

Využití platformy MikroTik pro počítačové sítě středního rozsahu

Daniel Polišenský

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav informatiky a umělé inteligence

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Daniel Polišenský
Osobní číslo:	A22418
Studijní program:	B0613A140020 Softwarové inženýrství
Forma studia:	Prezenční
Téma práce:	Využití platformy MikroTik pro počítačové sítě středního rozsahu
Téma práce anglicky:	he use of the MikroTik platform for medium-scale computer networks

Zásady pro vypracování

1. Zpracujte literární rešerši na dané téma.
2. Provedte a popište základní konfiguraci routeru.
3. Implementujte a popište CAPsMAN pro hromadnou správu Wi-Fi přístupových bodů.
4. Implementujte a popište QoS.
5. Implementujte a popište vzdálený přístup do sítě pomocí VPN.
6. Popište možnosti využití dvou internetových přípojek a jednu variantu implementujte.
7. Popište možnosti správy pomocí skriptovací jazyku RouterOS a Pythonu. Některé příklady implementujte.

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam doporučené literatury:

1. LAMMLE, Todd. *CCNA – výukový průvodce*. 4. akt. vyd. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.
2. DISCHER, Stephen R.W. *RouterOS by Example. Understanding Mikrotik RouterOS Through Real Life Applications*. 2nd Edition. Isp Services, Inc., 2016. ISBN 978-0-692-77708-4.
3. MikroTik. *MicroTik* [online]. [cit. 2024-09-27]. Dostupné z: <https://mikrotik.com>
4. MikroTik. *MikroTik documentation wiki* [online]. [cit. 2024-09-27]. 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: **27. října 2024**
Termín odevzdání bakalářské práce: **2. června 2025**



L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 17. listopadu 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- 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;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- 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(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.
- při tvorbě této práce jsem použil nástroj generativního modelu AI [ChatGPT; <https://chatgpt.com>] za účelem zlepšení textu, kontroly pravopisu a jazykové korektury. Po použití tohoto nástroje jsem provedl/a kontrolu obsahu a přebírám za něj plnou zodpovědnost.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Tato práce se zabývá využitím platformy MikroTik při návrhu, implementaci a správě počítačových sítí středního rozsahu. Zaměřuje se na konfiguraci směrování, firewallu, VPN, QoS a automatizaci. Popsány jsou klíčové síťové technologie a vlastnosti zařízení MikroTik a na jejich základě je navržen konkrétní model síťové infrastruktury pro podnikové prostředí. Důraz je kladen na bezpečnost, spolehlivost a škálovatelnost řešení. Výsledkem je funkční návrh s ověřenou konfigurací, který může sloužit jako šablona pro podobné implementace.

Klíčová slova: MikroTik, počítačová síť, RouterOS, VPN, firewall, QoS, CAPsMAN, automatizace

ABSTRACT

This thesis focuses on the use of the MikroTik platform in the design, implementation, and management of medium-sized computer networks. It addresses the configuration of routing, firewall, VPN, QoS, and automation. Key networking technologies and the features of MikroTik devices are described, and a specific network infrastructure is designed for a model business environment. The design emphasizes security, reliability, and scalability. The result is a functional and verified configuration that can serve as a template for similar implementations.

Keywords: MikroTik, computer network, RouterOS, VPN, firewall, QoS, CAPsMAN, automation

OBSAH

ÚVOD.....	12
I TEORETICKÁ ČÁST	13
1. POČÍTAČOVÁ SÍŤ	14
1.1 MODEL ISO/OSI	14
1.2 PASIVNÍ SÍŤOVÉ PRVKY	14
1.2.1 Fyzická vrstva	14
1.2.2 Linková vrstva.....	14
1.2.3 Síťová vrstva	14
1.2.4 Transportní vrstva	14
1.2.5 Relační vrstva.....	14
1.2.6 Prezenční vrstva	14
1.2.7 Aplikační vrstva	14
1.3 AKTIVNÍ SÍŤOVÉ PRVKY.....	15
1.4 PASIVNÍ SÍŤOVÉ PRVKY	15
1.5 DRUHY SÍŤE.....	15
2. IP ADRESACE	17
2.1 IPv4 ADRESACE	17
2.1.1 Neveřejné adresy	17
2.2 IPv6 ADRESACE	17
3. ZAKLADNÍ SÍŤOVÉ PROTOKOLY	18
4. ZÁKLADNÍ SÍŤOVÉ SLUŽBY	19
ROUTOVACÍ PROTOKOLY IPv4	19
4.1.1 Routovací protokoly IGP	19
4.1.2 Routovací protokoly EGP	19
4.2 DHCP	19
4.3 DNS.....	19
4.4 NAT.....	20
4.4.1 Typy NATU	20
4.5 NTP	21
5. QOS.....	22
5.1 TYPY QoS	22
5.1.2 Parametry QoS	23
6. VPN.....	24
6.1 WIREGUARD	24
6.2 PPTP.....	24

6.3	IPSEC/ IKEv2	25
7.	VYUŽITÍ DVOU INTERNETOVÝCH PŘÍPOJEK	26
7.1	ZÁLOŽNÍ LINKA	26
7.2	SOUBĚŽNĚ VYUŽITÍ	27
8.	MIKROTIK	28
8.1	PRODUKTY MIKROTIK	28
8.2	PRODUKT ROUTERBOARD	28
8.2.1	Název desky	28
8.2.2	Vlastnosti desky	28
8.2.3	Vlastnosti rádia	29
8.2.4	Vlastnosti krytu	30
8.3	OPERAČNÍ SYSTÉM ROUTEOs	30
8.3.1	Možnosti správy systému	31
8.3.2	Firewall	34
II	PRAKTICKÁ ČÁST	42
9.	SÍŤ V MALÉ FIRMĚ	43
9.1	PŘÍPRAVA NA REALIZACI SÍTĚ	43
10.	KONFIGURACE ROUTERU	47
10.1	UŽIVATELÉ	48
10.2	AKTUALIZACE	48
10.3	HOSTNAME	53
10.4	VYTVOŘENÍ BRIDGE	54
10.5	PORT LIST	56
10.6	NTP	57
10.7	DNS	59
10.8	VLAN	60
10.9	PPPoE	60
10.10	IP ADRESACE	61
10.10.1	DHCP Server	63
10.11	ROUTOVÁNÍ	66
10.11.1	Source NAT	67
10.11.2	Failover	68
10.12	VPN	71
10.13	FIREWALL	72
10.14	QoS	76
10.14.1	Mangle	76
10.14.2	QoS Tree	77

10.15 CAPsMAN	78
10.15.1 Security	78
10.15.2 Datapath	78
10.15.3 Rates	79
10.15.4 Configuration	79
10.16 SERVICES	80
11. AUTOMATIZACE ZÁLOHOVÁNÍ POMOCÍ PYTHONU	81
11.1 POUŽITÉ TECHNOLOGIE	81
11.2 POPIS IMPLEMENTACE	81
11.3 VÝSLEDNÁ KONFIGURACE SKRIPTU	82
ZÁVĚR	83
SEZNAM POUŽITÉ LITERATURY	85
SEZNAM OBRÁZKŮ	88
SEZNAM TABULEK	90
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	91
SEZNAM PŘÍLOH	94

ÚVOD

S rozvojem digitalizace a narůstající závislostí firem na stabilní a bezpečné síťové infrastruktuře roste i potřeba efektivně navržených počítačových sítí. Tento požadavek se dnes netýká pouze velkých podniků, ale stále více i malých a středních firem, které často čelí výzvě, jak zajistit spolehlivé a bezpečné síťové prostředí s omezeným rozpočtem. Klíčem k úspěchu bývá volba vhodného technického řešení, které je zároveň cenově dostupné, výkonné a snadno spravovatelné.

Jedním z výrobců, kteří se zaměřují právě na tento segment, je lotyšská společnost MikroTik. Její produkty vynikají širokými možnostmi konfigurace, vysokou flexibilitou a nízkými pořizovacími náklady. Díky operačnímu systému RouterOS nabízí pokročilé funkce běžně dostupné spíše u dražších enterprise řešení. Právě proto je MikroTik ideální volbou pro nasazení v prostředí menších a středních podniků, kde je třeba kombinovat výkon, bezpečnost a nízké náklady.

Cílem této práce je prozkoumat a ověřit využitelnost zařízení MikroTik při návrhu a správě počítačové sítě středního rozsahu. Nejprve jsou vysvětleny základní síťové pojmy a technologie, popsány klíčové principy směrování, QoS, VPN, firewallu a možnosti operačního systému RouterOS. Následně je představen návrh konkrétní síťové infrastruktury pro modelový podnik, včetně implementace funkcí, jako je záložní internetové připojení, centrální správa Wi-Fi sítě pomocí CAPsMAN či automatizace.

Výsledkem je funkční síťové řešení, které splňuje běžné požadavky na výkon, bezpečnost i rozšiřitelnost. Tato práce tak může posloužit nejen jako akademická studie, ale i jako inspirace nebo návod pro správce sítí při implementaci podobných projektů v praxi.

I TEORETICKÁ ČÁST

1. POČÍTAČOVÁ SÍŤ

Je skupina několika počítačů, které jsou schopny si mezi sebou vyměňovat data [1].

1.1 Model ISO/OSI

1.2 Pasivní síťové prvky

Jedná se o model, který znázorňuje fungování počítačové sítě [2].

1.2.1 Fyzická vrstva

Zajišťuje síťovou komunikaci, na fyzické úrovni [2].

1.2.2 Linková vrstva

Zabezpečuje komunikaci mezi dvěma zařízeními. V této vrstvě probíhá práce s MAC (Media Access Kontrol) adresami, tedy fyzickými adresami síťových rozhraní v jednotlivých zařízeních [2].

1.2.3 Síťová vrstva

Síťová vrstva se stará o směrování dat mezi sítěmi a jejich doručení na cílovou IP adresu. Typickým protokolem této vrstvy je IP (Internet Protocol) [2].

1.2.4 Transportní vrstva

Zajišťuje přenos dat mezi koncovými zařízeními. A to jak za pomoci spojového protokolu TCP (Transmission Control Protocol), tak i nespojového protokolu UDP (User Datagram Protocol) [2].

1.2.5 Relační vrstva

Relační vrstva se stará o navázání a udržení spojení mezi dvěma zařízeními [2].

1.2.6 Prezenční vrstva

Zpracovává data z transportní vrstvy a převádí je na požadovaný formát, jako může být například JPEG, nebo GIF, se kterým pak pracuje aplikační vrstva. Zároveň se stará i o případné šifrování či dešifrování [2].

1.2.7 Aplikační vrstva

Na této vrstvě pracují aplikační protokoly, zajišťuje přenos jejich dat. Jedná se o protokoly, jako jsou https (Hypertext Transfer Protocol Secure), SFTP (SSH File Transfer Protocol), či Samba [2].

1.3 Aktivní síťové prvky

Aktivní síťové prvky jsou takové, které jsou schopny zpracovávat či vytvářet signál, přenášený po síti.

Router – slouží ke směrování komunikace mimo danou lokální síť.

Firewall – slouží k filtraci komunikace a zvyšuje tím zabezpečení sítě. Často bývá integrován s routerem jako jedno zařízení.

Switch – slouží pro propojení síťových prvků v rámci jedné lokální sítě.

Bridge – propojuje různé části jedné lokální sítě.

Acces Point – poskytuje přístup do bezdrátové sítě přes Wi-Fi (Wireless Fidelity)

1.4 Pasivní síťové prvky

Propojují aktivní síťové prvky. Sami o sobě negenerují ani nezpracovávají signál.

Kroucená dvoulinka – nejpoužívanější typ přenosového média v LAN sítích, oproti optickému vláknu má lepší mechanickou odolnost a nižší pořizovací cenu, Avšak nemá tak dobré přenosové vlastnosti jako optický kabel a navíc je vhodný jen krátké vzdálenosti. Je tak nejvhodnější k připojení koncových zařízení v síti. Jeho výhodou je také možnost přenosu elektrické energie pro napájení koncového zařízení pomocí PoE (Power over Ethernet), tento způsob napájení je vhodný u zařízení s nízkou spotřebou, jako jsou třeba bezpečnostní kamery.

Optické vlákno – jedná se o přenosové médium, s nejlepší možnou propustností a latencí. Jeho nevýhodou je vyšší pořizovací cena a menší odolnost oproti kroucené dvoulince. Z těchto důvodů má uplatnění převážně v páteřních spojích či v datacentrech.

Patch panely – bývají umístěné v rozvodných skříních a sdružují v sobě zakončení koncových zásuvek.

Rack – rozvodná skříň, do které se umísťují síťové prvky a zakončení datových rozvodů.

1.5 Druhy sítě

GAN (Global Area Network) – nejrozsáhlejší globální síť. Do této kategorie lze řadit síť Internet [1].

MAN (Metropolitan Area Network) – metropolitní síť, propojuje různé části města [1].

WAN (Wide Area Network) – jedná se o rozsáhlou síť propojující větší oblasti, jako jsou třeba města nebo státy [1].

LAN (Local Area Network) – nejmenší síť, jedná se o síť v rámci jedné organizace, či domácností [1].

WLAN (Wireless Local Area Network) – bezdrátová LAN. Typicky Wi-Fi.

VLAN (Virtual Local Area Network) – jedná se o virtuální LAN, která funguje tak, že se do hlaviček paketů přidá ID dané VLANy. Můžeme tak mít na jednom fyzickém kabelu několik oddělených logických sítí. VLAN představuje technologii, která je užitečná zejména ve větších sítích pro jejich segmentaci – přiřazujeme klienty do VLANu na základě předem definovaných pravidel. Klasický způsob přiřazování VLAN je statické nastavení portů na switchi či routeru [2].

Statická konfigurace VLAN však může být časově náročná jak z hlediska prvotního nastavení, tak i následné správy. Zejména ve větších sítích je vhodné zvážit využití pokročilejších metod, jako je NAC (Network Access Control), které umožňují dynamické přiřazování klientů do VLAN na základě bezpečnostních pravidel [3].

2. IP ADRESACE

IP adresa je základní identifikace zařízení v síti sloužící pro správné směrování. V jedné síti se může daná IP adresa vyskytovat pouze jednou, jinak by mohlo dojít ke zhroucení sítě. IP adresy existují ve dvou verzích, a to ve starší verzi 4 a novější 6.

2.1 IPv4 Adresace

IP adresa ve verzi IPv4 je tvořena 32 bity. Skupina adres pak tvoří jednu síť, přičemž počet bitů, které určují síťovou část adresy, stanovuje tzv. síťová maska. Zbývající bity slouží k adresaci jednotlivých zařízení (hostů) v rámci dané sítě. S rostoucím počtem zařízení připojených k Internetu však přestává být rozsah IPv4 adres dostačující. Tento problém částečně řeší technologie NAT (Network Address Translation), která umožňuje sdílení jedné veřejné IP adresy více zařízeními. Typickým příkladem je domácí nebo firemní LAN síť, která do sítě ISP (Internet Service Provider) vystupuje pod jednou společnou veřejnou IP adresou [2][4].

Pokud klient od ISP nedostane vlastní veřejnou IP adresu, je součástí vnitřní sítě poskytovatele. V takovém případě NAT probíhá nejen v rámci domácí sítě, ale i na straně poskytovatele. Z pohledu Internetu pak může více koncových uživatelů sdílet jednu veřejnou IP adresu poskytovatele.

2.1.1 Neveřejné adresy

Adresy vyhrazené pouze pro použití v neveřejných sítích, typicky LAN za NATem:

- **Třída A:** 10.0.0.0 – 10.255.255.255
- **Třída B:** 172.16.0.0–172.31.255.255
- **Třída C:** 192.168.0.0 – 192.168.255.255 [3]

2.2 IPv6 Adresace

Adresa je složena ze 128 bitů, což znamená výrazný nárůst adres oproti verzi 4. I když její využití stoupá, stále je oproti svému předchůdci malé. Vznikla převážně z potřeby řešit nedostatek veřejných adres verze 4 [2].

3. ZAKLADNÍ SÍŤOVÉ PROTOKOLY

UDP – jedná se o protokol pro nespojový přenos dat. To znamená, že neověřuje, zda data dorazila správně. Avšak díky absenci ověřování je rychlejší než protokol TCP, ale méně spolehlivý [2].

TCP – na rozdíl od protokolu UDP se jedná o protokol spojový. Jeho výhoda je, že ověřuje správné doručení dat, avšak za cenu nižší výkonnosti [2].

ICMP – jedná se o protokol, který není běžně používán pro přenos aplikačních dat, ale pro servisní účely. Nejznámější implementace tohoto protokolu je nástroj ping, či traceroute [2].

4. ZÁKLADNÍ SÍŤOVÉ SLUŽBY

Routovací protokoly IPv4

Směrovací protokoly slouží k určení cesty pro přenos dat. Dělí se na dvě základní skupiny, a to IGP (Interior gateway protocol) a EGP (Exterior gateway protocol) [2].

4.1.1 Routovací protokoly IGP

Protokoly typu IGP jsou určeny pro použití uvnitř autonomních systémů.

OSPF (Open Shortest Path First) – routovací protokol používá Dijkstra algoritmus k určení cesty, mimo jiné se zde zohledňuje i propustnost dané cesty, následně je pak vybrána cesta s nejnižší cenou [2].

RIP (Routing Information Protocol) - routovací protokol používající k výběru cesty, počet skoků, respektive počet zařízení, přes které musí paket projít, než je doručen cílovému zařízení [2].

4.1.2 Routovací protokoly EGP

Protokoly typu EGP jsou určeny na použití mimo autonomní systémy.

BGP (Border Gateway Protocol) – routovací protokol, používaný v Internetu. Páteřní routery sdílí s ostatními sítěmi, k nimž jsou připojeny. Následně pak zvolí nejvhodnější cestu k cíli na základě daných podmínek [4].

4.2 DHCP

DHCP (Dynamic Host Configuration Protocol) je protokol sloužící k dynamickému adresování klientů. Přiděluje jim IP adresy, masku a další síťové nastavení, jako je IP adresa DNS (Domain Name System) serveru a IP adresa gatewaye, což je adresa routeru, přes kterou má koncové zařízení posílat data, pokud jsou směrována do jiné sítě, či NTP (Network Time Protocol) serveru.

Výrazně zjednodušuje správu sítě, kdy by jinak bylo potřeba provést tuto konfiguraci ručně, což je v síti s velkým počtem zařízení časově náročně, navíc by lidskou chybou mohlo docházet ke kolizím IP adres a následně i k případnému zhroucení sítě.

4.3 DNS

DNS (Domain Name System) je služba, která zajišťuje překlad doménových jmen na IP adresy a překlad IP adres na doménová jména. Operuje převážně pomocí protokolu UDP,

ale v některých případech využívá i TCP (například při přenosech větších odpovědí nebo při rekurzivním dotazování). DNS server naslouchá na portu 53 u obou protokolů.

Round-Robin DNS je způsob, jakým lze pomocí DNS rovnoměrně rozdělovat zátěž mezi více serverů. Pro jedno doménové jméno existuje více IP adres, které DNS server vrací v cyklicky se měnícím pořadí. Klient použije adresu podle pořadí, které obdržel, a pokud daný server neodpovídá, pokračuje na další v seznamu [6].

Existují i pokročilejší služby, které kombinují Round-Robin DNS s proxy serverem. V tomto případě klient vždy obdrží IP adresu proxy, která požadavky dále směřuje na cílové servery. Proxy navíc dokáže rychle reagovat na výpadky – například tak, že přestane směřovat požadavky na nefunkční server, čímž se eliminuje problém, kdy by běžný DNS server stále poskytoval nefunkční IP adresu [6].

Základním předpokladem funkčnosti tohoto řešení je, aby byly všechny servery dostupné pod různými IP adresami identické – tedy aby poskytovaly stejnou aplikaci a stejná data. Jen tak má uživatel jistotu, že se vždy dostane ke stejné službě.

DDNS (Dynamic DNS) umožňuje dynamickou aktualizaci DNS záznamů. Tato technologie je užitečná zejména v případech, kdy má zařízení dynamicky přidělovanou IP adresu od poskytovatele. Aktualizace probíhá prostřednictvím klientské služby běžící na straně uživatele, která pravidelně informuje DNS server o aktuální IP adrese.

Díky DDNS je možné přistupovat k zařízení i při změně IP adresy, což by běžné DNS neumožňovalo. Dynamické DNS záznamy mají obvykle krátkou dobu platnosti (TTL – Time To Live), což umožňuje jejich rychlou aktualizaci při změně adresy [7].

4.4 NAT

NAT slouží pro úpravu IP adresy či portu v hlavičce paketu. RouteOs podporuje pouze klasický NAT pro IPv4. NAT64, který slouží pro překlady mezi IPv4 a IPv6, není v současnosti systémem podporován [8].

4.4.1 Typy NATU

Source NAT – Slouží pro změnu zdrojové IP adresy. V praxi je často využíván zejména pro změnu privátní adresy na veřejnou. V RouteOs existují dva typy, a to statický, kdy je adresa IPv4 adresa staticky zvolenou adresou. A maškaráda, ve které se zdrojová IPv4 adresa určuje dynamicky, dle zvoleného síťového rozhraní [8].

Destination NAT – Slouží pro změnu cílové IP adresy. Je často využíván zejména pro změnu veřejné adresy na privátní. Slouží tak pro zpřístupnění zařízení, jako je například webový server, v neveřejné síti přes veřejnou adresu [8].

4.5 NTP

NTP je protokol určený k synchronizaci času. Ve větších sítích a zejména v oblasti serverů se doporučuje využívat vlastní NTP server, tak aby ani při výpadku internetového připojení nemohlo dojít k tomu, že zařízení budou mít rozdílný čas, což by mohlo způsobit nesoulad mezi systémy.

5. QoS

QoS (Quality of Service) je v oblasti sítí služba určená k regulaci datových toků. Využívá se zejména pro garanci minimální rychlosti připojení klientů. Pomocí této služby můžeme nastavit minimální garantovanou rychlost či naopak maximální povolenou rychlost. Funguje tak, že ukládá přebytečné pakety do fronty, ze které jsou následně postupně odesílány podle zvolených pravidel.

Její využití je tedy vhodné i v menších sítích, aby nedocházelo k tomu, že by jeden uživatel plně využil šířku pásma linky, což by ostatním uživatelům znemožnilo využívat internetové připojení v základní kvalitě.

Nevýhodou je však vyšší zátěž zařízení, které řídí QoS, typicky routeru, a potřeba konstantní rychlosti linky, kvůli nutnosti nastavit maximální rychlost pro optimální fungování QoS. Dále je nevýhodou, že regulace provozu nastává až ve chvíli, kdy je překročena maximální rychlost.

5.1 Typy QoS

Simple Queues – jedná se o způsob uplatnění QoS, které se vztahuje na každého klienta zvlášť [9].

Queue Tree – sofistikovanější varianta uplatnění QoS, neřeší se zde přímo konkrétní klient, ale označení paketu. Tento způsob umožňuje širší uplatnění než Simple Queues, ale za cenu větších nároků na výkon, protože je potřeba před samotným uplatněním QoS označit každý jeden paket ve firewallu, což zvláště při rozsáhlejší implementaci QoS může být velmi výkonnostně náročné [9].

5.1.1 Metody řízení QoS

FIFO (First In First Out) – pakety opouštějí frontu v pořadí, v jakém došly [9].

RED (Random Early Detect) – náhodně zahazuje pakety [9].

SFQ (Stochastic Fairness Queuing) – každé spojení dostane stejný časový rámec na odesílání paketů [9].

PCQ (Per Connection Queuing) – jedná se o metodu, kdy je omezení aplikované na jednotlivá spojení, která je možné rozlišovat podle zdrojové a cílové IP adresy, nebo portu. Každé takové spojení je pak řízeno metodou FIFO. Je tak vhodná pro případy, kdy chceme

zajistit, aby se rychlost rovnoměrně rozložila mezi uživatelem, například podle využívané služby [9].

5.1.2 Parametry QoS

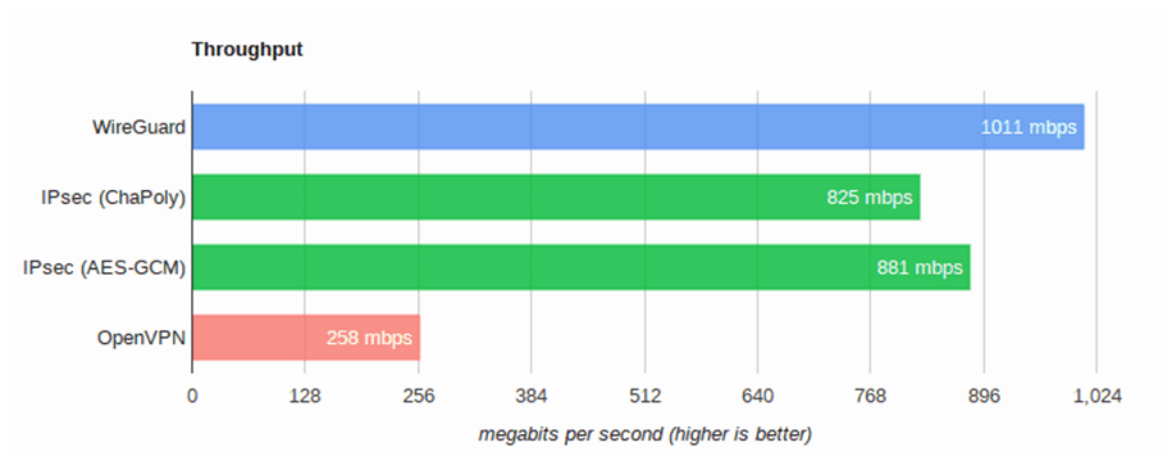
Burst – jedná se o parametr, který umožňuje specifikovat, na jak dlouho a do jaké výše může klient překročit maximální rychlost. Po uplynutí tohoto času bude uplatněno standardní nastavení [10].

6. VPN

VPN (Virtual Private Network) je označení služby propojující sítě, či zařízení, které nejsou mezi sebou přímo propojené, mezi sebou. Vznikne tak virtuální síť, která pro uživatele funguje podobně jako klasická LAN. Využití tak můžeme najít při propojení různých poboček společností, nebo při práci z domu, kdy je zaměstnanec díky VPN schopen přistupovat bezpečně do LAN společnosti.

6.1 Wireguard

Wireguard je relativně nová VPN. Jedná se o jednu z nejbezpečnějších a nejrychlejších VPN. Její nastavení je jednoduché. Je podporována na široké škále operačních systémů, včetně Linuxu, od verze jádra 5.6 je zde přímo zabudována, Windows, macOS, Android, iOS a různými typy routerů, včetně RouteOs od verze 7 [11][12][13]



Obrázek 1 Přehled rychlostí VPN protokolů [11]

6.2 PPTP

PPTP (Point-to-Point Tunneling Protocol) je starší VPN protokol, který byl široce používán především díky své jednoduchosti a nativní integraci do mnoha operačních systémů. Nabízí poměrně dobrou propustnost a snadné nasazení [14].

Jeho hlavní nevýhodou je však slabé zabezpečení. PPTP využívá autentizační protokol MS-CHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2), který byl již v roce 2012 prolomen a jeho použití je považováno za velmi rizikové [15].

Z tohoto důvodu se PPTP v dnešním prostředí nedoporučuje používat pro zabezpečené přenosy dat, zejména pokud jde o citlivé nebo důvěrné informace [14].

6.3 IPsec/ IKEv2

IPsec/IKEv2 představuje tradiční a osvědčené řešení pro VPN. IKEv2 slouží k bezpečné výměně šifrovacích klíčů a sjednání parametrů, zatímco IPsec zajišťuje šifrování a autentizaci datového přenosu. Toto řešení je široce podporováno na různých platformách disponuje dobrou propustností a zabezpečením. Jeho konfigurace v RouteOs je však, podle mých zkušeností, složitější [11].

7. VYUŽITÍ DVOU INTERNETOVÝCH PŘÍPOJEK

V dnešní době se stále častěji setkáváme se situací, kdy je jedna LAN síť připojena k Internetu prostřednictvím více přípojek. Tato praxe je obzvláště běžná ve větších sítích a přináší řadu výhod.

7.1 Záložní linka

Jedním z nejčastějších způsobů využití více přípojek je nasazení záložní linky. V tomto scénáři slouží jedna přípojka jako primární a přenáší veškerý síťový provoz. V případě jejího výpadku převezme automaticky její roli sekundární linka, která zajišťuje provoz do doby, než je primární spojení obnoveno.

V systému RouterOS lze tento mechanismus realizovat pomocí metrik v routovací tabulce. Pokud pro danou cílovou IP adresu existuje více možných tras, vybere se ta s nejnižší metrikou. Router zároveň průběžně kontroluje dostupnost zvolených cest. Pokud detekuje nefunkční trasu, automaticky přesměruje provoz na trasu s vyšší metrikou.

Standardní konfigurace ovšem ověřuje pouze dostupnost dalšího směrovače (např. brány poskytovatele), nikoli skutečnou konektivitu do Internetu. Tento nedostatek lze řešit například nástrojem Netwatch nebo vlastním skriptem, který testuje dostupnost Internetu například pomocí ICMP požadavků nebo DNS dotazů na veřejné servery.

Jedním z možných problémů při přepnutí mezi přípojkami je změna veřejné IP adresy, což může způsobit komplikace především z pohledu DNS záznamů. Po přepnutí může DNS stále odkazovat na původní, nyní nefunkční IP adresu. Řešením může být například:

- **BGP Multihoming** – umožňuje připojení k Internetu prostřednictvím více poskytovatelů, přičemž veřejná IP adresa zůstává stále stejná. Díky tomu nedochází při výpadku primární linky ke změně IP adresy ani k přerušení služeb. V praxi to znamená, že veškerý provoz je automaticky přesměrován přes dostupnou linku, aniž by bylo nutné aktualizovat DNS záznamy nebo provádět zásahy do konfigurace. Toto řešení je však závislé na podpoře BGP ze strany ISP [16].
- **Dynamický DNS (DDNS)**
- **Reverzní proxy**

Při správné implementaci je přechod mezi přípojkami pro uživatele (lokální i vzdálené) zcela transparentní.

7.2 Souběžné využití

Druhým způsobem využití více internetových přípojek je jejich souběžné zapojení prostřednictvím tzv. load balancingu. V tomto režimu je provoz aktivně rozkládán mezi obě přípojky, čímž lze optimalizovat přenosovou kapacitu a zlepšit výkon.

Existuje několik metod, jak load balancing realizovat:

- **Per-connection load balancing** – každé nové spojení je přiřazeno jedné z dostupných linek.
- **Forward proxy** – může být nasazena pro inteligentní směřování odchozího provozu na základě typu přenášených dat nebo aktuálního zatížení jednotlivých přípojek.
- **Reverse proxy** – u příchozího provozu (například při provozu vlastního webového serveru) může reverzní proxy sloužit ke směřování požadavků na různé přípojky nebo servery. Umožňuje tak rovnoměrné rozložení zátěže a zajištění dostupnosti i při výpadku jedné linky [17].
- **Round-Robin DNS** – DNS server postupně vrací různé IP adresy odpovídající různým přípojkám. Příchozí provoz je tak rovnoměrně rozložen mezi jednotlivé linky, což je výhodné například při provozu webových serverů [6].

Tento přístup má smysl zejména v situacích, kdy není dostupná jedna dostatečně kapacitní linka, a je tak nutné kombinovat více připojení. Pokud je však k dispozici stabilní a výkonné připojení, nemusí být složité rozkládání provozu nezbytné.

8. MIKROTIK

MikroTik je lotyšská společnost založená v roce 1996. Již v roce 1997 vytvořila svůj vlastní operační systém postavený na Linuxu a od roku 2002 vyrábí také vlastní hardware pod označením RouterBOARD. Společnost sídlí v Rize a v současnosti zaměstnává přibližně 280 pracovníků [18].

MikroTik se zaměřuje především na ISP a pokročilejší uživatele. Jeho produkty jsou známé širokou konfigurovatelností a příznivou cenou.

8.1 Produkty MikroTik

MikroTik se v oblasti hardwaru specializuje především na routery a bezdrátové spoje. V jeho nabídce však nechybějí ani access pointy nebo switche.

V oblasti softwaru vyvíjí vlastní operační systém RouterOS, který poskytuje pokročilé možnosti správy sítě a je využíván na všech zařízeních RouterBoard.

8.2 Produkt RouterBoard

Produkty RouterBoard mají specifické značení ve formátu:

<název desky> <funkce desky>-<vestavěné bezdrátové připojení> <funkce bezdrátové karty>-<typ konektoru>-<typ krytu> [19].

8.2.1 Název desky

Existují tři varianty, jak má být deska pojmenována, v závislosti na konkrétním modelu [19].

Tří znakové označení – první znak označuje sérii, druhé číslo počet portů, třetí pak potencionální počet bezdrátových rozhraní, zahrnuje i prázdné mPCI (Mini) a mPCIe (Mini PCI Express) sloty [19].

Slovo – jedná se o slovní označení modelu, jako je například cAP [19].

Speciální pojmenování – vztahuje na modely, které jsou jedinými zástupci své řady, nebo disponují více než devíti fyzickými síťovými porty. V takových případech je název zaokrouhlen na stovky, nebo odvozen od roku vydání [19].

8.2.2 Vlastnosti desky

Jednotlivé vlastnosti desky jsou označeny specifickými písmeny:

- **A** – zvýšená operační paměť nebo vyšší licence RouterOS.

- **D** – slot pro SSD (Solid State Drive) nebo M.2 disk.
- **U** – podpora USB (Universal Serial Bus).
- **e** – rozšíření pomocí PCIe (PCI Express) karty.
- **G** – gigabitová konektivita. Pokud není kombinováno s „L“, automaticky zahrnuje i „A“, „U“ a „H“.
- **i** – jeden PoE port (bez kontroleru).
- **L** – odlehčená verze modelu.
- **M** – slot M.2 podporuje PCIe i USB komunikaci.
- **P** – plná podpora PoE včetně kontroleru.
- **R** – miniPCIe slot s podporou PCIe i USB.
- **S** – obsahuje SFP port (Small Form-factor Pluggable) pro optické připojení.
- **H** – výkonnější CPU (Central Processing Unit).
- **x<N>** – udává počet jader procesoru (např. x2 = dvoujádrový CPU) [19].

8.2.3 Vlastnosti rádia

V případě, že má model zabudovaný modul WLAN, jsou jeho vlastnosti specifikované ve formátu <pásmo> <výkon na řetězec> <protokol> <počet řetězců> [19].

Pásmo – určuje podporované frekvenční pásmo. Označuje se buď číslem „5“ pro 5 GHz, „2“ pro 2,4 GHz nebo „52“ pro kombinaci obou pásem [19].

Výkon na stream – pokud není uvedeno jinak, jeho hodnota je méně než 23dBm (decibel-miliwatt) pro 802.11a a 24dBm pro 802.11g. Dále existují další tři možnosti:

- **High (H)** – 23-24 dBm pro 802.11a a 24-27 dBm pro 802.11g.
- **High Power (HP)** – 25-26 dBm pro 802.11a a 28-29 dBm pro 802.11g.
- **Super High Power (SHP)** – více než 27 dBm pro 802.11a a více než 30 dBm pro 802.11g [19].

Počet streamů – pokud není uvedeno jinak, má pouze jeden stream. Jinak existuje značení „D“ pro dva a „T“ pro tři [19].

Protokol – pokud není uvedeno jinak, zařízení standardně podporuje 802.11a/b/g. V případě rozšířené podpory se používá zkratkové označení protokolu: „n“ pro 802.11n, „ac“ pro 802.11ac a „ax“ pro 802.11ax [19].

Konektor – pokud není uvedeno jinak, zařízení má ve všech variantách jeden konektor. Použité označení je „MMCX“ pro konektor typu Micro-Miniature Coaxial a „u.FL“ pro ultra-miniature coaxial RF konektor [19].

8.2.4 Vlastnosti krytu

Označení krytu specifikuje mechanické provedení zařízení:

- **BE** – černá edice krytu.
- **BU** – pouze deska (pokud je model standardně prodáván s krytem).
- **EM** – obsahuje prostor pro rozšiřující paměť.
- **LM** – obsahuje prostor pouze pro základní paměť.
- **TC** – vertikální kryt.
- **RM** – verze pro uchycení do racku.
- **IN** – kryt pro interiérové umístění.
- **OUT** – kryt pro exteriérové umístění [19].

8.3 Operační systém RouteOs

Operační systém RouterOS je operační systém určený pro aktivní síťovou infrastrukturu. Je založený na Linuxu a jeho velkou výhodou je multiplatformnost. Lze jej nainstalovat na architektury ARM (Advanced RISC Machine), ARM64/AMPERE, MIPSBE (Microprocessor without Interlocked Pipeline Stages Big Endian), MMIPS (Microprocessor without Interlocked Pipeline Stages Micro), SMIPS (Small MIPS), TILE (Tilera Multicore Architecture), PPC (PowerPC) a x86 (Intel x86 Architecture) [20].

Jedná se o systém, který je předinstalovaný v hardwaru RouterBoard.

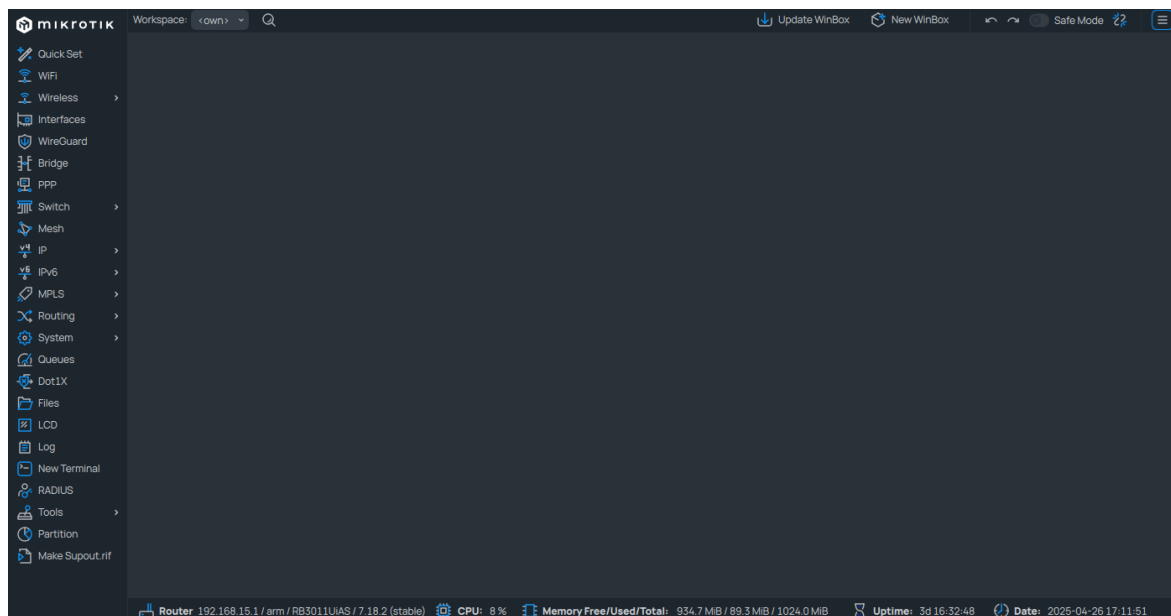
Systém je navržen, aby fungoval nezávisle na výrobci hardwaru, a je tak možné ho nainstalovat na jakýkoli hardware splňující minimální požadavky, díky tomu tak, až na výjimky lze mít aktuální verzi RouteOs i v nejstarších RouterBoardech, pokud na to výkonnostně stačí [21].

Ačkoli je systém postaven na Linuxu, umožňuje využívat přímo pouze svou nástavbu, a nikoli samotný Linux.

8.3.1 Možnosti správy systému

Systém RouterOS nabízí širokou škálu možností správy. Při jejich nastavování je však nezbytné dbát na bezpečnost. Je vhodné používat pouze bezpečné způsoby přístupu a zároveň omezit, kdo k těmto prostředkům může přistupovat. To lze zajistit buď přímo v nastavení managementu, a to omezením rozsahu IP adres, anebo prostřednictvím firewallu. Častým problémem bývá nesprávně nakonfigurovaný vzdálený přístup, kdy je možné spravovat zařízení i z veřejné sítě mimo LAN.

Winbox – Portable desktopová aplikace určená ke kompletní správě systému RouterOS. Nabízí nejširší možnosti konfigurace a je primárním nástrojem pro správu MikroTik zařízení. Umožňuje připojení nejen pomocí IP adresy, ale i pomocí MAC adresy, což je výhodné v případech, kdy zařízení není ve stejné síti jako konfigurační stanice.

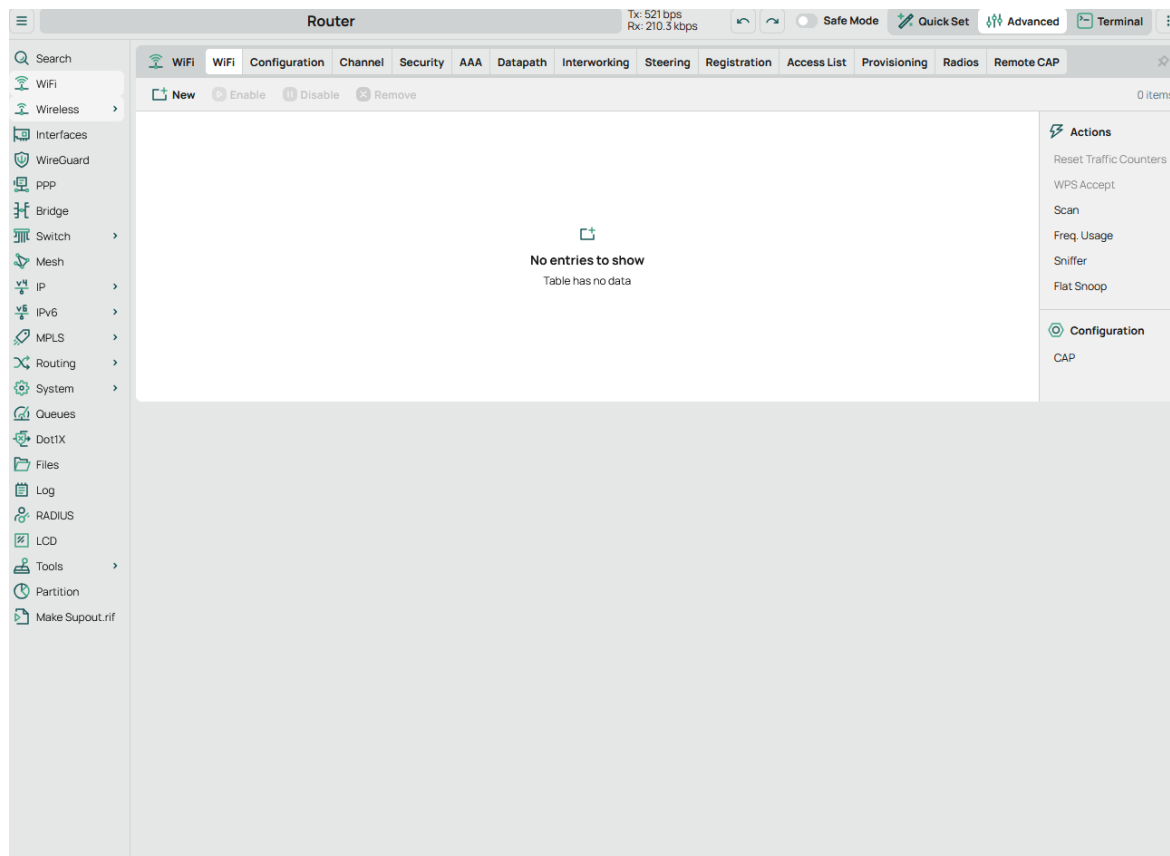


Obrázek 2 Rozhraní aplikace Winbox

Telnet – protokol pro vzdálený přístup přes CLI (Command Line Interface), pracující na protokolu TCP, standardně na portu 23. Nepodporuje šifrování přenášených dat, a proto není z hlediska bezpečnosti doporučován.

SSH (Secure Shell) – poskytuje stejné možnosti jako Telnet, ale na rozdíl od něj zajišťuje šifrovaný přenos dat. Standardně používá port 22 a je považován za bezpečnější alternativu.

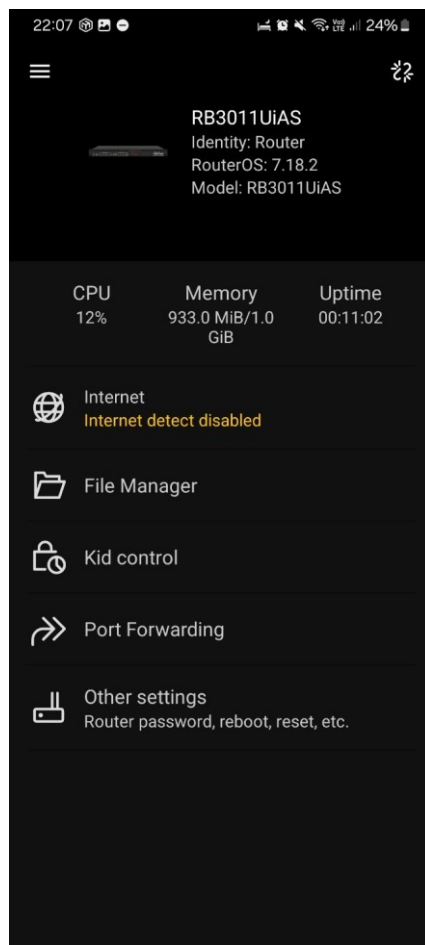
Webové rozhraní – nabízí grafické uživatelské rozhraní podobné Winboxu. K dispozici je jak přes protokol http (Hypertext Transfer Protocol), nepodporujícího šifrování, či https s šifrováním.



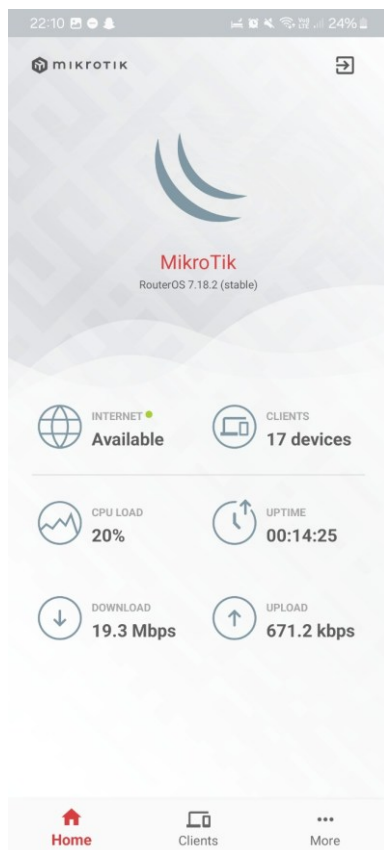
Obrázek 3 Webové rozhraní RouterOS

Mobilní aplikace – MikroTik nabízí dvě oficiální aplikace pro Android i iOS:

- **MikroTik Pro** – pokročilá aplikace pro kompletní správu RouterOS.
- **MikroTik Home** – zjednodušená varianta vhodná pro běžné uživatele bez předchozích zkušeností s RouterOS.



Obrázek 4 Rozhraní aplikace Mikrotik Pro



Obrázek 5 Rozhraní aplikace Mikrotik Home

API (Application Programming Interface) – umožňuje komunikaci s RouterOS prostřednictvím vlastní aplikace. Pro šifrovaný přenos využívá ve výchozím nastavení port 8729 a port 8728 pro nešifrovaný přenos [22].

FTP (File Transfer Protocol) – slouží k nešifrovanému přenosu souborů. Lze ho využít například k přenosu aktualizací systému RouterOS nebo k zálohování konfigurací. Pracuje na protokolu TCP a standardně používá port 20, pro přenos souborů a 21 pro zaslání příkazů.

8.3.2 Firewall

Firewall v systému RouterOS není pouze souborem běžných pravidel pro filtrování komunikace, které jsou umístěny v sekci „Filter Rules“, ale obsahuje i několik dalších pokročilých možností konfigurace. Mezi hlavní funkce patří „Mangle“ a „NAT“, které rozšiřují možnosti správy síťového provozu.

Chain – slouží k oddělení a kategorizaci paketů tak, aby nebylo nutné kontrolovat všechna pravidla pro každý paket. Obecně lze říci, že chain reprezentuje stav paketu v rámci jeho zpracování v zařízení.

Pro „Filter Rules“ existují tyto předdefinované chainy:

- **input** – zpracovává pakety, jejichž cílem je samotné zařízení (např. router). Klíčový pro zabezpečení routeru, zejména pokud má veřejnou IP adresu.
- **output** – zpracovává pakety generované samotným zařízením.
- **forward** – zpracovává pakety, které zařízením pouze procházejí.

Pro „Mangle“ existují chainy:

- **prerouting** – stav paketu před provedení směrování.
- **postrouting** – stav paketu po provedení směrování.
- **output**
- **input**
- **forward**

Pro „NAT“ existují chainy:

- **srcnat** – stav paketu, kdy dochází ke změně zdrojové IP adresy.
- **dstnat** – stav paketu, kdy dochází ke změně cílové IP adresy
- **input**
- **output**

Správná volba chainu je klíčová pro funkčnost a bezpečnost firewallu. Navíc je možné si vytvořit i vlastní chainy, což může při správné implementaci vést ke snížení zátěže CPU a lepšímu zabezpečení.

Filter Rules – jedná se o pravidla pro filtrování paketů, neklíčovější funkci firewallu. Pravidla se aplikují v rámci jednotlivých chainů. Každý chain má své vlastní pořadí pravidel a každé pravidlo je vyhodnocováno v rámci tohoto pořadí. Nejdůležitější akce, které můžeme s pakety provést, jsou:

- **Accept** – schválení volného průchodu paketu.
- **Add dst to address list** – přidá cílovou IP adresu do námi zvoleného adresního listu.
- **Add src to address list** – přidá zdrojovou IP adresu do námi zvoleného adresního listu.
- **Drop** – zahození paketu.
- **Reject** – odmítnutí paketu, na rozdíl od pravidla „drop“ zašle zprávu o zamítnutí.

- **Jump** – přenesení paketu do jiného chainu, i do chainu vytvořeného administrátorem.
- **Log** – pouze vytvoří záznam o aplikaci pravidla.
- **Fasttrack connection** – aplikuje na pakety daného spojení FastTrack, který za účelem zrychlení průchodu paketů a šetření zdrojů firewallu neaplikuje již na dané spojení pravidla firewallu a QoS.
- **Trapit** – funguje pouze pro protokol TCP, kdy vytvoří spojení s protějším bodem, ale již dále ignoruje zasílaná data [23].

Avšak potřebujeme ještě blíže specifikovat, na které pakety se mají pravidla vztahovat. Mezi základní kritéria, podle kterých jsme schopni pakety rozlišovat, patří:

- **Chain** – určuje chain, pro které dané pravidlo platí.
- **Src. Address** – zdrojová IP adresa.
- **Dst. Address** – cílová IP adresa.
- **Src. Address List** – zdrojová IP adresa se musí vyskytovat v daném listu.
- **Src. MAC Address** – zdrojová MAC adresa, lze uplatnit, jen pokud se zdroj nachází ve stejné síti jako firewall. Jinak z principu fungování počítačových sítí nelze MAC adresu klienta zjistit.
- **Protocol** – použitý protokol.
- **Src. Port** – zdrojový port.
- **Dst. Port** – cílový port.
- **Any. Port** – zdrojový či cílový port.
- **In. Interface** – příchozí rozhraní.
- **In. Bridge Port** – příchozí rozhraní v rámci bridge.
- **Out. Bridge Port** – odchozí rozhraní v rámci bridge.
- **Out. Interface** – odchozí rozhraní.
- **In. Interface List** – příchozí rozhraní se vyskytuje ve zvoleném listu.
- **In. Bridge Port List** – příchozí rozhraní, v rámci bridge, se vyskytuje ve zvoleném listu.

- **Out. Interface List** – odchozí rozhraní se vyskytuje ve zvoleném listu.
- **Out. Bridge Port List** – odchozí rozhraní, v rámci bridge, se vyskytuje ve zvoleném listu.
- **Packet Mark** – označení paketů provedené v „Mangle“.
- **Connection Mark** – označení spojení provedené v „Mangle“.
- **Routing Mark** – označení routovací tabulky, do které daný paket spadá.
- **Connection State** – stav daného spojení.
- **Connection NAT State** – rozlišuje, zda je na dané spojení uplatněn daný druh NATu.
- **TTL (Time To Live) host** – klasifikace zařízení na základě doménového jména cílového hostitele (DNS jména) [25].

Mangle je funkce firewallu sloužící primárně ke značení síťového provozu. Tyto značky se následně využívají pro další zpracování, například pro routování, QoS, nebo specifická pravidla firewallu.

Pořadí uplatňování pravidel je stejné jako u „Filter Rules“, avšak zde je důležité brát v potaz parametr „passthrough“. Ten určuje, zda má firewall po shodě s pravidlem pokračovat v kontrole i vůči další pravidlům, nebo zda bude z dalšího zpracování vyřazen.

Parametry pro vyhodnocení pravidel jsou stejné jako u Filter Rules.

Kromě značení umí Mangle také měnit některé položky v IP hlavičce, například TTL.

Existuje několik typů značení:

- **Mark connection** – označí celé spojení vybranou značkou. Tuto značku je možné zobrazit i ve výpisu aktivních spojení.
- **Mark packet** – označí každý jednotlivý paket. Tento typ značení je užitečný například pro QoS, ale kvůli způsobu fungování může výrazně zatěžovat CPU.
- **Mark routing** – slouží výhradně pro účely směrování. Určuje routovací tabulku, která se má na paket stahovat [26].

NAT – v této sekci firewallu se nastavují pravidla pro NAT, jeho fungování bylo již popsáno v předchozí kapitole. I zde je systém fungování podobný jako u „Filter Rules“.

Service Port – v této sekci, servisní služby zařízení, jako je například FTP, můžeme dané služby buď zakázat, nebo změnit jejich porty.

Connections – v této sekci uvidíme všechna připojení procházející routerem. Pro zobrazení těchto připojení je třeba mít nastavené „Filter Rules“. Můžeme zde dané připojení i ukončit.

Addres List – zde můžeme spravovat skupiny IP adres, které pak můžeme použít pro snazší nastavení například pravidel ve firewallu.

8.3.3 CAPsMAN

CAPsMAN (Controlled Access Point system Manager) je systém pro hromadnou správu přístupových bodů. Umožňuje vytvořit centrální konfiguraci pro Wi-Fi síť a následně ji distribuovat na jednotlivá AP, čímž výrazně zefektivňuje jejich správu.

Přidání AP do správy je velmi jednoduché – stačí u jakéhokoli RouterBoard AP podržet tlačítko Reset po dobu 15 sekund nebo manuálně nastavit řízení Wi-Fi rádia přes CAPsMAN v rozhraní AP.

I když vyhledávání CAPsMAN serveru probíhá na druhé vrstvě modelu ISO/OSI, je pro co nejjednodušší chod doporučeno specifikovat IP adresu serveru v DHCP, pokud je to možné.

8.3.4 Možnosti automatizace

RouterOS disponuje širokou škálou možností automatizace, a to jak interních – pomocí proprietárního skriptovacího jazyka, tak externích – například pomocí Python skriptů. Interní skripty lze kromě ručního spuštění provádět i automaticky prostřednictvím zabudovaného plánovače úloh.

Externí automatizaci lze realizovat pomocí nástrojů, jako jsou například Python skripty, využívající knihovny Netmiko či Paramiko. Tyto knihovny umožňují připojení k zařízení přes SSH a provádění širokého spektra operací. Netmiko je knihovna vytvořená speciálně pro správce sítí a obsahuje předdefinované funkce pro práci se síťovými prvky. Naopak Paramiko poskytuje pouze základní podporu SSH, bez specifických funkcí pro síťovou administraci.

Automatizací lze výrazně zvýšit efektivitu správy sítě a umožnit provádění operací, které by jinak byly kvůli časové náročnosti prakticky nerealizovatelné.

Příklady automatizace vhodné pro Python skripty:

- **Vyhledávání klientů** – Ve větších sítích je tato funkce velmi užitečná. Pomocí správného přístupu lze přistoupit ke všem síťovým prvkům současně a získat tak téměř okamžitě schéma zapojení sítě. V tomto případě vycházíme z ARP tabulky, která zobrazuje MAC adresy připojené k jednotlivým portům. Pro správnou funkčnost je však nutné vyloučit spoje mezi aktivními síťovými prvky, aby nedocházelo k nesprávné interpretaci dat.

- **Hromadná konfigurace** – Pokud potřebujeme provést konfiguraci na více zařízeních současně, lze využít Python skript pro hromadnou konfiguraci. Je však nutné zohlednit rozdílné syntaxe mezi modely zařízení, například v rámci značení portů. Proto je vhodné před provedením akce ověřit typ zařízení a podle toho upravit konfiguraci.
- **Zálohování** – Zálohování na externí zařízení je nesmírně důležité. Toto lze provést pomocí python skriptu, které se připojí pomocí SSH k síťovému prvku. Následně vytvoříme soubor se zálohou a ten poté pomocí SFTP přehrajeme na PC, či server.

Příklady automatizace vhodné pro interní skriptování:

- **Kontrola stavu UPS (Uninterruptible Power Supply)** – v případě výpadku napájení může skript zaslat notifikaci e-mailem a informovat o zbývající kapacitě baterie nebo obnovení napájení.
- **Kontrola stavu internetového připojení** – skript může periodicky testovat dostupnost Internetu například pomocí pingu na spolehlivé servery. V případě výpadku lze automaticky přepnout na sekundární připojení, pokud je dostupné, a informovat administrátora.
- **Automatické aktualizace** – RouterOS nekontroluje dostupnost aktualizací automaticky. Pro automatizaci této operace je nutné vytvořit skript, který aktualizace nejen stáhne a nainstaluje, ale ideálně i provede zálohu před samotnou instalací.
- **Monitorování stavu sítě** – pomocí pingu lze sledovat dostupnost síťových prvků a v případě výpadku okamžitě informovat administrátora. Nicméně pro komplexní monitoring sítě je zpravidla vhodnější využít specializovaný software, jako je například PRTG (Paessler Router Traffic Grapher) Network Monitor.

8.3.5 Licencování

Existuje sedm druhů licencí, které se značí jako 0-6.

Tabulka 1 Přehled licencí RouteOs [27]

Úroveň	0	1	3	4	5	6
PPPoE tunely	24h zkušební	1	200	200	500	neomezeno
PPTP tunely	24h zkušební	1	200	200	500	neomezeno

L2TP tunely	24h zkušební	1	200	200	500	neomezeno
OVPN tunely	24h zkušební	1	200	200	neomezeno	neomezeno
EoIP tunely	24h zkušební	1	neomezeno	neomezeno	neomezeno	neomezeno
VLAN rozhraní	24h zkušební	1	neomezeno	neomezeno	neomezeno	neomezeno
Pravidla front	24h zkušební	1	neomezeno	neomezeno	neomezeno	neomezeno
HotSpot aktivní uživatelé	24h zkušební	1	1	200	500	neomezeno
Aktivní relace správce uživatelů	24h zkušební	1	10	20	50	neomezeno
Bonding rozhraní	24h zkušební	1	neomezeno	neomezeno	neomezeno	neomezeno
RADIUS	24h zkušební	-	neomezeno	neomezeno	neomezeno	neomezeno
Bezdrátový AP režim (PtMP)	24h zkušební	-	ne	ano	ano	ano
Cena	zdarma	registrace	neprodejné	\$45	\$95	\$250

Na zařízeních RouterBoard je již z výroby aktivována licence odpovídající účelu zařízení, pokud bychom chtěli, je zde však možnost licenci za poplatek zvýšit. Pokud chceme použít systém na jiném hardwaru, například na počítači, musíme si již vždy koupit potřebnou licenci.

II PRAKTICKÁ ČÁST

9. SÍŤ V MALÉ FIRMĚ

Praktická konfigurace a zapojení sítě vychází z potřeb malé firmy o maximálně 30 zaměstnancích. Navržené řešení musí splňovat následující požadavky:

- Zálohované připojení k Internetu.
- Možnost vzdáleného přístupu do firemní sítě pomocí VPN.
- Garantovaná rychlost internetového připojení pro každého uživatele.
- Připojení pracovních stanic prostřednictvím kroucené dvojlinky.
- Zabezpečená Wi-Fi síť pro zaměstnance s přístupem do interní sítě.
- Samostatná Wi-Fi síť pro hosty.

Síťová infrastruktura měla být navržena s důrazem na nízké pořizovací náklady, jednoduchost, bezpečnost, spolehlivost a automatizaci. Cílem bylo vytvořit standardizované a snadno spravovatelné řešení, které poskytne stabilní připojení zaměstnancům i návštěvníkům firmy, přičemž minimální potřeba administrace umožňuje využití outsourcingu správy IT.

Vzhledem k velikosti a charakteru firmy se obvykle jedná o několik místností, které nejsou od sebe výrazně vzdálené. Zpravidla tak nebývá potřeba zřizovat více než jeden rack.

Ačkoli je dnes běžné, že mnohá zařízení využívají bezdrátové připojení, hlavní způsob připojení klientských zařízení byl realizován pomocí kroucené dvoulinky, a to kvůli vyšší stabilitě, nižší latenci a spolehlivosti. Wi-Fi síť slouží především pro mobilní zařízení zaměstnanců a pro hosty prostřednictvím oddělené VLAN.

S ohledem na rostoucí trend práce z domova bylo nezbytné nasadit VPN řešení, ideálně některé z volně dostupných variant, jako je například WireGuard. Vzhledem k častému využívání cloudových služeb není potřeba umožňovat další přístupy z Internetu do lokální sítě.

Protože je připojení k Internetu pro chod firmy zásadní, musí být řešeno jako maximálně dostupné, a to i v podmínkách omezeného rozpočtu.

9.1 Příprava na realizaci sítě

Pro co nejideálnější realizaci bylo klíčové správně určit současné i budoucí potřeby firmy a realizovat tak co nejlepší možné řešení v rámci daných podmínek. Při analýze budoucích

potřeb bylo nutné zohlednit faktory jako potenciální rozšíření firmy, zřízení nových pracovišť nebo přechod na nové technologie a služby.

Ačkoli se mohou zvýšené náklady vyplývající z této analýzy z pohledu vedení firmy zdát jako zbytečně náročné, v dlouhodobém horizontu přinesou optimální řešení. Z analýzy byly získány tyto závěry:

- Počet současných pracovních stanic je 25, ale je třeba počítat s možností rozšíření až na 35–40 v horizontu 3–5 let.
- Síťová infrastruktura musí být modulární, aby umožnila snadné rozšíření bez nutnosti rozsáhlé rekonstrukce.
- Použití PoE switche zajistí možnost napájení AP a případně dalších zařízení bez nutnosti samostatného napájení.
- Záložní internetové připojení bude řešeno pomocí druhého ISP, který bude připojen jako failover ISP a využit v případě výpadku primární linky. Obě tyto přípojky budou mít symetrickou rychlost 200Mb.
- VPN přístup bude zajištěn prostřednictvím řešení WireGuard, které nabízí vysokou úroveň zabezpečení, nízké nároky na výkon a jednoduchou konfiguraci.
- Vnitřní síť bude rozdělena do VLAN, které oddělí zaměstnaneckou síť a síť hostů.
- Bezpečnost bude řešena centrálním firewallem, který zároveň bude zajišťovat směrování mezi sítěmi a přístupová pravidla.
- Všechny AP budou podporovat minimálně Wi-Fi 5 a centrální správu, čímž se zjednoduší administrace a zvýší kvalita pokrytí.
- Síťové prvky budou umístěny v centrálním racku, který bude zálohován UPS, čímž se minimalizuje dopad výpadků elektrické energie.
- Síť bude podporovat pouze IPv4, vzhledem k aktuálním potřebám a kompatibilitě s co největším množstvím zařízení a služeb.

Pro síť tohoto typu byl zvolen výkonnější router MikroTik RB5009UPr+S+, který bude sloužit i jako centrální bod pro připojení ostatních síťových prvků. Tento router kombinuje vysoký výkon s kompaktními rozměry a zároveň nabízí širokou škálu funkcí potřebných pro moderní síťovou infrastrukturu. Díky podpoře PoE umožňuje napájení připojených zařízení přímo ze svých portů, čímž se zjednodušuje kabeláž a instalace.

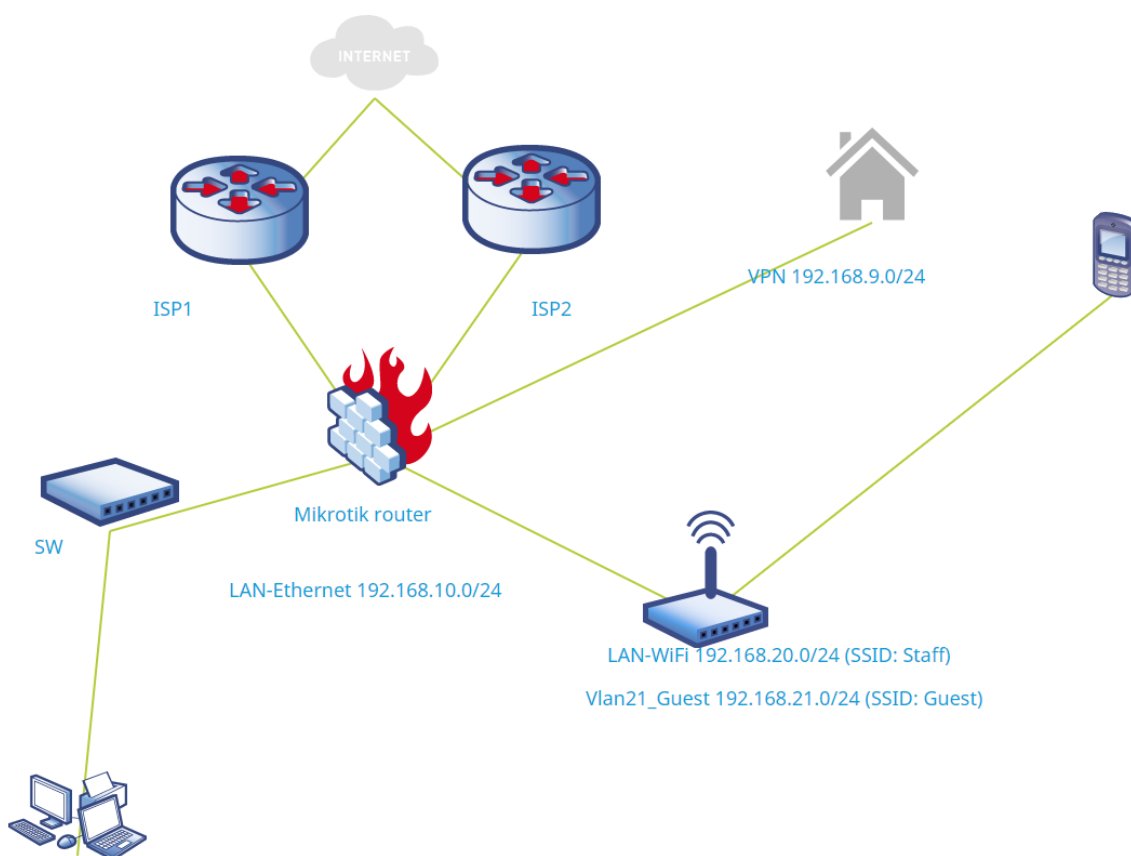
Router MikroTik RB5009UPr+S+ je vybaven devíti gigabitovými ethernetovými porty, jedním 10Gbps SFP+ portem a dostatečným výkonem pro směrování, firewall, VPN a další pokročilé funkce.

Standardní klientská zařízení byla z hlediska nákladů připojena převážně prostřednictvím kabelového připojení ke gigabitovému switchi, který zajišťoval distribuci datového připojení v rámci jednotlivých segmentů sítě. V tomto případě již nebylo nutné, aby se jednalo o spravovatelný switch.

Pro bezdrátové připojení byla navržena instalace přístupových bodů MikroTik cAP ax, které podporují moderní standard Wi-Fi 6 (802.11ax).

Přístupové body MikroTik cAP ax zároveň podporují centrální správu prostřednictvím CAPsMAN, což výrazně usnadňuje administraci bezdrátové sítě a umožňuje rychlé nasazení, správu a aktualizaci všech přístupových bodů z jednoho místa.

Navržená kombinace routeru RB5009UPr+S+, gigabitového switchu a přístupových bodů cAP ax tak poskytne dostatečný výkon, flexibilitu a rozšiřitelnost potřebnou pro spolehlivý provoz firemní sítě.



Obrázek 6 Zjednodušené schéma sítě

10. KONFIGURACE ROUTERU

Ačkoli bylo možné veškerou konfiguraci provést také prostřednictvím příkazového řádku, pro účely této práce byla zvolena konfigurace pomocí aplikace WinBox. Tato aplikace byla vyhodnocena jako uživatelsky přívětivější a vhodnější pro přehledné nastavení zařízení.

Následně bylo přistoupeno k samotnému routeru. Pro provedení konfigurace bylo nezbytné připojit router do stejné sítě jako počítač, ze kterého byla konfigurace prováděna.

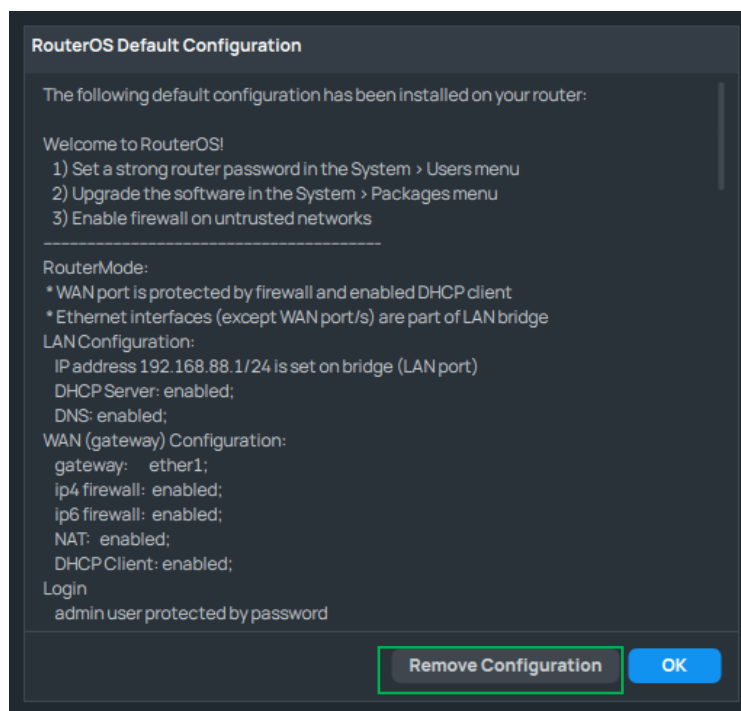
Po spuštění aplikace WinBox se v tabulce dostupných zařízení zobrazil příslušný router.

☐	MAC Address	IP Address	Identity	Version	Board	Uptime	Board's Port
☒	F4:1E:57:D8:B2:34	192.168.88.1	MikroTik	7.16.2 (stable) 2024-11-26 12:09:40	RB5009UPr+S+	00:05:44	bridge/ether2

Obrázek 7 Výpis nalezených zařízení

Bylo vybráno příslušné zařízení a zadány přihlašovací údaje, uvedené na routeru.

Při prvním přihlášení bylo zobrazeno dialogové okno s možností aplikace výchozího nastavení. Ačkoli toto nastavení může v praxi v některých případech usnadnit práci, pro důkladnější pochopení systému RouterOS bylo v rámci této práce odmítnuto.

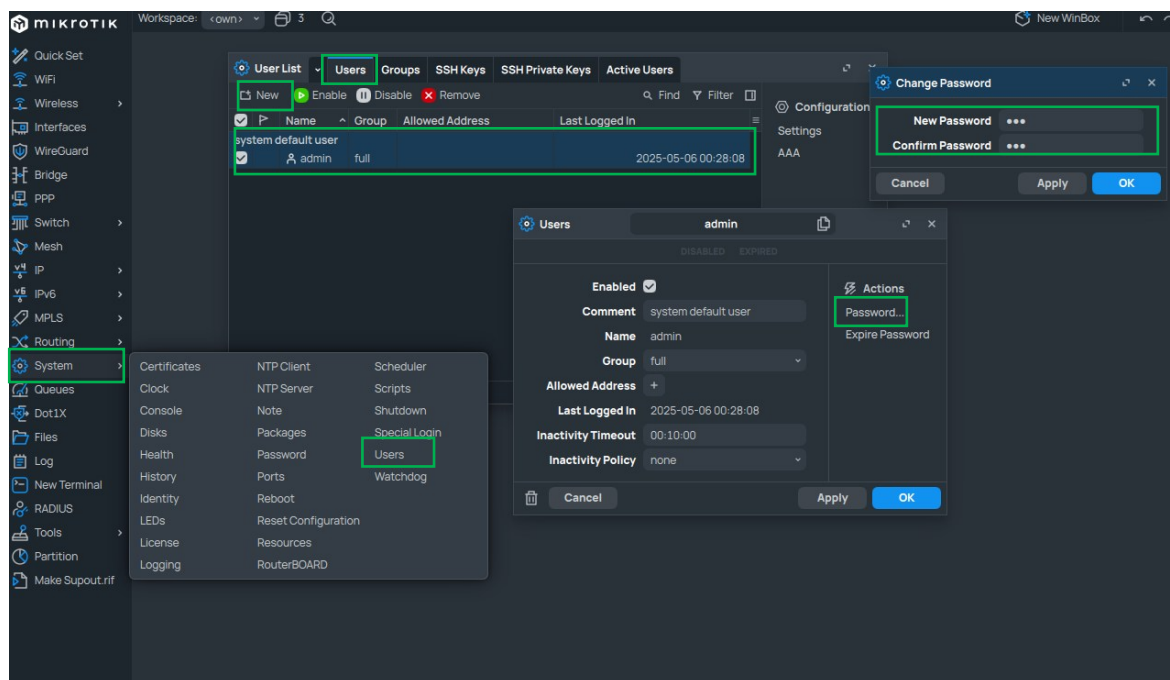


Obrázek 8 Výchozí konfigurace

Protože odebrání konfigurace odstranilo i nastavení uživatele admin, pomocí kterého bylo zařízení spravováno, došlo k odpojení aplikace WinBox. Následně bylo nutné se k zařízení opětovně připojit pomocí uživatele admin, tentokrát již bez hesla, protože výchozí heslo pro účet admin bylo prázdné.

10.1 Uživatelé

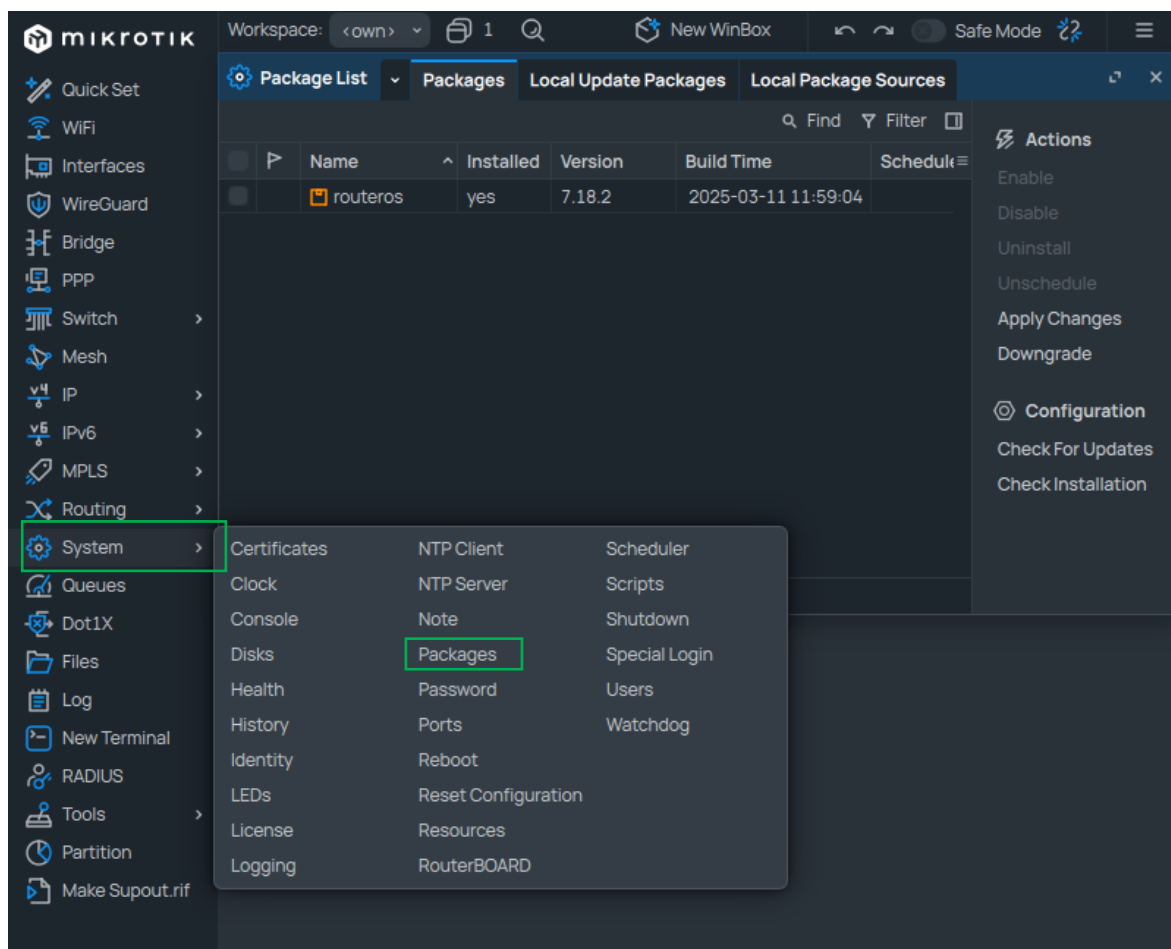
Jako první bylo tak potřeba změnit heslo na výchozí admin účet. Heslo bylo změněno v sekci System a v záložce Users.



Obrázek 9 Změna hesla

10.2 Aktualizace

Ještě před samotnou konfigurací byla zkontrolována aktuálnost operačního systému, aby bylo od začátku pracováno s nejnovější verzí. V sekci System byla vybrána záložka Packages, kde jsou zobrazeny aktuálně nainstalované balíčky a jejich verze.



Obrázek 10 Výpis nainstalovaných balíčků

Ačkoli má systém integrovaný nástroj na aktualizace balíčků přímo v rámci OS, vzhledem k tomu, že router v daném okamžiku ještě neměl přístup k Internetu, bylo nutné přejít na webové stránky výrobce a zkontrolovat, zda je k dispozici novější verze.

RouterOS v7

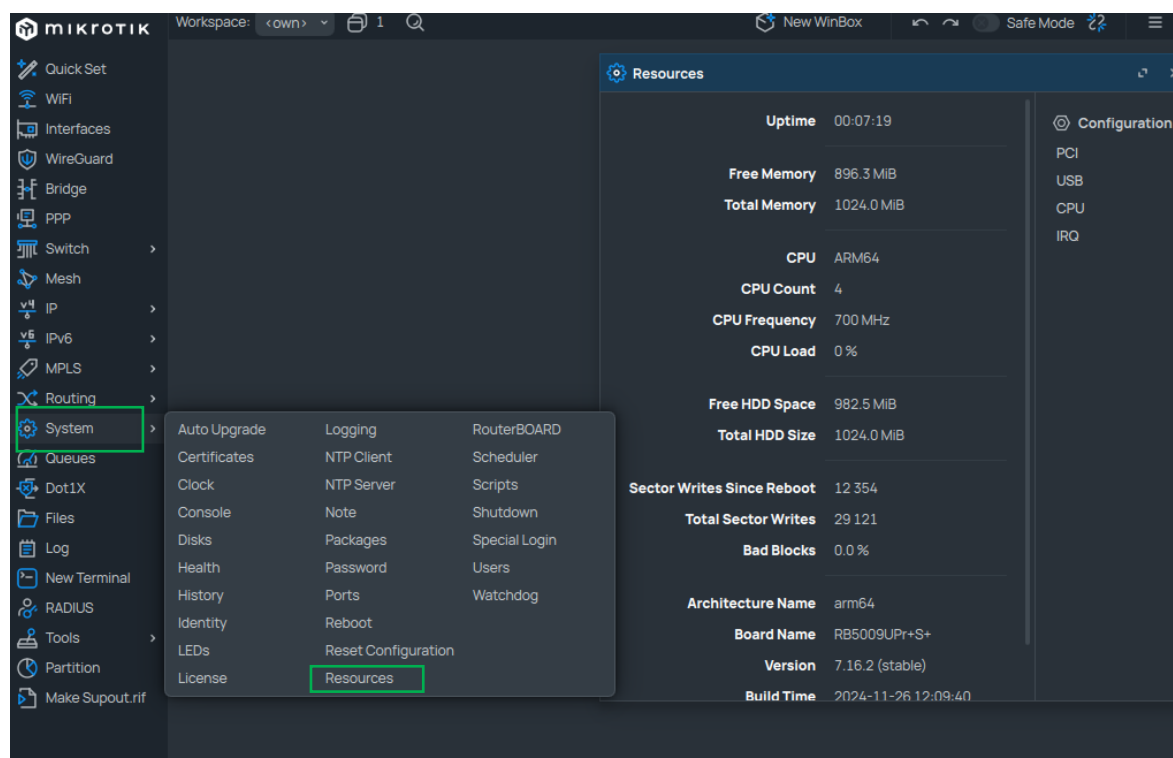
	7.18.2 Stable	7.19beta8 Testing
ARM		
Main package		
Extra packages		
ARM64 / AMPERE		
Main package		
Extra packages		
ISO image for AMPERE		
MIPSBE		
Main package		
Extra packages		
MMIPS		
Main package		
Extra packages		
SMIPS		
Main package		
Extra packages		
TILE		
Main package		
Extra packages		
PPC		
Main package		
Extra packages		
X86		
Main package		
Extra packages		
CD Image		
Install image		
GENERAL		
Netinstall (Windows)		
Netinstall (Windows 64bit)		
Netinstall (CLI Linux)		
The Dude client		
Bandwidth test		
Mikrotik.mib		
FlashFig		
Changelog		

Obrázek 11 Výpis dostupných balíčků na webu Mikrotik

Na obrázku je zobrazen výpis dostupných verzí a architektur. V tomto okamžiku byl relevantní balíček Main package, který obsahoval samotný operační systém. V balíčku Extra packages by pak bylo možné nalézt přídatné moduly, například modul pro propojení s UPS.

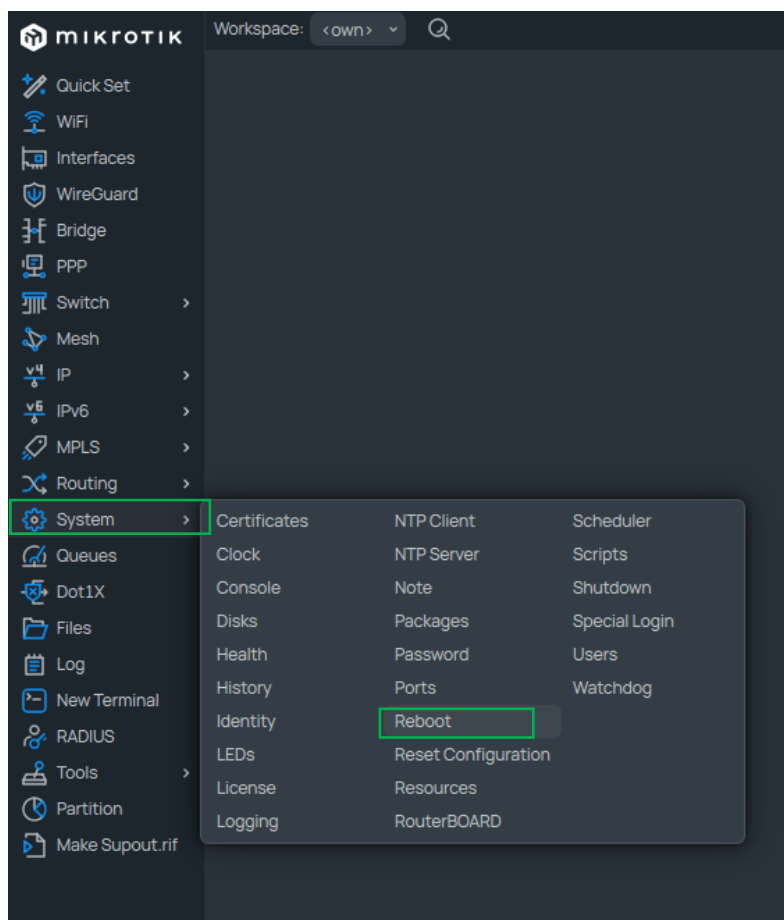
V daném případě byla k dispozici novější verze 7.18. Bylo tak rozhodnuto stáhnout novější stabilní verzi operačního systému. Před samotným stažením byla ještě ověřena architektura

zařízení. Pro její zobrazení je třeba v aplikaci WinBox přejít do sekce System a následně do záložky Resources, kde jsou zobrazeny základní informace o routeru.



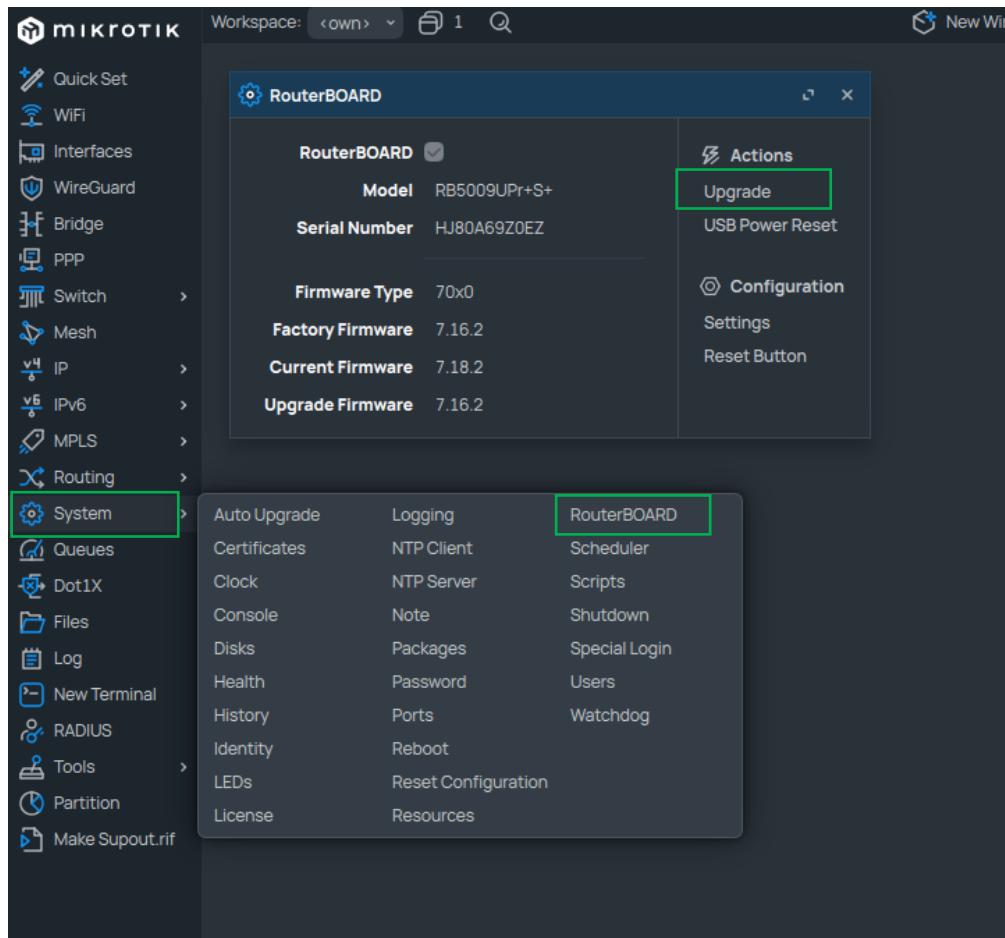
Obrázek 12 Záložka Resources

Bylo zjištěno, že architektura routeru je ARM64. Následně byl stažen odpovídající balíček. V hlavním menu byla otevřena sekce Files a k nahrání balíčku postačilo přetáhnout soubor z počítače pomocí myši. Poté byl router restartován prostřednictvím záložky Reboot v sekci System.



Obrázek 13 Restart

Po restartu již byla nová verze připravena k nasazení. Pro finální dokončení aktualizace byla v sekci System zvolena záložka RouterBOARD a byl proveden upgrade firmwaru.

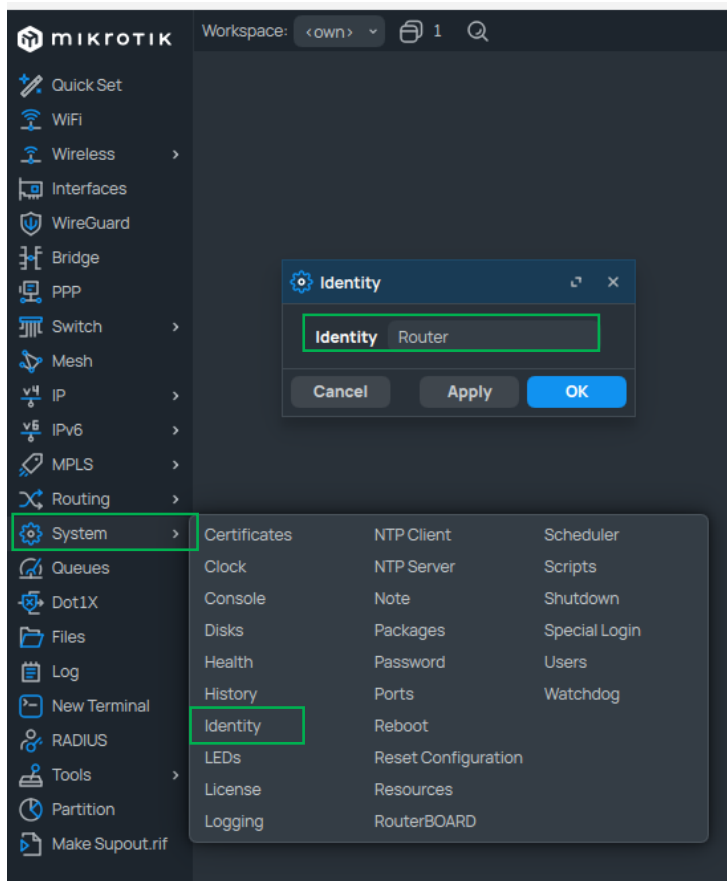


Obrázek 14 Zálůžka RouterBOARD

Byla zvolena možnost Upgrade a router byl následně ještě jednou restartován. Aktualizace tak byla úspěšně dokončena.

10.3 Hostname

Změna hostname z výchozího názvu Mikrotik na Router proběhla v sekci Systém v záložce Identity.

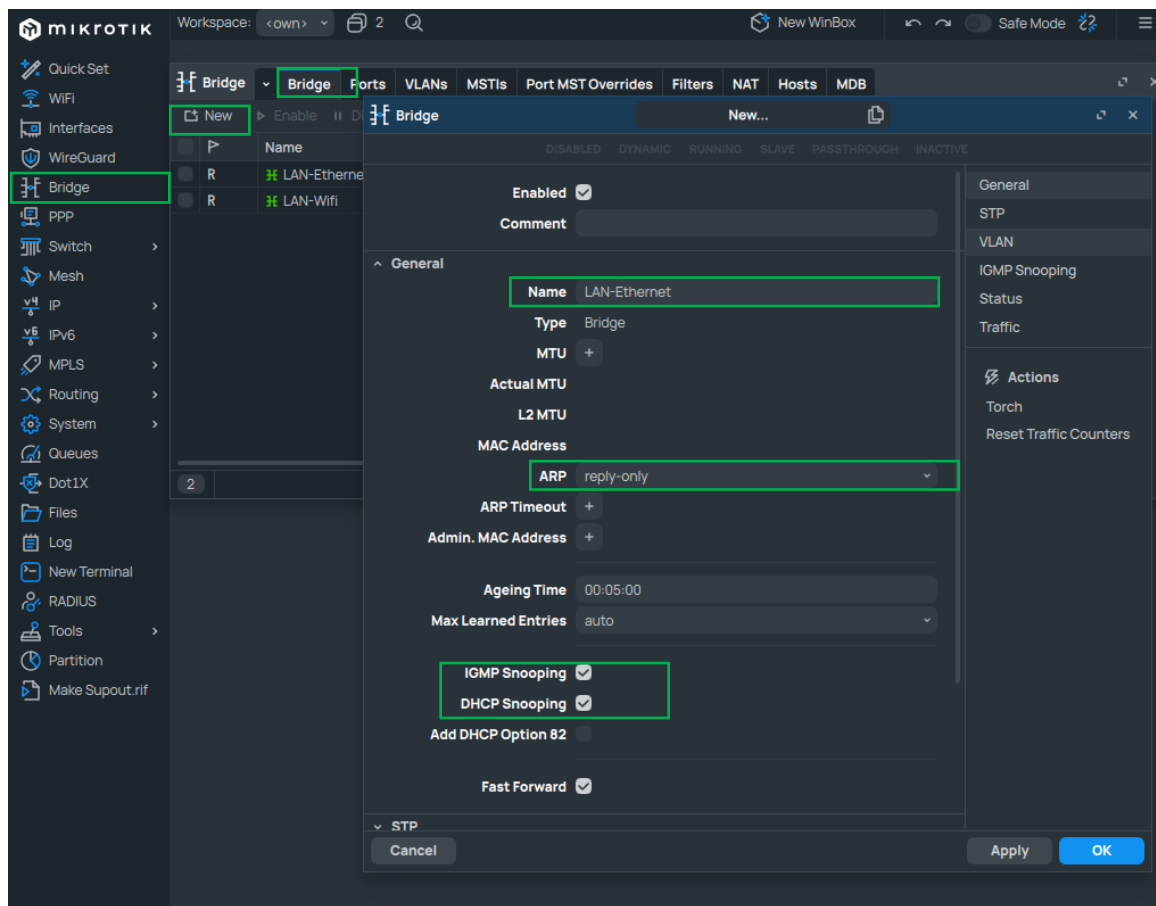


Obrázek 15 Hostname

10.4 Vytvoření bridge

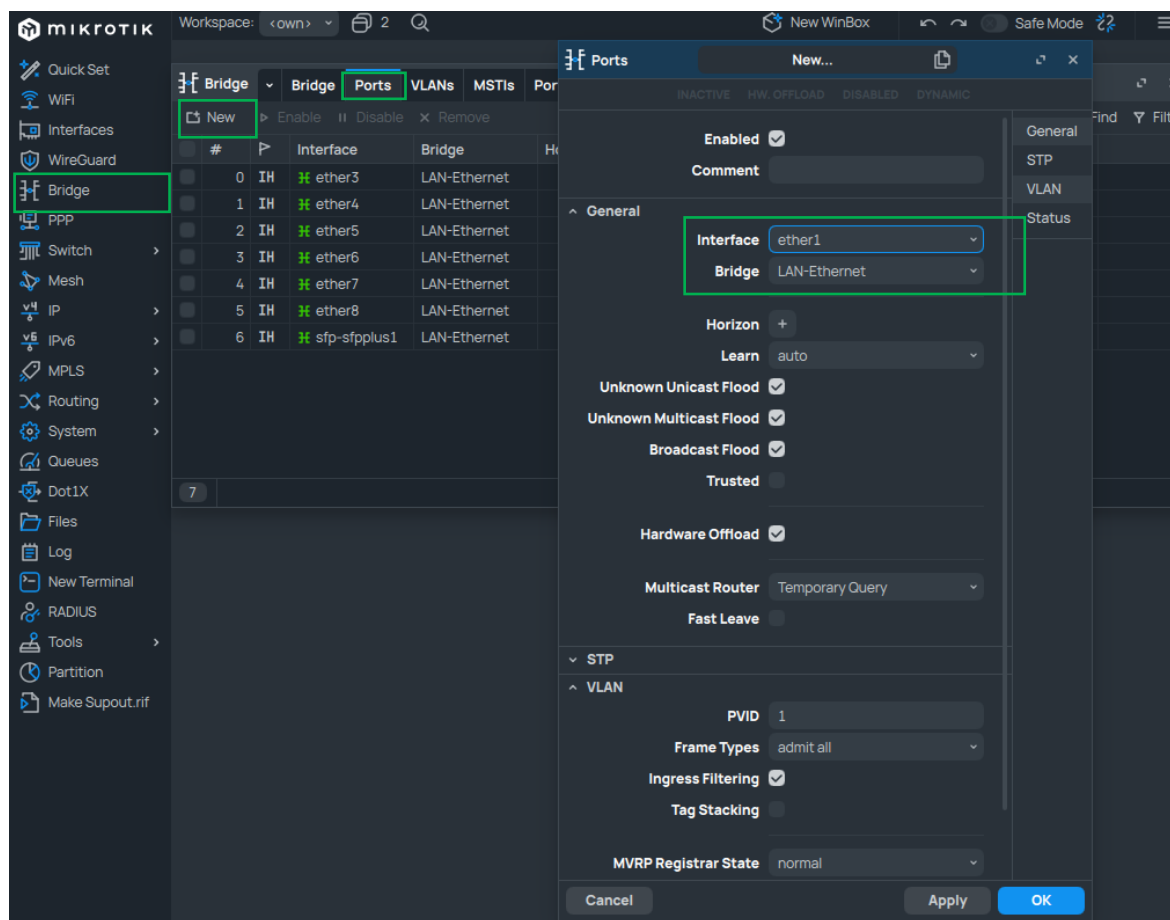
V levém menu byla vybrána sekce Bridge a byl vytvořen nový bridge, který byl pojmenován LAN-Ethernet a LAN-Wifi (pro zařízení připojená prostřednictvím bezdrátové sítě). Byly nastaveny následující parametry:

- ARP bylo nastaveno na hodnotu reply-only. Tímto nastavením je výrazně omezena možnost útoku typu Man-in-the-Middle, kdy útočník předstírá jinou MAC adresu, než ve skutečnosti má. Zároveň tím je znemožněno neoprávněné nastavení statické IP adresy v síti, protože každá takto nastavená stanice musí mít správcem vytvořený záznam v ARP tabulce.
- DHCP Snooping byl aktivován, aby bylo možné zabránit neoprávněnému přidělování IP adres. Pouze důvěryhodné DHCP servery tak mohou odpovídat na DHCP žádosti.
- IGMP (Internet Group Management Protocol) Snooping byl aktivován, čímž byl optimalizován multicastový provoz, například pro IP kamery či streamované video v rámci sítě.



Obrázek 16 Založení bridge

Následně byly v záložce Ports přidány do bridge LAN-Ethernet jednotlivé porty určené pro LAN. Bridge LAN-Wifi zůstal prozatím bez přiřazených portů.

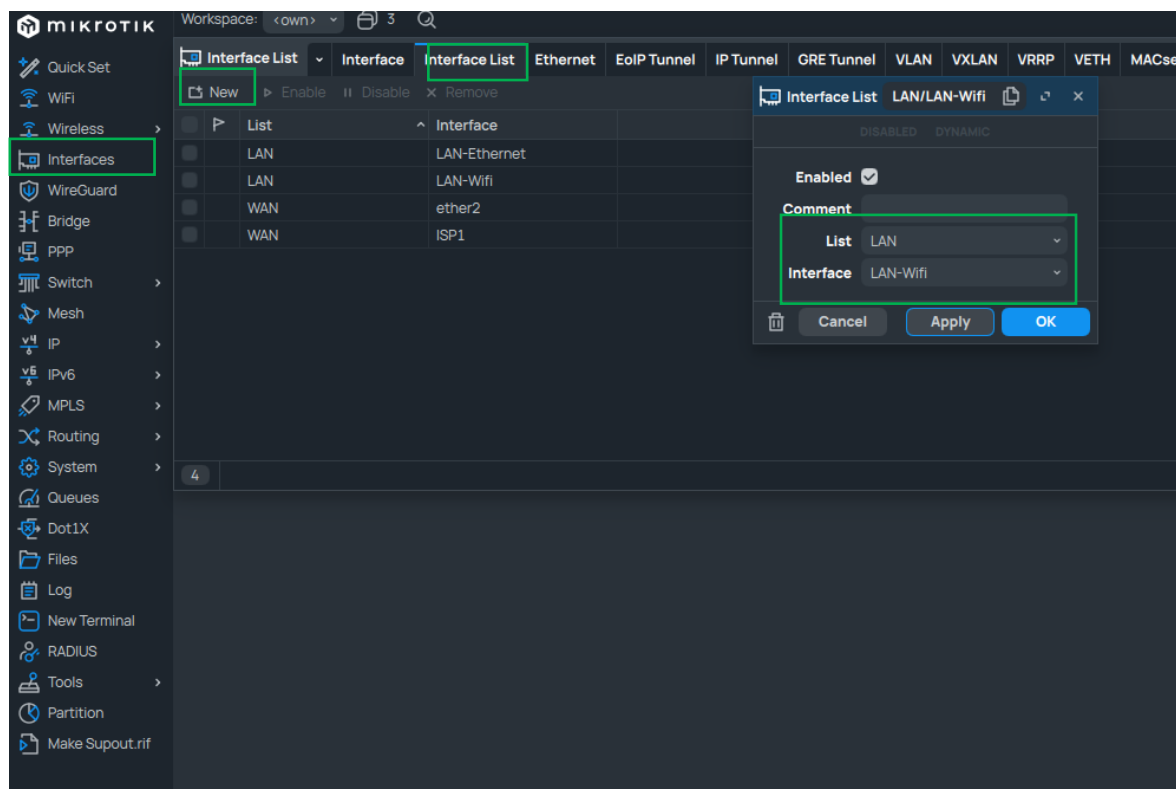


Obrázek 17 Přidání portu do bridge

10.5 Port list

Pro zjednodušení správy pravidel firewallu a zajištění přehlednější konfigurace byly vytvořeny seznamy portů (port listy). Tyto seznamy umožnily seskupit více portů do jedné logické skupiny, což usnadnilo správu přístupových pravidel a zvýšilo čitelnost nastavení.

Byly vytvořeny dva základní seznamy – LAN a WAN. Pro jejich vytvoření bylo třeba přejít do sekce Interfaces a do záložky Interface List. Zde byla přiřazena rozhraní Lan-Ethernet a Lan-WiFi do listu LAN a rozhraní ISP1 a ether2 do listu WAN.

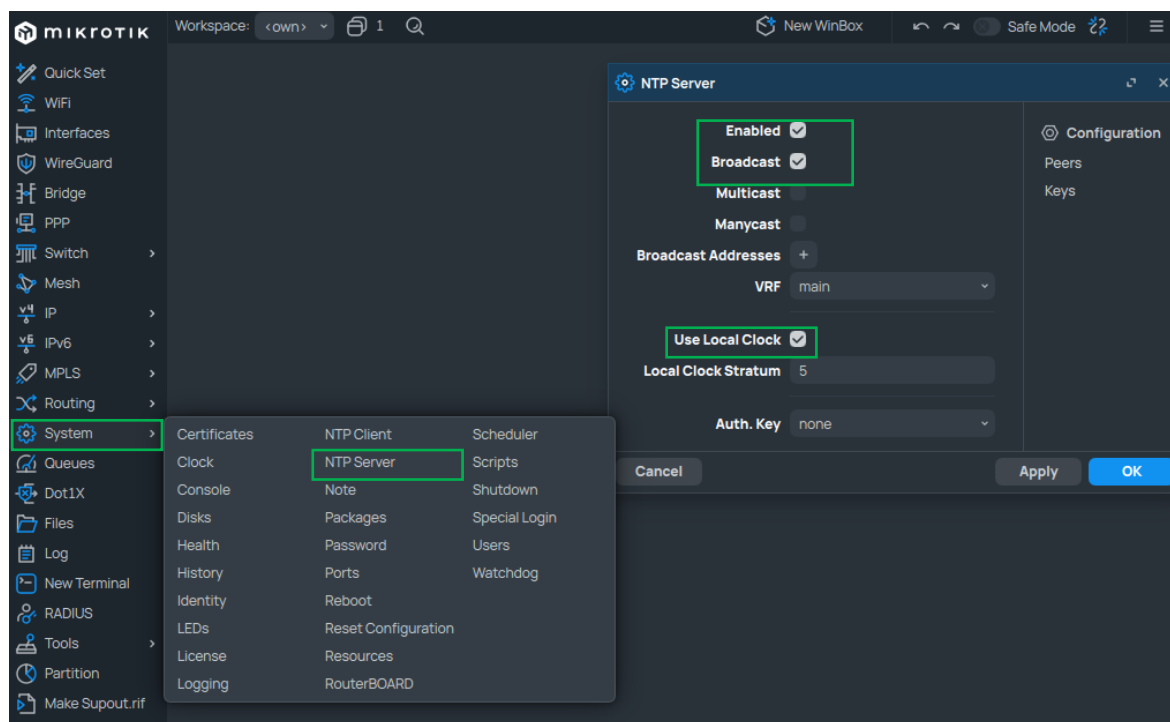


Obrázek 18 Přidání portu do listu

10.6 NTP

Z důvodu potřeby jednotného času na všech zařízeních v síti byl vytvořen vlastní NTP server.

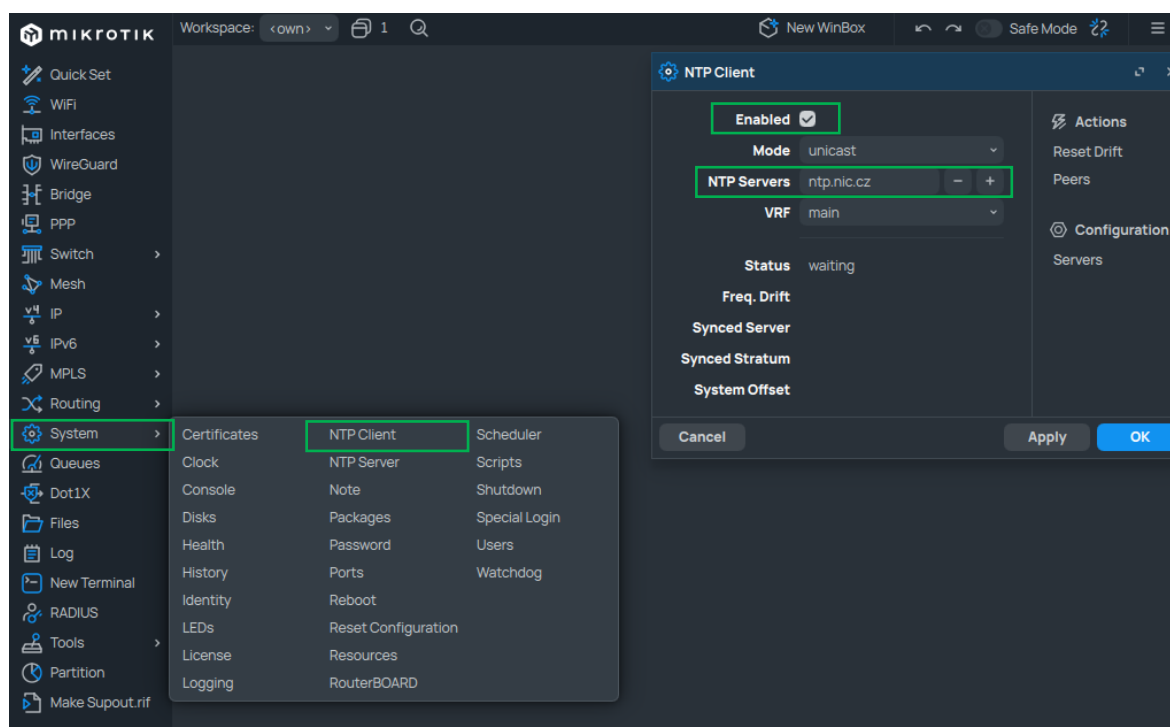
V sekci System a záložce NTP Server byl NTP server aktivován a současně byla povolena možnost Broadcast, čímž bylo umožněno, aby klientská zařízení mohla server automaticky objevit prostřednictvím broadcastových zpráv. Dále byla aktivována možnost Use Local Clock, díky které server poskytuje čas přímo ze svého interního hardwarového hodinového obvodu.



Obrázek 19 NTP server

Nyní byl NTP server nakonfigurován, avšak bylo ještě potřeba zajistit synchronizaci interních hodin s některým z důvěryhodných externích NTP serverů.

V sekci System a záložce NTP Client byl aktivován NTP klient a následně nastaven NTP server ntp.nic.cz.



Obrázek 20 NTP klient

Tím byla konfigurace samotného NTP hotova.

10.7 DNS

Následně bylo přistoupeno k nastavení DNS serveru v sekci IP a záložce DNS.

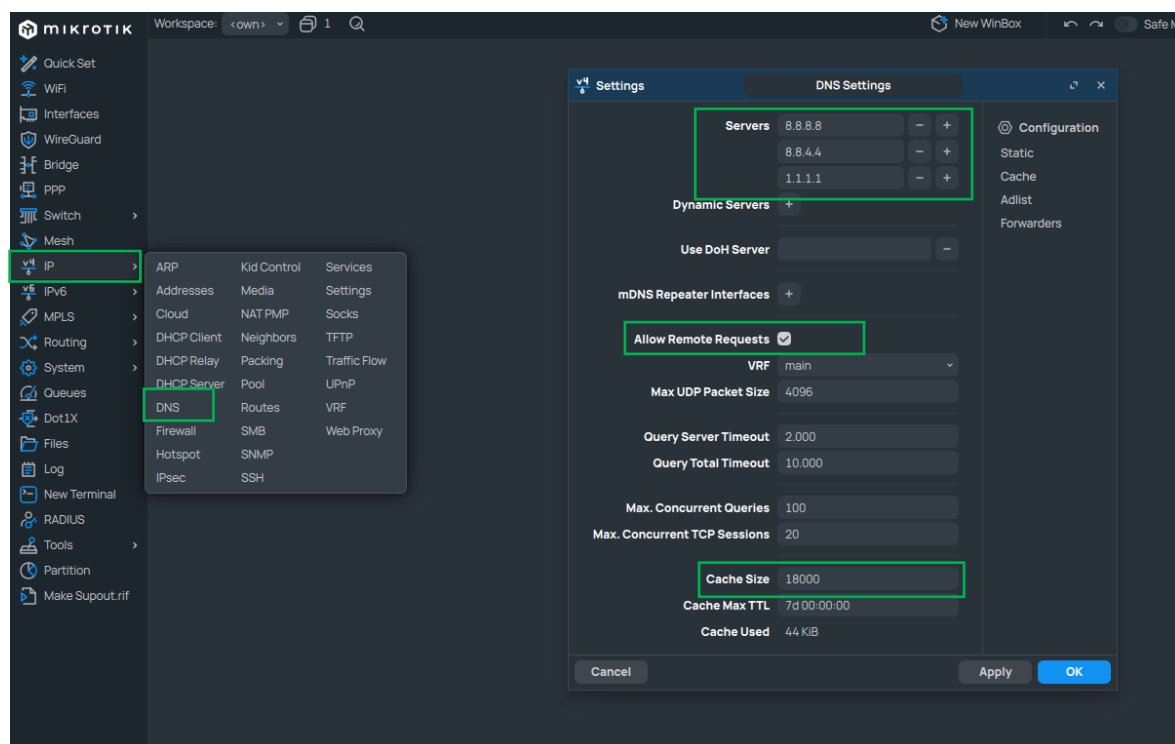
Zde byly jako zdroje DNS serveru nastaveny následující IPv4 adresy:

- 8.8.8.8 (Google DNS)
- 8.8.4.4 (Google DNS)
- 1.1.1.1 (Cloudflare DNS)

Použitím více DNS serverů je zajištěna redundance a zvýšená dostupnost v případě výpadku některého ze serverů.

Dále byla velikost DNS cache navýšena na hodnotu 18 000 KiB, čímž je optimalizována rychlost opakovaných dotazů.

Jako poslední byla aktivována volba Allow Remote Request, čímž je umožněno klientům v LAN zasílat dotazy na tento DNS server.

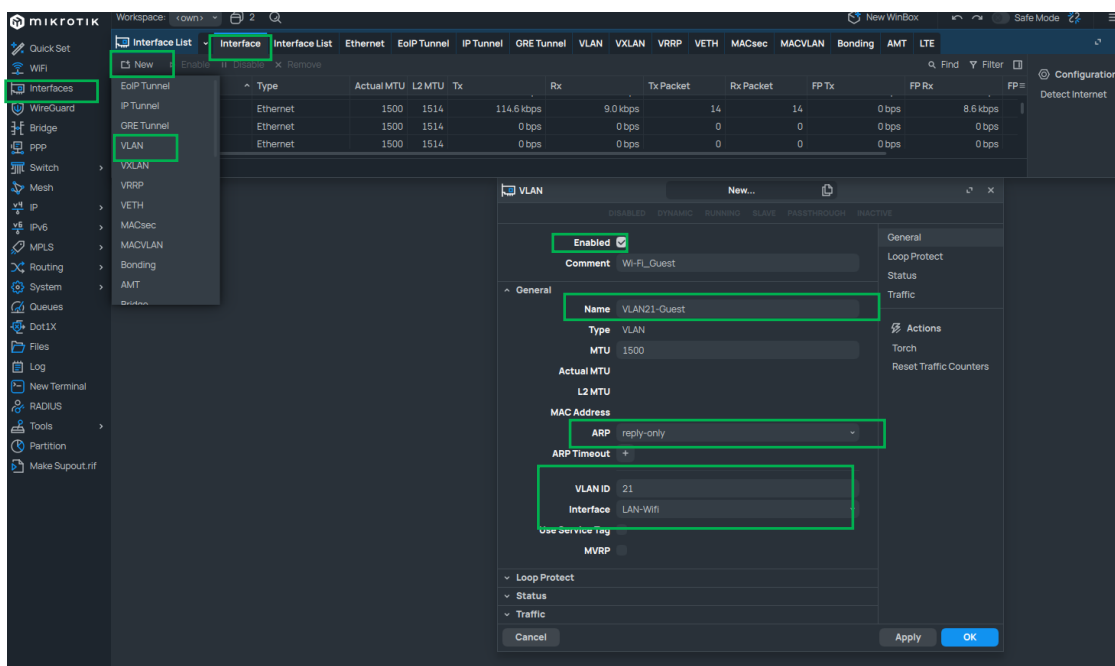


Obrázek 21 DNS

10.8 VLAN

Následně byla vytvořena VLAN s ID 21, která slouží jako síť pro hostovskou Wi-Fi.

V sekci Interfaces a v záložce Interface byla vytvořena nová VLAN. Byl zvolen název VLAN21-Guest, který obsahuje i ID VLANy pro lepší přehlednost. Do pole Comment byl stručně uveden účel této VLANy Wi-Fi_Guest. Parametr ARP byl nastaven na hodnotu read-only. Nakonec byla tato VLAN přiřazena k rozhraní LAN-Wifi, které přenáší provoz této sítě.

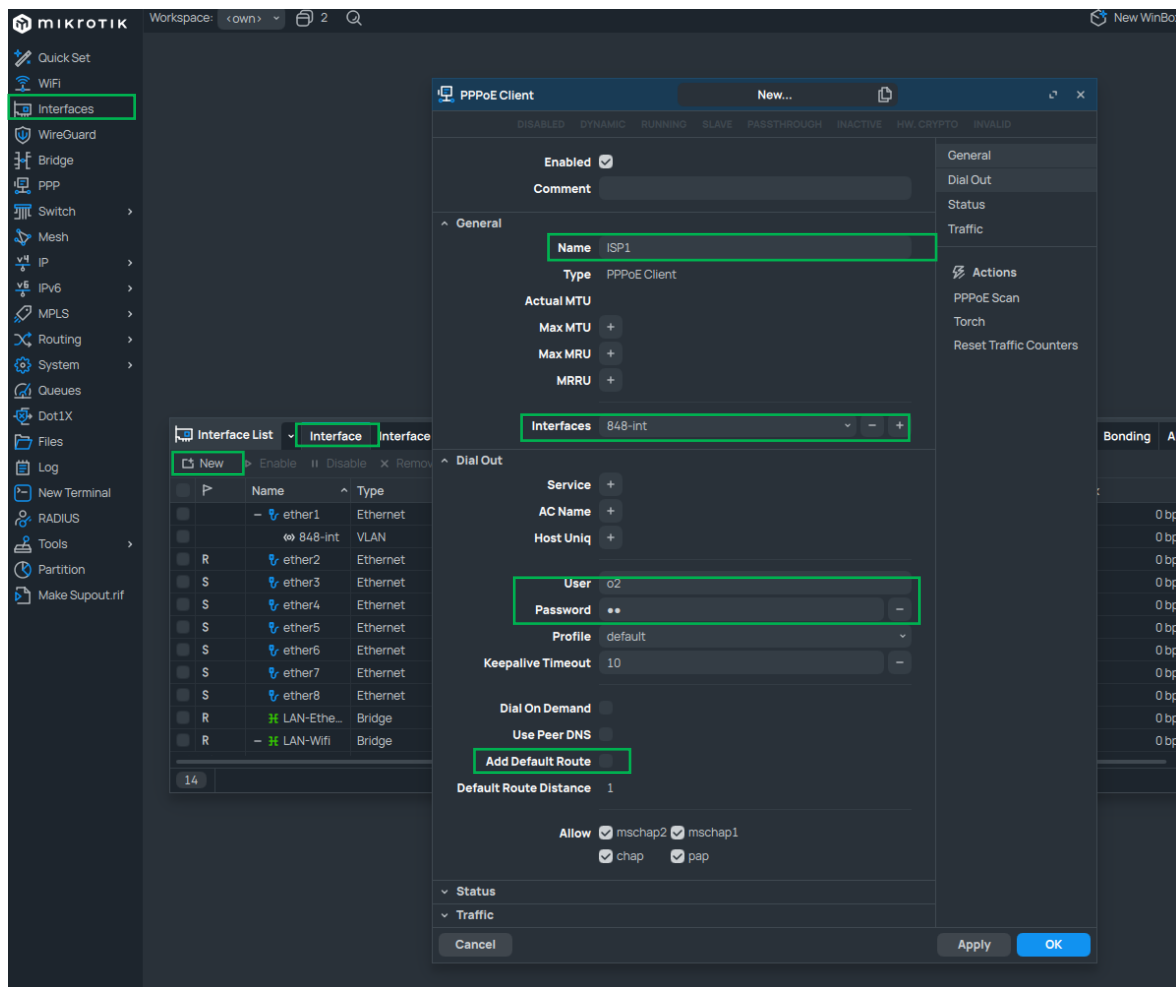


Obrázek 22 Hostovská VLAN

10.9 PPPoE

Vzhledem k tomu, že primární poskytovatel internetového připojení (ISP) připojuje své zákazníky pomocí PPPoE běžícího na VLAN 848, bylo nejprve nutné vytvořit VLAN 848 pod rozhraním ether1.

Následně byl na této VLAN vytvořen PPPoE klient, do kterého byly zadány přihlašovací údaje poskytnuté ISP.



Obrázek 23 PPPoE

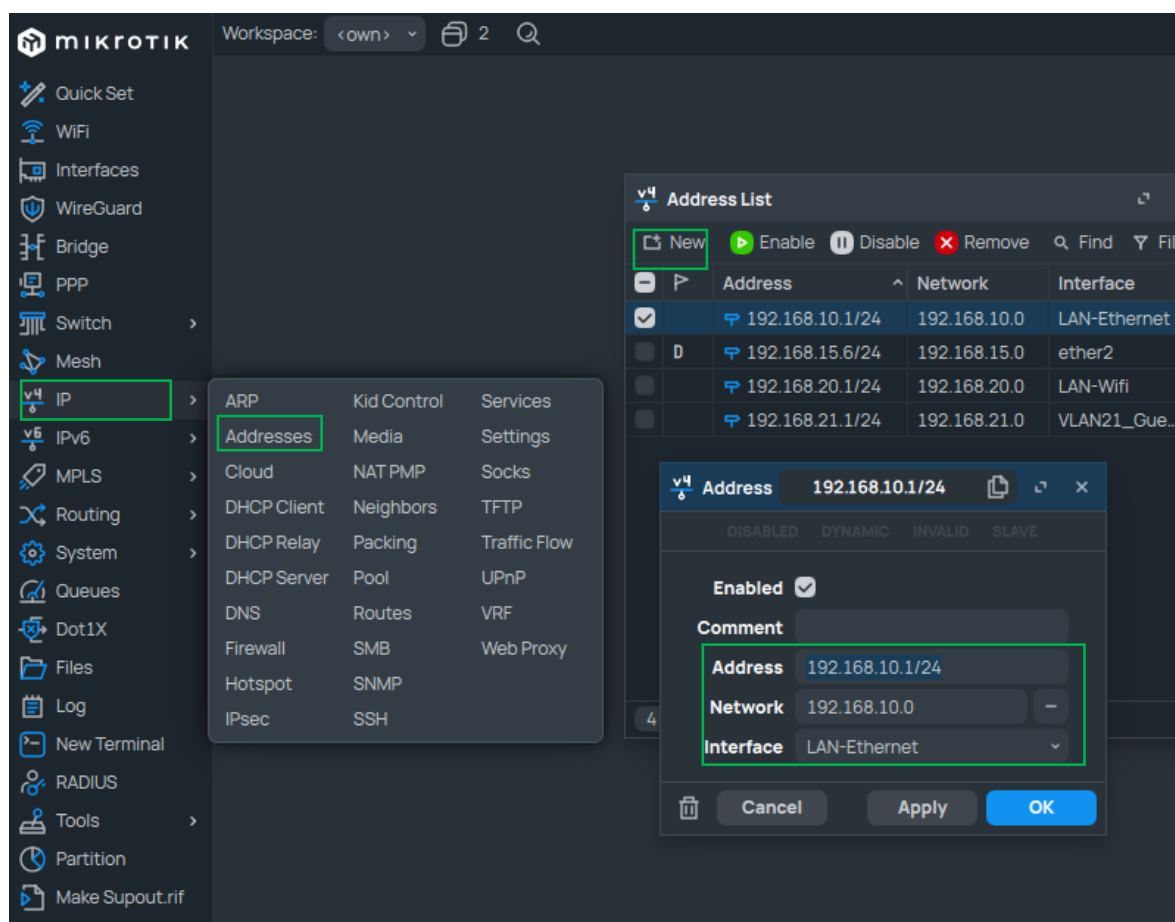
10.10 IP adresace

V této fázi bylo přistoupeno k nastavení IPv4 adres na jednotlivých rozhraních podle schématu sítě:

Tabulka 2 IPv4 adresy routeru

Interface	IPv4 adresa
ISP1	PPoE (ISP1)
ether2	DHCP (ISP2)
LAN-Ethernet	192.168.10.1
LAN-WiFi	192.168.20.1
VLAN21_Guest	192.168.21.1

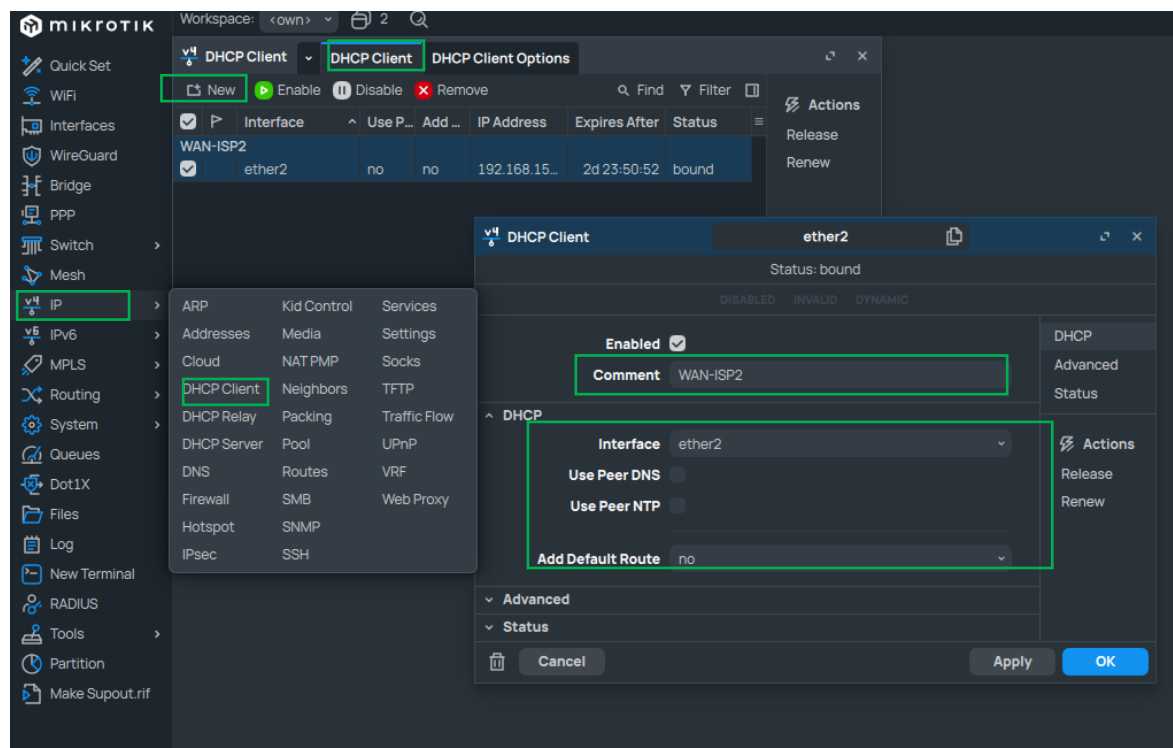
Nastavení statických IPv4 adres bylo provedeno v sekci IP prostřednictvím záložky Addresses. Na jednotlivá rozhraní byly přiřazeny odpovídající adresy.



Obrázek 24 Statické IPv4 adresy

Následně bylo potřeba nastavit porty, které mají získávat IPv4 adresu dynamicky. V sekci IP byla zvolena záložka DHCP Client a zde byl povolen DHCP klient na rozhraní ether2. Byl přidán vhodný komentář a současně byly deaktivovány následující volby:

- Use Peer DNS (nepřebírat DNS server od DHCP)
- Use Peer NTP (nepřebírat NTP server od DHCP)
- Add Default Route (nevytvářet automaticky výchozí trasu)



Obrázek 25 Dynamické IPv4 adresy

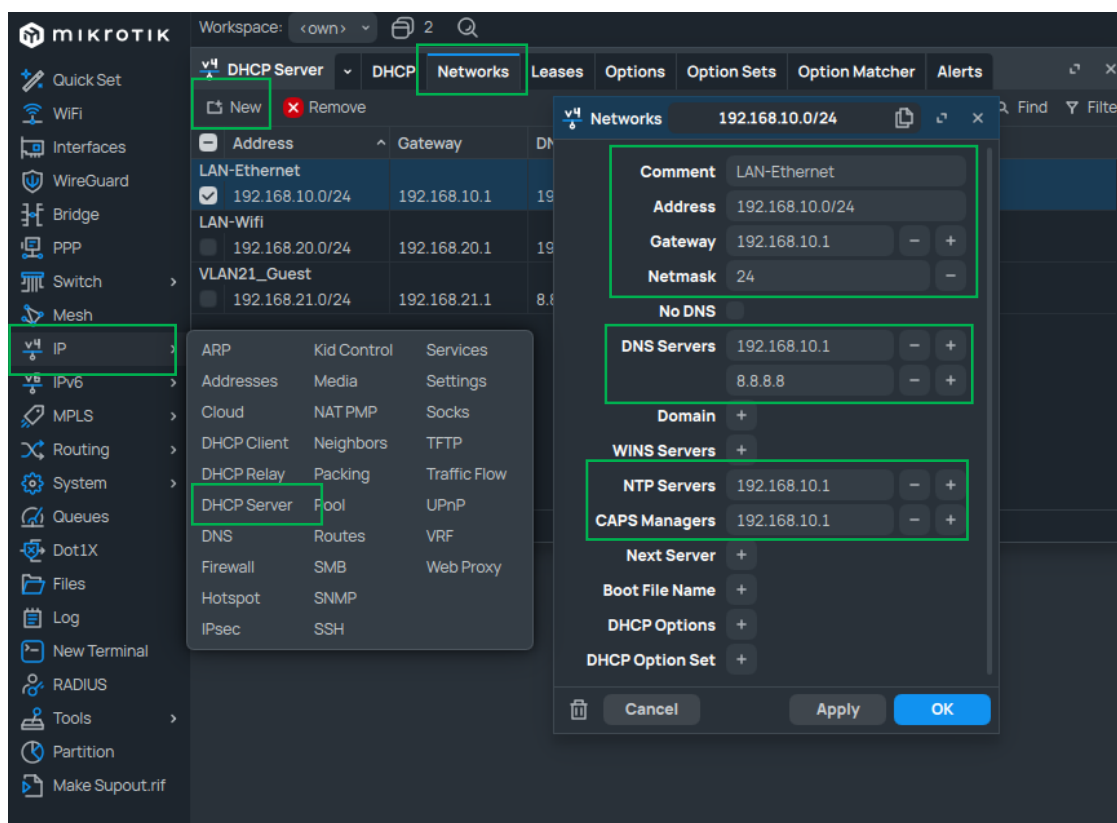
10.10.1 DHCP Server

Na základě návrhu sítě byly definovány rozsahy IPv4 adres a další parametry, které má DHCP server poskytovat.

- Lan-Ethernet:
 - Sít': 192.168.10.0/24
 - Přidělováný rozsah: 192.168.10.10–192.168.10.250
 - Gateway: 192.168.10.1
 - DNS: 192.168.10.1, 8.8.8.8
 - NTP server: 192.168.10.1
 - CAPS Manažer: 192.168.10.1
- Lan-WiFi:
 - Sít': 192.168.20.0/24
 - Přidělováný rozsah: 192.168.20.10–192.168.20.250
 - Gateway: 192.168.20.1

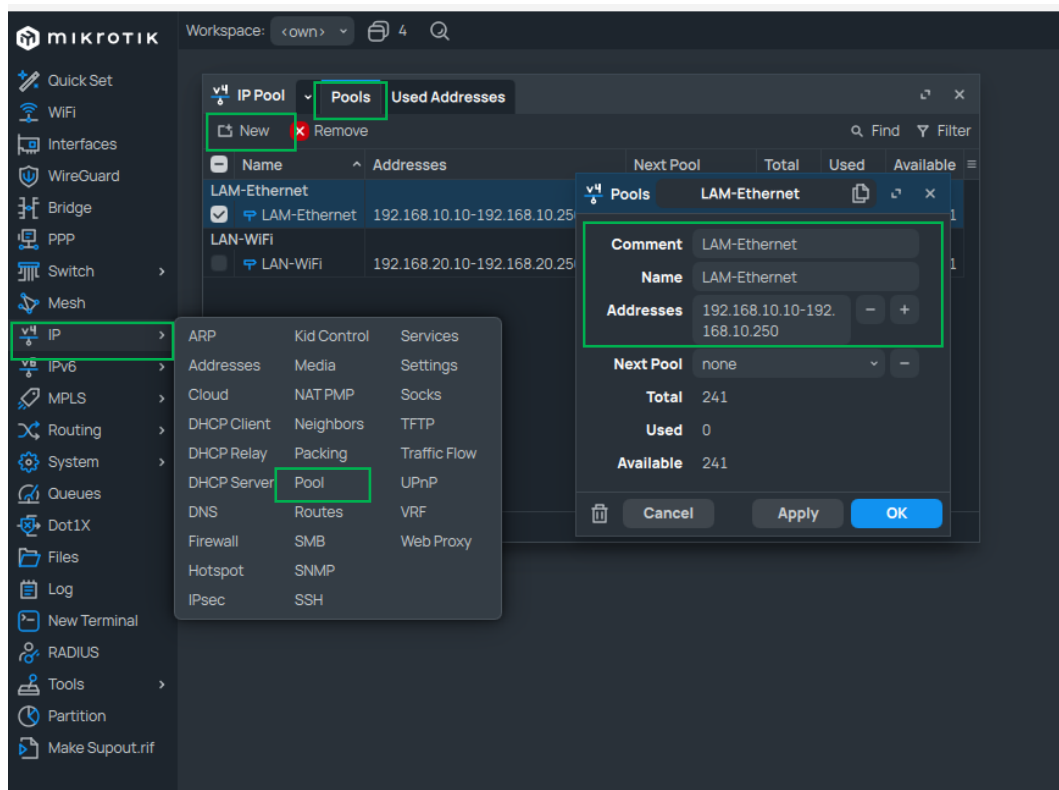
- DNS: 192.168.20.1, 8.8.8.8
- NTP server: 192.168.20.1
- CAPS Manažer: 192.168.20.1
- VLAN21_Guest:
 - Síť: 192.168.21.0/24
 - Přidělování rozsah: 192.168.21.10–192.168.21.250
 - Gateway: 192.168.21.1
 - DNS: 192.168.21.1, 8.8.8.8
 - NTP server: 192.168.21.1

V sekci IP a v záložce DHCP Server byla zvolena podzáložka Networks, kde byly vyplněny základní údaje o každé síti, kterou má DHCP server obsluhovat. Byly zadány hodnoty pro síť, gateway, DNS, NTP a případně i CAPS manažera. Pro každou síť byl přidán stručný komentář.



Obrázek 26 Vytvoření sítě pro DHCP

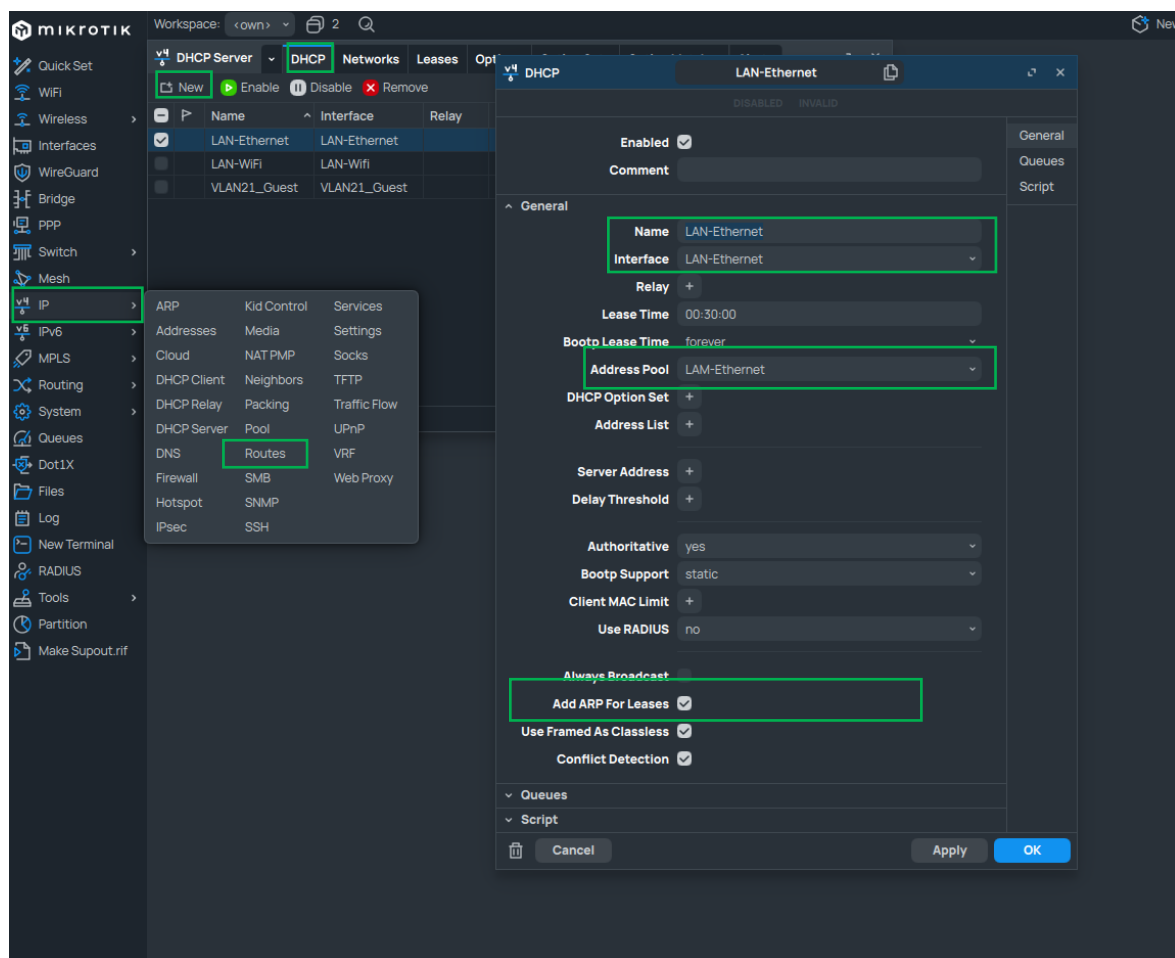
Po vytvoření všech definovaných sítí bylo potřeba vytvořit Address Pool pro každou z těchto sítí. Jedná se o rozsah IPv4 adres, které má DHCP server přidělovat. V sekci IP byla otevřena záložka Pools a zde byly vytvořeny potřebné pooly.



Obrázek 27 IPv4 pool

Po dokončení všech přípravných kroků bylo přistoupeno k samotnému vytvoření DHCP serveru. V sekci IP, v záložce DHCP Server a v podzáložce DHCP byly vytvořeny jednotlivé servery, ke kterým byly přiřazeny odpovídající rozsahy adres a rozhraní, na kterých mají servery běžet.

Následně byla aktivována možnost Add ARP for leases, čímž bylo zajištěno automatické přidávání dynamických ARP záznamů pro všechny adresy přidělené DHCP serverem. Tato funkce je nezbytná, protože ARP tabulka je nastavena do režimu read-only. Automatické přidávání ARP záznamů z DHCP pronájmů tak zaručuje, že zařízení získávající IP adresu z DHCP serveru mohou plnohodnotně komunikovat v síti.



Obrázek 28 DHCP server

Tímto krokem byla úspěšně dokončena konfigurace DNS serveru.

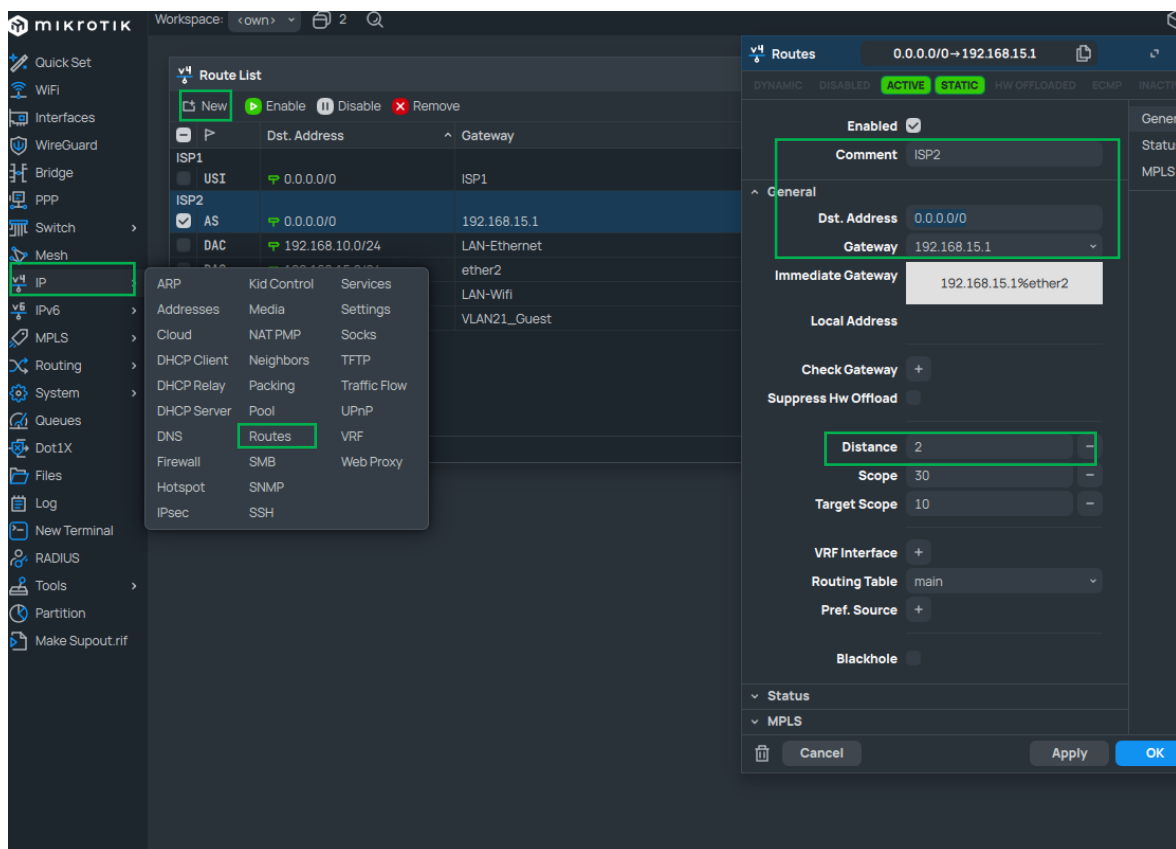
10.11 Routování

Byly vytvořeny následující statické routy, které zajišťují přístup do Internetu prostřednictvím obou poskytovatelů připojení.

Tabulka 3 Routy

Cíl	Gateway	Metrika
0.0.0.0/0	ISP1	1
0.0.0.0/0	192.168.15.1	2

V sekci IP a záložce Routes byly přidány obě výchozí routy.



Obrázek 29 Routy

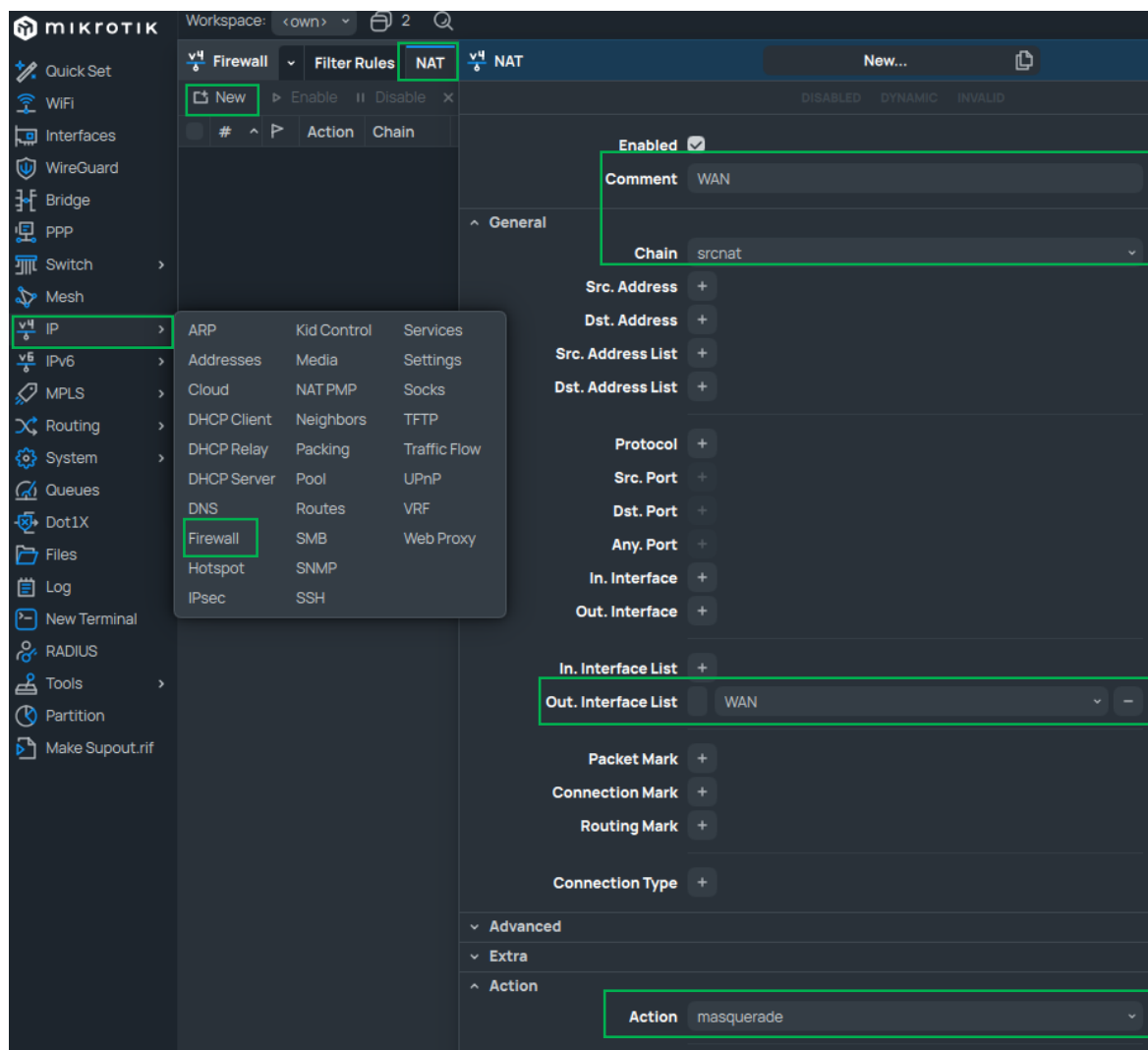
Primární ruta byla nastavena přes rozhraní ISP1 (ISP1) díky nižší metrice. V případě nedostupnosti této trasy bude automaticky použita záložní trasa s metrikou 2, odkazující na rozhraní ether2 (ISP2).

10.11.1 Source NAT

Pro zajištění přístupu do sítě ISP pod jedinou veřejnou IP adresou byla implementována maškaráda (masquerade). Veškeré pakety odcházející z vnitřní sítě přes porty ISP1 (ISP1) a ether2 (ISP2), které byly zahrnuty v port listu WAN, jsou překládány tak, že jejich zdrojová adresa je nahrazována veřejnou IP adresou přidělenou poskytovatelem.

Konfigurace byla provedena v sekci IP v záložce Firewall a podzáložce NAT, kde bylo vytvořeno pravidlo typu srcnat s následujícími parametry:

- **Chain:** srcnat
- **Out. Interface List:** WAN
- **Action:** masquerade



Obrázek 30 Maškaráda

Tímto nastavením je zajištěno, že zařízení v lokální síti mohou komunikovat s Internetem bez nutnosti přidělení veřejných IP adres.

10.11.2 Failover

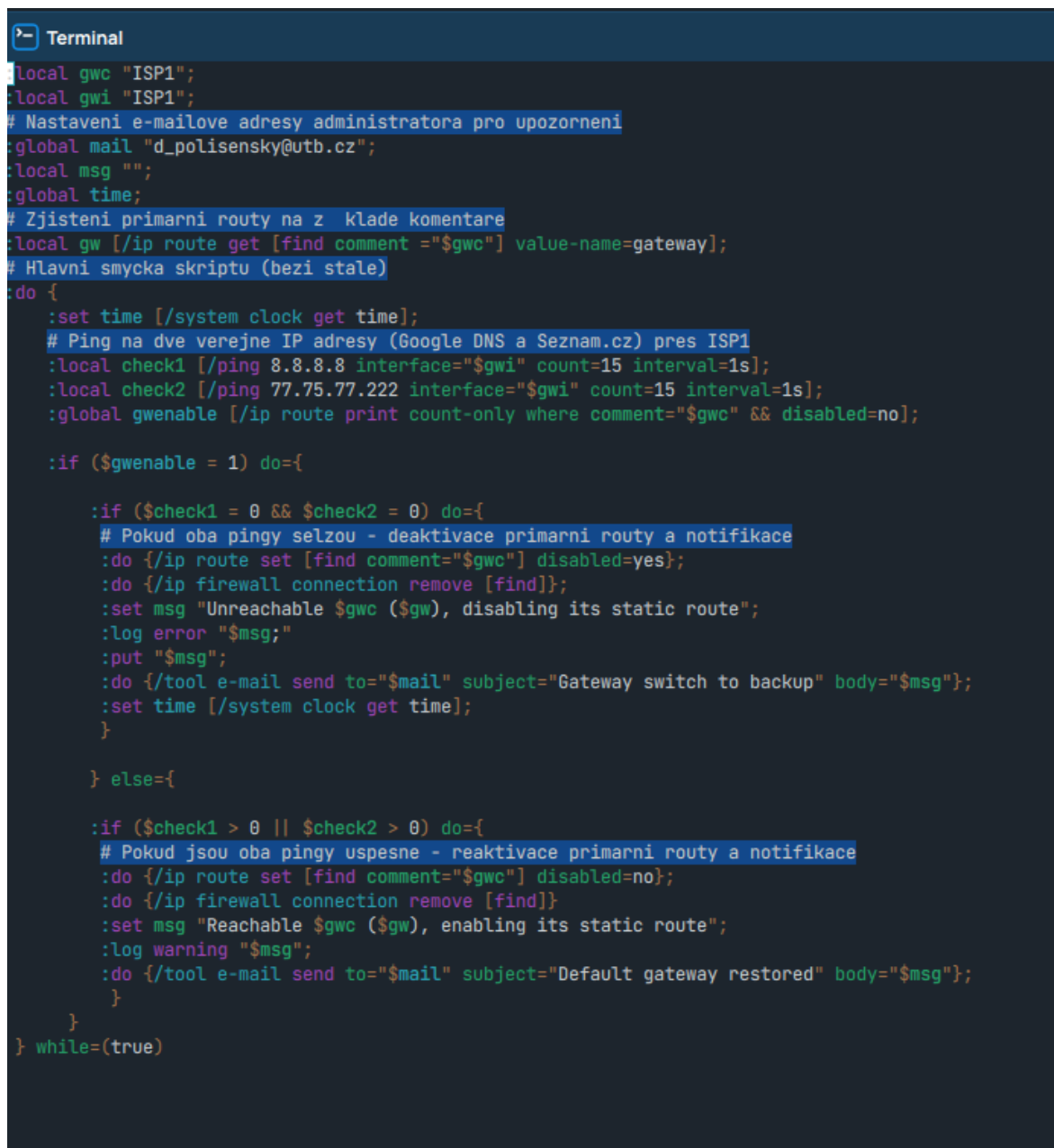
Aby bylo zajištěno, že zařízení v lokální síti budou mít trvalý přístup k Internetu i v případě výpadku primárního poskytovatele (ISP1), byl vytvořen automatizovaný monitorovací skript v systému RouterOS.

V terminálu byl následujícím příkazem vytvořen skript:

```
/system/script/ add name=failover
```

Následně byl otevřen editor skriptu příkazem:

```
/system script edit failover source
```



```

Terminal
:local gwc "ISP1";
:local gwi "ISP1";
# Nastaveni e-mailove adresy administratora pro upozorneni
:global mail "d_polisensky@utb.cz";
:local msg "";
:global time;
# Zjisteni primarni routy na z klade komentare
:local gw [/ip route get [find comment ="$gwc"] value-name=gateway];
# Hlavni smycka skriptu (bezi stale)
:do {
    :set time [/system clock get time];
    # Ping na dve verejne IP adresy (Google DNS a Seznam.cz) pres ISP1
    :local check1 [/ping 8.8.8.8 interface="$gwi" count=15 interval=1s];
    :local check2 [/ping 77.75.77.222 interface="$gwi" count=15 interval=1s];
    :global gwenable [/ip route print count-only where comment="$gwc" && disabled=no];

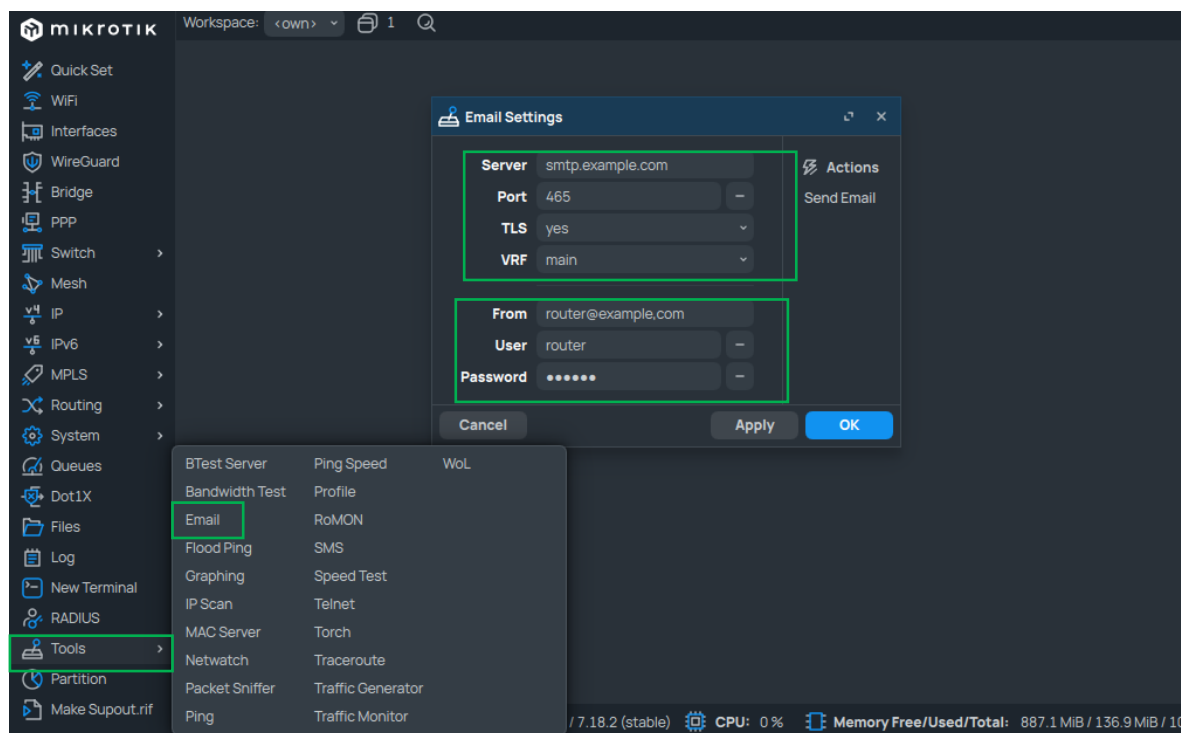
    :if ($gwenable = 1) do={
        :if ($check1 = 0 && $check2 = 0) do={
            # Pokud oba pingy selzou - deaktivace primarni routy a notifikace
            :do {/ip route set [find comment="$gwc"] disabled=yes};
            :do {/ip firewall connection remove [find]};
            :set msg "Unreachable $gwc ($gw), disabling its static route";
            :log error "$msg";
            :put "$msg";
            :do {/tool e-mail send to="$mail" subject="Gateway switch to backup" body="$msg"};
            :set time [/system clock get time];
        }
        :else={
            :if ($check1 > 0 || $check2 > 0) do={
                # Pokud jsou oba pingy uspesne - reaktivace primarni routy a notifikace
                :do {/ip route set [find comment="$gwc"] disabled=no};
                :do {/ip firewall connection remove [find]};
                :set msg "Reachable $gwc ($gw), enabling its static route";
                :log warning "$msg";
                :do {/tool e-mail send to="$mail" subject="Default gateway restored" body="$msg"};
            }
        }
    }
} while=true)

```

Obrázek 31 Failover skript

Skript pravidelně ověřuje dostupnost Internetu prostřednictvím dvou veřejných IP adres (Google DNS a Seznam.cz). V případě, že obě adresy nejsou dosažitelné, dojde k deaktivaci statické trasy směřující na ISP1, vymazání aktivních spojení a odeslání upozornění administrátorovi e-mailem. Po obnovení konektivity je statická trasa opět aktivována a systém informuje o návratu k primární bráně prostřednictvím zvoleného SMTP serveru.

Aby mohly být zasílány e-mailové notifikace, byly v sekci Tools a záložce Email nastaveny parametry SMTP serveru, odesílatele a případně ověřovací údaje.

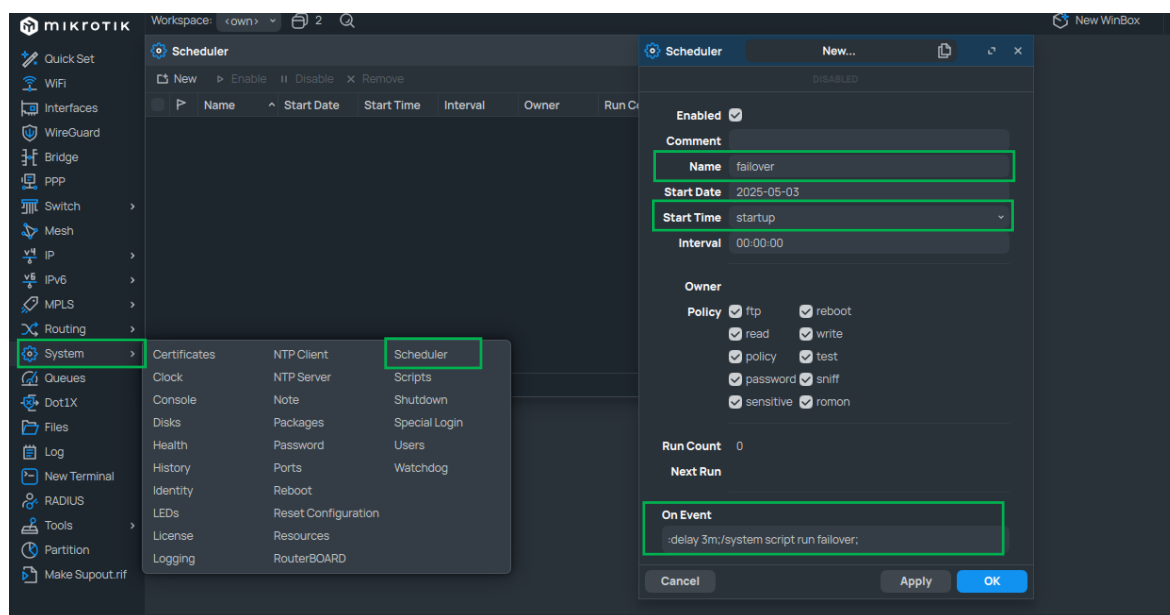


Obrázek 32 Nastavení SMTP

V samotném skriptu byl použit příkaz:

```
/tool e-mail send to="admin@exaxmple.com" subject="Subject" body="Text"
```

Po dokončení skriptu bylo ještě nutné zajistit jeho automatické spouštění po startu systému. V sekci System v záložce Scheduler byl vytvořen nový plánovač, který spouští skript tři minuty po spuštění systému, aby měl systém dostatek času pro inicializaci všech komponent.



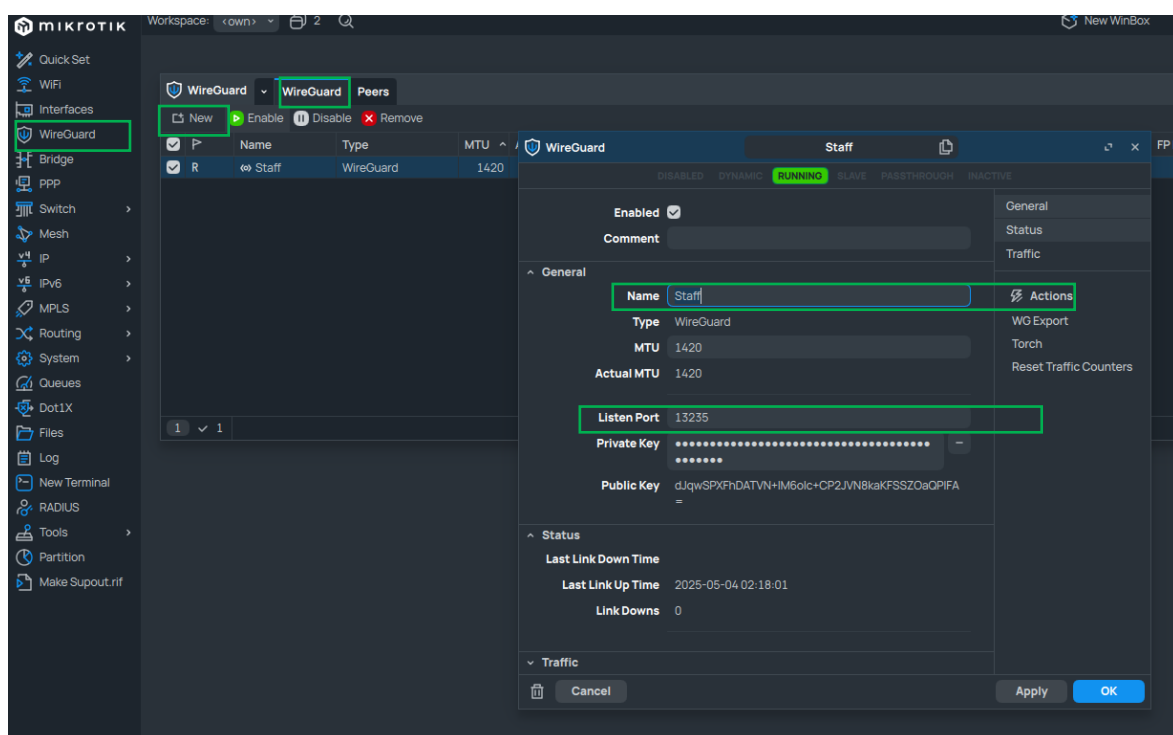
Obrázek 33 Failover scheduler

Tímto způsobem bude administrátor automaticky informován o změně stavu internetového připojení, například o přepnutí na záložní linku nebo obnovení hlavního připojení.

10.12 VPN

Jak správce, tak někteří zaměstnanci vyžadují vzdálený přístup do sítě pomocí VPN. Z těchto důvodů byla implementována WireGuard VPN.

V sekci WireGuard bylo vytvořeno nové WireGuard rozhraní, které slouží pouze pro připojení zaměstnanců a správce. Z důvodu zabezpečení mu byl změněn port z výchozího 13231 na 13235.

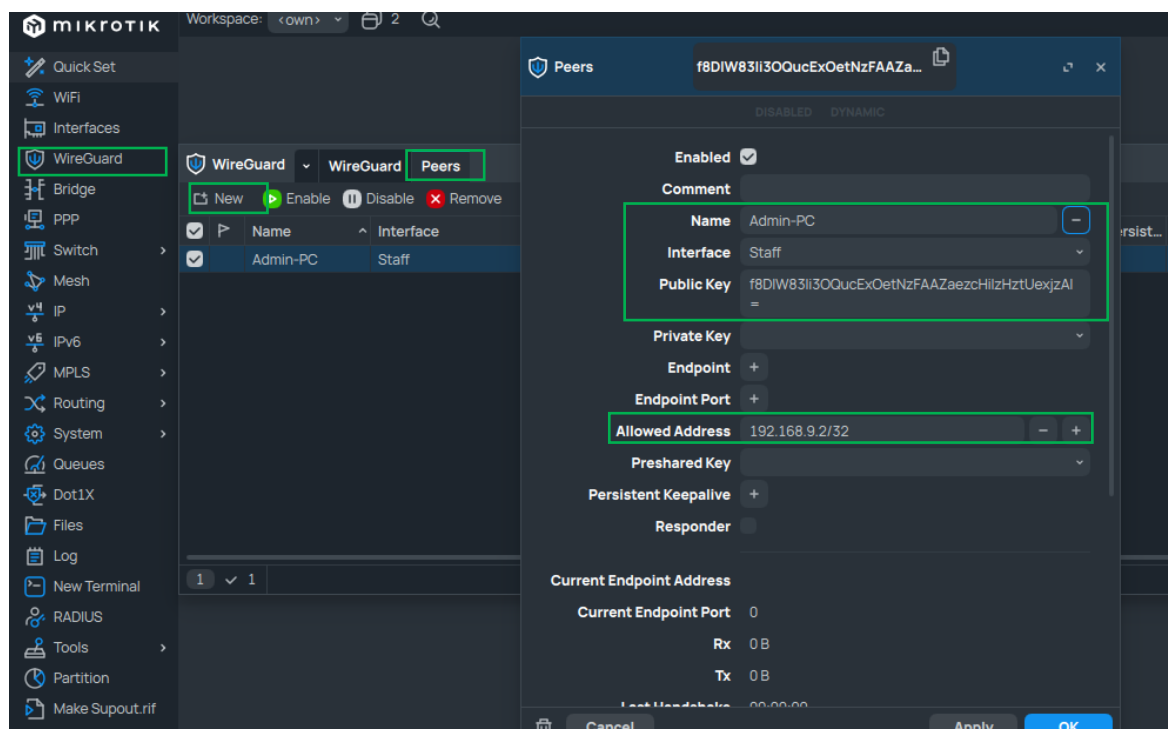


Obrázek 34 Wireguard rozhraní

Po vytvoření rozhraní byl vygenerován veřejný šifrovací klíč, který musel být následně vyměněn s klienty.

Následně byla rozhraní Staff přidělena IP adresa 192.168.9.1/24 a byl vytvořen source NAT pro provoz odcházející přes toto rozhraní na IP adresu 192.168.9.1.

Tím byla dokončena konfigurace samotného WireGuard rozhraní. Dále bylo potřeba přidat peery. V záložce peer byly přiřazeny k rozhraní Staff, byl vyplněn jejich veřejný klíč, jako Allowed Address byla zadána jejich adresa v rámci VPN tunelu a nakonec bylo přidáno vhodné jméno.

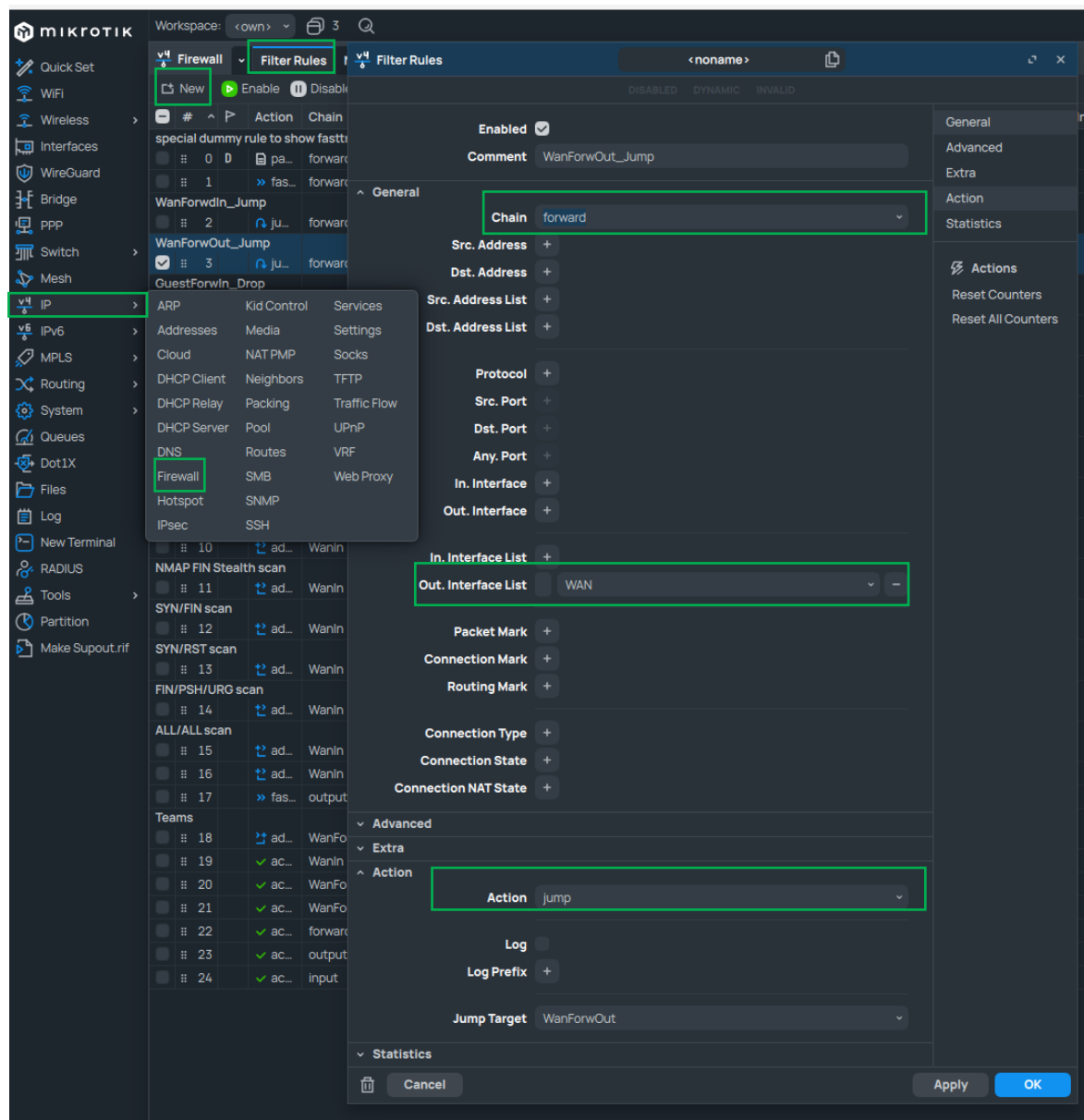


Obrázek 35 Wireguard peer

10.13 Firewall

Pro zajištění bezpečnosti a řízení síťového provozu byla implementována sada pravidel v části IP Firewall.

Přešlo se do sekce IP, do záložky Firewall a podzáložky Filter Rules. Zde byla vytvořena pravidla, v jejichž rámci musely být vždy specifikovány správný chain, klasifikátor a akce, případně další parametry.



Obrázek 36 Vytvoření filter rule

Tímto způsobem byla vytvořena všechna potřebná pravidla. Výsledná konfigurace poté vypadala takto:

```

Flags: X - disabled, I - invalid; D - dynamic
0 D ;; special dummy rule to show fasttrack counters
  chain=forward action=passthrough

1 chain=forward action=fasttrack-connection hw-offload=yes src-address-list=Private dst-address-list=Private log=no log-prefix=""

2 ;; WanForwIn_Jump
  chain=forward action=jump jump-target=WanForwIn in-interface-list=WAN log=no log-prefix=""

3 ;; WanForwOut_Jump
  chain=forward action=jump jump-target=WanForwOut out-interface-list=WAN log=no log-prefix=""

4 ;; GuestForwIn_Drop
  chain=forward action=drop in-interface=VLAN21_Guest out-interface-list=!WAN log=no log-prefix=""

5 ;; GuestIn_Drop
  chain=input action=drop in-interface=VLAN21_Guest log=no log-prefix=""

6 ;; WanIn_Jump
  chain=input action=jump jump-target=WanIn in-interface-list=WAN log=no log-prefix=""

7 ;; dropping port scanners
  chain=WanIn action=drop src-address-list=port scanners log=no log-prefix=""

8 ;; WanIn_Accept_Wireguard
  chain=WanIn action=accept protocol=udp dst-port=13235 log=no log-prefix=""

9 ;; WanIn_DropMotDsnated
  chain=WanIn action=drop connection-nat-state=!dstnat log=no log-prefix=""

10 ;; Port scanners to list
  chain=WanIn action=add-src-to-address-list protocol=tcp psd=21,3s,3,1 address-list=port scanners address-list-timeout=2w log=no log-prefix=""

11 ;; NMAP FIN Stealth scan
  chain=WanIn action=add-src-to-address-list tcp-flags=fin,!syn,!rst,!psh,!ack,!urg protocol=tcp address-list=port scanners address-list-timeout=2w log=no log-prefix=""

12 ;; SYN/FIN scan
  chain=WanIn action=add-src-to-address-list tcp-flags=fin,syn protocol=tcp address-list=port scanners address-list-timeout=2w log=no log-prefix=""

13 ;; SYN/RST scan
  chain=WanIn action=add-src-to-address-list tcp-flags=syn,rst protocol=tcp address-list=port scanners address-list-timeout=2w log=no log-prefix=""

14 ;; FIN/PSH/URG scan
  chain=WanIn action=add-src-to-address-list tcp-flags=fin,psh,urg,!syn,!rst,!ack protocol=tcp address-list=port scanners address-list-timeout=2w log=no log-prefix=""

15 ;; ALL/ALL scan
  chain=WanIn action=add-src-to-address-list tcp-flags=fin,syn,rst,psh,ack,urg protocol=tcp address-list=port scanners address-list-timeout=2w log=no log-prefix=""

16 chain=WanIn action=add-src-to-address-list tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg protocol=tcp address-list=port scanners address-list-timeout=2w log=no log-prefix=""

17 chain=output action=fasttrack-connection hw-offload=yes log=no log-prefix=""

18 ;; Teams
  chain=WanForwOut action=add-dst-to-address-list protocol=tcp address-list=Voice address-list-timeout=4w2d log=no log-prefix="" tls-host=*teams.microsoft.com*

19 chain=WanIn action=accept log=no log-prefix=""

20 chain=WanForwIn action=accept log=no log-prefix=""

21 chain=WanForwOut action=accept log=no log-prefix=""

22 chain=forward action=accept log=no log-prefix=""

23 chain=output action=accept log=no log-prefix=""

24 chain=input action=accept log=no log-prefix=""
[admin@tikrofik] >

```

Obrázek 37 Výpis filter rules

Pravidla byla rozdělena do několika chainů, což přispělo k přehlednosti a modularitě konfigurace a k efektivnějšímu využití zdrojů firewallu. V následujících odstavcích jsou popsány hlavní funkce a nastavení firewallu:

- Zrychlení průchodu známých spojení (FastTrack)
 - Pro zvýšení výkonu interní komunikace (LAN–LAN) a výstupu routeru byl aktivován FastTrack. Tento mechanismus umožňuje přeskočit části zpracování paketů pro spojení, která jsou již známá.
- Ochrana před skenováním a útoky z internetu

- Byl vytvořen vlastní chain WanIn, sloužící pro příchozí komunikaci do routeru z WAN, obsahuje sadu pravidel, která detekují a blokují pokusy o port scanning a podobné typy útoků.
- Detekce port skenerů: Pomocí různých kombinací TCP příznaků jsou identifikovány pokusy o stealth skenování (například NMAP FIN scan, SYN/FIN scan apod.). Tyto adresy jsou uloženy do seznamu port scanners s platností dva týdny.
- Blokace skenerů: Pokud adresa patří do seznamu port scanners, je provoz z této adresy automaticky zablokován.
- Povolení WireGuard VPN: Na UDP portu 13235 je povolen vstupní provoz pro VPN připojení.
- Základní ochrana WAN: Blokován je veškerý provoz, který není součástí NATovaných spojení.
- Segmentace sítě a řízení přístupu
 - Privátní sítě (192.168.9.0/24, 192.168.10.0/24, 192.168.20.0/24) jsou definovány v seznamu Private.
 - Guest VLAN s ID 21 (192.168.21.0/24) má omezený přístup – je povolen pouze výstup na WAN, přístup do ostatních sítí a k routeru je zakázán.
- Monitoring a řízení provozu
 - V chainu WanForwOut je pravidlo, které přidává cílové adresy komunikace směřující na *.teams.microsoft.com do seznamu Voice. Tímto způsobem lze snadno sledovat provoz využívající služby Teams (například VoIP hovory).
- Modularita pravidel
 - Pravidla jsou rozdělena do vlastních chainů:
 - **WanIn** – zpracování provozu přicházejícího z WAN na router
 - **WanForwIn** – zpracování provozu přicházejícího z WAN skrz router (například port forwarding)
 - **WanForwOut** – zpracování provozu odcházejícího směrem do WAN

- Tento přístup umožňuje snadnější správu a rozšíření firewallu v budoucnosti a zároveň šetří jeho zdroje.

Použitá konfigurace firewallu splňuje zásady segmentace sítě, zajišťuje základní ochranu před skenováním a útoky z Internetu a zároveň umožňuje efektivní řízení provozu (například prioritizace Teamsu). Důraz byl kladen na výkon (FastTrack) i bezpečnost (blokace neautorizovaného přístupu).

10.14 QoS

Pro zajištění vyšší kvality služby v síti byl na routeru MikroTik implementován mechanismus pro prioritizaci datového provozu. Cílem bylo zajistit dostatečnou šířku pásma a nízkou latenci pro Microsoft Teams a zároveň rozdělit dostupnou konektivitu mezi běžný upload a download.

10.14.1 Mangle

Prvním krokem bylo použití mangle pravidel, která umožňují označit pakety podle typu provozu. Následně lze s označenými pakety pracovat v QoS.

Mangle pravidla byla vytvořena v sekci IP v záložce Firewall a podzáložce Mangle. Konfigurace probíhá podobně jako ve Filter Rules.

Výsledná konfigurace mangle vypadá následovně.

```
[admin@mikrotik] > /ip/firewall/mangle/ print
Flags: X - disabled, I - invalid; D - dynamic
0 D ;; special dummy rule to show fasttrack counters
  chain=prerouting action=passthrough

1 D ;; special dummy rule to show fasttrack counters
  chain=forward action=passthrough

2 D ;; special dummy rule to show fasttrack counters
  chain=postrouting action=passthrough

3 ;; WanForwIn_Jump
  chain=forward action=jump jump-target=WanForwIn in-interface-list=WAN log=no log-prefix=""

4 ;; WanForwOut_Jump
  chain=forward action=jump jump-target=WanForwOut out-interface-list=WAN log=no log-prefix=""

5 ;; Voice
  chain=WanForwIn action=mark-packet new-packet-mark=VoiceDownload passthrough=no src-address-list=Voice log=no log-prefix=""

6 ;; Voice
  chain=WanForwOut action=mark-packet new-packet-mark=VoiceUpload passthrough=no dst-address-list=Voice log=no log-prefix=""

7 ;; Upload
  chain=WanForwOut action=mark-packet new-packet-mark=Upload passthrough=no log=no log-prefix=""

8 ;; Download
  chain=WanForwIn action=mark-packet new-packet-mark=Download passthrough=no log=no log-prefix=""
```

Obrázek 38 Výpis mangle

Pro QoS byly vytvořeny čtyři značky paketů:

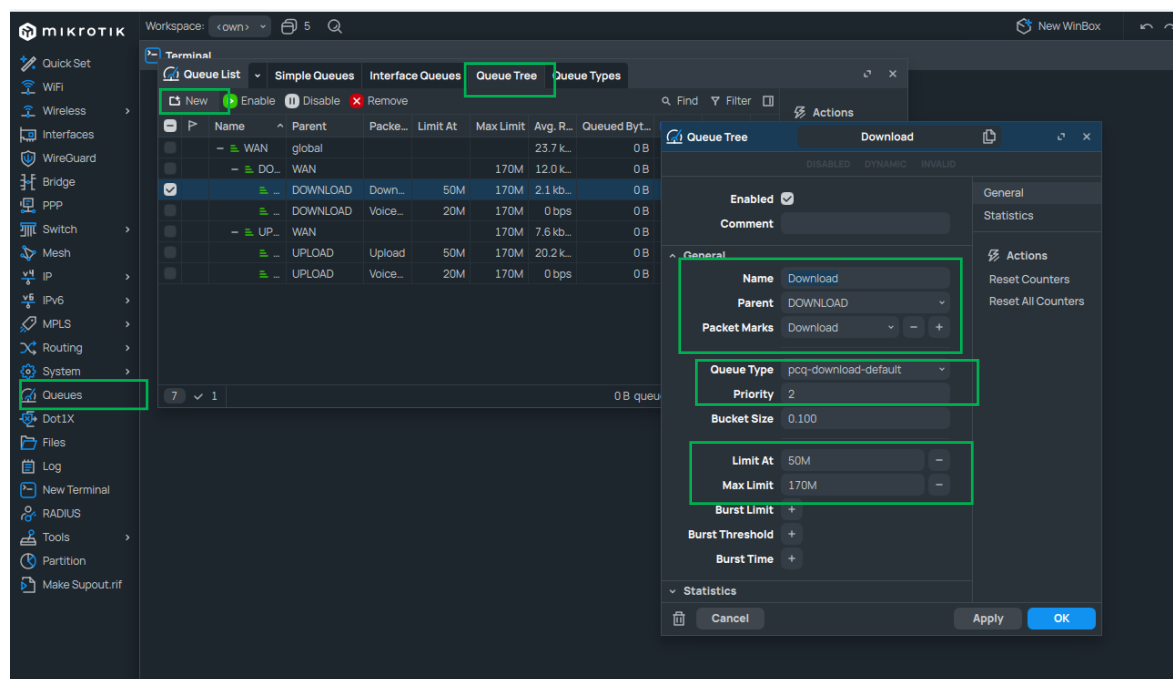
- **VoiceDownload** – příchozí provoz Microsoft Teams

- **VoiceUpload** – odchozí provoz Microsoft Team
- **Download** – běžný příchozí provoz
- **Upload** – běžný odchozí provoz

10.14.2 QoS Tree

Po označení paketů byla nastavena hierarchie front pomocí Queue Tree, což umožňuje efektivní řízení šířky pásma a prioritizaci provozu.

Jednotlivé stromy byly vytvořeny v sekci Queues v záložce Queue tree, kde byly specifikovány parametry jako typ fronty, maximální rychlost, garantovaná rychlost, priorita, označení paketů, rodič a jméno.



Obrázek 39 Vytvoření QoS tree

Pro řízení provozu byla použita fronta typu PCQ.

Byly vytvořeny dvě hlavní větve – DOWNLOAD a UPLOAD – každá s maximální kapacitou 170 Mbit/s, odpovídající rychlosti internetového připojení, sníženého o 15 %, což je podle mých zkušeností optimální hodnota, pokud chceme zajistit správné fungování minimální garantované rychlosti.

Uvnitř těchto větví byly definovány dílčí fronty:

- VoiceDownload / VoiceUpload

- minimální garantovaná šířka pásma 20 Mbit/s
- priorita 1 (nejvyšší)
- Download / Upload
- minimální garantovaná šířka pásma 50 Mbit/s
- priorita 2

	Name	Parent	Packet Marks	Limit At	Max Limit	Avg. R...	Queued Byt...	Bytes	Packets
[-]	WAN	global				115.9...	0 B	1916...	2 480 ...
[-]	[-] DOWNLOAD	WAN			170M	61.6 k...	0 B	1786...	1 660 ...
	[-] Download	DOWNLOAD	Download	50M	170M	57.2 k...	0 B	1776...	1 646 ...
	[-] VoiceDownload	DOWNLOAD	VoiceDownload	20M	170M	0 bps	0 B	10.0 ...	13 425 ...
[-]	[-] UPLOAD	WAN			170M	44.6 k...	0 B	129.7...	819 8...
	[-] Upload	UPLOAD	Upload	50M	170M	54.1 k...	0 B	128.5...	810 8...
	[-] VoiceUpload	UPLOAD	VoiceUpload	20M	170M	0 bps	0 B	1283...	9 018 ...

Obrázek 40 Výpis QoS tree

Tato konfigurace zajišťuje, že provoz aplikace Microsoft Teams má vždy přednost před běžným datovým provozem, zejména v případě zahlcení linky.

10.15 CAPsMAN

Pro správu bezdrátových sítí byla použita služba CAPsMAN, která umožňuje centrální řízení všech přístupových bodů v síti. Mimo jiné umožňuje také tvorbu virtuálních SSID, díky čemuž lze na jednom fyzickém rozhraní provozovat více bezdrátových sítí současně.

Konfigurace CAPsMANu byla provedena v sekci wireless a v záložce CAPsMAN.

10.15.1 Security

Pro každou síť byla vytvořena samostatná bezpečnostní politika:

- **staff** – autentizace pomocí WPA2-PSK s šifrováním AES-CCM.
- **guest** – autentizace pomocí WPA2-PSK s šifrováním AES-CCM.

10.15.2 Datapath

Datapath určuje způsob, jakým jsou bezdrátová data přenášena mezi klienty a zbytkem sítě.

Byly vytvořeny dva datapath profily:

- **staff** – bylo povoleno přeposílání mezi klienty (client-to-client forwarding=yes), použit byl bridge LAN-Wifi a zapnuto lokální směrování (local-forwarding=yes).

- **guest** – přeposílání mezi klienty bylo zakázáno, lokální směrování bylo deaktivováno. Pro oddělení sítě byl použit VLAN ID 21 a režim přenosu use-tag.

10.15.3 Rates

V podzáložce Rates byl vytvořen vlastní profil rychlostí s následujícím nastavením:

- Název profilu: rate
- Základní rychlost (basic): 12 Mbps
- Podporované rychlosti (supported): 12 Mbps, 18 Mbps, 24 Mbps

Toto nastavení omezuje použití pouze na vyšší přenosové rychlosti a tím zajišťuje vyšší stabilitu a výkon bezdrátové sítě.

10.15.4 Configuration

Byly vytvořeny čtyři samostatné konfigurace bezdrátových sítí:

- **staff_5** – síť Staff na frekvenčním pásmu 5 GHz s vypnutým rozšířeným kanálem (extension-channel=disabled).
- **staff_2.4** – síť Staff na frekvenčním pásmu 2,4 GHz s vypnutým rozšířeným kanálem.
- **guest_5** – síť Guest na frekvenčním pásmu 5 GHz s rozšířeným kanálem (extension-channel=XXXX) a šířkou řídicího kanálu 20 MHz.
- **guest_2.4** – síť Guest na frekvenčním pásmu 2,4 GHz.

Ve všech případech bylo jako umístění zvoleno indoor a země nastavena na Czech Republic.

Tyto konfigurace byly vytvořeny v sekci Wireless v záložce CAPsMAN a podzáložce configuration, kde bylo k dané konfiguraci přiřazeno nastavení, jako je SSID, jméno konfigurace, pásmo, security profil, datapath a jiné.

Pro připojení AP k serveru CAPsMAN bylo zapotřebí podržet tlačítko Reset po dobu, než kontrolka napájení přestala blikat. Poté bylo zařízení automaticky restartováno, vyhledalo CAPsMAN server a navázalo s ním spojení. Následně byly k přístupovému bodu přiřazeny příslušné Wi-Fi konfigurace a tím bylo jeho nastavení úspěšně dokončeno.

10.16 Services

Na závěr byly v sekci IP v záložce Services deaktivovány nepotřebné služby Telnet, API a API-SSL, aby tyto možnosti správy nebyly zbytečně aktivní a neotevíraly potenciální bezpečnostní rizika.

11. AUTOMATIZACE ZÁLOHOVÁNÍ POMOCÍ PYTHONU

Pro zajištění pravidelného zálohování konfigurace MikroTik routerů a minimalizaci rizika ztráty konfigurace byla implementována automatizace procesu zálohování pomocí skriptu v programovacím jazyce Python. Tato automatizace umožnila snadné hromadné zálohování většího množství zařízení bez nutnosti manuálních zásahů správce.

11.1 Použité technologie

Pro realizaci zálohovacího skriptu byly využity následující knihovny:

- Netmiko – knihovna usnadňující připojení k síťovým zařízením přes SSH a odesílání příkazů (využita pro ovládání RouterOS).
- Paramiko – knihovna zajišťující přenos souborů pomocí SFTP (využita pro stažení zálohovaného souboru).
- Multiprocessing – standardní Python knihovna umožňující paralelní zpracování více zařízení současně (urychlení záloh více routerů).
- OS, JSON, datetime – standardní Python knihovny použité pro práci se souborovým systémem, konfigurací a časem.

11.2 Popis implementace

Skript umožnil provedení následujících kroků:

- **Načtení seznamu routerů** – byly načteny IP adresy routerů ze souboru routers.json, který obsahoval seznam zálohovaných zařízení ve formátu JSON.
- **Navázání SSH připojení** – pro každé zařízení bylo navázáno SSH připojení pomocí knihovny Netmiko, přihlašovací údaje byly načteny z proměnných prostředí.
- **Zjištění základních informací o zařízení** – ze zařízení byly získány informace o názvu (hostname) a modelu routeru, které byly následně použity v názvu zálohovacího souboru.
- **Vytvoření zálohy na routeru** – na routeru byl spuštěn příkaz `/system backup save`, čímž byla vytvořena záloha aktuální konfigurace do souboru ve formátu backup.

- **Stažení zálohy do lokálního úložiště** – pomocí knihovny Paramiko (SFTP) byl zálohovací soubor stažen z routeru do předem definovaného lokálního adresáře mikrotik_backups.
- **Paralelní zpracování** – pro urychlení procesu byly zálohy jednotlivých zařízení prováděny paralelně pomocí knihovny multiprocessing (10 paralelních procesů).

11.3 Výsledná konfigurace skriptu

Níže je uveden přehled klíčových parametrů skriptu:

- Zálohy byly ukládány do složky: mikrotik_backups
- Název záloh obsahoval: hostname zařízení, model zařízení, datum a čas zálohy (například MainRouter_RB4011_20250506_150045.backup)
- Seznam routerů: routers.json (formát: ["192.168.88.1", "192.168.89.1", ...])
- Počet paralelních procesů: 10
- 10.12.4 Výhody navrženého řešení
- Automatizace – celý proces zálohování probíhal bez nutnosti manuálního zásahu.
- Redundance a bezpečnost – zálohy byly pravidelně ukládány na bezpečné úložiště.
- Škálovatelnost – bylo možné snadno přidávat další zařízení bez změn ve skriptu.
- Přehlednost – názvy záloh obsahovaly všechny důležité informace o zařízení a čase zálohy.

Tímto způsobem byla dokončena implementace automatizovaného systému zálohování konfigurací MikroTik routerů. Výsledné řešení umožnilo snadné a spolehlivé hromadné zálohování všech síťových zařízení bez nutnosti manuálních zásahů správce.

ZÁVĚR

Cílem této práce bylo navrhnout a realizovat moderní, bezpečnou a rozšiřitelnou síťovou infrastrukturu pro firmu střední velikosti s ohledem na současné i budoucí potřeby organizace. Na základě provedené analýzy a vyhodnocení požadavků byl navržen a implementován komplexní návrh zahrnující segmentaci sítě pomocí VLAN, zabezpečený vzdálený přístup prostřednictvím VPN, redundantní připojení k Internetu a centrální správu bezdrátových sítí.

V rámci praktické části byl realizován návrh a konfigurace hlavních síťových prvků s využitím směrovače MikroTik RB5009UPr+S+, switche, centrálního rozvaděče a záložního napájení. Byla implementována pravidla firewallu, rozdělení sítě do logických celků pomocí VLAN, VPN přístup pro zaměstnance a správce pomocí WireGuard a failover mechanismus pro zajištění vysoké dostupnosti internetového připojení.

Dále byla navržena a realizována automatizace zálohování konfigurací síťových zařízení pomocí skriptu v jazyce Python, což přispělo k efektivnější správě sítě a zvýšení bezpečnosti. Celá síť byla navržena tak, aby umožňovala snadné rozšíření a přizpůsobení budoucím potřebám firmy, včetně možnosti připojení nových pracovišť.

Navržené řešení přineslo následující přínosy:

- Dostatečná bezpečnost díky segmentaci sítě, centrálnímu firewallu a pravidlům řízení přístupu.
- Zajištění vysoké dostupnosti služeb pomocí redundantního připojení a failover mechanismu.
- Jednoduchá správa sítě díky centralizované konfiguraci a automatizaci záloh.
- Předpoklady pro budoucí rozšíření bez nutnosti zásadních zásahů do infrastruktury.
- Kvalitní bezdrátové připojení díky centrální správě přístupových bodů.

Práce tak splnila stanovené cíle a přispěla k vytvoření stabilního a bezpečného síťového prostředí vhodného pro každodenní provoz firmy i její další rozvoj.

SEZNAM POUŽITÉ LITERATURY

- [1] Nováček, Šimon. Lekce 1 - Sítě – Typy používaných sítí. [online]. ITnetwork.cz, [cit. 1. 1. 2025]. Dostupné z: <https://www.itnetwork.cz/site/zaklady/site-typy-pouzivanych-siti>
- [2] LAMMLE, Todd. CCNA – výukový průvodce. 4. akt. vyd. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.
- [3] FORTINET. FortiNAC – Network Access Control [online]. [cit. 12. 1. 2025] Dostupné z: <https://www.fortinet.com/products/network-access-control>
- [4] Klusaitė, Laura. What are IP address classes, and how are they used? [online]. NordVPN, 6. března 2025 [cit. 8.4. 2025]. Dostupné z: <https://nordvpn.com/blog/ip-address-classes/>
- [5] Amazon Web Services. What is Border Gateway Protocol? [online]. [cit. 25. 1. 2025]. Dostupné z: <https://aws.amazon.com/what-is/border-gateway-protocol/>
- [6] CLOUDFLARE. Round-robin DNS [online]. [cit. 18. 2. 2025]. Dostupné z: <https://www.cloudflare.com/learning/dns/glossary/round-robin-dns/>
- [7] Cloudflare. What is dynamic DNS (DDNS)? [online]. [cit. 20. 2. 2025]. Dostupné z: <https://www.cloudflare.com/learning/dns/glossary/dynamic-dns/>
- [8] MikroTik. NAT. [online]. [cit. 25. 2. 2025]. Dostupné z: <https://help.mikrotik.com/docs/spaces/ROS/pages/3211299/NAT>
- [9] MikroTik. Queues. [online]. [cit. 26. 2. 2025]. Dostupné z: <https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues>
- [10] MikroTik. Queue Burst. [online]. [cit. 13. 2. 2025]. Dostupné z: <https://help.mikrotik.com/docs/spaces/ROS/pages/137986091/Queue+Burst>
- [11] KRČMÁŘ, Petr. WireGuard: moderní a snadno použitelná VPN v linuxovém jádře. Root.cz [online]. 23. 5. 2019 [cit. 8. 4. 2025]. Dostupné z: <https://www.root.cz/clanky/wireguard-moderni-a-snadno-pouzitelna-vpn-v-linuxovem-jadre/>
- [12] WIREGUARD. WireGuard VPN. [online]. [cit. 2. 3. 2025]. Dostupné z: <https://www.wireguard.com/>

- [13] MIKROTIK. WireGuard. [online]. [cit. 8. 3. 2025]. Dostupné z: <https://help.mikrotik.com/docs/spaces/ROS/pages/69664792/WireGuard>
- [14] GLOBYTĚ, Ema. What is PPTP (Point-to-Point Tunneling Protocol). [online]. NordVPN, 16. srpna 2023 [cit. 8. 4. 2025]. Dostupné z: <https://nordvpn.com/blog/what-is-pptp-protocol/>
- [15] MIKLE, Ondrej. Rozdělení a panuj: hrubou silou na MS-CHAPv2 klíče. [online]. Root.cz, 13. srpna 2012 [cit. 8. 4. 2025]. Dostupné z: <https://www.root.cz/clanky/rozdeleni-a-panuj-hrubou-silou-na-ms-chapv2-klice/>
- [16] NOCTION. Multihoming – a complete step-by-step Guide [online]. [cit. 16. 2. 2025]. Dostupné z: <https://www.noction.com/knowledge-base/multihoming>
- [17] CLOUDFLARE. What is a reverse proxy? [online]. [cit. 16. 2. 2025]. Dostupné z: <https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/>
- [18] MIKROTIK. About Us [online]. [cit. 18. 2. 2025]. Dostupné z: <https://mikrotik.com/aboutus>
- [19] MIKROTIK. Product Naming [online]. [cit. 20. 2. 2025]. Dostupné z: <https://help.mikrotik.com/docs/spaces/ROS/pages/17498146/Product+Naming>
- [20] MIKROTIK. Download Center [online]. [cit. 22. 2. 2025]. Dostupné z: <https://mikrotik.com/download>
- [21] MIKROTIK. Software Specifications [online]. [cit. 22. 2. 2025]. Dostupné z: <https://help.mikrotik.com/docs/spaces/ROS/pages/19136707/Software+Specifications#SoftwareSpecifications-HardwareSupport>
- [22] MIKROTIK. API [online]. [cit. 25. 2. 2025]. Dostupné z: <https://help.mikrotik.com/docs/spaces/ROS/pages/47579160/API>
- [23] MIKROTIK. Filter [online]. [cit. 2. 3. 2025]. Dostupné z: <https://help.mikrotik.com/docs/spaces/ROS/pages/48660574/Filter>.
- [24] MIKROTIK. Packet Flow in RouterOS [online]. [cit. 2. 3. 2025]. Dostupné z: <https://help.mikrotik.com/docs/spaces/ROS/pages/328227/Packet+Flow+in+RouterOS>
- [25] MIKROTIK. Common Firewall Matchers and Actions [online]. [cit. 8. 4. 2025]. Dostupné z:

<https://help.mikrotik.com/docs/spaces/ROS/pages/250708064/Common+Firewall+Matchers+and+Actions>

[26] MIKROTIK. Mangle [online]. [cit. 8. 4. 2025]. Dostupné z: <https://help.mikrotik.com/docs/spaces/ROS/pages/48660587/Mangle>

[27] MIKROTIK. RouterOS license keys [online]. [cit. 8. 4. 2025]. Dostupné z: <https://help.mikrotik.com/docs/spaces/ROS/pages/328149/RouterOS+license+keys>

SEZNAM OBRÁZKŮ

Obrázek 1 Přehled rychlostí VPN protokolů [11].....	24
Obrázek 2 Rozhraní aplikace Winbox	31
Obrázek 3 Webové rozhraní RouteOs	32
Obrázek 4 Rozhraní aplikace Mikrotik Pro	33
Obrázek 5 Rozhraní aplikace Mikrotik Home	34
Obrázek 6 Zjednodušené schéma sítě	46
Obrázek 7 Výpis nalezených zařízení	47
Obrázek 8 Výchozí konfigurace	47
Obrázek 9 Změna hesla.....	48
Obrázek 10 Výpis nainstalovaných balíčků.....	49
Obrázek 11 Výpis dostupných balíčků na webu Mikrotik.....	50
Obrázek 12 Záložka Resources.....	51
Obrázek 13 Restart.....	52
Obrázek 14 Záložka RouterBOARD	53
Obrázek 15 Hostname.....	54
Obrázek 16 Založení bridge.....	55
Obrázek 17 Přidání portu do bridge.....	56
Obrázek 18 Přidání portu do listu	57
Obrázek 19 NTP server.....	58
Obrázek 20 NTP klient	58
Obrázek 21 DNS	59
Obrázek 22 Hostovská VLAN	60
Obrázek 23 PPOE	61
Obrázek 24 Statické IPv4 adresy	62
Obrázek 25 Dynamické IPv4 adresy.....	63
Obrázek 26 Vytvoření sítě pro DHCP	64
Obrázek 27 IPv4 pool	65
Obrázek 28 DHCP server.....	66
Obrázek 29 Routy	67
Obrázek 30 Maškaráda.....	68
Obrázek 31 Failover skript.....	69
Obrázek 32 Nastavení SMTP.....	70
Obrázek 33 Failover scheduler	70
Obrázek 34 Wireguard rozhraní.....	71

Obrázek 35 Wireguard peer	72
Obrázek 36 Vytvoření filter rule	73
Obrázek 37 Výpis filter rules	74
Obrázek 38 Výpis mangle	76
Obrázek 39 Vytvoření QoS tree	77
Obrázek 40 Výpis QoS tree	78

SEZNAM TABULEK

Tabulka 1 Přehled licencí RouteOs [27]	39
Tabulka 2 IPv4 adresy routeru	61
Tabulka 3 Routy	66

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

API	Application Programming Interface
ARM	Advanced RISC Machine
BGP	Border Gateway Protocol
CAPsMAN	Controlled Access Point system Manager
CHAPv2	Microsoft Challenge-Handshake Authentication Protocol version 2
CPU	Central Processing Unit
DDNS	Dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EGP	Exterior Gateway Protocol
FIFO	First In First Out
FTP	File Transfer Protocol
GAN	Global Area Network
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
MMIPS	Microprocessor without Interlocked Pipeline Stages Micro
mPCI	Mini PCI
mPCIe	Mini PCI Express

MIPSBE	Microprocessor without Interlocked Pipeline Stages Big Endian
NAC	Network Access Control
NAC	Network Address Translation
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PCIe	PCI Express
PCQ	Per Connection Queuing
PoE	Power over Ethernet
PPC	PowerPC
PPTP	Point-to-Point Tunneling Protocol
PRTG	Paessler Router Traffic Grapher
QoS	Quality of Service
RED	Random Early Detect
RIP	Routing Information Protocol
SFQ	Stochastic Fairness Queuing
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SMIPS	Small MIPS
SSH	Secure Shell
SSD	Solid State Drive
TCP	Transmission Control Protocol
TILE	Tilera Multicore Architecture
TTL	Time To Live
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus

VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
x86	Intel x86 Architecture

SEZNAM PŘÍLOH

Příloha P I: Výpis konfigurace MikroTik RouterOS

Příloha P 2: Python skript pro zálohování

PŘÍLOHA P I: VÝPIS KONFIGURACE MIKROTIK ROUTEROS

Tato příloha obsahuje export konfiguračního souboru zařízení MikroTik použitého v praktické části práce. Přílohu lze nalézt v přiloženém souboru.

PŘÍLOHA P 2: PYTHON SKRIPT PRO ZÁLOHOVÁNÍ

Tato příloha obsahuje Python skript, popsany v praktické části, který slouží k automatickému zálohování konfigurace MikroTik. Přílohu lze nalézt v přiloženém souboru.