup konfigurace

5.2 Konfigurace MikroTiku

V prvním kroku je třeba připojit zařízení MikroTik k počítači síťovým kabelem, zapojit zdroj do sítě a spustit aplikaci WinBox. Tu je možno stáhnout z webových stránek výrobce.

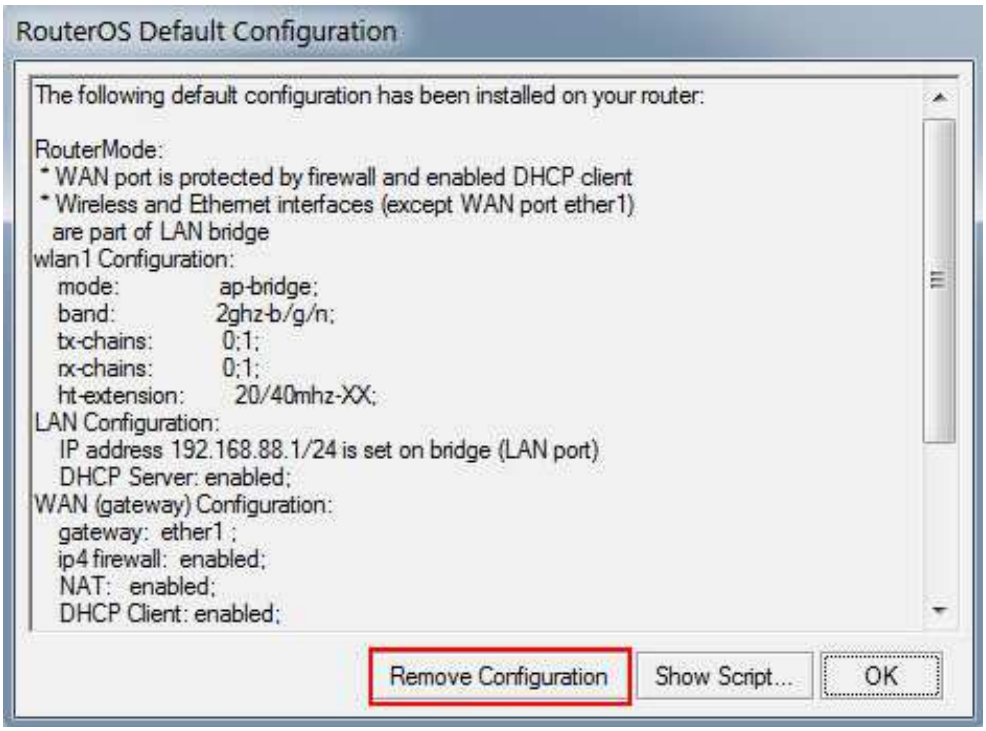
Po spuštění WinBoxu je třeba přejít na záložku *Neighbors*, jak je vidět na obrázku (Obr. 7).



Obr. 7 - Neighbors

Do MikroTiku se dá připojit přes MAC adresu, po vyplnění defaultního jména admin s prázdným heslem.

Dále je třeba vymazat základní konfiguraci přednastavenou od výrobce, protože je nutné začít s čistým RouterOS. Ihned po přihlášení se ukáže obrazovka, kde je možnost tuto konfiguraci vymazat, tedy použít položku *Remove Configuration* (Obr. 8).

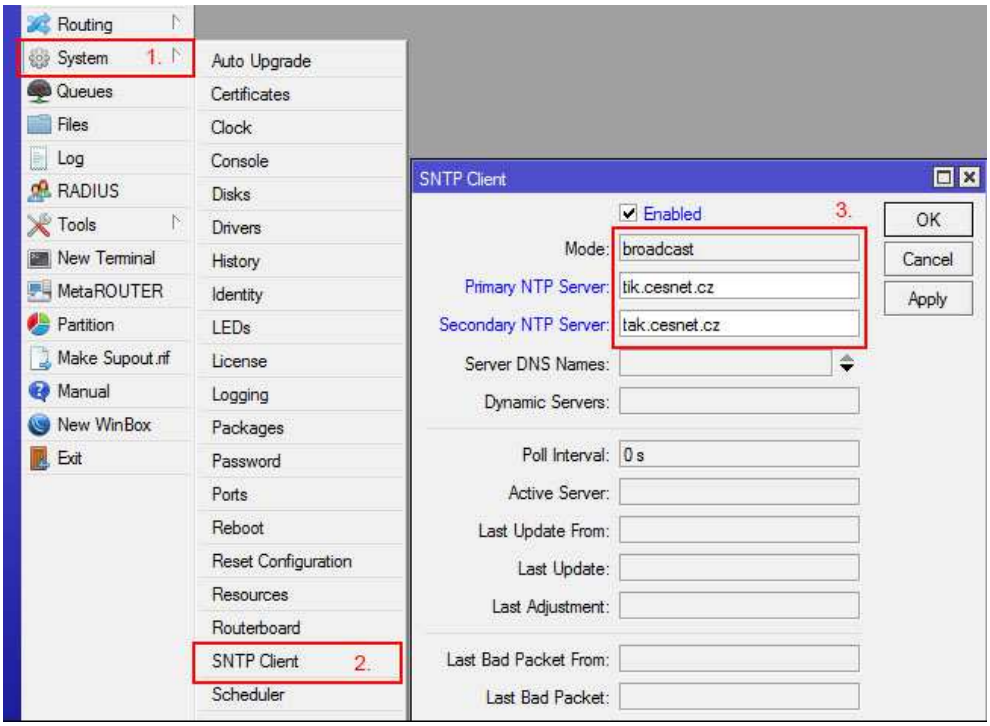


Obr. 8 - Default Configuration

Nyní je dosaženo stavu, kdy je MikroTik bez všech nastavení od výrobce a je možno začít s konfigurací nastavení sítě.

5.2.1 Nastavení data a času

Nejdříve ze všeho je nutné nastavit datum a čas pomocí protokolu NTP. Díky tomuto nastavení budou mít všechny logovací soubory i případné soubory zálohy správný datum a čas. Z menu *System* je třeba vybrat volbu *SNTP Client* a do kolonek vyplnit adresy serverů zajišťujících synchronizaci času v Internetu. Je možné je nastavit i pomocí názvů, např. tik.cesnet.cz a tak.cesnet.cz, jak ukazuje obrázek (Obr. 9).



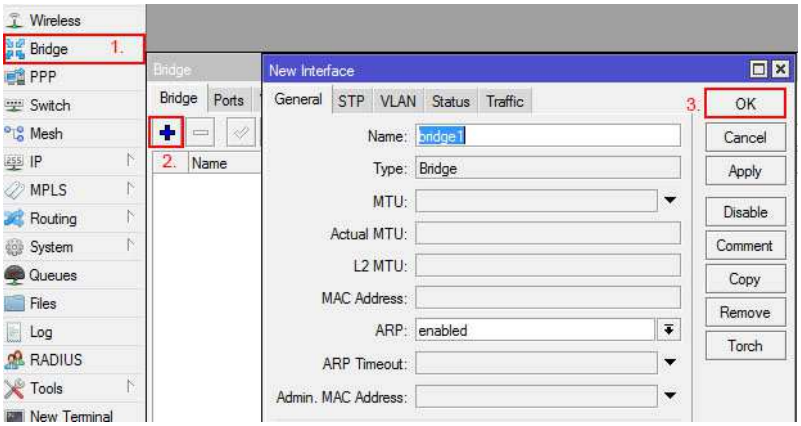
Obr. 9 - Nastavení NTP

5.2.2 Vytvoření bridge

Bridge (most) slouží ke spojení několika síťových rozhraní do jednoho. V tomto případě se použije z toho důvodu, aby se všechna rozhraní tvářila jako jedno a sdílela i všechna další nastavení, jako IP adresu, nastavení DHCP apod.

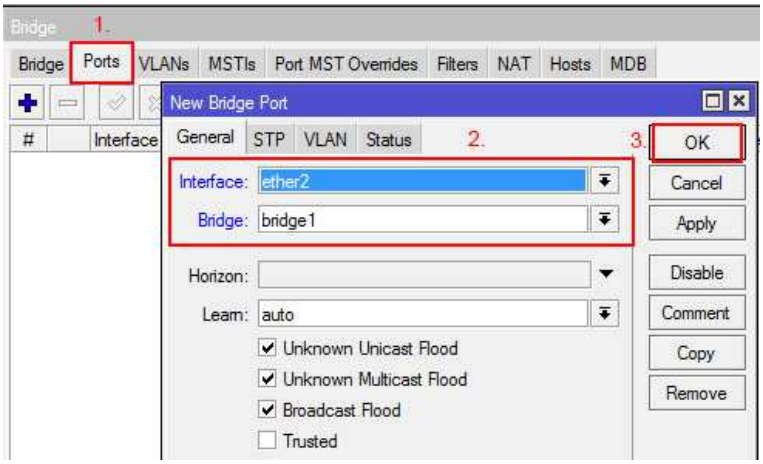
Stejně tak při nastavování zabezpečení a firewallu je pak možné vytvářet pravidla na bridge, pro všechna rozhraní najednou a tím si práci zjednodušit.

Po kliknutí na *Bridge* v levém menu se otevře nabídka pro vytvoření bridge (Obr. 10). Nový bridge bude vytvořen použitím tlačítka „+“. Dále je nutné do takto vytvořeného bridge ještě přidat síťová rozhraní MikroTiku. Jsou to fyzická rozhraní (ether1-5) a anténa pro příjem wifi signálu (wlan1).



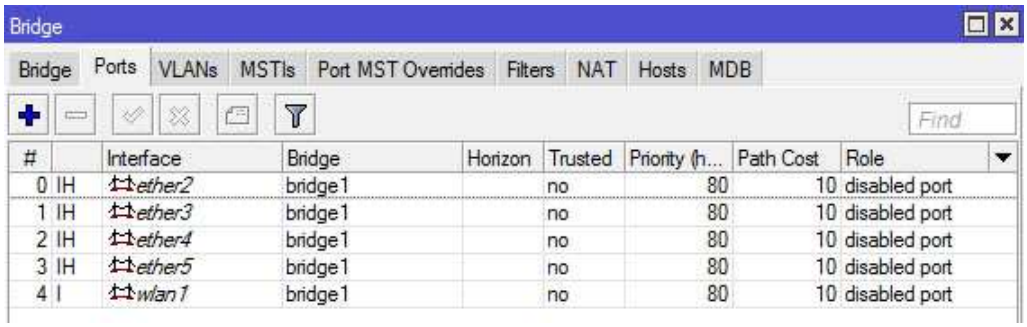
Obr. 10 - Vytvoření bridge

Po vybrání záložky *Ports* se do ní postupně přidají všechna rozhraní včetně wlan1, kromě ether1 (Obr. 11). Tím bude zajištěno, že jak pevná rozhraní RJ45, tak wifi budou sdílet stejná nastavení a budou v jedné síti. Ether1 se nevybírá proto, že do tohoto portu bude zapojen kabel k Internetu a nastaví se na něm adresa poskytovatele, která bude odlišná od adresy vnitřní.



Obr. 11 - Přidání portů do bridge

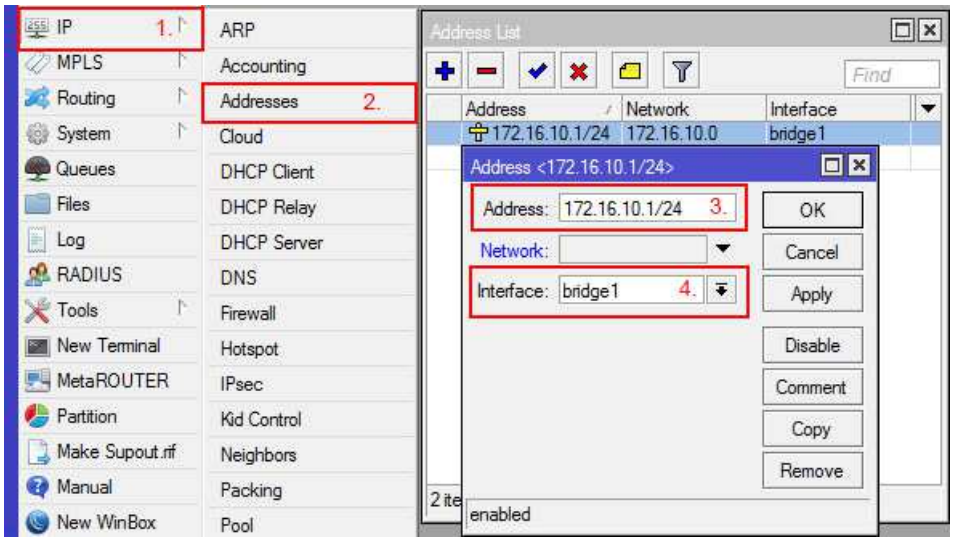
Po vytvoření bridge a přidání portů musí cílový stav vypadat jako na obrázku (Obr. 12).



Obr. 12 - Vytvořený bridge

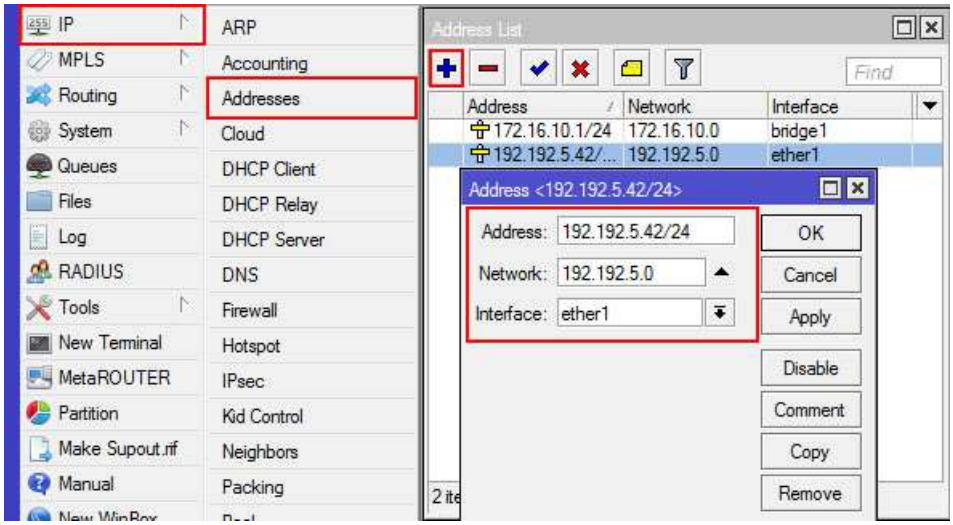
5.2.3 Nastavení IP adres

Na každém rozhraní v MikroTiku je možné nastavit IP adresu s délkou prefixu. V tomto případě je třeba nastavit IP adresu do Internetu přidělenou poskytovatelem na rozhraní ether1 a IP adresu vlastního zařízení na vytvořený bridge. Z neveřejného rozsahu je možné vybrat adresu 172.16.10.1/24, kterou nastavíme na bridge1 (Obr. 13). Zadaný prefix zajistí dostatek volných adres pro eventuální přidávání dalších zařízení do sítě.



Obr. 13 - Vnitřní IP adresa

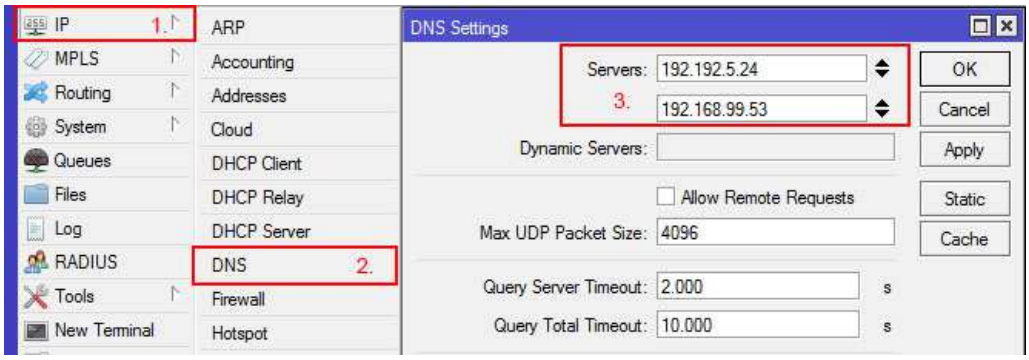
Dále je nutné nastavit IP adresu přidělenou poskytovatelem na rozhraní ether1. To se provede použitím tlačítka *Přidat* (symbol „+“), vyplněním údajů od poskytovatele Internetu a hlavně nastavením rozhraní ether1. Opět nesmíme zapomenout na délku prefixu za lomítkem (Obr. 14).



Obr. 14 - IP adresa poskytovatele Internetu

5.2.4 DNS server

Zprovoznění DNS serveru umožňuje posílat dotazy na překlad adres do Internetu. Ve většině případů je IP adresa (nebo několik adres) DNS serveru přidělena od vlastního poskytovatele, který zajišťuje konektivitu. Tyto adresy je třeba zadat ve volbě *DNS* v MikroTiku (Obr. 15).

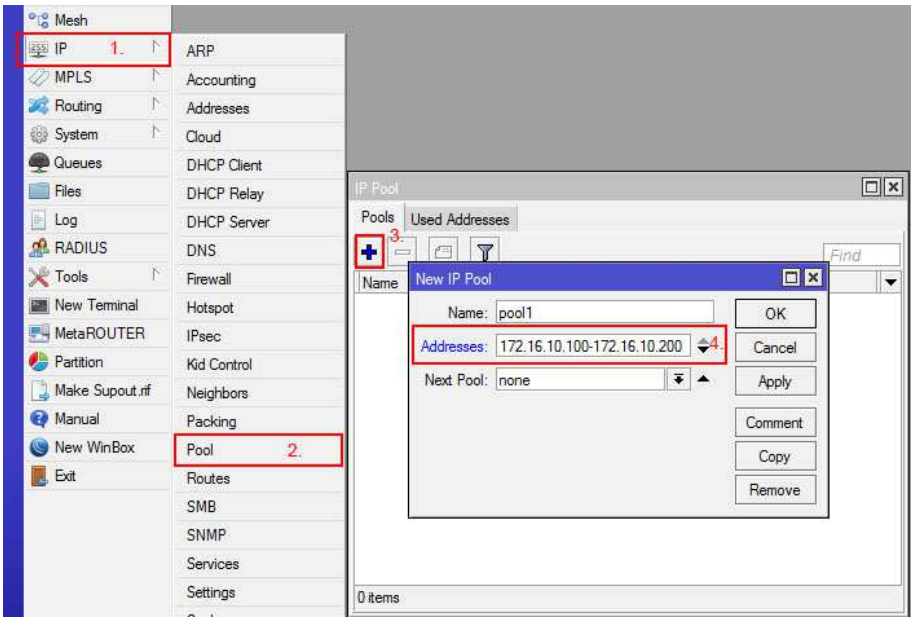


Obr. 15 - Servery DNS

5.2.5 DHCP server

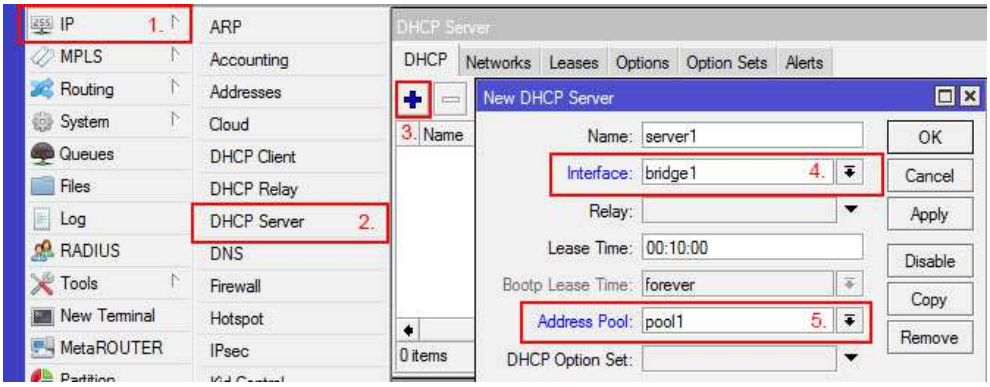
Aby bylo možné zprovoznit DHCP, je třeba nejdříve určit tzv. pool, tedy rozsah adres, které se budou přidělovat. V tomto případě bude rozsah 172.16.10.100 - 172.16.10.200. Tím je zajištěna možnost připojit až 100 zařízení, vznikne tedy dostatečná rezerva.

Po výběru položky *Pool* je třeba tyto hodnoty nastavit do pole *Addresses* (Obr. 16).



Obr. 16 - DHCP Pool

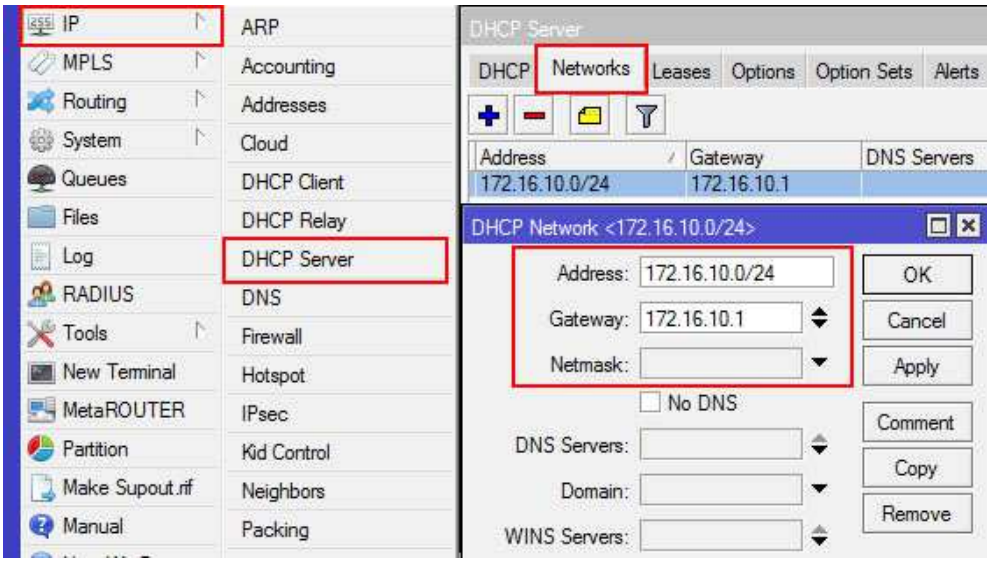
V dalším kroku konfigurace přidělování adres pro počítače v síti je potřeba zprovoznit DHCP server a v něm nastavit nově vytvořený pool, tedy zvolit z menu *IP* položku *DHCP Server*, vytvořit nový a vybrat rozhraní bridge1 (Obr. 17).



Obr. 17 - DHCP Server

Poslední věcí, kterou je nutné udělat, je nastavení údajů, které se budou přidělovat koncovým uzlům ve vnitřní síti. Jedná se o IP adresu sítě, masku, DNS a gateway, tedy bránu, kudy budou počítače ve vnitřní síti posílat pakety ven do Internetu.

Nastavení se provede v *DHCP Serveru* na záložce *Networks*. Do adresy je nutné zadat IP adresu vytvářené sítě s prefixem, tedy 172.16.10.0/24 a jako bránu nastavit MikroTik, tedy adresu 172.16.10.1. (Obr. 18).

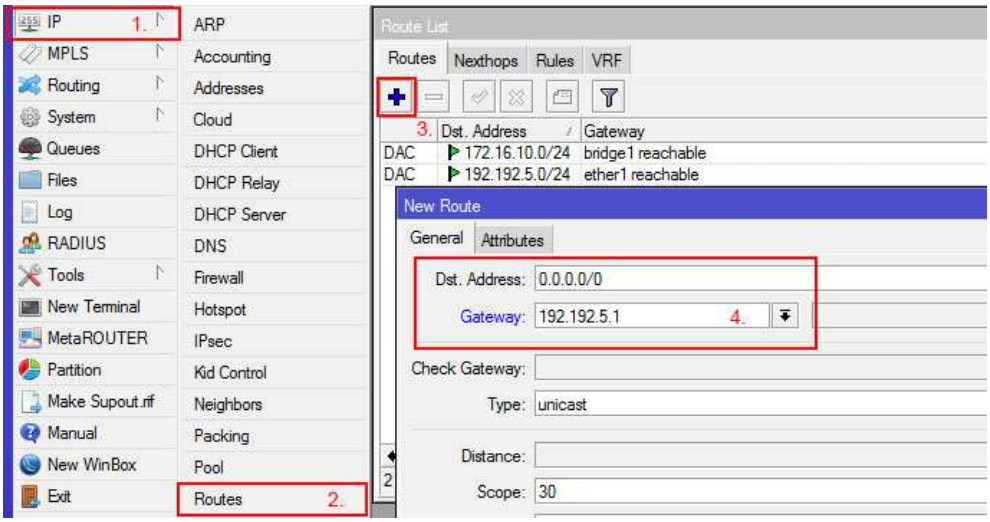


Obr. 18 - DHCP Network

5.2.6 Routy

Aby zapojení fungovalo, je třeba nastavit routing (směrování). S tím souvisí nastavení gateway, tedy brány, kudy půjdou pakety do Internetu. Dvě routy již byly nastaveny dynamicky MikroTikem podle zadaných IP adres, je tedy nutné přidat ještě jednu, s bránou od poskytovatele.

Pro přidání nové routy v menu *IP* a *Routes* se opět použije tlačítko „+“ a jako koncovou adresu *Dst. Address* je třeba zadat default gateway 0.0.0.0/0, tedy všechny pakety, pro které neexistuje jiná routa, použijí toto nastavení. Do políčka *Gateway*, tedy brána, se zapíše gateway poskytovatele internetu, v tomto případě 192.192.5.1 (Obr. 19).



Obr. 19 - Routy

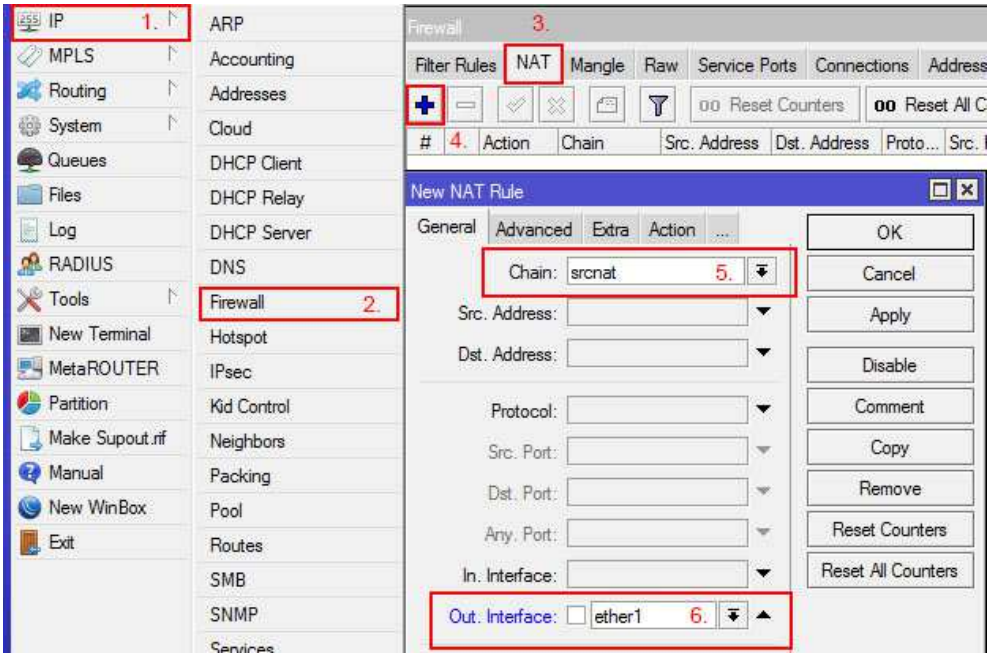
5.2.7 NAT

V tomto kroku je třeba zprovoznit překlad vnitřních adres do veřejného rozsahu a opačně. Tím bude zabezpečeno, že vnitřní síť zůstane skryta před veřejnou částí Internetu, což je důležité z hlediska zabezpečení.

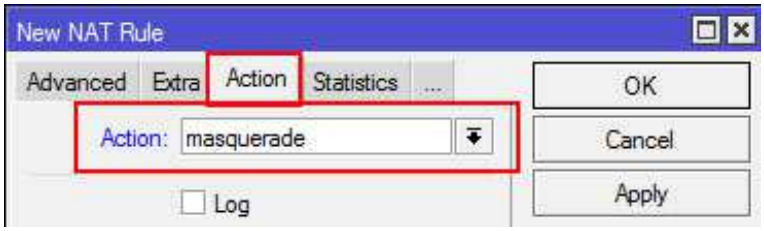
V menu *IP* se použije volba *Firewall* a vybere záložka *NAT*. Při vytváření nového pravidla je nutné z roletkového menu vybrat volbu *srcnat* a tuto volbu přiřadit na vnější rozhraní Ether1 (Obr. 20).

Aby byl NAT funkční, je nutné nastavit akci *masquerade*, tedy tzv. maškarádu IP adres, která zajistí, že požadavky jdoucí ven budou překládány na venkovní rozhraní.

Tuto volbu je možné provést na záložce *Action*, vybráním *masquerade* z roletky (Obr. 21).



Obr. 20 - NAT



Obr. 21 - Masquerade

V tento okamžik je síť hotová a počítač, připojený kabelem do portu 2-5 na zařízení MikroTik by již měl mít konektivitu do Internetu. Toto je možné ověřit příkazem *ping* z PC, například na DNS server Google, tedy na adresu 8.8.8.8, případně zadáním jakékoli funkční Internetové adresy do prohlížeče.

5.2.8 Wifi AP

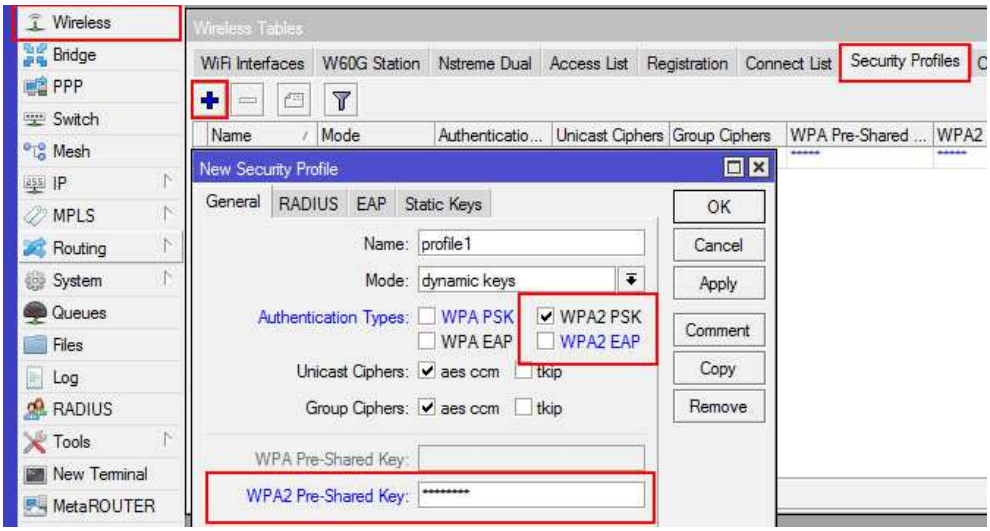
V následujícím kroku je třeba zprovoznit wifi, aby bylo možné do sítě připojit i bezdrátová zařízení, jako jsou notebooky, tablety a mobilní telefony.

Je třeba vytvořit přístupový bod, ke kterému se budou tato zařízení připojovat. Tento přístupový bod se vytvoří na rozhraní wlan1, které bylo už v předchozích krocích přidáno do bridge1. Připojení klienti tak budou dostávat IP adresy ze stejného poolu, jako počítače, připojené po síťovém kabelu. Stejně tak dostanou i nastavení gateway.

Dříve, než se přistoupí k nastavení wlan1, je nutné ho povolit. To je možné provést tak, že se rozhraní označí a modrým zatržítkem *enable* povolí, protože standardně je wifi rozhraní vypnuto a tedy zašedlé.

Wifi síť je potřeba zabezpečit heslem, proto je nutné nejdříve vytvořit bezpečnostní profil, kam bude heslo uloženo.

V menu se zvolí položka *Wireless* a následně záložka *Security Profiles*. Použitím tlačítka „+“ se vytvoří nový profil, kde je nutné zaškrtnout volbu WPA2 PSK, ponechat zaškrtnuto AES (Advanced Encryption Standard) a do kolonky WPA2 Pre-Shared Key vyplnit heslo (Obr. 22). Toto heslo budou zadávat uživatelé při připojování k wifi.



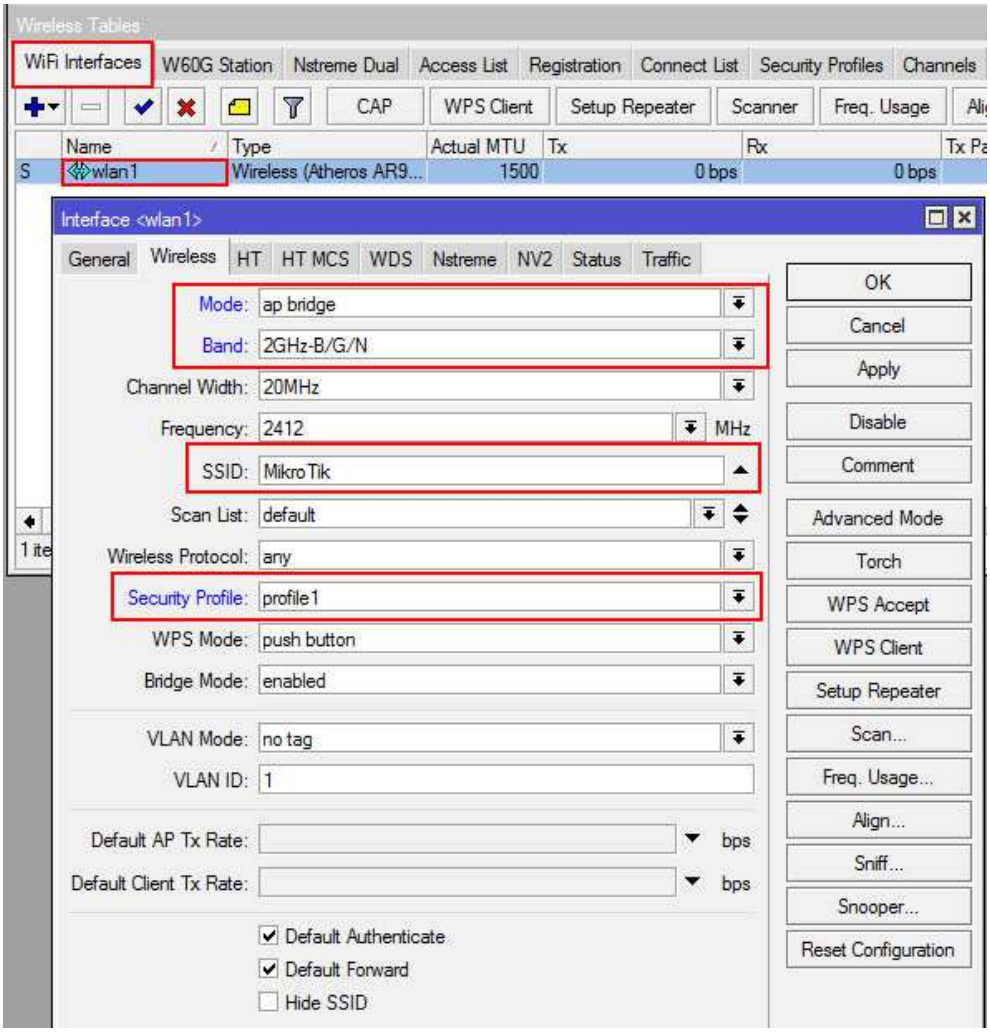
Obr. 22 - Wifi Profile

Je-li profil vytvořen, je možné přistoupit k nastavení samotného wifi rozhraní a přiřadit mu vytvořený profil.

Pro toto nastavení se zvolí záložka *WiFi Interfaces*, kde bude vidět jediné rozhraní wlan1. Dvojitým kliknutím je možné se dostat do konfigurace tohoto rozhraní. Tady je třeba nastavit následující položky:

- *Mode*, kde se z roletky vybere volba ap bridge,
- *Band*, zde se zvolí 2 GHz B/G/N,
- *SSID*, tady je nutné vyplnit zvolený název sítě,
- *Security profile*, zde se vybere již vytvořený profile1.

Ostatní položky je možné ponechat tak, jak jsou (Obr. 23).



Obr. 23 - Wifi rozhraní

Tímto byla ukončena základní konfigurace MikroTiku, která zajišťuje, že počítačová síť funguje a uživatelé se mohou připojit přes wifi i po kabelu.

Pro využití tiskárny a NASu je třeba jen správně nastavit IP adresy v těchto zařízeních, protože ty většinou bývají pevné, tedy nepřidělují se pomocí DHCP.

V tomto případě je na výběr jakákoli z adres, které nejsou součástí vytvořeného poolu, např. tato konfigurace:

- IP adresa 172.16.10.2 pro tiskárnu.
- IP adresa 172.16.10.3 pro NAS.
- Maska 255.255.255.0.
- Gateway 172.16.10.1.

6 ZABEZPEČENÍ

Zprovozněním sítě nastavení MikroTiku zdaleka nekončí, ještě je potřeba jej zabezpečit, protože bude trvale připojen do Internetu a dá se tedy předpokládat, že by se mohl stát terčem útoků.

Pro správné zabezpečení musí být nastaveno několik základních věcí:

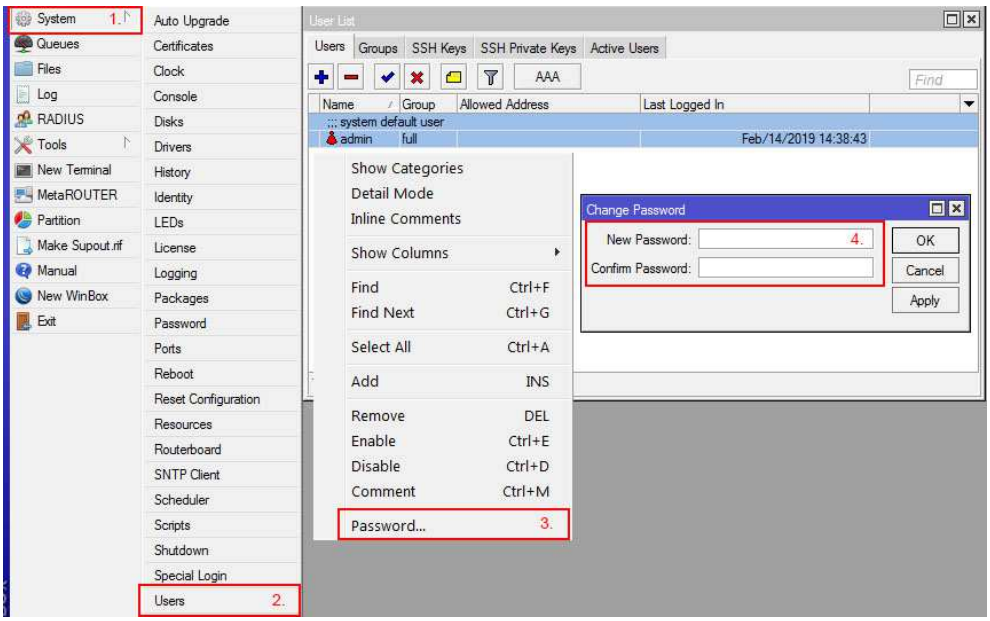
- heslo pro účet administrátora,
- vypnutí nepoužívaných služeb na zařízení MikroTik,
- pravidla ve firewallu.

6.1 Nastavení hesla administrátora

Továrním přihlášením do MikroTiku je účet admin s prázdným heslem. Toto nastavení samozřejmě nemůže zůstat, proto je nutné ho změnit.

Změna hesla je možná v menu *System*, kde je k nalezení položka *Users*. Tady je vidět seznam uživatelů, kteří mají přístup do zařízení, případně je možné také vytvářet uživatele nové.

Pro změnu hesla je třeba vyvolat místní kontextovou nabídku, tedy použít pravé tlačítko myši a kliknout přímo na uživateli admin. Z této nabídky následně vybrat položku *Password* a pak už jen zadat 2x nové heslo (Obr. 24).



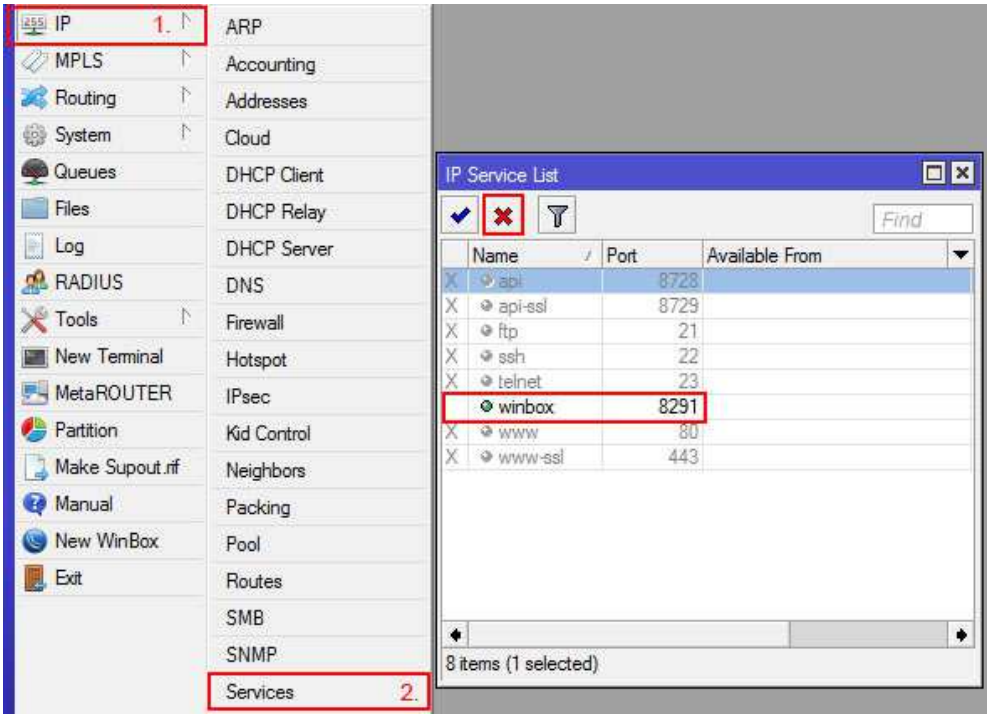
Obr. 24 - Users

6.2 Vypnutí nepoužívaných služeb

MikroTik má v základu povoleny služby, které se týkají přímo zařízení a přístupu na něj a vzhledem k tomu, že v tomto případě zůstanou nevyužity, je lepší je vypnout. Jedná se o:

- API (Application Programming Interface), tato služba je využívána vývojáři aplikací, např. pro mobilní telefony.
- FTP, služba se používá pro výměnu souborů mezi počítačem a zařízením MikroTik.
- SSH, služba pro přístup do administrace.
- Telnet, stejně jako SSH se používá pro konfiguraci zařízení.
- WWW, i tato služba je určena pro přístup do administrace.

Z menu, pod položkou *IP*, je třeba vybrat *Services*. Zobrazí se přehled, kde je následně možné jednotlivé služby deaktivovat červeným křížkem.



Obr. 25 - Services

Při deaktivaci služeb je nutné ponechat aktivní položku Winbox, protože jinak by přestala fungovat i tato aplikace a k MikroTiku by už nebylo možné se přihlásit. (Obr. 25).

Pokud by v budoucnu vyvstala potřeba některé ze služeb opět použít (např. přístup přes www rozhraní), je možné tuto službu opět povolit modrým zatržítkem.

6.3 Firewall

Firewall slouží k zabezpečení celé sítě a také samotného zařízení. Jednou z položek zabezpečení je NAT, který byl nastaven v předchozích krocích.

Jak bylo popsáno v první části práce, firewall MikroTiku rozlišuje tři tzv. *chainy*, do kterých vstupují pakety. Přímo na těchto chainech se nastavují jednotlivá pravidla, kdy se definuje, co se bude dít s příchozím paketem.

Po vstupu do chainu je paket testován podle vytvořených pravidel odshora dolů a zkoumá se, zda pravidlům vyhovuje. Pokud ne, je na konci stromu posledním pravidlem zahozen.

Chainy slouží k rozlišení tří základních stavů a podle toho se taky jmenují:

- **Input** - pakety určené přímo pro zařízení MikroTik. V tomto případě se bude jednat o přístup pro administraci, konkrétně o WinBox, který běží na portu 8291 a také povolení protokolu ICMP, kvůli následné diagnostice, minimálně proto, abychom zjistili, jestli je zařízení dostupné z Internetu.
- **Forward** - zde se jedná o pakety, které zařízením prochází. Jde o pakety určené pro provoz směrem ven a dovnitř do sítě, tedy pakety z rozhraní bridge na rozhraní ether1, čímž se zajistí přístup ke konektivitě do Internetu.
- **Output** - v tomto chainu se řeší pakety, které jsou vytvořeny na zařízení a odesílají se směrem ven. V tomto případě na tomto chainu není třeba nastavit nic.

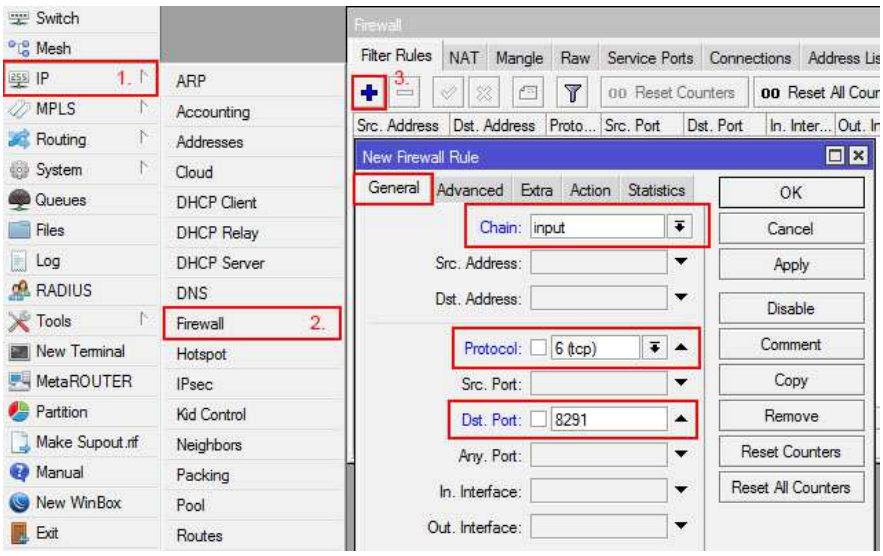
Důležité je uvědomit si, že dříve než se vytvoří zákazové pravidlo *Drop*, je nutné mít vytvořeno pravidlo pro povolení přístupu, který bude potřeba.

Typicky se bude jednat o přístup do administrace, protože pokud nebude povolen, po aktivaci zákazu se na MikroTik už nebude možné připojit.

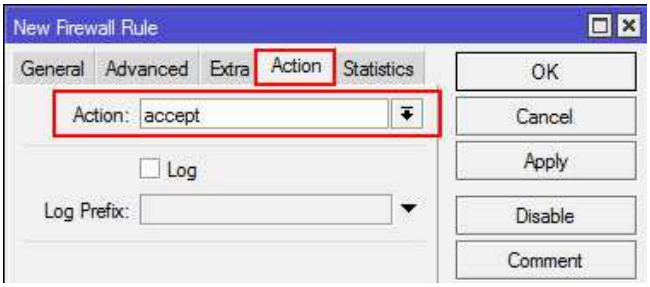
6.3.1 Input chain

Nejdříve je třeba vytvořit pravidlo pro povolení přístupu pro aplikaci WinBox. Je třeba přidat v menu *IP* a *Firewall* nové pravidlo, v nabídce *Chain* vybrat *Input* a jako protokol zvolit TCP a cílový port 8291 (Obr. 26).

Dále na záložce *Action* vybrat *Accept*, tedy průchod paketů povolit (Obr. 27).

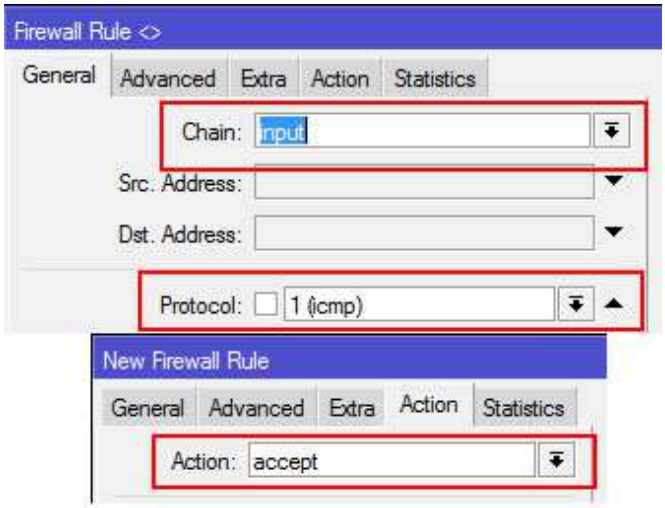


Obr. 26 - Pravidlo pro WinBox



Obr. 27 - Povolení pravidla WinBox

Stejným způsobem je třeba vytvořit pravidlo pro příkaz *ping*, tedy protokol ICMP. Opět se pod položkou *IP* zvolí *Firewall*, tlačítkem „+“ přidá nové pravidlo a v chainu *Input* se zadá protokol ICMP. A podobně jako v předchozím případě musí být pravidlo povoleno na záložce *Action* (Obr. 28).

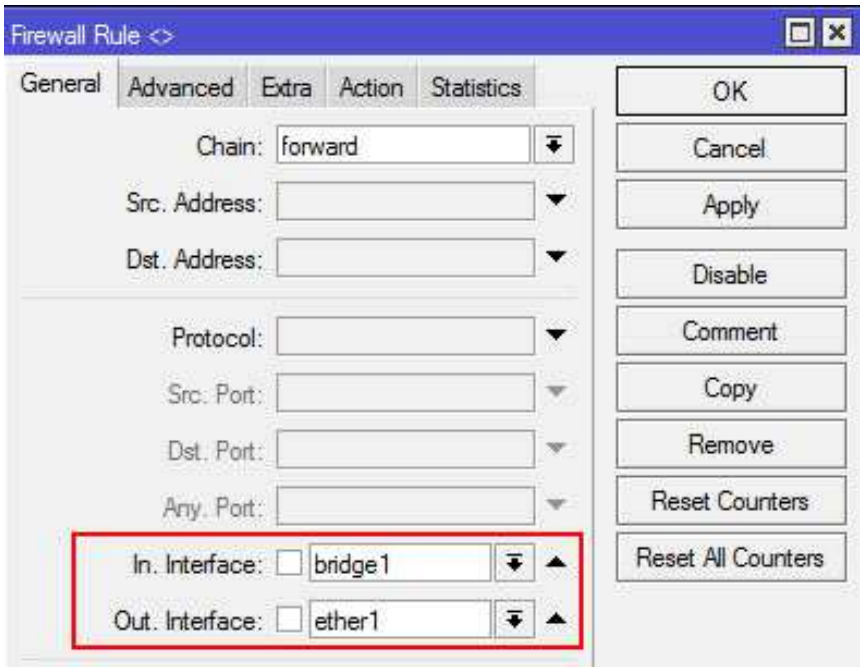


Obr. 28 - Pravidlo pro Ping

6.3.2 Forward chain

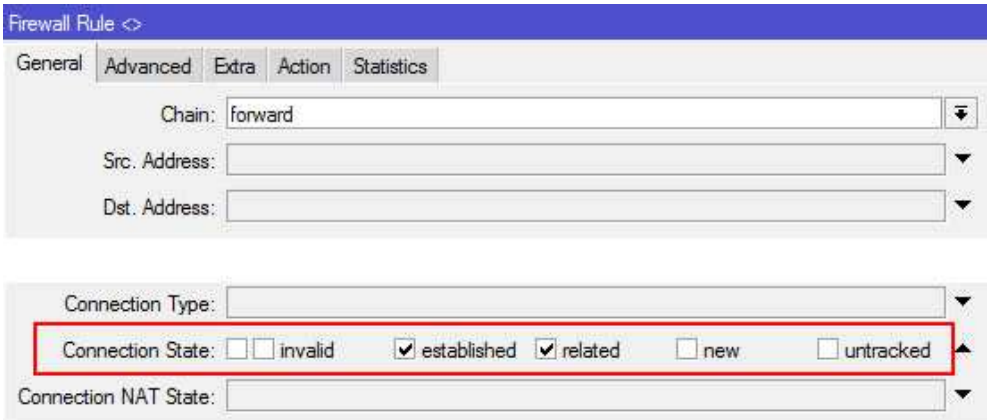
V tomto kroku je třeba nastavit pravidla pro pakety, které jdou skrz MikroTik. Jedná se o požadavky z vnitřní sítě do Internetu a také opačným směrem.

Tentokrát není nutné vybírat konkrétní protokol, ale rozhraní, je tedy třeba zvolit rozhraní vnitřní (bridge1) a vnější (ether1). Samozřejmě je důležité nezapomenout na záložce *Action* vybrat *Accept* (Obr. 29).



Obr. 29 - Pravidlo pro Forward

Dále je třeba vytvořit pravidlo pro průchod paketů pro navázaná spojení. Po přidání nového pravidla na záložce *General* je nutné otevřít roletku *Connection state* a pomocí zatržítek aktivovat volby *established* a *related* (Obr. 30).



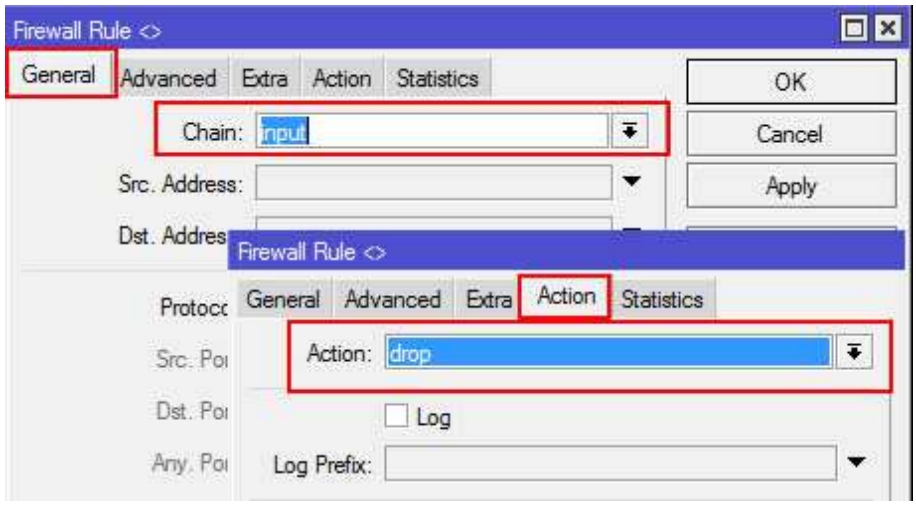
Obr. 30 - Connection State

6.3.3 Drop - zákazové pravidlo

Tento krok je poslední při vytváření pravidel firewallu a znamená, že bude zakázáno vše, co nebylo v předchozích krocích povoleno. Znovu je třeba upozornit, že pokud není správně vytvořeno pravidlo pro vzdálený přístup do administrace, aktivací pravidel *Drop* dojde k „odstřihnutí“ od MikroTiku a nebude jiná možnost, než jej pomocí resetu obnovit do továrního nastavení a začít s konfigurací od začátku.

Pravidla *Drop* je třeba nastavit na obou chainech, tedy jak na Input, tak na Forward.

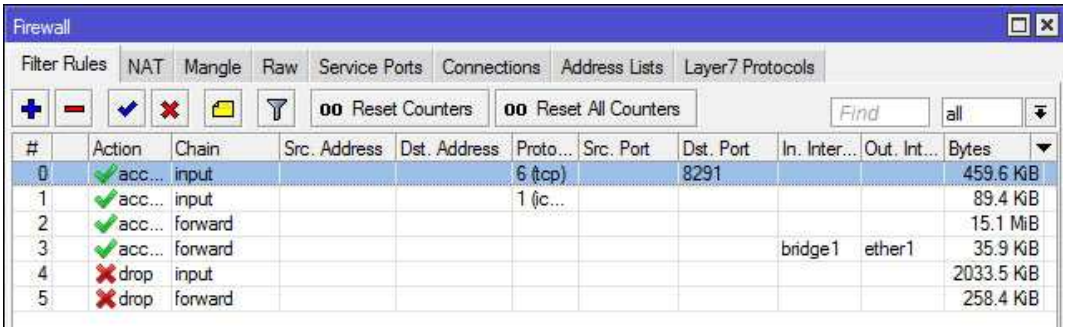
Při tvorbě nového pravidla pro chain *Input* se pouze přidá nové pravidlo, vybere chain a na záložce *Action* z roletkového menu vybere *Drop* (Obr. 31).



Obr. 31 - Drop Input

To stejné se provede na chainu *Forward*. V nastavení nového pravidla se zvolí chain *Forward* a na záložce *Action* z roletkového menu vybere *Drop*.

V celkovém přehledu pravidel se zobrazí všechna vytvořená pravidla, poslední pravidla Drop by měla být na konci, jak ukazuje obrázek (Obr. 32).



Obr. 32 - Pravidla ve Firewallu

6.3.4 Otestování provozu

Abychom si byli jisti, že všechna nastavení jsou funkční tak, jak bylo záměrem, je třeba provést několik jednoduchých testů.

Nejdříve je nutné ověřit, zda je funkční konektivita do Internetu a překlad adres. Do adresního řádku prohlížeče na počítači nebo tabletu stačí zadat libovolnou webovou stránku a je-li správně načtena i zobrazena, vše funguje korektně.

Dále je nutné vyzkoušet, je-li dostupná tiskárna a NAS. To je možné provést příkazem *ping* z jakéhokoli počítače, připojeného do sítě. Pokud je tiskárna připojena, vrátí se z její adresy odpověď.

Stejným způsobem je možné ověřit i viditelnost připojeného NASu, tentokrát ovšem *ping* povede na jeho adresu.

Obr. 33 - Ping na tiskárnu

Tímto posledním krokem je konfigurace zařízení MikroTik v malé firmě ukončena, je možno připojit ostatní počítače a začít je používat. Všechna nastavení, která byla provedena, se v MikroTiku ukládala ihned, není tedy potřeba žádný dodatečný restart.

Stejně tak po výpadku napájení zůstávají všechna nastavení zachována.

7 PROPOJENÍ SÍTÍ

U středně velké firmy se předpokládá, že má více kanceláří, respektive poboček, které se mohou nacházet v různých místech libovolně daleko od sebe. Zjednodušeně řečeno, jedná se o několik výše popsaných malých firem, které je nutné propojit mezi sebou, aby bylo možné používat sdílené pracovní prostředky, např. tiskárny nebo NAS.

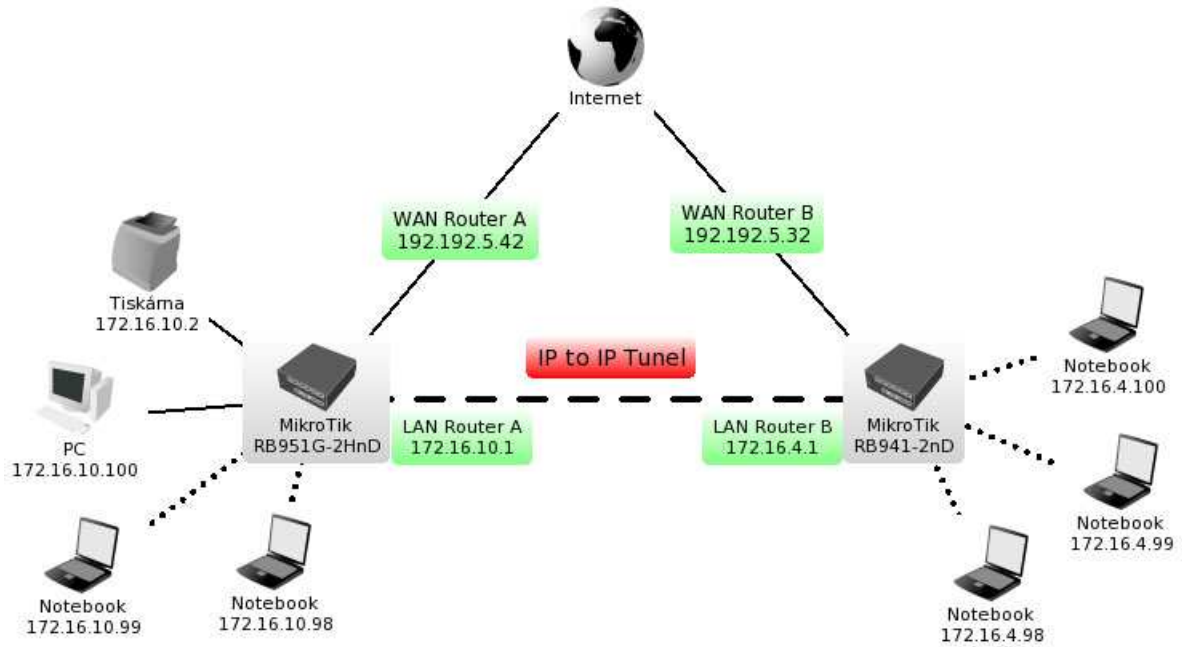
Propojení spočívá v několika krocích:

- vytvoření tunelu mezi jednotlivými zařízeními MikroTik,
- nastavení správného routování,
- povolení dodatečných pravidel ve firewallu.

Výše uvedené činnosti zajistí, že vytvořená síť bude pro uživatele přístupná z kterékoli pobočky oběma směry.

Pro přehlednost byla zařízení MikroTik pojmenována Router A a Router B. Mezi těmito routery bude vytvořen IPIP (IP-to-IP) tunel a nastaveno routování tak, aby se vnitřní sítě navzájem viděly. Tím bude zajištěno, že zaměstnanci firmy A budou moci používat prostředky firmy B a opačně.

Cílový stav ukazuje obrázek (Obr. 34).



Obr. 34 - Propojení sítí

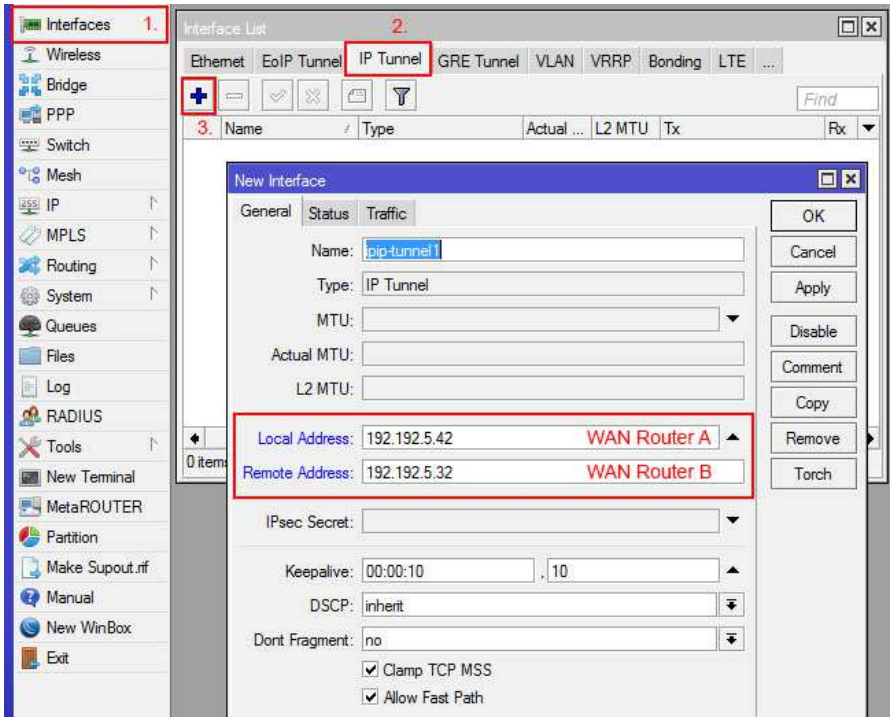
Jediným omezením v případě propojování tunelem je to, že každá síť musí být v jiném vnitřním adresním rozsahu, to znamená, že pokud má MikroTik firmy A vnitřní adresu 172.16.10.1/24, musí mít druhý MikroTik ve firmě B adresu jakoukoli jinou, z povoleného vnitřního rozsahu, např. 172.16.4.1/24.

Předpokládá se, že obě pobočky, tedy firma A i firma B, mají MikroTik správně nastaven a vnitřní síť i přístup do Internetu je plně funkční.

V tomto případě byl použit MikroTik z předchozího nastavení malé firmy jako Router A a menší zařízení, konkrétně RB941-2nD jako Router B. Obě zařízení byla nakonfigurována shodně, pouze se lišily jejich vnitřní a vnější IP adresy.

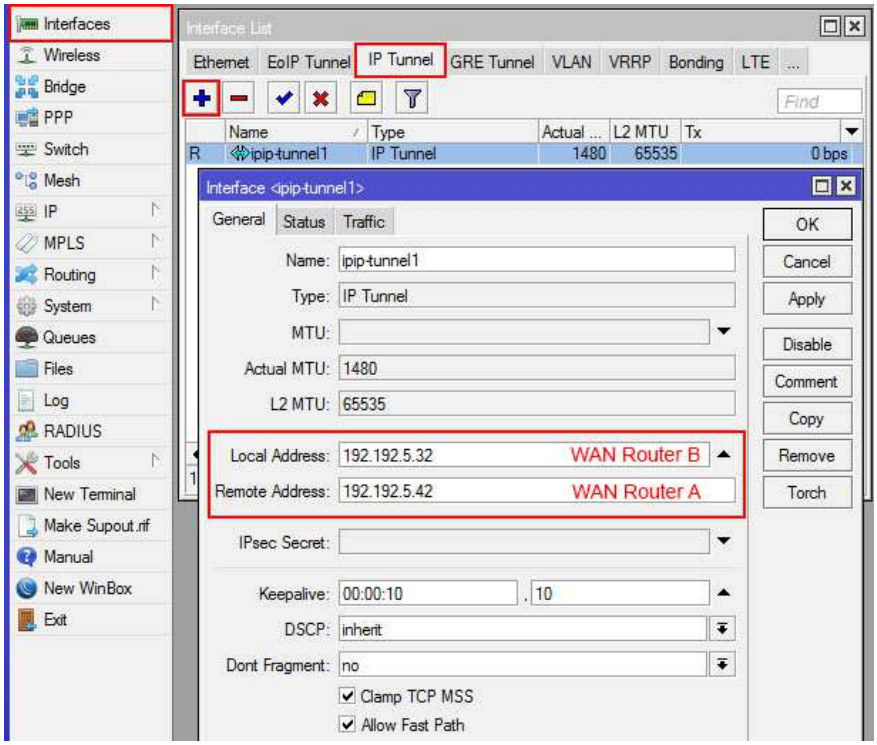
7.1 Vytvoření IPIP tunelu

Po přihlášení do administrace Routeru A pomocí aplikace WinBox se v menu *Interfaces* vybere záložka *IP Tunnel* a zvolí vytvořit nový (symbol „+“). Do kolonky *Local Address* je třeba vyplnit vnější adresu routeru, tedy tu, která je nastavena na ether1. Do další kolonky *Remote Address* se zapíše vnější adresa Routeru B, jak je uvedeno na obrázku (Obr. 35). Po uložení tlačítkem OK je nastavení tohoto routeru hotovo a je možné přejít k vytvoření tunelu na protější straně.



Obr. 35 - Vytvoření tunelu v Routeru A

Po přihlášení do Routeru B je třeba opakovat stejný postup jako v předchozím případě, tedy v menu vybrat *Interfaces*, záložku *IP Tunnel* a zvolit vytvoření nového. Tady vyplnit stejné kolonky, jen v opačném pořadí, jak je uvedeno na obrázku (Obr. 36).



Obr. 36 - Vytvoření tunelu v Routeru B

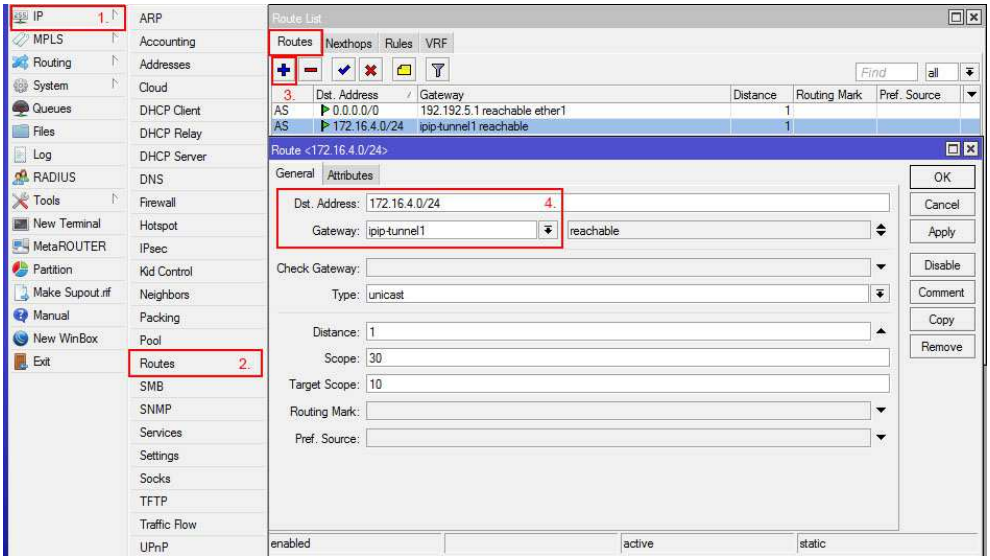
Tímto je vytvoření tunelu hotovo. Ještě je potřeba přidat správné routy na obou stranách, aby na sebe viděly vnitřní sítě.

7.2 Nastavení routování

Pro funkční propojení vnitřních sítí je důležité nastavit správné routy, tedy každému zařízení musí být řečeno, kam má posílat pakety, určené pro protější síť. Routy je nutné nastavit na obou zařízeních, podobně jako v případě IPIP tunelu.

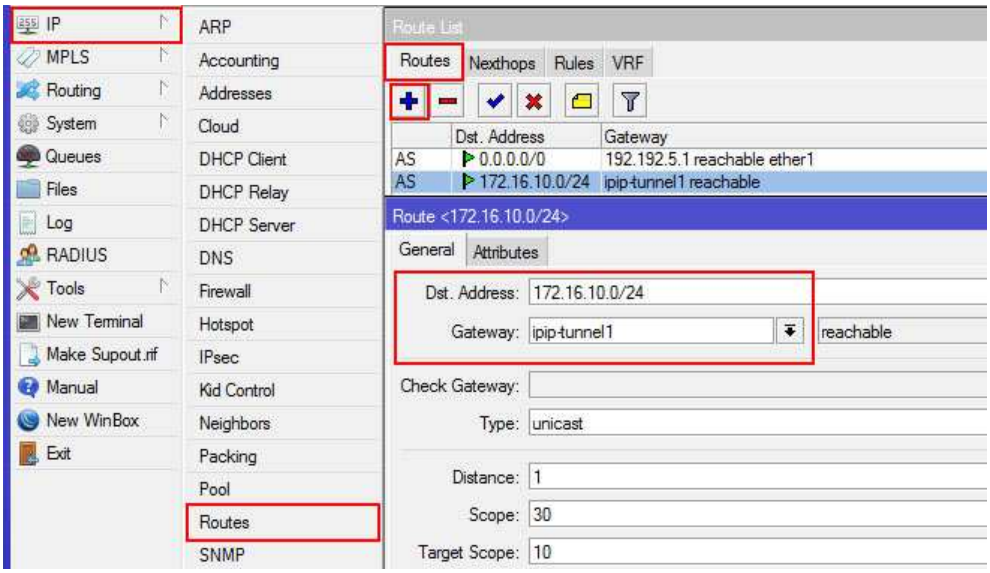
Nastavení routování je v menu skryto pod položkami *IP* a *Routes*. Po zvolení modrého symbolu „+“ v Routeru A je možné přidat další routu, která bude mít v poli *Dst. Address* IP adresu vnitřní sítě Routeru B, tedy 172.16.4.0/24. Aby bylo vše funkční, musí být jako *Gateway* vybrán nově vytvořený tunel, tedy položka ipip-tunnel1.

Správné nastavení routování pro Router A je ukázáno na obrázku (Obr. 37).



Obr. 37 - Nastavení routy A

Aby propojení správně fungovalo, je třeba tu samou operaci provést i na Routeru B, jenom do kolonky *Dst. Address* je v tomto případě nutné zadat adresu vnitřní sítě Routeru A, tedy 172.16.10.0/24, jak ukazuje obrázek (Obr. 38).



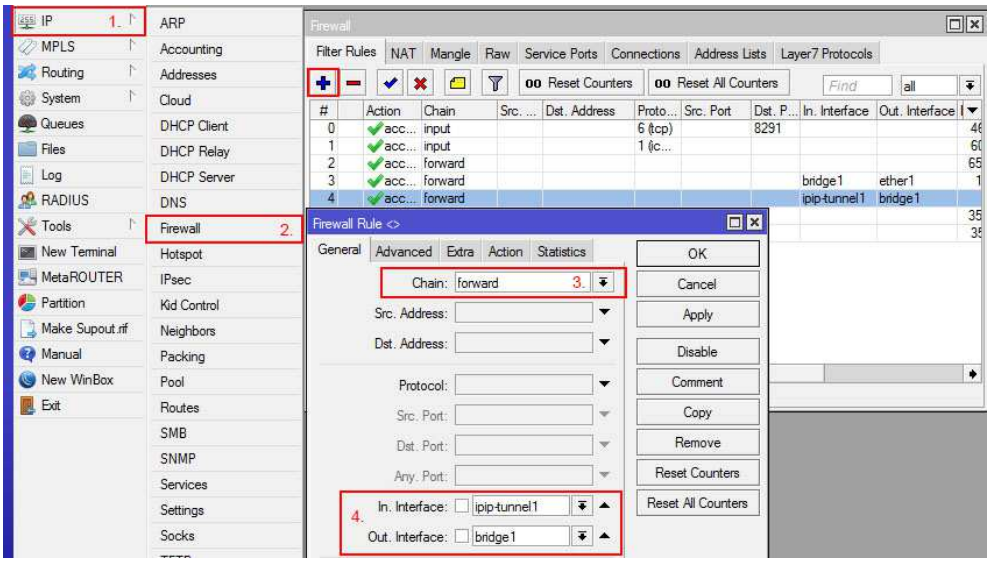
Obr. 38 - Nastavení routy B

7.3 Povolení propojení ve firewallu

Pro správné propojení tunelu je ještě nutné nastavit pravidla ve firewallu tak, aby korektně procházely pakety mezi oběma sítěmi. Tento poslední krok je velmi důležitý, protože při správně nastaveném a zabezpečeném MikroTiku se zatím uživatelé z obou firem navzájem nevidí.

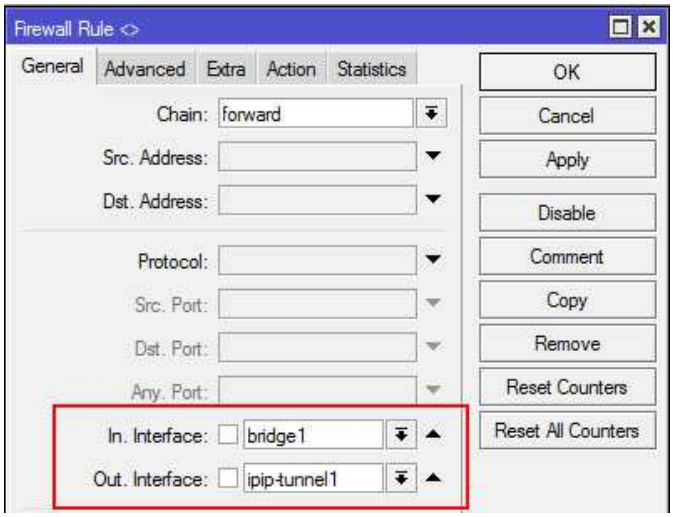
Je nutné vytvořit dvě pravidla pro průchod MikroTikem oběma směry, tedy v prvním pravidle směrem dovnitř a druhým směrem ven. Jedná se o pravidla v chainu *Forward* a týkají se vnitřních a vnějších rozhraní.

Jako první je třeba nastavit opět Router A. V menu *IP* a *Firewall* je nutné založit nové pravidlo, vybrat chain *Forward*, jako interní rozhraní *In. Interface* zadat vytvořený tunel, tedy ipip-tunnel1 a do kolonky externího rozhraní *Out. Interface* vybrat bridge1, jak je patrné z obrázku (Obr. 39). Na záložce *Action* je samozřejmě nutné zvolit *Accept*.



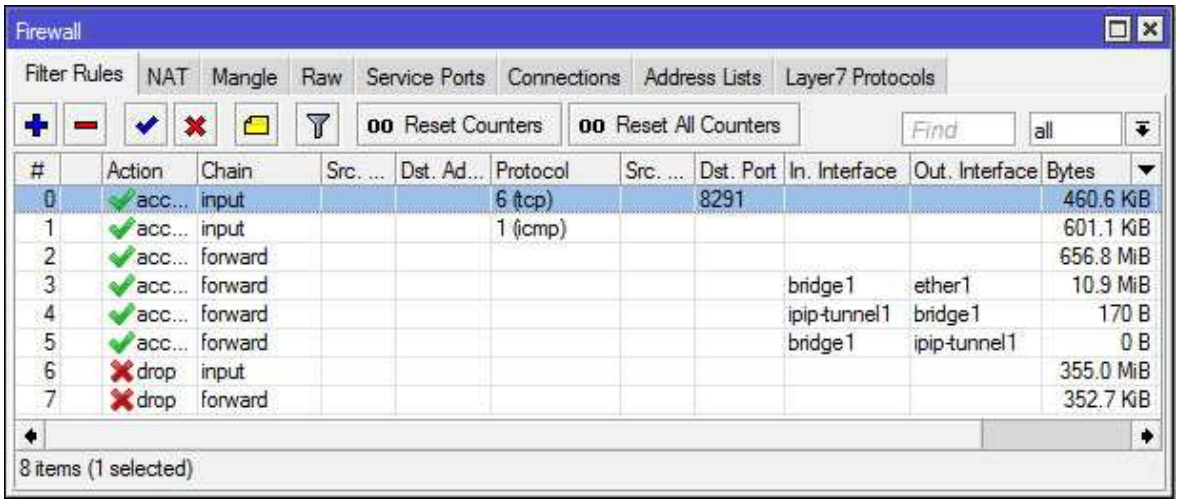
Obr. 39 - Pravidlo pro příchozí pakety

To stejné pravidlo se musí vytvořit ještě jednou, ale tentokrát vybrat rozhraní opačně. Opět tedy přes volbu z menu je třeba zadat nové pravidlo a v chainu *Forward* nastavit jako interní rozhraní bridge1 a jako externí ipip-tunnel1, jak je vidět na obrázku (Obr. 40).



Obr. 40 - Pravidlo pro odchozí pakety

Důležité je nezapomenout tato dvě pravidla vytvořit také v Routeru B. Po jejich vytvoření by firewally v obou routerech MikroTik měly vypadat stejně, jak ukazuje obrázek (Obr. 41).



Obr. 41 - Nastavení firewallu v routerech

7.4 Otestování provozu

Správné propojení zařízení a vnitřních sítí je opět možné provést příkazem *ping* z příkazové řádky počítačů, zapojených v protějších sítích. Tedy ze sítě A se ověří pingem na adresu 172.16.4.100, že je PC ze vzdálené pobočky B viditelné, jak je vidět na obrázku (Obr. 42).

Obr. 42 - Test vzdálené sítě

Tímto je ukončeno propojení vzdálených sítí a je možné bez problémů využívat prostředky vzdálené sítě. Lze si tedy ve vzdálené pobočce B připojit a nainstalovat tiskárnu nebo NAS z pobočky A a trvale tato zařízení využívat.

ZÁVĚR

Téma vytvoření nebo propojení sítí je velmi dobře dostupné v mnoha knihách, bohužel téměř vždy předpokládá hlubší znalosti problematiky sítí, což může být pro mnoho správců v malých firmách limitující.

Cílem práce proto bylo využít zařízení MikroTik s operačním systémem RouterOS jako platformu pro zřízení a zabezpečení malé sítě, protože i když se tento operační systém může jevit složitý, je možné v několika krocích dospět k funkčnímu a zabezpečenému řešení. Tuto síť potom propojit s jinou sítí do funkčního celku, včetně zabezpečení, a vytvořit tak návod, pomocí kterého bude možné toto propojení realizovat.

První část práce se věnovala základním pojmům, týkajících se sítí. Byly vyjmenovány typy sítí, prvků, protokolů a popsány základní funkcionality, které jsou k vytvoření malé sítě potřeba. Dále byly popsány produkty, které firma MikroTik vyrábí, včetně jejich značení a licencování, pro lepší orientaci případných zájemců o tuto problematiku. V samostatné kapitole také byly popsány vybrané funkce samotného operačního systému RouterOS, který je možné konfigurovat mnoha různými způsoby.

Ve druhé části bylo zařízení MikroTik krok za krokem nastaveno, byly na něm zprovozněny všechny služby, které jsou pro funkční síť potřeba, s důrazem na nastavení zabezpečení, kterému bývá často věnováno mnohem méně pozornosti, než si zaslouží.

V posledním kroku byla dvě zařízení propojena mezi sebou a tím došlo k realizaci propojení dvou nezávislých sítí. Veškerá konfigurace byla otestována a použita v ostrém provozu.

Vzhledem k tomu, že pro zařízení MikroTik není publikováno mnoho zdrojů v českém jazyce, byla práce koncipována jako návod a už během vzniku druhé, praktické části se jako návod používala, bylo do ní tedy možné zapracovat i připomínky, vzniklé z praxe.

Do budoucna je autorem počítáno s postupným rozšiřováním práce při zachování jednoduchosti a vytvoření postupu pro připojení zaměstnanců pomocí zabezpečeného VPN tunelu a využití MikroTiku jako přístupového bodu pro zřízení mobilního pracoviště, např. při krizovém řízení.

SEZNAM POUŽITÉ LITERATURY

[1] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5. aktualizované vydání. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

[2] TRULOVE, James. *Sítě LAN*. Praha: Grada Publishing a.s., 2009. ISBN 978-80-247-2098-2.

[3] Wendell ODOM. *Počítačové sítě bez předchozích znalostí*. Brno: CP Books, 2005. ISBN 80-251-0538-5.

[4] KABELOVÁ Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5. aktualizované vydání. Brno: Computer Press, 2012. ISBN 978-80-251-2236-5.

[5] DISCHER, Stephen. *RouterOS by Example.* 1. vydání. USA, 2011. ISBN 978-0-615-54704-6.

[6] MikroTik. *Company profile.* [online]. 2018 [cit. 2019-1-30]. Dostupné z: https://www.mikrotik.com/download/share/mt_profile.pdf

[7] MikroTik: *Products.* [online]. 2018 [cit. 2019-1-30]. Dostupné z: https://mikrotik.com/products

[8] BURGESS, Dennis. *Learn RouterOS.*2. vydání. Rumford: Lulu.com, 2011. ISBN 978-1-105-06959-8.

[9] MikroTik Wiki. *Manual: License.* [online]. 2018 [cit. 2019-1-30]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:License

[10] MikroTik Wiki. *Manual: Winbox*. [online]. 2018 [cit. 2019-2-13]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Winbox

[11] MikroTik Wiki. *Manual: Webfig*. [online]. 2018 [cit. 2019-2-13]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Webfig

[12] MikroTik Wiki. *Manual: RouterOS features*. [online]. 2018 [cit. 2019-2-13]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:RouterOS_features

[13] MikroTik Wiki. *Manual: System backup*. [online]. 2018 [cit. 2019-2-13]. Dostupné z:https://wiki.mikrotik.com/wiki/Manual:Configuration_Management#System_Backup

[14] MikroTik Wiki. *Manual: IP/Firewall.* [online]. 2018 [cit. 2019-2-13]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:IP/Firewall

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES Advanced Encryption Standard

AP Access Point

API Application Programming Interface

ATA Advanced Technology Attachment

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

FTP File Transfer Protocol

GAN Global Area Network

HTTP Hypertext Transfer Protocol

ICMP Internet Control Message Protocol

IDE Integrated Drive Electronics

IP Internet Protocol

IPIP IP in IP

IPSec IP Security

ISP Internet Service Provider

L2TP Layer Two Tunneling Protocol

LAN Local Area Network

MAN Metropolitan Area Network

MUM MikroTik User Meetings

NAS Network Access Storage

NTP Network Time Protocol

OSPF Open Shortest Path First

OVPN Open VPN

PPTP Point to Point Tunneling Protocol

QoS Quality of Service

RIP Routing Information Protocol

SATA Serial ATA

SMTP Simple Mail Transfer Protocol

SSH Secure Shell

SSID Service Set Identifier

SSTP Secure Socket Tunneling Protocol

TCP Transmission Control Protocol

UDP User Datagram Protocol

VPN Virtual Private Network

WAN Wide Area Network

WPA2 Wifi Protected Access 2

SEZNAM OBRÁZKŮ

SEZNAM TABULEK