

Univerzita Pardubice  
Fakulta ekonomicko-správní

Současné trendy v bezdrátových datových sítích z pohledu využití ve firmě

Diplomová práce

2024

Bc. Jiří Koula

Univerzita Pardubice  
Fakulta ekonomicko-správní  
Akademický rok: 2023/2024

# ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Bc. Jiří Koula**  
Osobní číslo: **E22454**  
Studijní program: **N0688A140007 Informatika a systémové inženýrství**  
Specializace: **Informační a bezpečnostní systémy**  
Téma práce: **Současné trendy v bezdrátových datových sítích z pohledu využití ve firmě**  
Zadávací katedra: **Ústav systémového inženýrství a informatiky**

## Zásady pro vypracování

**Cílem práce je vytvořit návrh bezdrátové datové sítě pro modelový subjekt v několika variantách s využitím moderních vysokorychlostních technologií.**

**Osnova:**

- Identifikovat možnosti vhodných bezdrátových technologií.
- Sestavit návrh v několika variantách.
- Porovnat a zhodnotit jednotlivé varianty.

Rozsah pracovní zprávy: **cca 50 stran**  
Rozsah grafických prací:  
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.  
KIZZA, Joseph Migga. Guide to computer network security. Fourth edition. Cham, Switzerland: Springer-Verlag, 2017. Computer communications and networks. ISBN 978-3-319-55605-5.  
GAST, Matthew S. 802.11ac: A Survival Guide: Wi-Fi at Gigabit and Beyond. USA: O'Reilly Media, 2013. ISBN 978-1449343149.  
SATRAPA, Pavel. IPv6: internetový protokol verze 6. 4. aktualizované a rozšířené vydání. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-43-0.

Vedoucí diplomové práce: **RNDr. Ing. Oldřich Horák, Ph.D.**  
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **1. září 2023**  
Termín odevzdání diplomové práce: **30. dubna 2024**

**prof. Ing. Jan Stejskal, Ph.D. v.r.**  
děkan

L.S.

**prof. Ing. Jitka Komárková, Ph.D. v.r.**  
garant studijního programu

V Pardubicích dne 1. září 2023

Prohlašuji:

Práci s názvem Současné trendy v bezdrátových datových sítích z pohledu využití ve firmě jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 4. 2024

Bc. Jiří Koula v. r.

## **PODĚKOVÁNÍ**

Chtěl bych poděkovat své rodině a přítelkyni za podporu a trpělivost při studích. Dále bych chtěl poděkovat vedoucímu práce RNDr. Ing. Oldřichovi Horákovi, Ph.D. za cenné rady a odborné vedení, které mi poskytl. Také bych chtěl poděkovat Markovi Stejskalovi za odborné konzultace a zapůjčení síťových zařízení.

## **ANOTACE**

Tato diplomová práce se zabývá návrhem bezdrátové sítě pro modelový subjekt, a to celkem ve třech variantách, který využívá moderních vysokorychlostních technologií za účelem zvýšení rychlosti, spolehlivosti a snížení latence. V práci jsou nejprve shrnuty náležitosti, které jsou nezbytné pro provoz těchto bezdrátových sítí. V textu jsou dále prezentovány příklady využití těchto technologií ve světě. Práce obsahuje detailní popis konfigurace přijímové antény, routeru, switchu a přístupových bodů od výrobců MikroTik, TP-Link, Ruijie Networks a Ubiquiti pracujících s mesh technologií. Nakonec je provedeno ekonomické zhodnocení a vyhodnocení nasazení síťových prvků.

## **KLÍČOVÁ SLOVA**

bezdrátové sítě, Wi-Fi 6, IEEE 802.11ax, zabezpečení sítě, přístupový bod

## **TITLE**

Current trends in wireless data networks from the perspective of enterprise use

## **ANNOTATION**

This thesis deals with the design of a wireless network for a model entity in a total of three variants, using modern high-speed technologies to increase speed, reliability and reduce latency. The thesis first summarizes the essentials that are necessary for the operation of these wireless networks. Examples of the use of these technologies in the world are then presented. The thesis includes a detailed description of the configuration of the receiving antenna, router, switch and access points from manufacturers MikroTik, TP-Link, Ruijie Networks and Ubiquiti working with mesh technology. Finally, an economic evaluation and assessment of the deployment of network elements is carried out.

## **KEYWORDS**

wireless networking, Wi-Fi 6, IEEE 802.11ax, network security, access point

# OBSAH

SEZNAM OBRÁZKŮ A TABULEK .....	10
SEZNAM ZKRATEK A ZNAČEK .....	13
ÚVOD.....	16
1 Současný stav bezdrátových sítí v ČR.....	17
1.1 Struktura přístupu k internetu .....	17
1.2 Legislativa bezdrátového připojení v ČR .....	18
1.2.1 Podmínky využívání pásma 60 GHz .....	19
1.2.2 Podmínky využívání pásma 6 GHz .....	20
2 Bezdrátové sítě.....	21
2.1 Frekvenční pásma .....	21
2.1.1 Frekvenční pásmo 2,4 GHz .....	21
2.1.2 Frekvenční pásmo 5 GHz .....	21
2.1.3 Frekvenční pásmo 6 GHz .....	21
2.1.4 Frekvenční pásmo 60 GHz .....	21
2.2 Standardy IEEE 802.11.....	22
2.2.1 IEEE 802.11ac .....	22
2.2.2 IEEE 802.11ad.....	22
2.2.3 IEEE 802.11ax.....	22
2.2.4 IEEE 802.11be.....	23
2.2.5 Shrnutí rozdílů a inovací.....	23
2.3 Wi-Fi 6/6E .....	23
2.3.1 OFDMA.....	24
2.3.2 MU-MIMO .....	24
2.3.3 1024-QAM.....	25
2.3.4 BSS Color .....	26
2.3.5 TWT.....	26

2.4	Síťová topologie mesh .....	27
2.5	IPv4 .....	28
2.6	IPv6 .....	29
2.6.1	Adresní prostor a datagram .....	29
2.6.2	Adresování a zabezpečení místní sítě .....	30
2.7	Zabezpečení bezdrátových sítí .....	30
2.7.1	Bezpečnostní protokoly WPA2 a WPA3 .....	31
2.7.2	Firewall .....	32
2.8	Moderní bezdrátové technologie ve světě .....	33
2.8.1	Oblast vzdělání .....	33
2.8.2	Oblast zdravotnictví .....	33
2.8.3	Oblast veřejných prostor .....	34
3	Popis a analýza výchozího stavu .....	35
4	Návrhy bezdrátové počítačové sítě .....	39
4.1	Návrh sdílených síťových prvků .....	39
4.1.1	Popis routeru MikroTik RB1100AHx2 .....	41
4.1.2	Popis switchu TP-Link TL-SG2428P .....	41
4.1.3	Popis UPS ADLER .....	42
4.2	Konfigurace sdílených síťových prvků .....	44
4.2.1	Konfigurace routeru MikroTik RB1100AHx2 .....	44
4.2.2	Konfigurace switchu TP-Link TL-SG2428P .....	46
4.3	Modelová varianta I. (MikroTik & TP-Link) .....	48
4.3.1	Konfigurace přijímové antény MikroTik Wire nRAY 60 GHz .....	48
4.3.2	Konfigurace Wi-Fi 6 mesh sítě TP-Link .....	52
4.4	Modelová varianta II. (Ubiquiti) .....	56
4.4.1	Konfigurace přijímové antény Ubiquiti UISP Wave Nano 60 GHz .....	56
4.4.2	Konfigurace Wi-Fi 6E mesh sítě Ubiquiti .....	60



4.5	Modelová varianta III. (Ubiquiti & Reyee) .....	64
5	Ekonomické náklady a zhodnocení přínosu .....	68
	ZÁVĚR .....	71
	POUŽITÁ LITERATURA .....	72
	PŘÍLOHY .....	79

## SEZNAM OBRÁZKŮ A TABULEK

Obrázek 1 – Mapa z portálu RLAN ČTÚ.....	20
Obrázek 2 – OFDMA .....	24
Obrázek 3 – MU-MIMO.....	25
Obrázek 4 – Porovnání 256-QAM a 1024-QAM .....	25
Obrázek 5 – BSS Coloring.....	26
Obrázek 6 – Infrastruktura mesh topologie .....	27
Obrázek 7 – Sít'ová topologie .....	38
Obrázek 8 – Rozvaděč XtendLan WS-15U-64-BLACK-U .....	40
Obrázek 9 – Rozmístění prvků v rozvaděči.....	40
Obrázek 10 – MikroTik RB1100AHx2 .....	41
Obrázek 11 – TP-Link TL-SG2428P.....	42
Obrázek 12 – Offline systém UPS .....	43
Obrázek 13 – UPS ADLER 400 W .....	43
Obrázek 14 – MikroTik Wire nRAY 60 GHz .....	48
Obrázek 15 – Přidání rozhraní do bridge.....	49
Obrázek 16 – Wireless nastavení.....	50
Obrázek 17 – Sít'ový provoz.....	51
Obrázek 18 – TP-Link EAP610.....	52
Obrázek 19 – URL Filtering .....	54
Obrázek 20 – Ubiquiti UISP Wave Nano 60 GHz .....	56
Obrázek 21 – Návrh v UISP Design Center .....	57
Obrázek 22 – Nastavení bezdrátového módu .....	58
Obrázek 23 – Hodnoty signálu antény.....	59
Obrázek 24 – Ubiquiti UniFi U6 Enterprise .....	60
Obrázek 25 – Nastavení rádii.....	62
Obrázek 26 – Reyee RG-RAP2260(G).....	64
Obrázek 27 – Seznam zařízení.....	65
Obrázek 28 – Nastavení parametrů vysílání .....	66
Obrázek 29 – Blokové schéma RB1100AHx2 .....	82
Obrázek 30 – Připojení k routeru v aplikaci WinBox .....	83
Obrázek 31 – Úvodní informace o nastavení a menu WinBox .....	83
Obrázek 32 – Nastavení uživatele .....	84

Obrázek 33 – Nastavení názvu zařízení.....	84
Obrázek 34 – Vytvoření rozhraní bridge .....	85
Obrázek 35 – Přidání rozhraní do bridge.....	85
Obrázek 36 – Nastavení IP adres .....	86
Obrázek 37 – Nastavení výchozí brány .....	86
Obrázek 38 – Nastavení DHCP serveru .....	87
Obrázek 39 – Nastavení služeb.....	87
Obrázek 40 – Nastavení firewallu .....	88
Obrázek 41 – Nastavení DNS.....	88
Obrázek 42 – Nastavení NTP serveru.....	89
Obrázek 43 – Nastavení IP adresy switche.....	89
Obrázek 44 – Nastavení výchozí brány switche .....	89
Obrázek 45 – Nastavení PoE portů switche.....	90
Obrázek 46 – Nastavení NTP serverů switche .....	90
Obrázek 47 – Nastavení uživatele .....	92
Obrázek 48 – Nastavení názvu zařízení.....	92
Obrázek 49 – Vytvoření rozhraní bridge .....	93
Obrázek 50 – Nastavení IPv4 adresy .....	93
Obrázek 51 – Povolení balíčku IPv6 .....	94
Obrázek 52 – Nastavení IPv6 adresy .....	94
Obrázek 53 – Nastavení výchozí brány .....	94
Obrázek 54 – Nastavení DNS serverů .....	95
Obrázek 55 – Nastavení NTP serverů.....	95
Obrázek 56 – Bezdrátové hodnoty připojení .....	96
Obrázek 57 – Update firmware zařízení .....	96
Obrázek 58 – Omada Software Controller .....	96
Obrázek 59 – Nastavení přihlašovacích údajů.....	97
Obrázek 60 – Popis záložek nastavení Omada .....	97
Obrázek 61 – Nastavení kontroleru .....	98
Obrázek 62 – Nastavení karty Wireless Networks .....	99
Obrázek 63 – Přidání AP do kontroleru.....	100
Obrázek 64 – Nastavení IP adresy AP .....	100
Obrázek 65 – Nastavení frekvencí a šířky kanálu .....	101
Obrázek 66 – Síťová nastavení .....	101

Obrázek 67 – Nastavení DNS .....	102
Obrázek 68 – Nastavení NTP serveru.....	102
Obrázek 69 – Aktualizace firmware .....	102
Obrázek 70 – Port Management .....	103
Obrázek 71 – Kapacita rádií .....	103
Obrázek 72 – Test rychlosti .....	103
Obrázek 73 – Seznam zařízení UniFi .....	104
Obrázek 74 – Skenování kanálů .....	105
Obrázek 75 – Nastavení sítě .....	106
Obrázek 76 – Nastavení Wi-Fi .....	107
Obrázek 77 - Síťová nastavení.....	108
Obrázek 78 – Nastavení Wi-Fi .....	109
Obrázek 79 – Omezení rychlosti koncového zařízení .....	110
Obrázek 80 – Omezení rychlosti dle SSID .....	110
Obrázek 81 – Reye Mesh .....	110
Obrázek 82 – Připojená zařízení .....	111
Obrázek 83 – Úvodní obrazovka nastaveného AP .....	111
Tabulka 1 – Vybrané radiové kmitočty využívané v praktické části.....	19
Tabulka 2 – Údaje k využívání rádiových kmitočtů pro vysokorychlostní spoje typu bod-bod .....	19
Tabulka 3 – Shrnutí rozdílů jednotlivých standardů.....	23
Tabulka 4 – Porovnání WPA2 a WPA3 .....	32
Tabulka 5 – Srovnání vybíraných routerů .....	36
Tabulka 6 – Srovnání vybíraných switchů .....	37
Tabulka 7 – Použité sdílené síťové prvky .....	39
Tabulka 8 – Parametry nastavení DHCP serveru .....	45
Tabulka 9 – Ekonomické náklady .....	68
Graf 1 – Vývoj počtu služeb přístupu k internetu dle technologií.....	17
Graf 2 – Vývoj počtu přístupů k internetu prostřednictvím bezdrátových technologií Wi-Fi dle inzerované rychlosti.....	18

## **SEZNAM ZKRATEK A ZNAČEK**

DSL	Digital Subscriber Line
VDSL	Very High Speed DSL
ADSL	Asymmetric Digital Subscriber Line
FTTH/B	Fiber To The Home/Building
LTE	Long Term Evolution
U-NII	Unlicensed National Information Infrastructure
DFS	Dynamic Frequency Selection
EIRP	Equivalent Isotropically Radiated Power
DSSS	Direct Sequence Spread Spectrum
OFDM	Orthogonal Frequency Division Multiplexing
MU-MIMO	Multi User Multiple Input Multiple Output
IEEE	Institute of Electrical and Electronics Engineers
QAM	Quadrature Amplitude Modulation
OFDMA	Orthogonal Frequency Division Multiple Access
CCA	Clear Channel Assessment
TWT	Target Wake-up Time
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IANA	Internet Assigned Numbers Authority
NAT	Network Address Translation
MAC	Media Access Control
WPA	Wi-Fi Protected Access
AES	Advanced Encryption Standard

TKIP	Temporal Key Integrity Protocol
PSK	Pre Shared Key
RADIUS	Remote Authentication Dial In User Service
AR	Augmented Reality
VR	Virtual Reality
LED	Light-Emitting Diode
PoE	Power over Ethernet
QoS	Quality of Service
SFP	Small Form-factor Pluggable
VLAN	Virtual Local Area Network
ACL	Access Control List
UPS	Uninterruptible Power Supply
MNDP	MikroTik Neighbor Discovery Protocol
WAN	Wide Area Network
DHCP	Dynamic Host Configuration Protocol
NTP	Network Time Protocol
R/STP	Rapid/Spanning Tree Protocol
LLDP	Link Layer Discovery Protocol
HTTPS	Hypertext Transfer Protocol Secure
SSID	Service Set Identifier
DNS	Domain Name System
RSSI	Received Signal Strength Indication
SOHO	Small Office/Home Office
VPN	Virtual Private Network

AP	Access Point
DFS	Dynamic Frequency Selection
PMF	Protected Management Frames
URL	Uniform Resource Locator
GUI	Graphical User Interface
MTU	Maximum Transmission Unit
PTMP	Point To MultiPoint
ARP	Address Resolution Protocol
IGMP	Internet Group Management Protocol

## ÚVOD

V dnešní době je pro firmy klíčové držet krok s neustálým vývojem technologií, které umožňují efektivnější komunikaci. Jedním z nejnápadnějších trendů v oblasti bezdrátových technologií jsou technologie Wi-Fi 6 a Wi-Fi 6E, která využívá přenosové pásmo 6 GHz. V rámci dvoubodových spojů jsou to síťová zařízení pracující na frekvenci 60 GHz. V kontextu rychlého technologického pokroku nabízí tato práce ucelené informace a doporučení, které mohou sloužit jako hodnotný průvodce pro firmy, které se snaží lépe porozumět a efektivně využít moderní bezdrátové technologie ve svém podnikání.

Práce se v první části zabývá analýzou současného stavu bezdrátových sítí v České republice, představuje strukturu přístupu k internetu a zkoumá legislativní aspekty využívání frekvenčních pásem 6 GHz a 60 GHz.

Teoretická část práce představuje bezdrátové sítě a jejich frekvenční pásma, včetně nejnovějšího standardu IEEE 802.11ax. V kapitole Wi-Fi 6/6E jsou detailně popsány jednotlivé technologie tohoto standardu. Další kapitoly teoretické části se zaměřují na síťovou topologii mesh, IPv4 a jeho nástupce IPv6. Další kapitola se věnuje zabezpečení bezdrátových sítí a představuje standard zabezpečení WPA3. Poslední kapitola této části se věnuje moderním bezdrátovým technologiím ve světě. Kapitola představuje několik vybraných scénářů nasazení vysokorychlostních bezdrátových technologií v různých institucích a firmách.

Ve třetí části této práce je prezentována výchozí situace v modelové firmě a popsána síťová topologie.

V praktické části je navržena bezdrátová počítačová síť. Nejprve je realizován návrh síťových prvků. Poté je provedena konfigurace hlavního routeru a switchu. Praktická část je následně rozdělena na tři modelové varianty, které obsahují konfiguraci přijímové antény pracující na frekvenci 60 GHz a bezdrátové Wi-Fi 6/6E mesh sítě.

V poslední kapitole práce jsou zhodnoceny navržené modelové varianty.

Cílem práce je vytvořit návrh bezdrátové datové sítě pro modelový subjekt v několika variantách s využitím moderních vysokorychlostních technologií a poskytnout ucelený pohled na využití moderních bezdrátových technologií ve firmách, přičemž se práce snaží nejen teoreticky popsat, ale i prakticky aplikovat tyto technologie s důrazem na jejich konkrétní využití ve firemním prostředí.

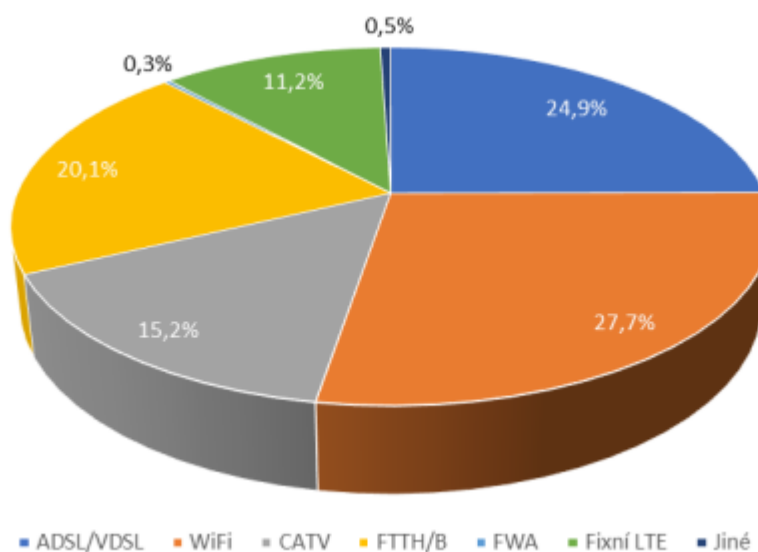


# 1 SOUČASNÝ STAV BEZDRÁTOVÝCH SÍTÍ V ČR

Tato kapitola obsahuje popis současného stavu struktury přístupu k internetu a také popis současného stavu bezdrátových sítí v České republice. Dále je popsána vybraná legislativa bezdrátového vysokorychlostního připojení včetně podmínek využívání bezdrátového bezlicenčního pásma 6 GHz a licenčního pásma 60 GHz.

## 1.1 Struktura přístupu k internetu

Poskytovatelé internetu nabízejí přístupy k internetu prostřednictvím několika technologií, které umožňují různou rychlost připojení. Z následujícího grafu 1 vyplývá, že mezi nejvíce zastoupené technologie v České republice patří bezdrátová technologie Wi-Fi, DSL technologie ADSL/VDSL, optická technologie FTTH/B a bezdrátová technologie LTE/5G. Celkový počet přístupů k internetu je tak téměř z 40 % tvořen bezdrátovým přístupem k internetu. Z tohoto důvodu je třeba neustále vyvíjet nové bezdrátové standardy pro dosažení vyšší datové propustnosti s čímž souvisí rozšiřování a regulace frekvenčních pásem. [1]

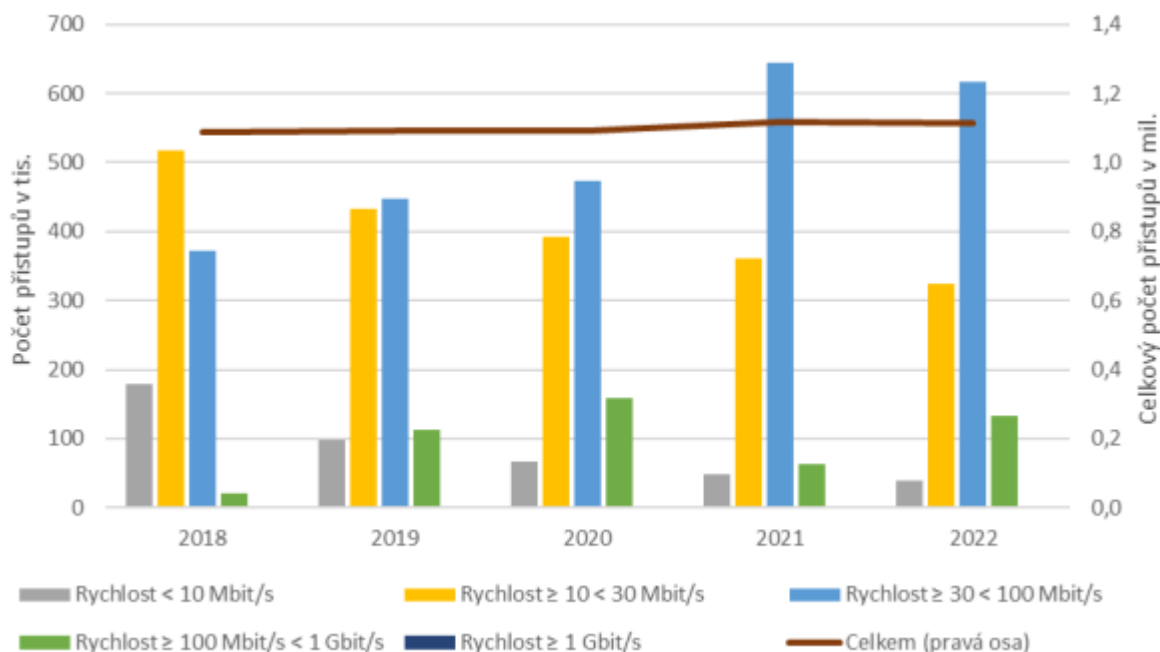


Graf 1 – Vývoj počtu služeb přístupu k internetu dle technologií

Zdroj: [1]

Přístup k internetu prostřednictvím bezdrátových technologií je dlouhodobě nejvyužívanější službou. Rozdělení dle inzerované rychlosti je zobrazeno na následujícím grafu 2. Z grafu plyne, že nejnižší sledovaný rozsah rychlosti <10 Mbit/s klesá, ale k nárůstu rychlosti nad 100 Mbit/s dochází jen velmi pomalu. Kolísání této rychlosti mezi lety 2018 a 2022 je způsobeno zejména novelizací všeobecného oprávnění, které zavazuje poskytovatele internetu k jasnějšímu uvádění reálných rychlostí připojení k internetu. [2] Se zvyšující se datovou

náročností jednotlivých technologií, mezi které patří například smart cities nebo cloud computing, bude stoupat počet připojených zařízení v sítích a bude tak nutné rychlost bezdrátového připojení navyšovat, aby byla zajištěna dostupnost a stabilita. [1]



Graf 2 – Vývoj počtu přístupů k internetu prostřednictvím bezdrátových technologií Wi-Fi dle inzerované rychlosti

Zdroj: [1]

## 1.2 Legislativa bezdrátového připojení v ČR

Český telekomunikační úřad stanoví využívání rádiových kmitočtů na základě všeobecných oprávnění, kde jsou stanoveny veškeré podmínky, podle kterých lze konkrétní kmitočtová pásma využívat. Ke konkrétním nařízením je přiřazována technická norma ČSN ETSI EN. [3]

V následující tabulce 1 jsou zobrazeny vybrané rádiové kmitočty, které jsou aplikovány v praktické části práce. Uvnitř budov jsou v praktické části využívána pásma 2,4 GHz, 5 GHz a 6 GHz. Pro zajištění konektivity je pak použita venkovní instalace typu bod-bod 60 GHz technologie.

V pásmu 5 GHz jsou zpravidla využívány pouze U-NII-1 kanály, mezi které patří kanály 36, 40, 44 a 48. [4] Tyto kanály jsou určeny pro vnitřní použití. Ostatní kanály spadající do U-NII-2 nebo U-NII-3 nemusí routery plně podporovat, jelikož je třeba aplikovat technologii DFS, která umožňuje měnit kanály, aniž by se překrývaly s armádními radarovými nebo

meteorologickými stanicemi. Podmínky pro využívání pásem 6 GHz a 60 GHz jsou shrnuty v následujících podkapitolách. [3]

Tabulka 1 – Vybrané radiové kmitočty využívané v praktické části

Kmitočtové pásmo	Maximální vyzářený výkon	Všeobecné oprávnění	Harmonizovaná norma (ČSN ETSI EN)
2 400–2 483,5 MHz	100 mW e.i.r.p	VO-R/12/11.2021-11	300 328
5 150–5 250 MHz	200 mW e.i.r.p		301 893
5 945–6 425 MHz	23 dBm e.i.r.p		Nestanovena
57–64 GHz	55 dBm e.i.r.p		302 217-2

*Zdroj: Upraveno na základě [5]*

V případě potřeby využití dalších kmitočtových pásem je třeba se vždy řídit nejnovějším všeobecným oprávněním, které vysílání na daném pásmu upravuje. Tato všeobecná oprávnění vždy vydává Český telekomunikační úřad, který je ústřední správní úřad v oblasti elektronických komunikací v České republice.

### 1.2.1 Podmínky využívání pásma 60 GHz

V České republice je možné provozovat legálně pásmo 60 GHz pro venkovní instalace od ledna 2020. [5] Pro stanice pevného vysokorychlostního spoje typu bod-bod je vyhrazeno kmitočtové pásmo 57–64 GHz, což představuje možnost využití čtyř kanálů a to 58 320 MHz, 60 480 MHz, 62 640 MHz a 64 800 MHz. [5] [6] [7]

Stanice v tomto kmitočtovém pásmu podléhají oznamovací povinnosti, a to včetně klientských stanic a stanic v režimu slave. Tyto stanice lze tak uvádět do provozu na základě provedení oznámení prostřednictvím registračního portálu ČTÚ. V následující tabulce 2 jsou uvedeny požadované údaje pro využívání těchto rádiových kmitočtů. [5]

Tabulka 2 – Údaje k využívání rádiových kmitočtů pro vysokorychlostní spoje typu bod-bod

Oznamovaný údaj	Povinnost
Zeměpisné souřadnice stanice uvedené v geodetickém systému WGS-84	ANO
Zisk použité antény	ANO
Střední výkon	ANO
Hlavní směr vyzařování	NE
Zabraná šířka pásma	ANO
Požadovaný poměr úrovně užitečného signálu k úrovni rušení	ANO
Vysílací radiový kmitočet	ANO
MAC Wireless adresa	ANO

*Zdroj: Upraveno na základě [5]*

V praktické části práce se jedná o klientskou stanici a oznámení této stanice je tak povinen provést provozovatel přidruženého přístupového bodu, v tomto případě ISP. [5]

Na následujícím obrázku 1 je ukázka z portálu RLAN, který provozuje Český telekomunikační úřad. Jsou zde veřejně zobrazeny veškeré registrované stanice. U každé stanice je uveden její název, druh a parametry, které jsou v povinně oznamovaných údajích. U každé stanice lze tak přehledně zjistit zisk antény, přivedený výkon, EIRP, šířku pásma nebo GPS polohu. [5] [8]

V seznamu jsou u každého spoje nebo vysílače uvedeny ovlivněné stanice v okolí. Na portále je k dispozici koordinační kalkulačka pro kontrolu potencionálních konfliktů konkrétních zařízení s okolními stanicemi. Zejména se jedná o možnosti rušení vzhledem k vysílání na stejném frekvenčním rozsahu. [8] Od data registrace stanice je záznam platný 18 měsíců. Před uplynutím této doby je nutné, aby provozovatel stanice prodloužil její platnost. Provozovatel také zodpovídá za správnost a aktualizaci daných údajů. [9]



Obrázek 1 – Mapa z portálu RLAN ČTÚ

Zdroj: [8]

### 1.2.2 Podmínky využívání pásma 6 GHz

Evropská unie schválila uvolnění pásma Lower-6 GHz pro nelicencované šíření v roce 2021. Členské země EU tyto frekvence uvolnily nejpozději do 1. prosince 2021. [10]

Všeobecné oprávnění VO-R/12/03.2021-3, které vydal Český telekomunikační úřad v březnu 2021 umožňuje rádiovým zařízením využívat 6 GHz pásmo v rozsahu 5 945–6 425 MHz, a to uvnitř budov do maximálního vyzářeného výkonu 23 dBm. Jakékoliv použití vně budov nebo uvnitř silničních vozidel není povoleno. [5] Toto pásmo dle uvolněného rozsahu umožňuje využít 3x 160 MHz kanál, 6x 80 MHz kanál, 12x 40 MHz kanál a 24x 20 MHz kanál.

## **2 BEZDRÁTOVÉ SÍTĚ**

V této části diplomové práce jsou nejprve popsány nejčastěji používaná frekvenční pásma a následně nejnovější bezdrátové standardy a technologie. Také jsou zde uvedeny jednotlivé vlastnosti bezdrátové technologie Wi-Fi 6/6E anebo také síťová topologie mesh. Na závěr jsou popsány moderní bezdrátové technologie ve světě.

### **2.1 Frekvenční pásma**

Rádiové spektrum je rozděleno na frekvenční pásma, která mohou být licenční nebo bezlicenční. V této práci jsou využívána bezlicenční pásma 2,4 GHz, 5 GHz, 6 GHz a licenční pásmo 60 GHz.

#### **2.1.1 Frekvenční pásmo 2,4 GHz**

Rozsah 2,4 GHz byl v minulosti nejpoužívanějším frekvenčním pásmem. Uplatňují ho standardy IEEE 802.11, 802.11b, 802.11g, 802.11n a také nejnovější standardy IEEE 802.11ax a IEEE 802.11be. Celkem pro toto pásmo existuje 13 kanálů, kde každý má šířku 22 MHz. Mezi nejčastěji využívané kanály patří kanál 1, 6 a 11, jelikož se nepřekrývají a lze tak dosáhnout nižšího rušení. Tento frekvenční rozsah využívá v závislosti na standardu modulaci DSSS, OFDM nebo MIMO OFDM. [11, s. 32–35]

#### **2.1.2 Frekvenční pásmo 5 GHz**

V současné době se jedná o jedno z nejpoužívanějších frekvenčních pásem. Rozsah 5 GHz je využíván standardy IEEE 802.11a, 802.11n, 802.11ac a také nejnovějšími IEEE 802.11ax a IEEE 802.11be. V tomto rozsahu existuje 23 kanálů, které se nepřekrývají. Jednotlivé kanály mají odstup 5 MHz. Oproti 2,4 GHz dosahuje toto pásmo vyšší přenosové rychlosti, avšak za cenu kratšího dosahu signálu a horší průchodnosti signálu přes překážky. [11, s. 35]

#### **2.1.3 Frekvenční pásmo 6 GHz**

Jak již bylo zmíněno, jedná se o nejnovější bezlicenční pásmo, které bylo v České republice uvolněno v roce 2021. Na rozdíl od pásem 2,4 GHz a 5 GHz nabízí vyšší propustnost a nižší latenci. Toto frekvenční pásmo využívají moderní standardy IEEE 802.11ax a IEEE 802.11be. [5]

#### **2.1.4 Frekvenční pásmo 60 GHz**

Frekvenční pásmo 60 GHz využívá standard IEEE 802.11ad. [5] Při porovnání s frekvenčními pásmy 2,4 GHz a 5 GHz vyniká frekvenční pásmo 60 GHz v šířce kanálu, kde se jedná o kanály široké 2,16 GHz. To umožňuje využití tohoto frekvenčního pásma pro poskytování

vysokorychlostního internetu, kde je možné dosahovat přenosových kapacit až několik Gbit/s. [12]

## **2.2 Standardy IEEE 802.11**

Institute of Electrical and Electronics Engineers je mezinárodní nezisková organizace, která sídlí v USA. IEEE 802.11 je skupina standardů pro bezdrátové LAN sítě, které jsou známé pod obchodním označením Wi-Fi. [11, s. 48] [13, s. 421] Certifikaci Wi-Fi určuje instituce Wi-Fi Alliance, která schvaluje jednotlivá zařízení a poskytuje jim certifikaci. Od organizace IEEE se tedy liší tím, že aplikuje vlastní pečeť o schválení testovaným bezdrátovým zařízením. [11, s. 48–49]

### **2.2.1 IEEE 802.11ac**

Standard IEEE 802.11ac využívající frekvenční pásmo 5 GHz byl vydán v roce 2013 a je také označován jako Wi-Fi 5. Dle specifikace musí zařízení podporovat teoretickou propustnost alespoň 1 Gbit/s. Šířku pásma je možné využívat až do hodnoty 160 MHz, zatímco ve standardu 802.11n je maximální hodnotou 40 MHz. Podporuje technologii MU-MIMO a modulaci s hustotou až 256-QAM, zatímco starší 802.11n využívá modulaci 64-QAM. [14, s. 1–4] [15]

### **2.2.2 IEEE 802.11ad**

Standard IEEE 802.11ad byl schválen již v roce 2012, avšak v České republice bylo možné jeho využití v rámci venkovního spoje typu bod-bod teprve od roku 2020. 60 GHz pásmo je v současné době využíváno zejména na venkovní spoje poskytovatelů internetového připojení. Do síťových zařízení, která se využívají ve vnitřních prostorech zatím příliš neproniká, a to vzhledem ke špatné průchodnosti signálu přes překážky. [16] Teoretická přenosová rychlost je až 8 Gbit/s při využití technologie OFDM. Je zde dostupný režim s úsporou energie, který se využívá u zařízení, která jsou napájena baterií. Původně byl standard zamýšlen na velmi rychlý přenos na krátké vzdálenosti, zejména pak pro bezdrátové displeje, distribuce HDTV anebo komunikace v rámci AP. [17]

### **2.2.3 IEEE 802.11ax**

Standard IEEE 802.11ax je standard schválený v roce 2021, který je označován jako Wi-Fi 6. Tento standard je zaměřený převážně na zlepšení spolehlivosti a celkové propustnosti sítě, kde je využíváno většího počtu zařízení, tedy například ve firmách nebo ve veřejných prostorech. Standard využívá přenosová pásma 2,4 GHz, 5 GHz a 6 GHz. Maximální teoretická rychlost je 9,6 Gbit/s. [18] Veškeré klíčové technologie tohoto standardu jsou detailně rozebírány v následující kapitole Wi-Fi 6/6E.

## 2.2.4 IEEE 802.11be

IEEE 802.11be je nejnovější schválený standard označovaný jako Wi-Fi 7, který poskytuje datovou propustnost až 46,1 Gb/s. Tento standard byl schválen v lednu 2024, ale první síťová zařízení se již objevují na trhu od roku 2023. V době psaní této práce jsou tyto zařízení nasazována minimálně, jelikož výrobci na trh uvádějí teprve zařízení se standardem IEEE 802.11ax. Standard opět využívá pásma 2,4 GHz, 5 GHz a 6 GHz, avšak používá modulaci 4096-QAM, šířku pásma až 320 MHz a podporuje technologii 16x16 MU-MIMO. [19]

## 2.2.5 Shrnutí rozdílů a inovací

V následující tabulce 3 jsou přehledně popsány vlastnosti jednotlivých generací Wi-Fi včetně nově schváleného standardu Wi-Fi 7.

Tabulka 3 – Shrnutí rozdílů jednotlivých standardů

	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E	Wi-Fi 7
<b>IEEE standard</b>	802.11ac	802.11ax	802.11ax	802.11be
<b>Přenosová pásma</b>	5 GHz	2,4 GHz, 5 GHz	2,4 GHz, 5 GHz, 6 GHz	2,4 GHz, 5 GHz, 6 GHz
<b>Maximální přenosová rychlost</b>	3,5 Gb/s	9,6 Gb/s	9,6 Gb/s	46 Gb/s
<b>Velikost kanálu</b>	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 160, 320 MHz
<b>Modulace</b>	256-QAM OFDM	1024-QAM OFDMA	1024-QAM OFDMA	4096-QAM OFDMA
<b>MIMO</b>	4x4 MU-MIMO	8x8 MU-MIMO	8x8 MU-MIMO	16x16 MU-MIMO

*Zdroj: Upraveno na základě [19] [20]*

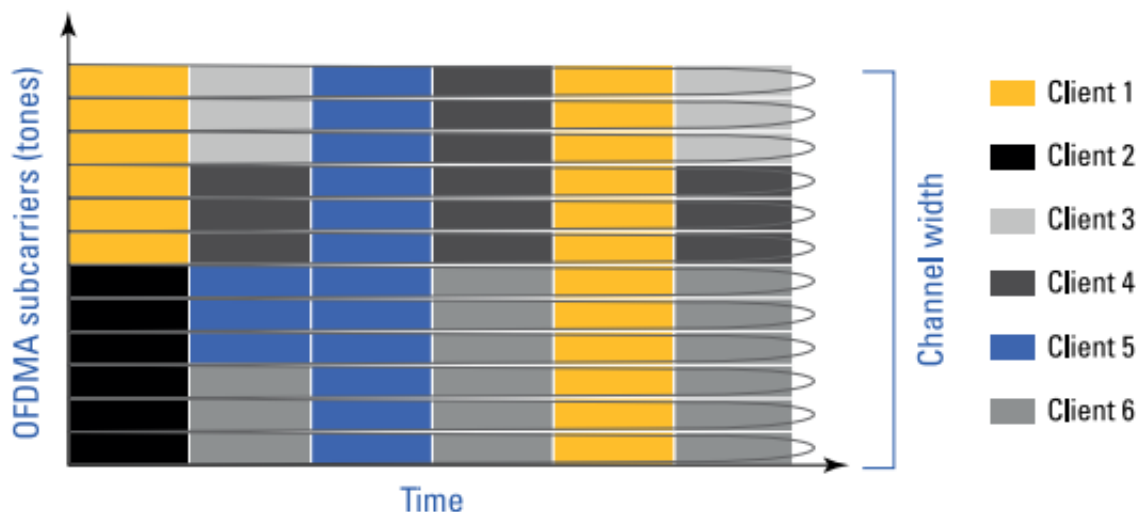
Nové standardy přinášejí vylepšení výkonu, efektivity, bezpečnosti a podporu více připojených zařízení současně, což je důležité z hlediska rostoucího počtu síťových zařízení a zvýšených nároků na šířku pásma.

## 2.3 Wi-Fi 6/6E

Praktická část diplomové práce je zaměřena na současné trendy v bezdrátových datových sítích z pohledu využití ve firmě, proto se nabízelo nasazení technologie Wi-Fi 6/6E. Dostupnost síťových zařízení pracujících s touto technologií se v roce 2024 neustále zvyšuje, a tak je možné vybírat mezi desítkami předních výrobců. V následujících podkapitolách jsou rozebrány jednotlivé vlastnosti tohoto standardu.

### 2.3.1 OFDMA

OFDMA (Orthogonal frequency-division multiple access) patří mezi největší přínosy standardu 802.11ax a je zobrazen na následujícím obrázku 2. Tento mechanismus je již využíván převážně v 5G sítích. [21] Velmi široké kanály 80 MHz, 80+80 MHz a 160 MHz trpí frekvenčně selektivním rušením, které snižuje dosažitelné přenosové rychlosti. OFDMA rozděluje Wi-Fi kanály na sub kanály, které se nazývají zdrojové jednotky (RU). Přístupový bod může přidělovat celý kanál jednomu uživateli nebo jej rozdělit tak, aby sloužil více uživatelům současně, a to na základě provozních potřeb klientů. [18, s. 11–12] Ve standardu IEEE 802.11ax lze rozdělit kanály o frekvencích 20, 40, 80 a 160 MHz na 9, 18, 37 a 74 zdrojových jednotek. [22] Paralelní přenos více uživatelům snižuje nadměrnou režii přenosu. [18, s. 12]



Obrázek 2 – OFDMA

*Zdroj: [18, s. 12]*

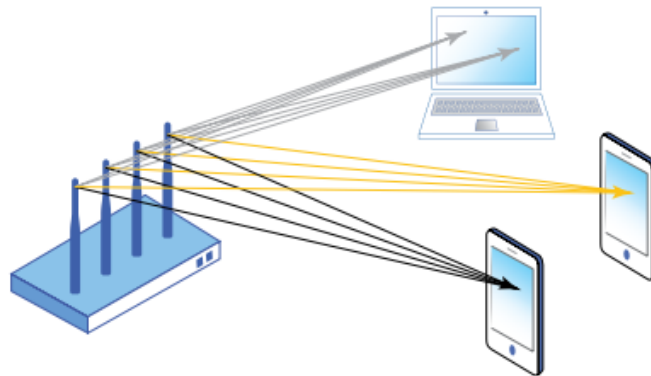
Na jednom 20 MHz kanálu lze tak odbavit až 9 různých uživatelů, zatímco na 160 MHz kanálu je to až 74 uživatelů. [18, s. 15] OFDMA je dobrou volbou pro většinu síťových aplikací a přispívá ke snížení latence a zvýšení efektivity přenosu. [18, s. 12]

### 2.3.2 MU-MIMO

Technologie MU-MIMO umožňuje přístupovému bodu vysílat více datových toků (teoreticky až do počtu antén AP) na více míst, a to pomocí prostorových proudů signálu a tvarování vysílané energie neboli beamformingu. [22] Původně bylo MU-MIMO zavedeno již standardem IEEE 802.11ac s podporou MU-MIMO 4x4 pouze pro downlink. Wi-Fi 6 umožňuje implementaci 8x8 MU-MIMO pro downlink i uplink, to znamená 8 datových toků do 8 míst a zvyšuje tak přenosovou kapacitu. [14, s. 6–9] [23]



IEEE 802.11ax umožňuje, aby OFDMA a MU-MIMO fungovaly současně anebo nezávisle na sobě. [23] Zatímco OFDMA zvyšuje účinnost, snižuje latenci a využívá se zejména pro přenos menších datových paketů, tak MU-MIMO zvyšuje kapacitu, datovou propustnost a je tak ideální pro velké datové pakety. OFDMA tedy umožňuje víceuživatelský přístup rozdělením kanálu. MU-MIMO umožňuje víceuživatelský přístup pomocí různých prostorových toků. [18, s. 16–18] Na následujícím obrázku 3 je zobrazena komunikace mezi síťovými zařízeními pomocí technologie MU-MIMO.

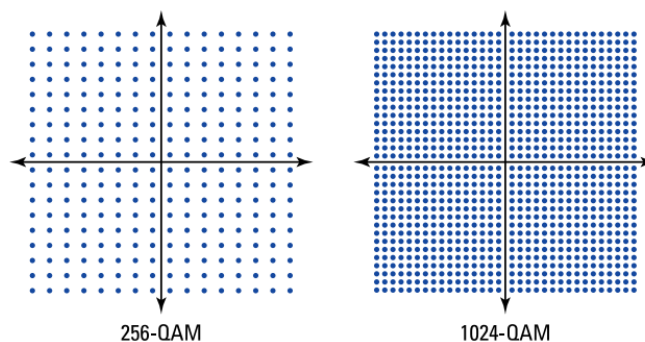


Obrázek 3 – MU-MIMO

*Zdroj: [18, s. 17]*

### 2.3.3 1024-QAM

Ačkoli primárním cílem nového standardu IEEE 802.11ax byla efektivita, tak se podařilo zvýšit i přenosovou rychlost. Při kvadraturní amplitudové modulaci (QAM) jsou data reprezentována amplitudou a fází nosného signálu. Amplituda a fáze nosného signálu jsou modulovány tak, aby reprezentovaly různé symboly, což umožňuje přenos více bitů dat v jednom symbolu. Oproti standardu IEEE 802.11ac, který využívá modulaci 256-QAM přináší Wi-Fi 6 asi o 20 % vyšší reálnou datovou propustnost, jelikož moduluje 10 bitů na symbol oproti 8 bitům na symbol u technologie Wi-Fi 5. Jednotlivé varianty QAM se tedy liší počtem symbolů a datovou propustností. Na následujícím obrázku 4 lze vidět porovnání dvou zmíněných variant. [18, s. 24–25]

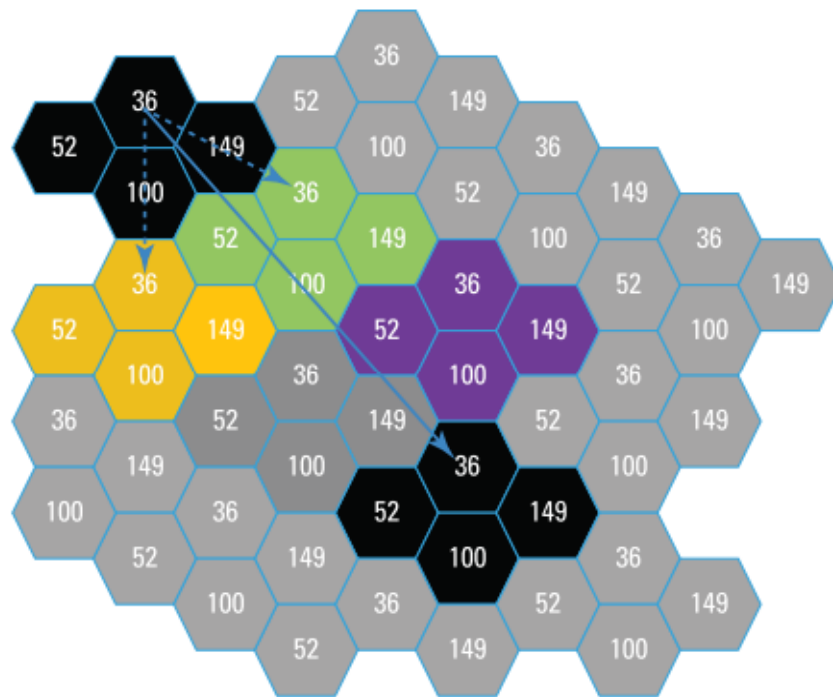


Obrázek 4 – Porovnání 256-QAM a 1024-QAM

*Zdroj: [18, s. 25]*

### 2.3.4 BSS Color

BSS Color (Basic Service Set Color) slouží k optimalizaci využití rádiového spektra a snižování rušení mezi jednotlivými AP. Jedná se o identifikátor, který je přidělen každému bezdrátovému síťovému zařízení. Když síťové zařízení komunikuje, tak přenáší také informaci o své barvě v rámci BSS Color a umožňuje ostatním zařízením detekovat, že přichází signál s jinou barvou. [18, s. 18–21] Každá BSS je identifikována hodnotou BSS Color, která se pohybuje od 1 do 63. Hodnota 0 znamená, že BSS Color není použita. [24] Pomocí barev se rozlišují rámce AP, na které je zařízení připojeno a také cizí rámce, jak zobrazuje obrázek 5. Při detekci vysílání jiné barvy na stejném kanále, tedy při detekci rušení, je možné nastavit hranici CCA (Clear Channel Assessment) a tím je ignorovat a začít vlastní vysílání. Je tedy možné přistupovat ke spektru i ve chvíli, kdy by bylo vysílání zastaveno, jelikož by byla detekována kolize. Tím se zároveň snižuje rušení, protože signál jiného AP je na nižší hodnotě. [18, s. 21] [25]



Obrázek 5 – BSS Coloring

*Zdroj: [18, s. 20]*

BSS Coloring detektuje barevný bit v PHY hlavičce standardu IEEE 802.11ax. To však znamená, že klienti pracující na starších standardech IEEE 802.11a/b/g/n nebudou schopni interpretovat barevný bit, jelikož využívají jiný formát PHY hlavičky. [18, s. 20]

### 2.3.5 TWT

TWT (Target Wake-up Time) je mechanismus pro úsporu energie síťového zařízení, který byl již v minulosti definován ve standardu 802.11ah-2016. [18, s. 23] AP je nyní schopné si

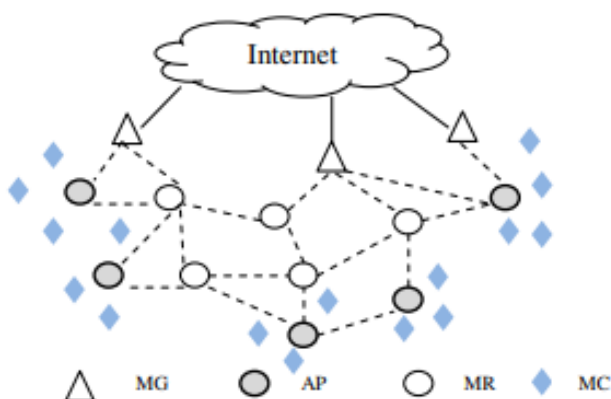
s klientem dohodnout přesný čas probuzení. Tím se velmi prodlouží doba spánku síťového zařízení a zároveň se prodlouží výdrž baterie tohoto zařízení. [25] TWT je tak ideální způsob úspory energie pro mobilní zařízení a IoT zařízení, která vyžadují úsporu energie. [18, s. 23–24]

## 2.4 Síťová topologie mesh

Síťová topologie mesh je definována jako uspořádání komunikačních uzlů v síti, kde je každý z uzlů přímo drátově anebo bezdrátově propojen s dalšími uzly. [26] Tato síťová topologie umožňuje vícenásobné přístupové propojení mezi síťovými prvky, na rozdíl od jiných typů topologií. Redundance spojení mezi prvky sítě nabízí výhodu v oblasti spolehlivosti sítě, protože kdykoli dojde k poruše jednoho z prvků sítě, tak síť nepřerušuje činnost, ale pouze najde jinou cestu k síťovému prvku a síť pokračuje ve funkci. [27, s. 13, 524]

V praktické části práce je využita právě topologie mesh, a to v konfiguraci, kdy jsou veškeré síťové prvky drátově propojené pro maximalizaci stability a propustnosti dat. Veškerá instalovaná zařízení disponují redundancí drátového spojení. Redundance v tomto případě funguje tak, že pokud dojde k výpadku drátové komunikace, tak se zařízení, kde došlo k výpadku, automaticky přepne do bezdrátové komunikace s dalšími AP, které jsou součástí mesh topologie a tím se zvyšuje spolehlivost a dostupnost počítačové sítě.

Na následujícím obrázku 6 lze vidět jedno z možných řešení mesh sítě, v případě, že jsou jednotlivé síťové prvky spojeny bezdrátově a drátový přístup k internetu mají pouze zařízení označené jako mesh gateway. Toto konkrétní řešení se využívá převážně v případě, kde není možné zařízení spojit drátově. Obrázek využívá následující značení: MG (Mesh Gateway), AP (Access Point), MR (Mesh Router), MC (Mesh Clients). [28]



Obrázek 6 – Infrastruktura mesh topologie

Zdroj:[28]

## 2.5 IPv4

IPv4 je čtvrtou verzí internetového protokolu (IP), který byl poprvé popsán v RFC 791. IPv4 poskytuje 32bitový adresní prostor a celkem tak obsahuje téměř 4,3 miliardy jedinečných IP adres. [13, s. 549–550] [29, s. 272–273]

Formát datagramu má stěžejní roli v rámci počítačových sítí, proto je důležité znát jeho náležitosti. IPv4 datagram obsahuje číslo verze, který označuje verzi datagramu protokolu IP, podle kterého router určuje, jak interpretovat zbytek IP datagramu. Délka záhlaví určuje, kde v IP datagramu začínají data. Typ služby umožňuje odlišit různé typy IP datagramů a délka datagramu určuje celkovou délku datagramu. [29, s. 268–269] IPv4 datagram obsahuje pole identifikace, příznaku a fragmentačního odsazení, které jsou určeny k identifikaci fragmentů a jejich opětovnému sestavení. Podle identifikačního čísla datagramu pak zařízení určí, které fragmenty jsou součástí většího fragmentu. [29, s. 270-272] Doba životnosti zaručuje, že datagram bude po určitém počtu průchodů zařízeními zahozen, aby neobíhal sítí navždy. Položka protokol označuje protokol transportní vrstvy, kterému se předává datová část IP datagramu. Kontrolní součet záhlaví je určený pro odhalování bitových chyb v IP datagramu. Následně je zde umístěna zdrojová a cílová IP adresa a část možnosti, která umožňuje prodloužení záhlaví IP. Poslední položkou datagramu jsou samotná data. [29, s. 269–270]

Maximální množství dat, které lze přenést rámcem spojové vrstvy, se označuje jako maximální přenosová jednotka (MTU). V případě, že některá z linek na trase mezi odesílatelem a příjemcem používá protokol spojové vrstvy, který má nižší MTU než odeslaný datagram, tak je třeba fragmentovat data tohoto IP datagramu. Než se fragmenty přesunou do transportní vrstvy v cíli, tak je nutné je znovu sestavit. IP fragmentace však zatěžuje routery a koncové systémy, které se musí navrhovat tak, aby tyto datagramy bylo možné rozdělovat a znovu sestavovat. Fragmentace je také snadno zneužitelná k DoS útokům, při kterém útočník odesílá vysoké množství fragmentů, čímž zatíží koncové zařízení. IPv6 pak fragmentaci zcela odstraňuje. [29, s. 272]

Překlad síťových adres (NAT) upravuje síťový provoz procházející přes router prepisováním zdrojové IP adresy a cílové IP adresy. Používá se pro přístup zařízení z lokální sítě do internetu, pomocí jedné veřejné IP adresy. To umožňuje jednak snížení využití IPv4 adres a také využívání privátního adresního prostoru. Datagramy, které přichází do NAT routeru, jsou rozděleny a zaslány na koncové zařízení podle překladové NAT tabulky. [29, s. 280–282] NAT je pro tyto účely také využíván v praktické části diplomové práce.

## 2.6 IPv6

Protokol IPv6 je následníkem staršího protokolu IPv4. Vývoj začal na začátku 90. let jako reakce na snižující se počet dostupného adresního prostoru IPv4. Vzhledem k tomu, že se podařilo snížit počet úbytku dostupných IP adres především díky beztržnímu adresování CIDR a mechanismům překladu adres NAT, tak se vývoj IPv6 výrazně zpomalil. [30, s. 23–24]

Dne 3. února 2011 byly rozděleny poslední adresy IPv4 společností IANA. To však neznamená, že nelze získat v dané oblasti IPv4 adresu, ale že místní poskytovatelé internetového připojení nedostanou žádný větší blok IP adres. Například v Evropě lze od RIPE NCC získat maximálně 1024 IPv4 adres, které jsou však oficiálně určeny pro přechodové mechanismy. [30, s. 25–26]

Hlavní nevýhodou tohoto protokolu je nekompatibilita s předchozí verzí IPv4, a to podstatným způsobem komplikuje nasazení novější IPv6, jelikož se zařízení nedostanou ke službám poskytovaným pouze pro IPv4. [30, s. 27]

Aktuálně v roce 2024 představuje IPv6 celosvětově okolo 40 % provozu, v České republice je to však pouze kolem 25 %. [30, s. 29] [31] Například modelová firma, kterou se zabývá praktická část diplomové práce a která představuje běžnou menší až střední firmu v České republice požaduje výstavbu sítě na základě IPv4, a to proto, že některá z koncových zařízení IPv6 nepodporují. Avšak veškerá nově navržená síťová zařízení v praktické části plně podporují IPv6 a na základě požadavku firmy v budoucnosti lze nasadit síť plně podporující pouze IPv6 bez přechodových mechanismů. Pokud by firma chtěla postupně nahrazovat koncová zařízení za zařízení, která IPv6 podporují, bylo by třeba udržovat dvojí konfiguraci, která však zvyšuje provozní náklady. K propojení a vzájemné komunikaci je nutné použít některý z přechodových mechanismů. Vzájemný překlad datagramů mezi IPv4 a IPv6 umožňuje například NAT64. [32]

### 2.6.1 Adresní prostor a datagram

Rozsah adresního prostoru IPv6 byl stanoven na čtyřnásobek IPv4, tedy na 128 bitů. Avšak 64 bitů je věnováno jako identifikátor rozhraní, z čehož vyplývá, že v jedné podsíti lze rozlišit miliardy miliard zařízení. [29, s. 285–287] [30, s. 33]

Ve formátu datagramu byl počet položek minimalizován a hlavička datagramu získala konstantní délku. Pořadí hlaviček je zvoleno tak, aby router mohl co nejrychleji zpracovat ty, které jsou pro něj určené. Pro zajištění bezpečnosti slouží dvě hlavičky, a to autentizační AH a šifrovací ESP. Autentizační hlavička umožňuje ověřit, zda je odesílatelem dat opravdu

konkrétní zařízení a zda nedošlo cestou ke změně dat. Hlavičkou pro šifrování lze celý obsah datagramu zašifrovat. [30, s. 33] Datagram může být opatřen jednou nebo oběma bezpečnostními hlavičkami v závislosti na zabezpečení, které je požadováno. Podle RFC 4301 je implementace ESP u zařízení podporující IPSec povinná, avšak u AH je pouze dobrovolná. V současné době se od používání AH odklání, jelikož ESP dokáže nabídnout stejné služby, a ještě další funkce navíc. [30, s. 225–227]

## **2.6.2 Adresování a zabezpečení místní sítě**

Adresace lokální sítě se dá navrhnout širokým počtem způsobů a nijak se dále nevázat na IPv4. Většina správců ovšem aplikuje topologie totožné s IPv4. Podsítě obou protokolů jsou tedy stejné a ke směrování se používají stejné aktivní síťové prvky, kde jsou na rozhraní přiděleny IPv4 a IPv6 adresy. [30, s. 331–332]

Jedním z uváděných přínosů IPv6 je opouštění technologie NAT a obnovení přímé vzájemné komunikace koncových zařízení, z čehož těží celá řada aplikací a jejich protokolů. Na druhou stranu, velkou výhodou NAT je jednostranné navazování spojení, které komplikuje útoky na zařízení v koncové síti. Touto problematikou se zabývá dokument RFC 4864 (Local Network Protection for IPv6). [30, s. 336–337] NAT je prospěšný také v tom, že skryje strukturu sítě. V tomto případě IPv6 poslouží jen napůl, jelikož strukturu sítě neskryje, ale identitu koncových zařízení ano, k čemuž slouží náhodně generované adresy pro ochranu soukromí podle RFC 4941. O základní zabezpečení místní sítě se pak stará firewall, který je integrovaný v koncovém síťovém prvku. Optimálně má pak zařízení stavový firewall, který ve výchozím nastavení propustí jen datagramy z adres, na které v nedávné době odešel datagram z místní sítě. Je také možné jednoduše aplikovat výjimky například na IP telefonii nebo další komunikátory. [29, s. 285–289] [30, s. 337–338]

## **2.7 Zabezpečení bezdrátových sítí**

Bezdrátové sítě se staly nedílnou součástí moderního síťového prostředí, poskytující flexibilitu při přístupu k informacím a službám. Avšak s rozvojem technologií a stoupajícím využitím bezdrátové komunikace se také zvyšuje riziko bezpečnostních hrozeb a útoků. Zabezpečení bezdrátových sítí je klíčové nejen pro ochranu citlivých dat a zachování důvěrnosti informací, ale také pro udržení nepřetržitého provozu a stability firemní infrastruktury.

Mezi základní a ověřené postupy, které zlepšují zabezpečení Wi-Fi, patří nastavení silného hesla pro veškeré přístupové body v síti a také pro koncová zařízení. [27, s. 424] Mezi vlastnosti silného hesla patří například minimální délka 8 znaků. Dále by mělo silné heslo obsahovat

kombinaci malých písmen, velkých písmen, číslic a speciálních znaků. Doporučuje se nikdy nepoužívat stejné heslo a také slovníková hesla, která obsahují běžná slova. Také se doporučuje pravidelná změna hesla alespoň jednou za 3 měsíce. Veškeré požadavky na tvorbu hesla však závisí na konkrétní organizaci. [33] Mezi další bezpečnostní opatření patří filtrování MAC adres, která povoluje přístup pouze zařízením s MAC adresou, které je v seznamu povolených zařízení, ale vzhledem k tomu, že se přenášené MAC adresy dají jednoduše odposlechnout, tak tato metoda není příliš efektivní. Doporučuje se udržovat software veškerých zařízení aktuální, jelikož jednotlivé aktualizace mohou obsahovat důležité bezpečnostní opravy. Mezi další bezpečnostní opatření, které je třeba vždy aplikovat, spadá chráněný přístup k Wi-Fi, který je popsán v následující podkapitole. [27, s. 424]

### **2.7.1 Bezpečnostní protokoly WPA2 a WPA3**

Zásadní součástí bezdrátového zabezpečení je zabránění neoprávněnému přístupu pomocí protokolů bezdrátového zabezpečení, které slouží k ochraně dat v bezdrátových sítích. [34] WPA (Wi-Fi Protected Access) je obchodní označení společnosti Wi-Fi Alliance pro zabezpečení bezdrátových sítí. WPA2 byl ratifikován jako nový bezpečnostní standard Wi-Fi v roce 2004, kde byl implementován AES, který poskytuje vyšší zabezpečení a výkon. [35] V rámci zabezpečení WPA se v minulosti používal protokol TKIP, který se však na nejnovějších zařízeních standardů 802.11ac a novější již nepoužívá, protokol není považován za bezpečný a u nových zařízení omezuje jejich rychlost. [14, s. 98] Ve WPA2 existují dva provozní režimy, předsdílený (PSK) pro osobní síť a podnikový režim pro větší firemní síť. V případě WPA2-PSK, přístupový bod ověřuje klienta na základě předem sdíleného hesla, zatímco ověřování v podnikovém režimu se provádí prostřednictvím protokolu EAP (Extensible Authentication Protocol) založeného na architektuře 802.1x. [34] EAP definuje formát zprávy mezi koncovými body, které se poté zapouzdří pomocí protokolu RADIUS pro přenos na ověřovací server. [29, s. 559–560]

V roce 2018 byl ratifikován Wi-Fi Protected Access 3 (WPA3). WPA3 má mnoho vylepšení zabezpečení oproti svým předchůdcům a poskytuje lepší metody šifrování a sdílení klíčů. V roce 2020 se stal povinným pro zařízení, která jsou certifikována. WPA3, podobně jako jeho předchůdce, má dva režimy provozu: WPA3-Personal a WPA3-Enterprise. WPA3 obsahuje přechodový režim, který se nazývá WPA3-SAE, kde jsou podporovány WPA2 a WPA3 současně, aby byla zajištěna zpětná kompatibilita. [34]

V praktické části diplomové práce je převážně využíván protokol WPA2 nebo WPA3 s předsdíleným klíčem, jelikož se firma zaměřovala na minimalizaci nákladů a nebylo možné aplikovat například RADIUS server pro implementaci WPA2-Enterprise nebo WPA3-Enterprise.

V následující tabulce 4 je uvedeno porovnání dvou aktuálně nejpoužívanějších protokolů bezdrátového zabezpečení WPA2 a WPA3.

Tabulka 4 – Porovnání WPA2 a WPA3

	WPA2	WPA3
<b>Rok vydání</b>	2004	2018
<b>Šifrovací metoda</b>	AES-CCMP	AES-CCMP, AES-GCMP
<b>Šifrovací klíč</b>	128-bit	128-bit (WPA3-Personal) 192-bit (WPA3-Enterprise)
<b>Typ šifry</b>	Bloková	Bloková
<b>Integrita dat</b>	CBC-MAC	SHA
<b>Správa klíčů</b>	PSK, 4-way handshake	SAE
<b>Autentifikace</b>	PSK, 802.1x	SAE, 802.1x

*Zdroj: Upraveno na základě [34] [35]*

## 2.7.2 Firewall

Firewall je nástroj, který poskytuje filtrování příchozích a odchozích paketů na základě údajů, které označují každý jednotlivý paket, tj. zdrojová IP adresa, cílová IP adresa, zdrojový port a cílový port. Firewall je kombinace hardwaru a softwaru, přes který prochází provoz z místní sítě do sítě internet. Většina firewallů pak plní dvě základní bezpečnostní funkce. První z nich je filtrování paketů založené na přijetí nebo odmítnutí, která je založená na definovaných pravidlech. Druhá bezpečnostní funkce je vytvoření aplikační brány, jež poskytuje služby uživatelům a zároveň chrání veškeré uživatele, kteří ji využívají jako prostředníka. [27, s. 251] [29, s. 262–263]

V současně nejrozšířenějších firewalllech je v případě zahození paketu vytvořen záznam a v případě nebezpečných reportů jsou tyto události reportovány správci sítě. Zásady přijetí nebo odmítnutí, které jsou používané ve firewalllech, jsou založeny na zásadách zabezpečení organizace. Běžně se používají dva následující přístupy. [27, s. 251–253]

První z nich je deny-everything-not-specially-allowed, který nastaví firewall takovým způsobem, že zakáže veškerý provoz a služby kromě předem určeného provozu podle potřeb organizace. Druhý přístup je allow-everything-not-specifically-denied, což povolí veškerý



síťový provoz a služby kromě těch, které jsou na seznamu „zakázaných“. Tento seznam definuje organizace dle svých bezpečnostních zásad. [27, s. 251–253]

## **2.8 Moderní bezdrátové technologie ve světě**

Moderní bezdrátové technologie jsou postupně nasazovány v různých oblastech. V následujících podkapitolách je představeno několik vybraných scénářů nasazení moderních bezdrátových technologií. Představují zejména důvody a potřebu nasazení těchto technologií a z toho plynoucí výhody pro organizace a koncové uživatele. Jednou z motivací diplomové práce je rozšíření těchto moderních technologií také v České republice.

### **2.8.1 Oblast vzdělání**

Do roku 2028 se očekává výrazný nárůst rozšířené reality (AR) a virtuální reality (VR), které vyžadují vysokou přenosovou rychlost. [36] [37] Dalším významným důvodem pro nasazení nejnovějších technologií je zvyšující se digitalizace tříd a vytváření chytrých kampusů na vysokých školách a zvyšující se požadavky na připojení ve velkých posluchárnách anebo přednáškových sálech. [38]

American University of Sharjan ve Spojených Arabských Emirátech požadovala pokrytí kampusu s rozlohou 1,5 km<sup>2</sup> moderní bezdrátovou technologií Wi-Fi 6. Na pokrytí kampusu bylo použito celkem 32 přístupových bodů, které pracují na standardu IEEE 802.11ax, což je znatelně méně než v případě použití starších standardů. Dále bylo možné využít zabezpečení na základě standardu WPA3. [39]

### **2.8.2 Oblast zdravotnictví**

Ve zdravotnictví je možné s nasazením Wi-Fi 6E optimalizovat kritickou infrastrukturu, snížit latenci a zvýšit rychlost připojení. V nemocnicích je vysoký počet pohybujících se osob, které potřebují využívat síťové technologie společně se zdravotnickými nástroji, které jsou také připojené do místní sítě. Výrazný nárůst zaznamenala během pandemie Covid-19 také telemedicína, což je dálkový přenos informací mezi doktorem a pacientem. [38]

V USA připadá na jednoho pacienta v průměru 10 až 15 připojených zdravotnických zařízení. Jedním z nejdůležitějších prvků Wi-Fi 6E je 6 GHz pásmo, ze kterého mohou IoT zařízení velmi těžít. Mezi tato zařízení patří například SaMD (software-as-a-medical-device), kde jsou na tablet připojené bezdrátové senzory. Dalším příkladem je použití rozšířené reality ke školení studentů medicíny v oblasti autopsie. [40]

### 2.8.3 Oblast veřejných prostor

V oblasti veřejných prostorů lze uvést příklad v San Franciscu, kde byla v roce 2023 nasazena na stadionu technologie Wi-Fi 6E. Od nasazení si management slibuje nejen zvýšení rychlosti a dostupnosti připojení pro desetitisíce návštěvníků, ale také zefektivnění provozu v oblasti provozních týmů. O pokrytí stadionu se zde stará 900 přístupových bodů, které jsou umístěny pod sedadly. Nasazení této technologie umožňuje aplikování biometrického vstupu, který probíhá v reálném čase. [41]

Dalším příkladem je kongresové centrum BEXCO v Jižní Koreji, které disponuje rozlohou 59 858 m<sup>2</sup> a 50 konferenčními místnostmi. Průměrná roční návštěvnost se pohybuje kolem 4,5 mil. osob. Síťová infrastruktura byla nově vystavěna na Wi-Fi 6 AP Cisco, které nabízí stabilnější a širší pokrytí celého areálu než starší technologie. Se stejným počtem přístupových bodů bylo dosaženo vyššího pokrytí a vymizela místa bez pokrytí bezdrátového internetu. Po nasazení nové technologie je možné využívat hlasové a video aplikace bez zvýšené latence i při připojení vyššího počtu zařízení. [42]

Posledním příkladem je vytvoření konektivity na Východofríských ostrovech v Německu pomocí 60 GHz technologie. V místě kempu pro stovky návštěvníků nebylo možné zajištění konektivity pomocí jiné než bezdrátové technologie. Bylo třeba přivést konektivitu na ostrov do místa kempu a následně pokrýt stanová místa, společné prostory, sociální zařízení a také registrační zónu. Celkově bylo potřeba vytvořit dostatečnou konektivitu pro vyšší stovky současně bezdrátově připojených zařízení. Po nasazení 60 GHz technologie bylo možné návštěvníky využívat vysokorychlostní připojení i v případě nepříznivých povětrnostních podmínek. Jedná se o modulární řešení, proto je možné pokrytí dále rozšiřovat. [43]

### 3 POPIS A ANALÝZA VÝCHOZÍHO STAVU

Pro návrh počítačové bezdrátové sítě byla jako modelový příklad vybrána fiktivní firma, která sídlí na okraji malé obce a nemá k dispozici jiné vysokorychlostní alternativy internetového připojení než bezdrátovou technologii. Kapitola dále obsahuje popis a odůvodnění výběru konkrétních síťových prvků a také prezentuje navrženou síťovou topologii.

V této firmě bylo třeba vytvořit bezdrátovou počítačovou síť pro nižší stovky bezdrátově připojených zařízení, mezi které patří například mobilní telefony, notebooky, tiskárny, senzory, CNC stroje nebo také bezdrátová zařízení sloužící pro sledování zásob skladu. Zařízení připojená drátově jsou v této firmě v menšině, jelikož firma nechce investovat do modernizace kabelových rozvodů. Kabelové rozvody byly již připravené v minulosti pomocí kroucené dvojlinky Cat 5E, která dosahuje přenosové rychlosti 1 Gbit/s, což je pro aktuální potřeby firmy dostatečné.

Mezi hlavní požadavky firmy patřilo nasazení bezdrátové technologie Wi-Fi 6 nebo Wi-Fi 6E s důrazem na nižší pořizovací cenu. Dalším požadavkem bylo vyřešení konektivity, která však musí být vyřešena bezdrátově, vzhledem k poloze firmy. V budoucnu se předpokládá navyšování počtu bezdrátových zařízení ve firmě.

Pro konektivitu firmy byla vybrána bezdrátová vysokorychlostní technologie pracující na frekvenci 60 GHz, která nabízí vysokou propustnost, nízkou latenci, ale krátký dosah. Vysílač je umístěn 700 m vzdušnou čarou od firmy, takže je použití této technologie možné bez vlivu na kvalitu připojení. Poskytovatel internetového připojení nabídl business symetrický tarif 500/500 Mbit/s za nižší než průměrnou tržní cenu v okolí, avšak firma si musí zařídit vlastní instalaci příjmové antény MikroTik nebo Ubiquiti, jelikož poskytovatel internetového připojení využívá právě řešení od těchto společností a jiná zařízení nejsou kompatibilní s poskytnutým přístupovým bodem.

Od poskytovatele internetového připojení byla přidělena IPv6 adresa pro anténu a následně celá místní počítačová síť pracuje s IPv4 adresami. Dále je přidělena veřejná IPv4 adresa pomocí NAT 1:1, tedy vnější rozhraní routeru firmy má IP adresu z privátního rozsahu poskytovatele, který následně na svém hlavním routeru používá NAT, kde se příchozím paketům přepíše cílová IP adresa, stejný postup je aplikován také u paketů odchozích. Toto řešení je velmi rozšířené a používá se z toho důvodu, že není třeba směřovat skrz síť poskytovatele speciální přidělený rozsah. Další nespornou výhodou je, že poskytovatel internetového připojení využije pouze jednu veřejnou IPv4 adresu.

Ve všech modelových variantách praktické části byla využita technologie mesh, která je plně modulární, to znamená, že lze dané modelové řešení aplikovat jak na menší a střední firmy, tak také na firmy o vyšších stovkách nebo tisících připojených bezdrátových zařízení. Tomu musí samozřejmě odpovídat hardwarové vybavení, které je nutné adekvátně zvolit podle konkrétních požadavků na počítačovou síť. Každá ze tří variant obsahuje kompletní nastavení příjmové antény a Wi-Fi sítě. Ostatní použité síťové prvky jsou pro každou variantu společné a jejich konfigurace je provedena v kapitole návrhu bezdrátové počítačové sítě.

Jako hlavní router bylo vybráno řešení od firmy MikroTik, konkrétně router MikroTik RB1100AHx2, který je často využíván v menších až středních firmách i ve své vylepšené verzi RB1100AHx4. V případě nasazení ve velkých firmách lze zvolit alternativní výkonnější zařízení od MikroTiku, avšak lze aplikovat stejné nastavení, jelikož všechny podnikové routery od MikroTiku využívají stejný operační systém MikroTik RouterOS. Modelové řešení se tak stává univerzálním a lze intuitivně aplikovat i na příbuzná zařízení. Na tento router jsou dále připojeny dual-band nebo také tri-band přístupové body, které pracují na frekvencích 2,4 GHz, 5 GHz a 6 GHz. Důvody vedoucí k výběru konkrétních přístupových bodů jsou vždy uvedeny v konkrétní modelové variantě.

V následující tabulce 5 jsou uvedeny tři routery, mezi kterými probíhal finální výběr pro nasazení ve firmě.

Tabulka 5 – Srovnání vybíraných routerů

Výrobce zařízení	MikroTik	Ubiquiti	Cisco
Označení zařízení	RB1100AHx2	EdgeRouter ER-12	C1111-8P
CPU	2-core, 1 GHz, P2020	4-core, 1 GHz, MIPS64	Neuvedeno
RAM	2 GB	1 GB	4 GB
Počet ethernet portů	13	10	8
Rychlost portů	10/100/1000 Mbit/s	10/100/1000 Mbit/s	10/100/1000 Mbit/s
L3 výkon 1518 bytů	4,2 Gbit/s	6,8 Gbit/s	Neuvedeno
Nejnižší aktuální cena	4 720 Kč	6 300 Kč	15 150 Kč

*Zdroj: [44] [45] [46]*

Alternativou k výběru řešení od MikroTiku bylo například řešení od firmy Cisco. Zatímco MikroTik RB1100AHx2 má pořizovací cenu od 4 720 Kč, alternativní zařízení z řady Cisco ISR 1100 Series začínají na částce 15 000 Kč za repasované kusy. Například při porovnání se zařízením Cisco C1111-8P nabízí řešení od MikroTiku mnohem nižší cenu za obdobný směrovací výkon. Naopak výhodou Cisca je přítomnost 8 PoE portů, avšak toto zařízení nabízí pouze jeden WAN port.

Další zvažovanou alternativou byl Ubiquiti EdgeRouter ER-12, který nabízí vyšší L3 výkon, ale nabízí méně ethernetových portů. Cena v porovnání s MikroTik zařízením je také vyšší.

Přítomnost PoE portů byla vyřešena podnikovým řešením od firmy TP-Link ve formě switchu TL-SG2428P, které lze využít k napájení některých přístupových bodů. Dalším důvodem je přijatelný počet portů pro potřeby modelové firmy a integrovaná platforma Omada Software. Detailně je popis tohoto zařízení uveden v kapitole, která se věnuje konfiguraci switchu v kapitole návrhu bezdrátové počítačové sítě.

V následující tabulce 6 jsou uvedeny tři switchy mezi kterými probíhal finální výběr. Veškeré tyto zařízení disponují PoE napájením a rychlostí jednotlivých portů až 1000 Mbit/s.

Tabulka 6 – Srovnání vybíraných switchů

Výrobce zařízení	TP-Link	Ubiquiti UniFi	HPE Aruba Instant On
Označení zařízení	TL-SG2428P	USW-24-POE	1930 24G POE
Počet ethernet portů	24	24	24
Rychlost ethernet portů	10/100/1000 Mbit/s	10/100/1000 Mbit/s	10/100/1000 Mbit/s
Počet SFP portů	4	2	4
Počet PoE/PoE+ portů	24	16	24
Maximální výkon PoE	250 W	95 W	370 W
Přepínací kapacita	56 Gbit/s	52 Gbit/s	128 Gbit/s
Nejnižší aktuální cena	7 360 Kč	10 199 Kč	12 090 Kč

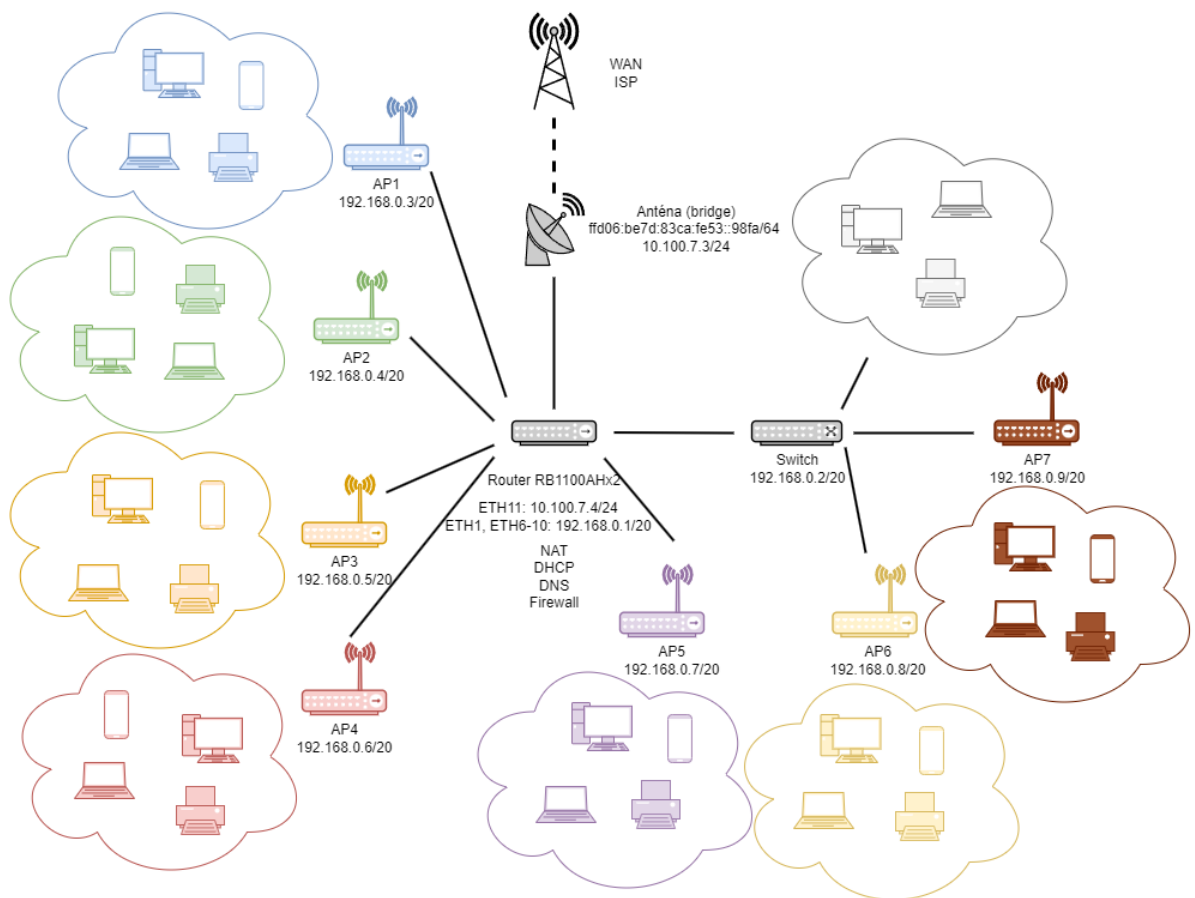
*Zdroj: [47]*

Mezi zvažovaná řešení patřil switch Ubiquiti UniFi USW-24-POE, který nabízí také 24 portů, avšak pouze 16 z nich je možné využít k napájení pomocí PoE, což je stále dostatečné množství, ale zároveň je možné zde napájet zařízení maximálně do celkového výkonu 95 W, což by nemusela být dostačující hodnota v závislosti na celkovém počtu přístupových bodů napájených pomocí tohoto switchu. Směrovací kapacita obou zařízení je obdobná. Zároveň je cena tohoto zařízení o 3 000 Kč vyšší, než u vybraného TP-Link switchu.

Další alternativou byl renomovaný výrobce HPE Aruba Instant On se svým zařízením 1930 24G POE, které nabízí 2x vyšší přepínací kapacitu, která by však v podmínkách modelové firmy neměla plně využít. Z tohoto důvodu bylo nakonec vybráno řešení od firmy TP-Link, které nabízí dostatečný výkon za přijatelnou cenu.

Na následujícím obrázku 7 je zobrazena navržená síťová topologie, dle které se provedla konfigurace síťových prvků v představených modelových variantách. Síťová topologie

obsahuje přístupový bod poskytovatele internetového připojení, příjmovou anténu firmy a následně také router, switch a jednotlivé přístupové body.



Obrázek 7 – Síťová topologie

Zdroj: Grafické rozhraní [50]

## 4 NÁVRHY BEZDRÁTOVÉ POČÍTAČOVÉ SÍTĚ

Tato kapitola se zabývá vlastním řešením bezdrátové počítačové sítě v modelové firmě. Nejprve kapitola obsahuje podrobný popis, návrh a odůvodnění výběru konkrétních síťových prvků a následně jsou zde vypracovány tři modelové varianty za využití různých vysokorychlostních bezdrátových řešení, které lze univerzálně aplikovat v reálném prostředí.

### 4.1 Návrh sdílených síťových prvků

V modelové firmě byla připravena technická místnost pro zřízení hlavního rozvaděče, kam jsou vyvedeny veškeré prvky kabeláže včetně připravené kabeláže pro přístup k internetu na střeše. V případě návrhu kabeláže je třeba dbát na několik základních zásad, jako je například definování požadavků sítě a její budoucí expanze, zvolený typ kabeláže nebo dodržení standardů a norem v oblasti kabeláže. Jelikož se tato práce zaměřuje zejména na bezdrátovou technologii, tak se zde počítá již s vyřešenou kabeláží. V tomto návrhu sdílených síťových prvků se tak popisují síťové prvky umístěné v hlavním rozvaděči, které jsou nutné pro provoz moderní počítačové sítě.

Po seznámení se strukturou kabeláže v celé firmě a dále také s veškerými požadavky firmy bylo třeba navrhnout kompletní osazení rozvaděče, které je přehledně uvedeno v následující tabulce 7 a následně i popsáno ve zbytku této kapitoly. Součástí není rozpis spotřebního materiálu.

Tabulka 7 – Použité sdílené síťové prvky

Kategorie hardware	Počet	Název hardware
Rozvaděč	1	XtendLan WS-15U-64-BLACK-U
Router	1	MikroTik RB1100AHx2
Switch	1	TP-Link TL-SG2428P
UPS	1	ADLER záložní zdroj UPS 400W 230V
Baterie	1	SSB olověná baterie AGM 12V 55Ah
Vyvazovací panel	2	Masterlan vyvazovací panel 1U, 24 mezer, plastový
Patch kabel	30	Masterlan patch kabel UTP, Cat5e (0,5m a 1m)
Rozvodný panel	1	Masterlan 19" rozvodný panel 8x 230V, hliníkový
Osvětlovací panel	1	EuroLan osvětlovací panel 1U LED
Záslepka	4	TRITON Záslepka 1U, černá

*Zdroj: Vlastní*

Rozvaděč je fyzické zařízení, které slouží k montáži a uspořádání síťových zařízení a komponentů do standardizovaného prostoru, a tím přispívá k efektivitě a spolehlivosti celé sítě. Rozvaděč je členěn na U jednotky o velikosti 44,45 mm. U rozvaděče je důležité vzít v úvahu potřeby konkrétní firmy a velikost její sítě.

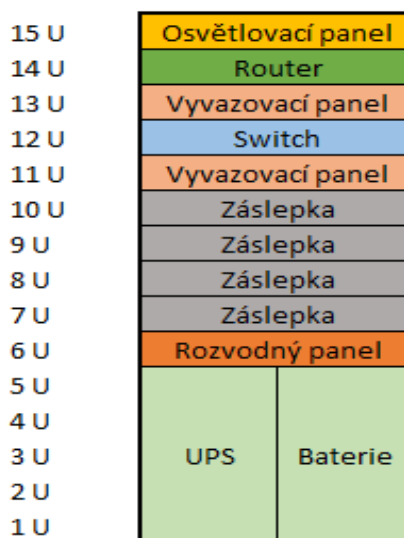
Pro vybranou firmu byl vybrán rozvaděč XtendLan WS-15U-64-BLACK-U, který má formát 19", kapacitu 15U a je zobrazen na obrázku 8. Důvodem výběru jsou ideální rozměry, poněvadž zde bude možné instalovat veškerá požadovaná zařízení, a navíc je počítáno s rezervou do budoucna. Rozměry rozvaděče jsou 600 x 450 x 769 mm, kdy dvířka jsou z bezpečnostního kaleného skla a ostatní strany jsou plně vyjma horního krytu, který má připravené otvory pro dva ventilátory. Součástí je bod pro připojení zemního vodiče a prostory pro kabeláž. [51]



Obrázek 8 – Rozvaděč XtendLan WS-15U-64-BLACK-U

*Zdroj: [51]*

Na následujícím obrázku 9 lze vidět rozmístění prvků v rozvaděči. Na nejvyšší U pozici je umístěn osvětlovací panel EuroLan 1U LED, který je standardizovaný a poskytuje LED osvětlení pro celý rozvaděč. [52] Vyvazovací panely jsou celkem dva MasterLan 1U, které mají 24 mezer pro kabeláž a slouží k organizaci kabeláže uvnitř rozvaděče. [53] Nevyužitý prostor byl zakryt záslepkami Triton 1U, které jsou vhodné pro zakrytí nepoužívaných pozic v datovém rozvaděči a lze je jednoduše demontovat. [54]



Obrázek 9 – Rozmístění prvků v rozvaděči

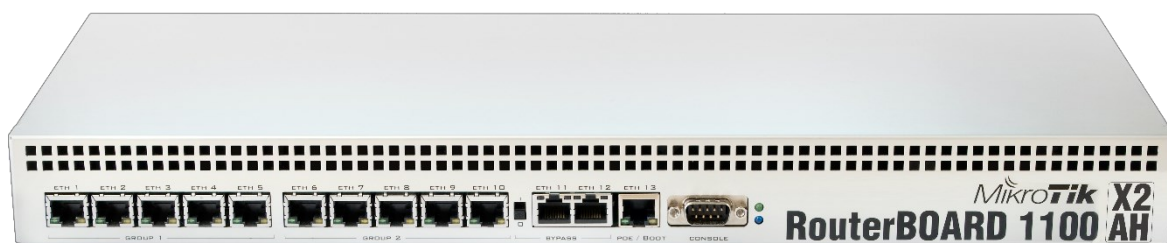
*Zdroj: Vlastní zpracování*



#### 4.1.1 Popis routeru MikroTik RB1100AHx2

Jako hlavní router byl vybrán MikroTik RB1100AHx2, který je osazen 13x 1 Gbit ethernetovými porty a je zobrazen na obrázku 10. Jedná se o dvoujádrový výkonný router, který je vhodný pro široké spektrum použití včetně použití ve středně velkých firmách. Důvodem výběru je oproti konkurenci cenově dostupné řešení s rozsáhlou podporou funkcí v operačním systému RouterOS. Jelikož tento systém běží i na dalších různě výkonných routerech MikroTiku, tak je možné využít nastavení routeru z následujících kapitol i u jiných routerů s podporou RouterOS a implementovat postup na další modelové příklady. Součástí tohoto modelu je MikroTik licence L6. [44]

Další předností tohoto routeru je možnost využití dvou portů v režimu bypass, kdy se porty 11 a 12 v případě výpadku napájení routeru spojí na fyzické vrstvě. To lze využít v případech, kdy využíváme redundantní zapojení a je například do jednoho portu připojena konektivita a do druhého portu připojen server. Router dále obsahuje PoE výstup na portu 13, kterým lze napájet další zařízení 12–24 V. Součástí je LED indikace každého portu. Router plně podporuje IPv4 a IPv6 a obsahuje integrovaný firewall. V routeru jsou integrované dva ventilátory pro efektivnější chlazení celého síťového prvku. Router je dodáván s úchyty pro montáž do rozvaděče, kde zabere pouze 1U. [44]



Obrázek 10 – MikroTik RB1100AHx2

*Zdroj: [44]*

V příloze lze nalézt obrázek 29 zobrazující blokové schéma tohoto routeru, ze kterého vyplývá, že router využívá procesor se dvěma jádry PowerPC P2020 1066MHz. CPU je připojeno ke dvěma switch čipům AR8327 kapacitou 1 Gbit/s. První switch čip je připojen na porty 1-5 a druhý switch čip je připojen na porty 6-10. Je tak důležité při zapojování dbát na rozložení zátěže právě mezi tyto dva switch čipy. Další 1 Gbit/s kapacitu poskytuje port 11. [44]

#### 4.1.2 Popis switchu TP-Link TL-SG2428P

Switch TP-Link TL-SG2428P nabízí 24 gigabytových portů s podporou PoE splňující standardy 802.3.af/at, s celkovým napájecím výkonem až 250 W a 4 gigabytové SFP porty,

kteře lze využít v případě potřeby k připojení optických vláken. Přepínací kapacita dosahuje hodnoty 56 Gbit/s. Nevýhodou jsou dva integrované větráky, které dosahují vyššího hluku a switch tak není vhodný do prostředí mimo serverovnu. V případě firmy, kde bude instalován, je však vyhrazeno místo oddělené a na hluku tak příliš nezáleží. [47]

Mezi softwarové funkce patří Storm Control, která chrání provoz proti broadcastovým a multicastovým bouřím. Tento switch nabízí podporu vrstev L2, L3 i L4 a nabízí tak velké množství funkcí z těchto vrstev. Nabízí plnou podporu IPv4 a IPv6 a také řízení síťového provozu pomocí QoS. Mezi další funkce patří VLAN, která se používá k usnadnění správy sítě, kdy je třeba agregovat koncová zařízení různého druhu, například různých firemních oddělení. Switch podporuje velké množství funkcionalit ACL, tedy řízení přístupu, kdy dle tabulky určuje, které zařízení má přístup k objektu a jaké operace může provádět a rozhoduje tedy o tom, jestli síťový provoz z daného zařízení může projít. Součástí je například MAC ACL, IP ACL nebo ACL vázané na rozhraní. [47]

Důvodem výběru je dostatečný počet ethernetových portů, které mohou být využity jednak na napájení přístupových bodů, anebo také na připojení koncových zařízení ve firmě. Do budoucna má firma možnost využít čtyř SFP portů pro připojení optických vláken. Dalším důvodem výběru je přívětivá cena tohoto zařízení oproti konkurenčním zařízením ve stejné kategorii. Switch je také připraven na instalaci do rozvaděče, kde zabere pouze 1U. [47] Switch je zobrazen na obrázku 11 a lze ho spravovat přes webové rozhraní nebo přes software Omada.



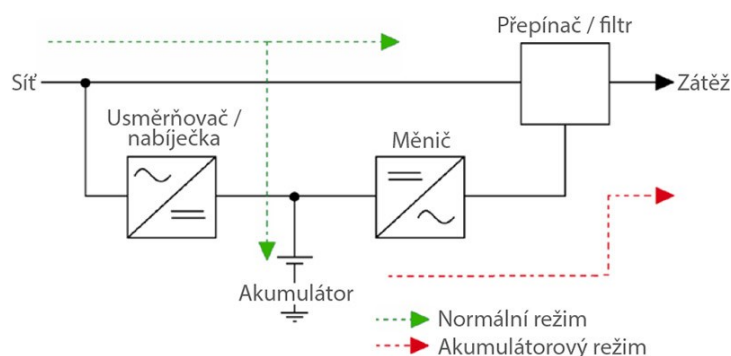
Obrázek 11 – TP-Link TL-SG2428P

*Zdroj: [47]*

### 4.1.3 Popis UPS ADLER

Využívání záložního zdroje UPS je nedílnou součástí moderních počítačových sítí. UPS poskytuje nepřetržitý zdroj elektrické energie pro veškerá zařízení na něj připojená a slouží také jako přepětová ochrana proti napětovým špičkám v rozvodné síti.

Důvodem výběru UPS ADLER 400 W, který je zobrazen na obrázku 13 je zejména jeho cena při srovnání s konkurenčními UPS, které mají integrované baterie. Jedná se o offline UPS systém. Při napájení ze sítě je veškerý hardware napájen přímo ze sítě a externí akumulátor je dobíjen. V případě výpadku elektrické energie se zdroj automaticky přepne na měnič napětí a elektrická energie je odebírána z 12 V akumulátoru. Doba přepnutí přepínače se pohybuje od 4 do 8 ms. [55] Po obnovení elektrické energie se zdroj automaticky přepne na napájení ze sítě a začne dobíjet akumulátor. Offline systém UPS se využívá u elektrických spotřebičů, kterým nevadí přerušování napětí v jednotkách několika milisekund, což splňují i vybrané síťové prvky. [55] [56]



Obrázek 12 – Offline systém UPS

*Zdroj:[55]*

Při celkovém příkonu všech použitých zařízení, který se bude pohybovat mezi 150 a 250 W, vydrží vybraná baterie SSB AGM 12 V 55 Ah dodávat elektrickou energii více než 3 hodiny, což je pro tyto účely dostačující doba. [57] [58] Pokud se budou následně přidávat další přístupové body nebo další hardware, může spotřeba stoupat až do 400 W, pro které je dimenzován použitý UPS, je zde tedy dostatečná rezerva. Avšak při vyšší zátěži už by bylo třeba využívat baterie o větší kapacitě, které UPS podporuje do velikosti 100 Ah. [56] Do UPS je připojen rozvodný panel, který nabízí montáž do 19" rozvaděče a poskytuje 8 zásuvek. Tyto elektrické zásuvky nabízí připojení pro adaptéry zařízení, případně pro PoE injektory. [56]



Obrázek 13 – UPS ADLER 400 W

*Zdroj:[56]*

## 4.2 Konfigurace sdílených síťových prvků

V následujících dvou podkapitolách byla provedena konfigurace routeru MikroTik RB1100AHx2 a switchu TP-Link TL-SG2428P dle schématu sítě.

### 4.2.1 Konfigurace routeru MikroTik RB1100AHx2

Pro konfiguraci routeru MikroTik byl využit program WinBox verze 6.49, který umožňuje správu MikroTik RouterOS pomocí grafického prostředí. Ve WinBoxu je možné využívat také terminál. Následující konfigurace proběhla v tomto grafickém rozhraní, avšak v příloze práce jsou uvedeny veškeré příkazy, které lze použít v konzolové části, včetně veškerých konfiguračních obrazovek.

Po prvotním připojení routeru bylo třeba router vyhledat v záložce „Neighbors“. Výchozí IP adresou routeru je 192.168.88.1/24. Druhou možností je připojení na základě MAC adresy pomocí služby MNDP, která byla využita i v tomto případě. Konfigurační obrazovka je uvedena na obrázku 30 v příloze.

Po prvním přihlášení k routeru se objevila hláška o výchozí konfiguraci routeru, kterou lze vidět na obrázku 31 v příloze. V tomto případě byla zvolena volba odebrání konfigurace pomocí tlačítka „Remove Configuration“. Alternativně lze použít příkaz v terminálu, který je uveden v příloze společně s ostatními příkazy potřebnými pro konfiguraci.

Nejprve bylo nutné změnit přístupové údaje, jelikož výchozí uživatel je nastaven bez hesla. Nastavení uživatelů se nachází v menu „System“ a následně v položce „Users“. Poté byl smazán výchozí uživatel admin a byl vytvořen uživatel sysadmin, kterému byla nastavena plná práva a vytvořeno heslo. Konfigurační obrazovka je zobrazena na obrázku 32 v příloze.

Dále byl nastaven název zařízení na Router-MikroTikRB1100, který slouží k identifikaci zařízení v místní síti. Nastavení se nachází v menu „System“ a záložce „Identity“, které je zobrazeno na obrázku 33 v příloze.

Poté bylo nezbytné v menu vybrat položku „Bridge“ a vytvořit rozhraní s názvem bridge, který slouží k vytvoření propojení mezi různými rozhraními ethernetu. Vybraná rozhraní, která byla vybrána mezi sebou komunikují na linkové vrstvě modelu ISO/OSI. STP bylo ponecháno na nastavení RSTP. Vytvoření bridge rozhraní je zobrazeno na obrázku 34 v příloze.

Po vytvoření bridge byla zvolena záložka „Ports“, kde byla přidána požadovaná rozhraní. V tomto případě bylo přiřazeno do bridge rozhraní eth1, kde byl připojen switch, čímž se rozloží zátěž mezi jednotlivé integrované switch čipy, jak bylo již zmíněno. Následně byly do

bridge přidány rozhraní eth6 až eth10, kde budou zapojeny AP1 až AP5 napřímo. Přidání rozhraní do bridge je zobrazeno na obrázku 35 v příloze.

Dalším nastavením, které bylo provedeno byla konfigurace IP adres, které se nachází v menu „IP“ a položce „Addresses“. Dle schématu sítě byla do rozhraní eth11 zapojena přijímová anténa s IP adresou 10.100.7.3/24. Routeru byla nastavena na rozhraní eth11 IP adresa 10.100.7.4/24. Ostatní požadovaná rozhraní jsou již přidána do rozhraní bridge. Dle schématu byla nastavena IP adresa 192.168.0.1/20 na rozhraní bridge, které obsahuje rozhraní eth1 a eth5 až eth10. Následně byly IP adresy okomentovány pro lepší přehlednost. Nastavení IP adres je zobrazeno na obrázku 36 v příloze.

Poté proběhla konfigurace směrování, které se nastavuje v menu „IP“, v záložce „Routes“. Jelikož má router nastavenou statickou IP adresu na rozhraní, které je připojeno do internetu, tak bylo nutné přidat výchozí bránu. V případě, že by získával router WAN IP adresu z DHCP serveru, nebylo by třeba toto nastavení provádět.

Jako cílová adresa (Dst. Address) byla nastavena IP adresa 0.0.0.0/0 a jako brána (gateway) IP adresa 10.100.7.1. Seznam všech nastavení lze nalézt v příloze na obrázku 37 v příloze. Poté byla dokončena konfigurace výchozí brány. Jedná se o bránu, kam se posílá veškerý síťový provoz, který se neshoduje s žádnou jinou konkrétní trasou.

Dalším krokem bylo nastavení DHCP serveru, které se nachází v menu „IP“ a záložce „DHCP Server“. Následně byla zvolena položka DHCP Setup, kde byly nastaveny parametry, které jsou zobrazeny v následující tabulce 8.

Tabulka 8 – Parametry nastavení DHCP serveru

Nastavení	Hodnota	Popis
DHCP Server interface	bridge	Rozhraní, na kterém bude zapnutý DHCP server
DHCP Address Space	192.168.0.0/20	Síťový rozsah IP adres
Gateway for DHCP Network	192.168.0.1	Výchozí brána pro DHCP server
Addresses to Give Out	192.168.0.100 - 192.168.15.254	Rozsah IP adres, které budou přiřazovány
DNS	10.254.253.250, 8.8.8.8, 8.8.4.4	DNS servery pro překlad adres
Lease time	1:00:00	Čas zapůjčení IP adresy

*Zdroj: Vlastní*

Na obrázku 38 v příloze je zobrazeno také nastavení ve WinBoxu, které je vygenerováno na základě DHCP setup.

Z důvodu zlepšení zabezpečení zařízení se doporučuje vypnout nepoužívané služby, které se týkají přístupu na zařízení. V tomto případě byly vypnuty veškeré služby, až na služby SSH a WinBox. SSH slouží pro zabezpečenou komunikaci se zařízením. Nastavení služeb je zobrazeno na obrázku 39 v příloze.

Dalším bezpečnostním prvkem, který bylo potřeba konfigurovat byl firewall. Nastavení pravidel firewallu bylo provedeno na základě doporučení oficiální MikroTik podpory, kdy první část pravidel přispívá ke snížení zátěže routeru, jelikož se bude router zabývat pouze nově připojenými zařízeními a nastaví možnost přístupu pouze z povolených IP adres. Poté bylo nastaveno pravidlo FastTrack pro rychlejší datovou propustnost. Kompletní seznam základních pravidel firewallu včetně konfigurační obrazovky lze vidět na obrázku 40 v příloze. Také byl v záložce „NAT“ na eth11 nastaven dynamický NAT, který zprostředkovává přístup do internetu zařízením, které používají privátní IP adresy, a to pomocí nastavení src nat masquerade. [59]

Dále proběhlo nastavení DNS serverů, jejichž hlavním úkolem je překlad doménových jmen a IP adres. Jako primární DNS server s IP adresou 10.254.253.250 byl nastaven DNS server od poskytovatele internetového připojení. Další dva sekundární DNS servery s IP adresami 8.8.8.8 a 8.8.4.4 provozuje společnost Google. Nastavení DNS je zobrazeno na obrázku 41 v příloze.

Pro korektní fungování veškerých funkcí routeru včetně logů bylo nutné provést synchronizaci času pomocí NTP serveru. Nastavení NTP serveru se nachází v menu „System“ a následně v záložce „SNTP Client“. Jako primární NTP server byl zvolen tik.cesnet.cz s IP adresou 195.113.144.201 a jako sekundární byl zvolen tak.cesnet.cz s IP adresou 195.113.144.238. Nastavení NTP serveru je zobrazeno na obrázku 42 v příloze.

#### **4.2.2 Konfigurace switche TP-Link TL-SG2428P**

Vybraný switch lze spravovat přes software Omada anebo přes webové rozhraní. V tomto postupu byla realizována konfigurace přes webové rozhraní, jelikož se jedná o univerzálnější řešení, protože není třeba používat TP-Link Omada Software kontroler.

Ve výchozím nastavení měl switch nastavenou IP adresu 192.168.0.1, přihlašovací jméno a heslo „admin“. Tato IP adresa byla použita pro přístup do webového rozhraní a následně byly zadány výchozí přihlašovací údaje. Tyto údaje bylo následně třeba změnit.

Nejprve byla nastavena IP adresa, jelikož ve výchozím nastavení používá tuto IP adresu více zařízení a mohlo by docházet ke kolizím v místní síti. Nastavení IP adresy se nachází v menu

„L3 Features“, v položce „Interface“. Dle připraveného schématu sítě byla nastavena statická IP adresa 192.168.0.2 s maskou 255.255.240.0. Nastavení IP adresy switchu lze nalézt v příloze na obrázku 43.

Poté proběhlo nastavení výchozí brány, které se nachází v položce „Static Routing“, následně bylo třeba kliknout na přidání pravidla. Výchozí bránou pro switch je router MikroTik RB1100AHx2 s IP adresou 192.168.0.1. Notace 0.0.0.0/0 definuje všechny možné IP adresy. Nastavení výchozí brány switchu jsou zobrazena na obrázku 44 v příloze.

Následně bylo třeba nastavit napájení přístupových bodů. V modelovém případě se počítá s napájením některých přístupových bodů právě přes switch. Jelikož switch podporuje aktivní PoE na základě standardů 802.3at/af, tak je možné i do portů, kde je zapnuté PoE zapojit zařízení, které napájení nevyžaduje bez vlivu na jeho funkčnost. Ve výchozím nastavení je PoE zapnuto na všech portech. Po přenastavení bylo PoE vypnuto na portu 1, který je připojen do routeru a následně také na portech 9–24 jelikož tyto porty slouží pro koncová zařízení, která nevyžadují napájení.

PoE status byl nastaven na „disable“. TP-Link má vytvořené power limit třídy, které určují, jaký limit výkonu bude určen pro jednotlivé porty. V tomto případě byla nastavena Class 4, kde je limit výkonu 30 W na port. Snižování limitu výkonu se využívá v případě, když je třeba napájet více zařízení a celkový výkon se blíží limitnímu 250 W výkonu zařízení. Vždy je však třeba dodržet požadovanou úroveň výkonu výrobce zařízení, které je na konkrétní port připojeno. Nastavení PoE portů switchu je zobrazeno na obrázku 45 v příloze.

Dále bylo nastaveno časové pásmo a také přidány NTP servery tik.cesnet.cz s IP adresou 195.113.144.201 a tak.cesnet.cz s IP adresou 195.113.144.238. Synchronizace času v síti je zásadní pro koordinaci událostí nebo také pro bezpečnost sítě, kdy jsou časová razítka důležitá například při auditu logů nebo pro sledování událostí v síti. Nastavení NTP serverů je zobrazeno na obrázku 46 v příloze.

Tato řada TP-Link smart switchů nabízí široké možnosti nastavení VLAN, STP, LLDP, QoS a zabezpečení včetně port security, ACL, DoS defend nebo 802.1x. Dále nabízí také široké možnosti monitorování vytížení CPU, RAM, síťového provozu a umožňuje diagnostiku jak zařízení, kde může být proveden link test, tak diagnostiku sítě pomocí ping a tracert.

Při konfiguraci konkrétního zabezpečení vždy záleží na konkrétních požadavcích firmy. Nastavení zabezpečení se nachází v záložce „Security“. Následně byl vypnut Telnet, jelikož

komunikace není šifrována a zbývá tak možnost využití SSH v případě potřeby konfigurace bez webového rozhraní, které tento switch také umožňuje. K webovému rozhraní byl nastaven přístup pouze pomocí protokolu HTTPS.

### 4.3 Modelová varianta I. (MikroTik & TP-Link)

V první modelové variantě byla vybrána přijímová anténa MikroTik Wire nRAY 60 GHz a pro firemní síť bylo vybráno řešení od firmy TP-Link. Následující podkapitoly obsahují postup konfigurace těchto síťových prvků a jejich základní popis.

#### 4.3.1 Konfigurace přijímové antény MikroTik Wire nRAY 60 GHz

V první modelové variantě, která byla vybrána zejména pro své nízké náklady a dobrý poměr cena a výkon, byla využita 60 GHz technologie v podobě MikroTik Wire nRAY 60 GHz. Dalším důvodem výběru této antény bylo splnění požadavků na kompatibilitu od poskytovatele internetového připojení. Jedná se o vysokorychlostní jednotku s rychlostí 1 Gbit/s a s dosahem až 1,5 km, která je napájena skrze PoE dle standardu 802.3af/at. Součástí jednotky je software RouterOS včetně licence L3 a díky tomu lze následující nastavení aplikovat na široké spektrum zařízení pracujících na stejném operačním systému. Stanice neobsahuje záložní 5 GHz rádio, což může snížit spolehlivost v případě špatných povětrnostních podmínek.



Obrázek 14 – MikroTik Wire nRAY 60 GHz

*Zdroj: [60]*

Pro konfiguraci antény MikroTik byl využit již zmíněný program WinBox verze 6.49. V několika oblastech je konfigurace obdobná jako v případě nastavování routeru MikroTik. Konfigurace uživatele (viz obrázek 47), identity zařízení (viz obrázek 48), DNS serveru (viz obrázek 54), NTP serveru (viz obrázek 55) je tak zobrazena pouze v příloze formou konfiguračních obrazovek.



Nejprve bylo třeba zařízení vyhledat v programu WinBox v záložce „Neighbors“. Výchozí IP adresou antény je 192.168.88.1/24. Po prvním přihlášení k anténě se objevila hláška o výchozí konfiguraci antény. V tomto případě byla zvolena volba odebrání konfigurace pomocí tlačítka „Remove Configuration“.

Dále byla v menu vybrána položka „Bridge“ a vytvořeno rozhraní s názvem bridge1, které je určeno k vytvoření propojení mezi bezdrátovou částí jednotky a ethernetem jednotky a je zobrazeno na obrázku 49 v příloze. Rozhraní, která byla vybrána, mezi sebou komunikují na linkové vrstvě modelu ISO/OSI. STP bylo ponecháno na nastavení RSTP.

Po vytvoření rozhraní bridge bylo možné přejít do vedlejší záložky „Ports“, kde bylo třeba přidat požadovaná rozhraní. V tomto případě bylo přiřazeno do bridge rozhraní eth1, které označuje ethernetové rozhraní a rozhraní wlan60, které označuje 60 GHz rozhraní antény. Konfigurace je zobrazena na následujícím obrázku 15.

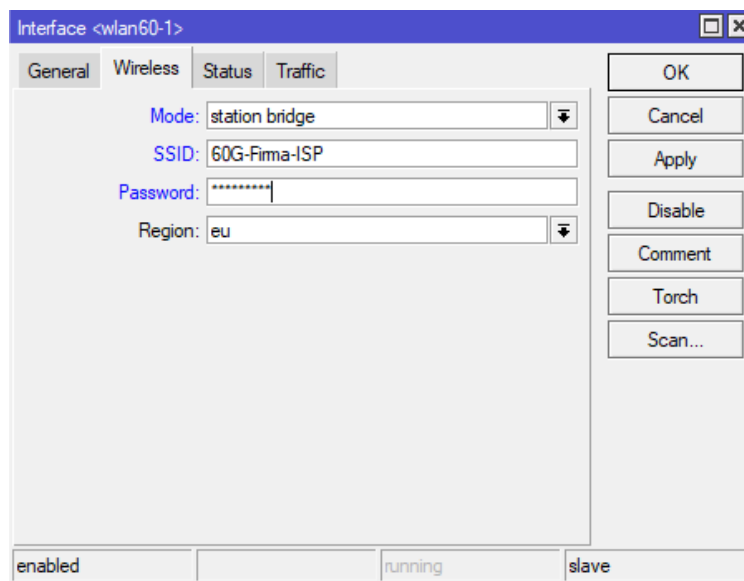
#	Interface	Bridge	Horizon	Trusted	Priority (h...)	Path Cost	Role	Root Pat...
1 H	ether1	bridge1		no	80	10	designated port	
0 I	wlan60-1	bridge1		no	80	10	disabled port	

2 items

Obrázek 15 – Přidání rozhraní do bridge

*Zdroj: Vlastní*

Dalším krokem bylo nastavení bezdrátového rozhraní, byla tedy vybrána záložka „Wireless“, následně položka „W60G“, kde bylo vybráno požadované rozhraní a otevřena karta „Wireless“. Zde byl nastaven mód zařízení station bridge, jelikož se jedná o stanici, zatímco ISP má na vysílači nastaven mód zařízení ap bridge. Poté bylo nastaveno SSID, heslo a region. Nastavení SSID a hesla neslouží pouze jako identifikátor, ale také jako základní zabezpečení připojení k zařízení. Tato nastavení lze vidět na následujícím obrázku 16.



Obrázek 16 – Wireless nastavení

*Zdroj: Vlastní*

Následně bylo provedeno nastavení IPv4 adresy, které se nachází v menu „IP“ a záložce „Addresses“. Dle schématu sítě byla nastavena statická IP adresa 10.100.7.3/24 na již vytvořené rozhraní bridge1. Nastavení IPv4 adresy je zobrazeno na obrázku 50 v příloze.

Dle požadavku poskytovatele měla mít anténa nastavenou také IPv6 adresu. Nejprve bylo třeba v menu „System“ a záložce „Packages“ povolit ipv6 balíček, který je v zařízeních MikroTik ve výchozím stavu vypnutý. To se provede vybráním požadovaného balíčku a následně stisknutím tlačítka enable. Na obrázku 51 v příloze jsou uvedeny veškeré balíčky, které jsou součástí firmware zařízení.

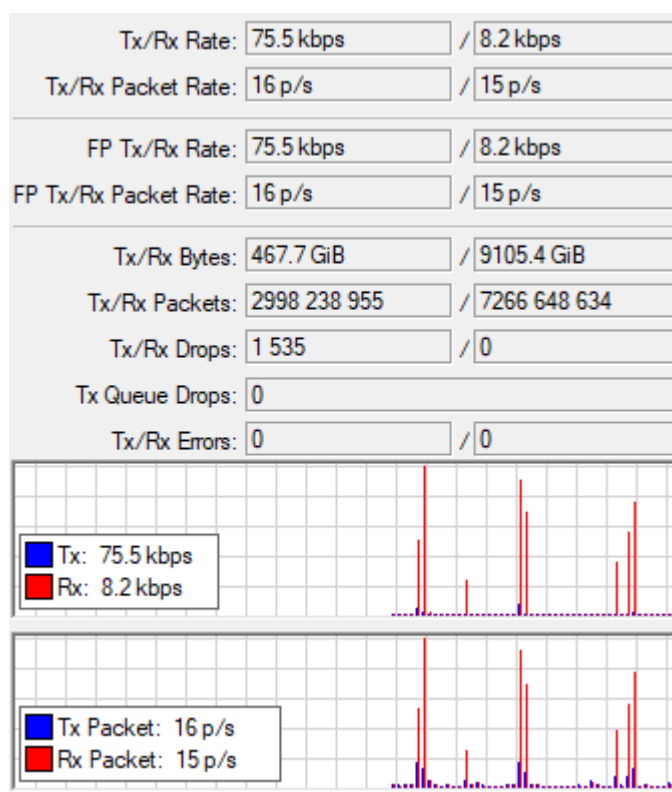
Po předchozím kroku se v menu objevila nová položka „IPv6“, kde byla vybrána záložka „Addresses“. Dle schématu sítě byla nastavena IPv6 adresa fd06:be7d:83ca:fe53::98fa/64. Nastavení IPv6 adresy je zobrazeno na obrázku 52 v příloze.

Poté bylo třeba nastavit směrování, které se nastavuje v menu „IP“ a v záložce „Routes“. Jako cílová IP adresa byla nastavena IP adresa 0.0.0.0/0 a jako brána IP adresa 10.100.7.1. Touto konfigurací byla nastavena výchozí brána. Jedná se o bránu, kam se následně posílá veškerý síťový provoz, který se neshoduje s žádnou jinou konkrétní trasou. Nastavení výchozí brány lze nalézt na obrázku 53 v příloze.

Potom bylo třeba se vrátit do menu „Wireless“, do položky „W60G“ a zvolit „Status“, kde se po připojení na vysílací anténu objeví hodnoty, dle kterých probíhá doladění. Je zde zobrazena síla signálu na stupnici od 0 do 100. MCS označuje konkrétní modulaci, v tomto případě bylo

dosaženo modulace 256-QAM. PHY Rate označuje rychlost dat, která je také v případě tohoto zařízení na maximu. RSSI je indikace síly přijatého signálu. Vyšší hodnoty signalizují silnější signál. Dosažená hodnota -55 dB je v tomto případě velmi dobrá. Bezdrátové hodnoty připojení jsou zobrazeny na obrázku 56 v příloze.

Ve vedlejší položce označené jako „Traffic“ je znázorněn aktuální síťový provoz na zařízení včetně grafu a celkových přenesených dat. Tato položka je zobrazena na následujícím obrázku 17.



Obrázek 17 – Síťový provoz

*Zdroj: Vlastní*

Nakonec bylo nutné aktualizovat anténu na nejnovější firmware, jelikož obsahuje zastaralou verzi operačního systému RouterOS 6. To je možné dvěma způsoby. V menu „System“ a záložce „Packages“ lze zvolit tlačítko „Check for Updates“, kde se vyhledá firmware online. V případě potřeby offline upgrade je možné stáhnout firmware na oficiálních stránkách výrobce, následně soubor nahrát na anténu v menu „Files“ a poté restartovat zařízení. Na obrázku 57 v příloze je uveden přehled verzí firmware.

Nyní byla konfigurace antény MikroTik v režimu bridge dokončena. Veškerá nastavení je možné provést také v konzoli zařízení. Příkazy jsou uvedeny v příloze této práce.

### 4.3.2 Konfigurace Wi-Fi 6 mesh sítě TP-Link

V této modelové variantě bylo vybráno řešení od firmy TP-Link, konkrétně pak řešení pro podnikové sítě Omada SDN. TP-Link Omada nabízí konfiguraci buď přímo ve firmwaru přístupového bodu, což se preferuje zejména při nastavování jednoho nebo dvou přístupových bodů, anebo pomocí kontroleru, a to buď hardwarového nebo softwarového pro správu většího počtu přístupových bodů. Kontroler spravuje veškerá připojená zařízení. [61]

Hlavním důvodem výběru je zejména nižší pořizovací cena, jelikož se firma TP-Link zaměřuje zejména na SOHO zařízení, tedy domácí prostředí, ale také na menší podnikové sítě, což je také případ modelové firmy. Pro porovnání jednotlivých modelových variant a pro nasazení do malých firem se však jedná o uspokojivé řešení. Pro robustnější síťové řešení od renomovaných výrobců, které se zaměřují na firemní prostředí doporučuji aplikovat další modelové varianty.

Pro konfiguraci byl využit softwarový kontroler Omada Software Controller V5. Jako přístupový bod byl vybrán TP-Link EAP610, který je vybaven 1 Gbit portem, který disponuje PoE napájením s podporou standardu 802.3af. Přístupový bod podporuje mimo jiné standard IEEE 802.11ax, tedy Wi-Fi 6 a je vybaven dual-band 2x2 MU-MIMO rádiem. [61]



Obrázek 18 – TP-Link EAP610

*Zdroj: [61]*

Výhodou použití řešení TP-Link Omada je, že veškeré síťové prvky z této řady sdílí velmi obdobné konfigurační prostředí v závislosti na aktuální verzi software. To znamená, že uvedený postup lze aplikovat na široké spektrum zařízení, což je dalším důvodem výběru zařízení v této modelové variantě.

Omada Software Controller V5 byl v tomto případě nainstalován na PC, které je třeba mít připojeno ve stejné síti jako síťové prvky, které bylo nutné konfigurovat. Výhodou tohoto softwaru je bezlicenční přístup a možnost vzdáleného přístupu přes cloud bez nutnosti VPN.

Pro spuštění software je třeba mít nainstalovanou aplikaci Java 8. Po stisknutí tlačítka „Launch“ proběhne přesměrování do webového prohlížeče. Poté bylo možné přejít na adresu localhost:8043, kde se zobrazí grafické rozhraní kontroleru. Na obrázku 58 v příloze je zobrazen Omada Software Controller.

Nejprve bylo nezbytné nastavit přístupové údaje hlavního administrátora a případně lze aktivovat přístup pomocí cloudu, které Omada podporuje, avšak pouze pro hardwarovou verzi. Na obrázku 59 v příloze lze vidět nastavení přihlašovacích údajů.

Poté bylo nutné zvolit tlačítko „Config New Setup“, který spustí průvodce prvotním nastavením kontroleru. Byl tedy nastaven název kontroleru, země umístění, aktuální časová zóna a notifikace aktualizací. Nastavení kontroleru je k nalezení v příloze, obrázek 60.

Následně proběhlo v druhém kroku nastavení názvu sítě, které se bude zobrazovat v kontroleru, jelikož je možné přes jeden kontroler spravovat více sítí. Konfigurace připojených AP byla přeskočena, jelikož proběhne až po dokončení průvodce prvotním nastavením. Obrázek 61 v příloze obsahuje popis jednotlivých záložek nastavení, které lze konfigurovat v případě potřeby. V základní konfiguraci jsou nejdůležitější první 4 položky.

Dále byla zvolena organizace a aktuální zvolená síť v pravém horním rohu. Poté bylo třeba v dolní části menu na levé straně přejít do nastavení. V první záložce „Site“ bylo ponecháno původní nastavení. Nastavují se zde zejména základní služby, tedy zapnutí indikační LED, limit šířky kanálu dle aktuálního umístění AP, mesh technologie, DFS, LLDP nebo vzdálený záznam. Mesh je ve výchozím nastavení zapnutý.

V případě, že by byl použit hardwarový kontroler, bylo by možné v záložce „Wired Networks“ nastavit porty v režimu WAN/LAN a také nastavit IP adresu zařízení na jednotlivých portech.

Poté bylo třeba v záložce „Wireless Networks“ konfigurovat veškerá nastavení bezdrátových zařízení, které se aplikuje na veškeré přístupové body, jež jsou adaptovány k tomuto kontroleru.

Jedná se o nastavení SSID, které bude vysíláno zařízením v okolí. Potom bylo třeba zvolit vysílací pásma. V tomto případě bylo zvoleno 2,4 GHz a 5 GHz, jelikož pásmo 6 GHz není podporováno vybranými přístupovými body. V budoucnu modelová firma může jednoduše přidat další přístupové body, které 6 GHz podporují a nastavení upravit. Na základě požadavku firmy bylo vybráno zabezpečení WPA-Personal, poněvadž je třeba směřovat k minimalizaci nákladů, proto nebylo možné použít například RADIUS server pro WPA-Enterprise.

Dalším krokem bylo zapnutí vysílání SSID, také bylo možné přiřadit bezdrátovou síť do zvolené VLAN. WPA mód byl zvolen WPA2-PSK/WPA3-SAE, to znamená, že zařízení, která nepodporují zabezpečení WPA3-SAE budou nadále pracovat ve WPA2 módu, díky tomu je možné připojovat i starší bezdrátová zařízení bez podpory WPA3.

Dále bylo možné zvolit nastavení PMF anebo také 802.11r, který umožňuje rychlejší roaming, avšak je vyžadována podpora koncového zařízení. Toto nastavení bylo nastaveno na vypnuto, jelikož aktuálně nepodporuje šifrování WPA3.

Následně byl nastaven limit na stahování a nahrávání dat pro každé připojené zařízení na 16 Mbit/s pro stahování a 2 Mbit/s pro nahrávání. Tento limit se využívá převážně v případech, kdy se očekává vysoký počet připojených zařízení, na které by nestačila konektivita sítě. Ve výchozím nastavení mají veškerá síťová zařízení neomezený limit.

Poté bylo možné nastavit plán vysílání SSID, toto nastavení se využívá ve specifických případech, například přes noc, kdy není bezdrátová síť využívána. Této funkce však v tomto případě nebylo využito. Mezi další nastavení patří Rate Control nebo také MAC filter, který je určen k povolení anebo blokování určitých MAC adres zařízení. Nejedná se však o příliš efektivní zabezpečení, jelikož MAC adresu síťové karty je schopný útočník odposlechnout. Veškerá nastavení karty wireless networks jsou zobrazena na obrázku 62 v příloze.

Na další kartě „Network Security“ je možné nastavit ACL pravidla, což představuje seznam zařízení, které mají povolení přistupovat k objektu a následně jim umožňuje provádět určité operace. Mezi další možnosti nastavení patří URL Filtering, který blokuje určený seznam URL, na která koncová zařízení nemohou přistupovat. Příklad takového pravidla je uveden na následujícím obrázku 19.

NAME	ENABLED	POLICY	SOURCE	FILTERING URLS
Gateway URL_Filtering...	<input checked="" type="checkbox"/>	Deny	Network:LAN	www.tp-link.com

Obrázek 19 – URL Filtering

*Zdroj: Vlastní*

V následujících záložkách je pak možné nastavit možnosti firewallu, NAT, QoS, VPN, CLI a dalších služeb. V tomto modelovém příkladě však tyto funkce nebyly konfigurovány, jelikož je základní konfigurace nevyžaduje. Je však důležité mít o těchto možnostech přehled a v případě, že budou vyžadovány, tak je efektivně aplikovat. Široké možnosti nastavení jsou důležité jako kritéria výběru konkrétního řešení.

Následně bylo třeba fyzicky připojit přístupové body dle schématu sítě a zvolit záložku „Devices“, kde se dostupné přístupové body zobrazí. Poté bylo třeba kliknout na položku „Adopt“, která přiřadí přístupové body ke kontroleru a přenesse zvolené konfigurace. Pokud by probíhalo nastavení bez kontroleru, bylo by třeba každý přístupový bod konfigurovat zvlášť, což komplikuje prvotní nastavení a případnou následnou správu počítačové sítě. Přidání AP do kontroleru je zobrazeno na obrázku 63 v příloze.

Po dokončení přidání přístupových bodů je zobrazen status „Connected“. Následně je ještě za statusem zobrazeno připojení, a to buď drátově anebo bezdrátově. V modelovém příkladě byla veškerá AP připojena drátově. V případě dostupnosti novější aktualizace firmware výrobce doporučuje tyto aktualizace instalovat ihned, případně nastavit automatické aktualizace v méně vytižené časy přístupu do sítě.

Po rozkliknutí jednotlivých AP bylo možné si zobrazit seznam připojených klientů, jejich MAC adres a aktuálně využívaného SSID a pásma. Také lze také zobrazit statistiky provozu, využití CPU a operační paměti AP.

Poté bylo třeba v jednotlivých AP přejít do položky „Config“ a dále rozkliknout položku „IP settings“. Ve výchozím nastavení je nastavený mód DHCP, ten je třeba vypnout a nastavit statickou IP adresu dle přiloženého schématu sítě. V tomto případě byla nastavena IP adresa 192.168.0.3 s maskou sítě 255.255.240.0, výchozí bránou 192.168.0.1 a DNS servery 10.254.253.250 a 8.8.8.8. Nastavení IP adresy je zobrazeno na obrázku 64 v příloze.

Další nastavení rádií konkrétního AP se doporučuje ponechat na položce „Auto“, jelikož je upravována šířka pásma a vysílací kanál na základě více sledovaných parametrů včetně aktuálního rušení v okolí AP. V dalších položkách menu si je možné zobrazit mapu sítě v případě použití hardwarového kontroleru. Dále je možné si zobrazit veškeré připojené klienty a procházet statistiky provozu. Také je možné procházet souhrnné zprávy provozu a na základě toho případně provést další konfiguraci zařízení.

Nyní byla dokončena konfigurace Wi-Fi mesh sítě s využitím AP TP-Link EAP610. Obdobný postup lze aplikovat na veškerá zařízení z řady TP-Link Omada a tento postup lze využít univerzálně. V základní sestavě vychází toto řešení nejlevněji, avšak v případě větší sítě je třeba připočítat náklady na hardwarový kontroler a také za vyšší řadu AP, které se v některých případech cenově vyrovnají s Ubiquiti AP, které jsou použity v alternativní modelové variantě.

## 4.4 Modelová varianta II. (Ubiquiti)

V modelové variantě II. byla použita přijímová anténa Ubiquiti UISP Wave Nano 60 GHz. Pro firemní síť byla nakonfigurována Wi-Fi 6E mesh síť založena na Ubiquiti UniFi U6 Enterprise. Následující podkapitoly popisují postup konfigurace těchto síťových zařízení.

### 4.4.1 Konfigurace přijímové antény Ubiquiti UISP Wave Nano 60 GHz

V této modelové variantě byla využita venkovní jednotka Ubiquiti UISP Wave Nano, která splňuje požadavky na kompatibilitu, jež je uvedena v podmínkách od poskytovatele internetového připojení. Jednotka pracuje na frekvenci 60 GHz a její teoretický dosah je až 5 km se ziskem rádia až 41 dBi. Propustnost jednotky je maximálně 2 Gbit/s. Stanice je vybavena také 5 GHz rádiem, které slouží pro záložní spojení v případě narušení 60 GHz rádia.

Jednotka disponuje GPS a Bluetooth připojením a mimo webové rozhraní podporuje také správu přes mobilní aplikaci UISP Mobile. Anténa je napájena pomocí PoE, jejíž injektor byl umístěn v rackové skříni a následně byl zapojen do routeru.



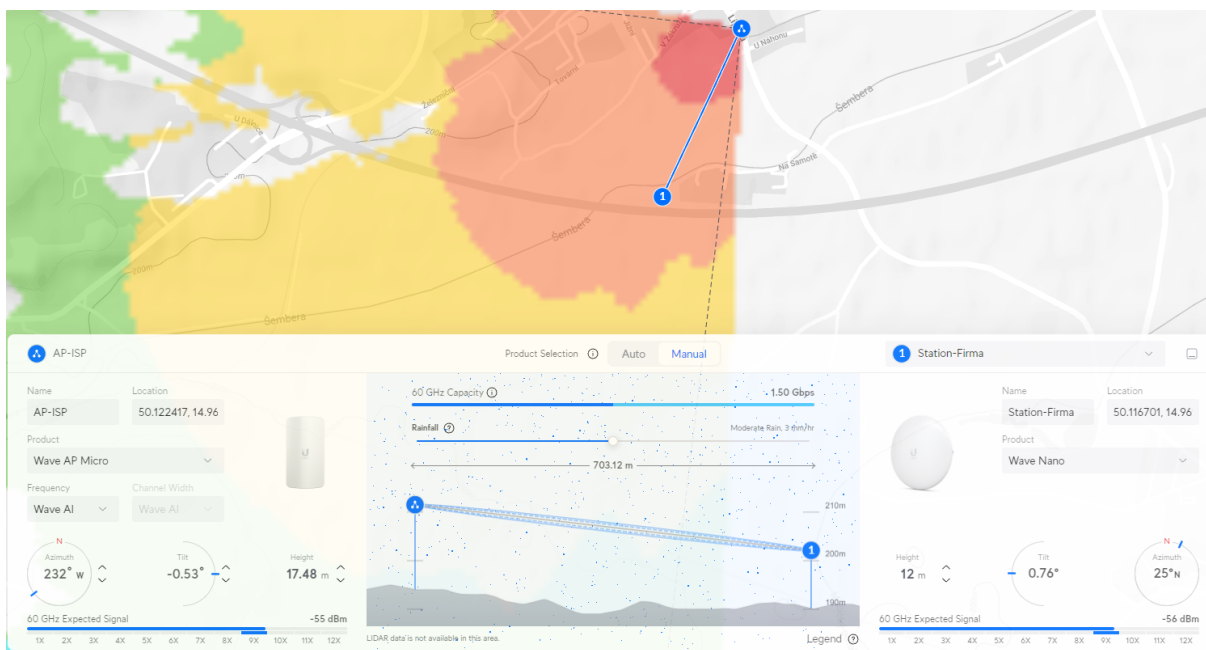
Obrázek 20 – Ubiquiti UISP Wave Nano 60 GHz

*Zdroj: [62]*

Výrobce doporučuje před zahájením instalace simulovat vyzařování signálu a další potřebné parametry. Zároveň je dobré upozornit, že se jedná pouze o simulaci a je třeba v reálném prostředí počítat převážně s nižšími hodnotami signálu a vyššími hodnotami rušení. Na následujícím obrázku 21 je zobrazen návrh připojení v UISP Design Center, který zobrazuje umístění sektorové antény Wave AP Micro, kterou provozuje poskytovatel internetového připojení a také anténu Wave Nano, která byla instalována na střechu modelové firmy.

Nejprve je ověřena kvalita signálu bez deště a poté je simulována kvalita signálu s deštěm, který lze nastavit od 0 do 6 mm/h. Anténa je od sektorové antény vzdálena 700 m, avšak stále poskytuje na 60 GHz kapacitu až 1,5 Gbit/s, a to i v případě simulovaného deště na úrovni 6 mm. Kapacita záložního 5 GHz rádia byla softwarem stanovena na teoretických 555 Mbit/s.





Obrázek 21 – Návrh v UISP Design Center

*Zdroj: [63]*

Po simulaci v programu bylo možné přistoupit k reálnému nastavení antény. Nejprve bylo třeba se připojit k zařízení. To je možné buď napřímo ethernetem, anebo pomocí Bluetooth a aplikace UISP Mobile. V tomto případě byl zvolen postup přes GUI antény, dále bylo třeba se přihlásit, výchozí přihlašovací jméno je u tohoto zařízení „ubnt“ a výchozí heslo je také „ubnt“.

Vzhledem k tomu, že sektorovou anténu Wave AP Micro spravuje poskytovatel internetového připojení, tak bylo třeba dodržet jeho požadovaná nastavení. V záložce „Wireless“ u 60 GHz rádia byla nastavena šířka kanálu 2 160 MHz na frekvenci 64 800 MHz. Na záložní 5 GHz rádio byla nastavena šířka kanálu 20 MHz a frekvence 5 240 MHz. Nastavení frekvencí a šířky kanálu jsou zobrazena na obrázku 65 v příloze.

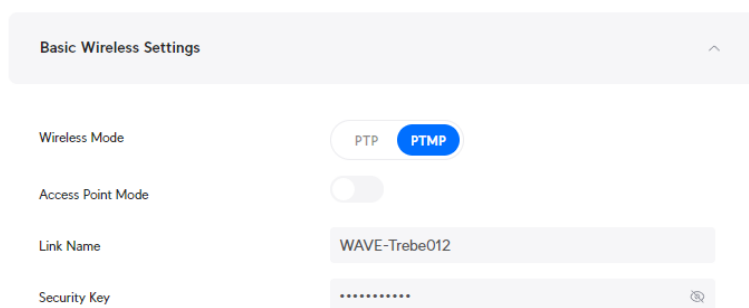
Dalším krokem bylo v záložce „Network“ nastavit anténu do režimu bridge, jelikož na routeru je nastavena statická IP adresa a DHCP server je spuštěn až na routeru. Poté byla nastavena statická IP adresa 10.100.7.3 s maskou 255.255.255.0 a výchozí bránou 10.100.7.1. Tyto IP adresy vychází ze schématu sítě a byly přiděleny od poskytovatele internetového připojení. Velikost MTU byla ponechána na výchozí hodnotě 1 500 bajtů, což je standardní maximální přenosová jednotka v ethernetu.

Dále bylo potřeba nastavit IPv6 adresu, která byla také přidělena. Byla tedy nastavena IP adresa fd06:be7d:83ca:fe53::98fa/64 a také výchozí brána fd06:be7d:83ca:fe53:ffff:ffff:ffff:ffff. V případě potřeby lze v budoucnu pracovat s IPv6 adresami i ve vnitřní síti organizace, jelikož

veškeré vybrané síťové prvky plně podporují IPv6 adresaci. Na obrázku 66 v příloze jsou zobrazena veškerá síťová nastavení.

Dále bylo třeba provést nastavení DNS serverů. Primární DNS server 10.254.253.250 je DNS serverem poskytovatele internetového připojení a sekundární DNS server 8.8.8.8 je veřejný DNS server od společnosti Google. Nastavení DNS je zobrazeno na obrázku 67 v příloze.

Poté bylo třeba dokončit nastavení na kartě „Wireless“, kde byl zvolen mód PTMP, tedy Point-to-Multi-Point, jelikož se anténa připojuje na sektorovou anténu, na kterou mohou být připojeny i další antény v okolí. Dále bylo třeba zadat Link Name a Security Key, které byly dodány od poskytovatele internetového připojení a slouží k navázání spojení se sektorovou anténou a chrání ji tak před neoprávněným připojením externího síťového zařízení.



Obrázek 22 – Nastavení bezdrátového módu

*Zdroj: Vlastní*

Následovně bylo třeba v záložce „System“ nastavit NTP server, který synchronizuje čas v síti. Byl zvolen server tik.cesnet.cz s IP adresou 195.113.144.201. Nastavení NTP serveru je zobrazeno na obrázku 68 v příloze.

Ve stejné záložce byla vybrána položka „Firmware“. Jelikož se jedná o novou řadu produktů, tak vychází aktuálně firmware v BETA testování. Každá tato aktualizace je velmi důležitá, jelikož přináší opravy chyb a nové funkce. Výrobce však musí přístup k BETA testování udělit, jinak je možné instalovat pouze běžně vydávané aktualizace, kdy poslední je ze srpna 2023 zatímco BETA firmware vyšel v lednu 2024. Přístup k beta testování byl výrobcem udělen a anténa byla tedy aktualizována na firmware 3.3.0-BETA4. Aktualizace firmware je zobrazena na obrázku 69 v příloze. V posledních aktualizacích byla přidána funkce port managementu. Na obrázku 70 v příloze lze přehledně zjistit, že se přes tento port zařízení napájí a jaká je aktuální rychlost připojení. Tato funkce má i další využití u sektorových antén z této řady.

Následně již bylo možné veškerá provedená nastavení uložit a vyčkat na spojení antény s AP. Potom bylo třeba anténu doladit jak vertikálně, tak horizontálně, aby bylo dosaženo co

nejlepšího signálu. Hodnoty signálu lze vidět na následujícím obrázku 23. Hodnoty přibližně odpovídají nasimulovaným hodnotám, ale z převážné většiny případů jsou tyto hodnoty horší, jelikož nasazení v reálném prostředí má mnoho faktorů, které software nedokáže úplně přesně simulovat. Lze tak vidět, že signál na záložním 5 GHz rádiu ze strany antény je v pořádku, avšak ze strany sektoru je horší na úrovni 72 dBm. Tento problém byl následně opraven v příštím vydání firmware zařízení.

Důležité bylo kontrolovat hodnoty maximální přenosové kapacity, která byla cílena na 1,5 Gbit/s, což je dostatečná hodnota a bude tak s rezervou stačit dodávanému tarifu. V případě přepnutí na záložní rádio se přenosová rychlost sníží.



Obrázek 23 – Hodnoty signálu antény

*Zdroj: Vlastní*

Na obrázku 71 v příloze lze zkontrolovat celkovou přenosovou kapacitu rádií. V případě, že by kapacita kolísala, je nutné anténu ještě dále doladovat, případně provést jiná nastavení šířky kanálu nebo také frekvence. Když byla anténa zajištěna proti dalšímu pohybu, tak bylo možné provést otestování rychlosti. K tomu slouží integrovaný nástroj pro ověření rychlosti mezi anténami. Z obrázku 72, který je uveden v příloze vyplynulo, že celková naměřená kapacita byla 1460 Mbit/s a odezva byla 0,86 ms. Rychlost stahování byla ustálena na hodnotě 780 Mbit/s a rychlost odesílání na hodnotě 680 Mbit/s. Testování proběhlo bez ztížených podmínek. V případě, že tyto podmínky nastanou, bude pravděpodobně rychlost klesat, a to v závislosti na celkovém úhrnu srážek. Na instalovanou vzdálenost 700 m se předpokládá, že k zapnutí záložního 5 GHz rádia bude docházet zcela ojediněle. Registraci stanice provedl poskytovatel internetového připojení. Nyní byla konfigurace příjmové antény dokončena.

#### 4.4.2 Konfigurace Wi-Fi 6E mesh sítě Ubiquiti

V druhé modelové variantě bylo vybráno řešení od firmy Ubiquiti, konkrétně pak jeden z nejvyšších modelů řady Ubiquiti UniFi U6 Enterprise, který je zobrazen na následujícím obrázku 24 a je vybaven 2,5 Gbit portem, který podporuje napájení skrze PoE+, tedy standard 802.3at. Přístupový bod podporuje standard 802.11ax ve variantě Wi-Fi 6E. Tento přístupový bod disponuje tri-band rádiem. 2,4 GHz podporuje 2x2 MU-MIMO, 5 GHz a 6 GHz pak podporuje 4x4 MU-MIMO. Zisk antén v pásmu 2,4 GHz je 3,2 dBi, v pásmu 5 GHz 5,3 dBi a v pásmu 6 GHz 6 dBi. Celková teoretická přenosová rychlost je celkem 10 200 Mbit/s. [64]



Obrázek 24 – Ubiquiti UniFi U6 Enterprise

*Zdroj: [64]*

Zařízení Ubiquiti UniFi lze konfigurovat dvěma způsoby. Prvním způsobem je UniFi Network Server, který je primární volbou při konfiguraci více přístupových bodů. Druhým způsobem je konfigurace přístupového bodu pomocí mobilní aplikace UniFi Network. UniFi Network Server je možné spustit na jakémkoliv zařízení s operačním systémem Windows, macOS nebo Linux. Ubiquiti podporuje také vlastní řešení pomocí hardwarového kontroleru, který disponuje operačním systémem UniFi OS.

Nejdříve bylo nutné vytvořit na PC UniFi Network server verze 8.0.28. Ten slouží pro kontrolu jednotlivých přístupových bodů v rámci Ubiquiti UniFi. Následně bylo možné přejít do webového rozhraní, které je přístupné z adresy 127.0.0.1:8080. K využívání tohoto rozhraní je nutná registrace na stránkách Ubiquiti.

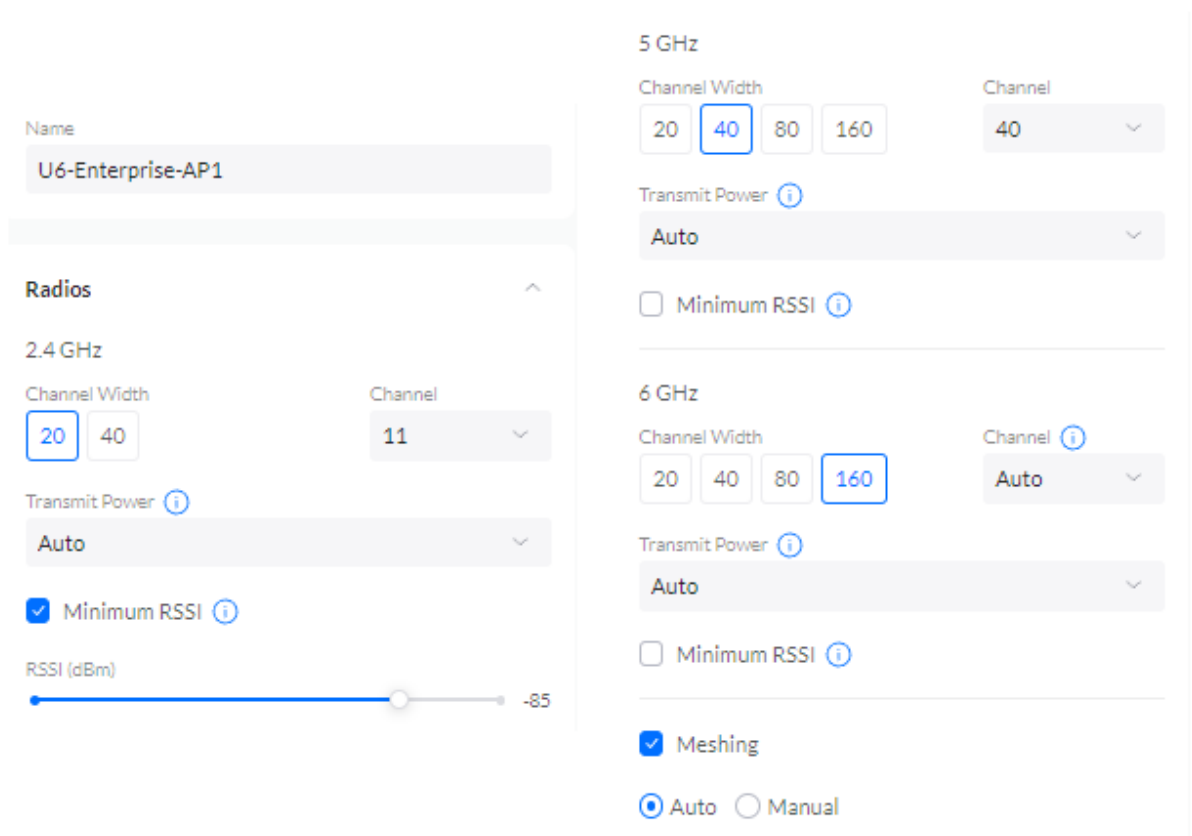
V dalším kroku bylo třeba přejít v menu do položky „UniFi Devices“, kde se zobrazí veškeré aktuálně dostupné přístupové body. Dále je třeba přístupový bod přidat do správy pomocí položky „Click To Adopt“. Přidání do správy trvá přibližně 3 minuty, poté se každé zařízení aktualizuje a restartuje. Seznam zařízení UniFi lze vidět na obrázku 73 v příloze.

Po přidání zařízení bylo třeba pokračovat v konfiguraci pomocí položky „Insights“, kde se nachází položka „RF Environment“, která je určena ke skenování vysílacích pásem v okolí a míry rušení. Na základě tohoto skenování je pak možné optimálně zvolit kanály k vysílání. Toto skenování trvá přibližně 10 minut.

Nejméně využité kanály jsou šedě označené, oranžová až červená barva pak označuje vyšší využití kanálu a tím pádem vyšší míru rušení. Na základě této analýzy byly následně zvoleny kanály v následujícím kroku. V pásmu 2,4 GHz se nepřekrývají při šířce kanálu 20 MHz pouze kanály 1, 6 a 11. Toto skenování je dostupné pro přenosová pásma 2,4 GHz a 5 GHz. Níže na obrázku 25 lze vidět přehled veškerých dostupných kanálů a míry jejich využití. Skenování kanálů je zobrazeno na obrázku 74 v příloze.

Po naskenování kanálů bylo možné přejít k nastavení rádií přístupového bodu, které se nachází v položce „Settings“. Nejprve byl přístupový bod přejmenován dle schématu sítě, v tomto případě AP1.

Následně bylo na 2,4 GHz rádiu nastavena šířka kanálu 20 MHz, kanál 11, minimum RSSI - 85 dBm a automatický vysílací výkon. V případě, že by byla hodnota high, tak by vznikalo nadměrné rušení, jelikož se přístupové body ve firmě vzájemně signálově překrývají. Tato hodnota se používá pouze, pokud jsou přístupové body dál od sebe. V ostatních případech se pak používá zpravidla hodnota auto, která zvolí vysílací výkon v závislosti na zařízení v okolí anebo se také používá hodnota medium. Na 5 GHz rádiu byla nastavena šířka kanálu 40 MHz, kanál 40 a automatický vysílací výkon. Na posledním 6 GHz rádiu byla nastavena šířka kanálu 160 MHz a kanál s vysílacím výkonem na automatickou hodnotu. Tyto šířky kanálu byly zvoleny zejména proto, že 2,4 GHz má mnohem lepší průchodnost překážkami a nižší šířka kanálu mu umožňuje připojit i vzdálenější zařízení. 5 GHz a 6 GHz je pak využíváno na velmi rychlý přenos dat na nižší vzdálenosti. Poté byla ještě nastavena položka Meshing na Auto, která umožní přístupovým bodům vysílat v režimu mesh.



Obrázek 25 – Nastavení rádií

*Zdroj: Vlastní*

Položka „Band Steering“ byla nastavena na balanced. Další možností je nastavit tuto hodnotu na off, kdy se budou zařízení připojovat na AP podle svých preferencí. V případě zvolení možnosti prefer 5 GHz budou zařízení, která podporují toto pásmo připojována primárně na 5 GHz. V tomto případě zvolená hodnota balanced bude vyrovnávat zátěž mezi jednotlivými pásmy dle aktuálního zatížení. Pro zařízení, která jsou připojena s horším signálem, bude preferováno pásmo 2,4 GHz, naopak pro zařízení, která mají kvalitní signál 6 GHz, bude preferováno právě toto rádio, které dosahuje nejvyšší přenosové rychlosti.

Dále bylo třeba nastavit IP adresu na položku static a dle schématu sítě provést síťové nastavení. U AP 1 byla tedy nastavena IP adresa 192.168.0.3 s maskou 255.255.240.0 a výchozí bránou 192.168.0.1. Také byly nastaveny IP adresy DNS serverů na hodnotu 10.254.253.250 a 8.8.8.8.

Na obrázku 75 v příloze je zobrazené grafické rozhraní nastavení sítě, kde byly nastaveny potřebné hodnoty. Mimo další nastavení pak patří vypnutí notifikační LED na přístupovém bodě nebo zapnutí SNMP.

Následně bylo možné uložit nastavení a přejít do hlavního menu „Settings“ a vybrat položku „WiFi“, kde se nastavují parametry Wi-Fi, které se následně aplikují na veškeré přístupové

body. Byla vybrána veškerá dostupná pásma vysílání 2,4 GHz, 5 GHz a 6 GHz. Mezi vybrané položky patří „Band Steering“ a „BSS transition“, který podporuje rychlejší přechod zařízení mezi jednotlivými AP. U těchto položek je vždy třeba plná podpora připojeného zařízení.

Další možné položky nastavení jsou „Client Device Isolation“, tedy izolace připojených zařízení, která zamezí komunikaci mezi zařízeními. Toto nastavení se nepoužilo, jelikož znemožňuje komunikaci například síťových tiskárnám. Dále „Proxy ARP“, který umožňuje propojit několik lokálních sítí pomocí protokolu ARP. Položka „UAPSD“ je určena pro úsporu energie v případě nečinnosti. Položka „Fast Roaming“ je určena pro podporu standardu 802.11r, avšak zařízení, která nepodporují tento standard mohou mít problémy s připojením k síti. Položka „WiFi Speed Limit“ je určena pro omezení rychlosti stahování a nahrávání v sítích, kde je rychlost třeba regulovat z důvodu omezené internetové konektivity. Běžně se nastavuje mezi 10–50 Mbit/s pro běžná zařízení. Položky „Multicast Enhancement“ a „Multicast and Broadcast Control“ jsou určeny pro konverzi síťového provozu.

V rámci konfigurace zabezpečení je možné nastavit filtr MAC adres v položce „MAC Address Filter“ a dále pak RADIUS server. V tomto případě byl využit bezpečnostní protokol WPA3. Také je možné nastavit čas vysílání bezdrátového připojení dle plánu. Na obrázku 76 v příloze jsou přehledně zobrazeny veškeré možnosti nastavení Wi-Fi, které bylo aplikováno na veškeré připojené přístupové body.

V další položce „Networks“ je možné nastavit virtuální sítě a také další položky, mezi které patří například povolení IPv6 podpory. Položky „IGMP Snooping“ a „DHCP Snooping“ jsou určeny k zapnutí stejnojmenných optimalizačních mechanismů. Dále je možné vybrat „Spanning Tree Protocol“, kde byl vybrán RSTP z důvodu rychlejší reakce oproti STP. Položka „Jumbo Frames“ je určena k povolení rámců větších než 1 500 bytů, tato položka byla vypnuta.

Nyní byla dokončena konfigurace sítě s využitím AP Ubiquiti UniFi. Totožný postup lze aplikovat na veškerá zařízení s operačním systémem UniFi OS, a tak se tento postup stává univerzálním řešením. Druhá modelová varianta je nejdražší, avšak nabízí využití zařízení renomovaného výrobce, který nabízí dlouhou podporu těchto zařízení. Tato zařízení jsou velmi často využívána ve velkých firmách, kde obsluhují tisíce připojených zařízení. Jedná se tak o vhodné řešení i pro největší firmy. Samozřejmostí je vhodnost využití i v modelové firmě, jelikož je řešení plně modulární a je tak možné velikost sítě plně přizpůsobit bez vlivu na výkon konkrétního přístupového bodu.

## 4.5 Modelová varianta III. (Ubiquiti & Reyee)

V této modelové variantě byla použita příjmová anténa Ubiquiti UISP Wave Nano 60 GHz, jejíž nastavení proběhlo v modelové variantě II. Pro firemní síť bylo využito řešení od firmy Ruijie Networks, konkrétně jejich značka Reyee. Ruijie Networks je jedním z předních světových dodavatelů síťových prvků a poskytuje komplexní síťová řešení pro vládní agentury, vzdělávací instituce, bankovní instituce nebo telekomunikační operátory. Ruijie Networks má více než 50 poboček a více než 60 obchodních zastoupení v různých zemích Asie, Evropy, Severní Ameriky a Jižní Ameriky. [65]

Jedním z důvodů výběru síťových řešení od této společnosti bylo rozhodnutí firmy před několika lety expandovat do Evropy. Jako první země pro expanzi byla vybrána Česká republika společně s Německem a Tureckem. V budoucnu se tak očekává větší nasazení těchto zařízení také v dalších zemích Evropy. Ruijie Networks obsadila v roce 2022 3. místo na trhu Enterprise Wi-Fi v Číně a 1. místo mezi produkty řady Wi-Fi 6. Jedná se tak o hojně rozšířené síťové prvky, které lze efektivně využívat, a proto jsou zahrnuty v této modelové variantě. [65]

Konkrétně byl vybrán bezdrátový Wi-Fi 6 AP Reyee RG-RAP2260(G), který je vybaven dvěma 1 Gbit LAN porty, z nichž jeden disponuje podporou napájení přes PoE. Jedná se o dual-band 2x2 MU-MIMO rádio. Výhodou je, že zařízení využívá stejné webové rozhraní jako další síťové prvky z této řady a postup tak lze aplikovat univerzálně. [66]



Obrázek 26 – Reyee RG-RAP2260(G)

*Zdroj: [66]*

Po připojení napájení AP bylo třeba se nejprve připojit na SSID @Ruijie-mxxxx, druhou možností bylo připojit se přes ethernet. V tomto případě bylo využito napájení pomocí PoE a odpadla tak potřeba využití adaptéru v místě instalace.

Výchozí IP adresa Reyee AP je 10.44.77.253 a výchozí přihlašovací heslo je „admin“. Po zadání přihlašovacího hesla se zobrazí síťová nastavení. Dle schématu sítě byla nastavena IP adresa 192.168.0.1 s maskou 255.255.240.0 a výchozí bránou 192.168.0.1. Jako DNS server



byl použit Google DNS 8.8.8.8. SSID bylo nastaveno na @Firma, dále bylo nastaveno heslo. Na obrázku 77 v příloze jsou zobrazena veškerá provedená síťová nastavení.

Následně se zobrazil seznam veškerých zařízení Reyee včetně jejich statusu, názvu, MAC adresy, IP adresy, software verze a modelového označení. Nejprve bylo třeba aktualizovat firmware na nejnovější verzi, jelikož se jedná o relativně nové zařízení a není dodáváno s aktuálním firmwarem. Původní firmware ještě nepodporoval Českou republiku.



SN	Status	Device Name	MAC Address	IP Address	Software Version	Device Model
CAR60X9046157	Online	Ruijie [Master]	54:16:51:46:EE:11	192.168.0.3	ReyeeOS 2.262.0.2404	RAP2260(G)

Obrázek 27 – Seznam zařízení

*Zdroj: Vlastní*

Po aktualizaci firmware bylo ověřeno připojení k internetu pomocí integrovaného diagnostického nástroje a také pomocí příkazu ping. Zařízení je nyní v režimu AP a o směrování se tak stará router MikroTik RB1100AHx2, na kterém je zapnutý DHCP server.

Poté bylo v menu vybráno nastavení Wi-Fi. AP podporuje vytvoření až 8 různých SSID. Pro předvedení funkčnosti byla k výchozímu SSID @Firma vytvořena SSID @IT\_oddeleni a @ucetni\_oddeleni. Každé SSID lze individuálně nastavit a v případě potřeby lze všechna zařízení připojená na určité SSID rozdělit pomocí VLAN. Dále lze pro jednotlivá SSID nastavit vysílací pásmo 2,4 GHz nebo 5 GHz. U vyšších řad Reyee AP s podporou Wi-Fi 6E přichází podpora 6 GHz pásma. Na obrázku 78 v příloze je zobrazeno provedené nastavení Wi-Fi.

Dalším krokem bylo rozkliknutí podmenu „Expand“, kde bylo třeba nastavit parametry vysílání radiové části, která je zobrazena na obrázku 28. Nastavení radiové části je rozděleno na 2,4 GHz a na 5 GHz. Při výběru země byla vybrána Česká republika. Výběr země ovlivňuje omezení, jak lze radiovou část nastavit dle místní legislativy, která jsou integrována ve firmware.

Položka „Channel Width“ tedy šířka pásma byla nastavena na Auto. Další možnosti jsou 20 MHz/40 MHz/80 MHz. V širších kanálech je přenos dat rychlejší, avšak dochází k většímu rušení. Jelikož se jedná o mesh síťový prvek, který bude mít v dosahu další stejné síťové prvky, tak je vhodné nastavit hodnotu Auto, kdy si AP bude šířku kanálu upravovat dle aktuálního rušení v konkrétním prostředí. [67]

Položka „Multicast Rate“ byla nastavena na Auto. Jedná se o datovou propustnost broadcast a multicast paketů. Vyšší rychlost multicast vysílání může vést k vyšší ztrátovosti paketů. Nižší rychlost multicast vysílání může způsobit vyšší provoz na bezdrátovém rozhraní. V tomto

případě je opět vhodné nastavit hodnotu na Auto, kdy si AP bude regulovat nastavení dle aktuální situace v síti. Toto nastavení doporučuje také výrobce. [66] [67]

Dále byl nastaven „Disconnection Threshold“ na hodnotu -90 dBm. Čím vyšší je prahová hodnota, tím snazší je pro klienta udržení relace. AP si automaticky jednotlivé klienty předávají.

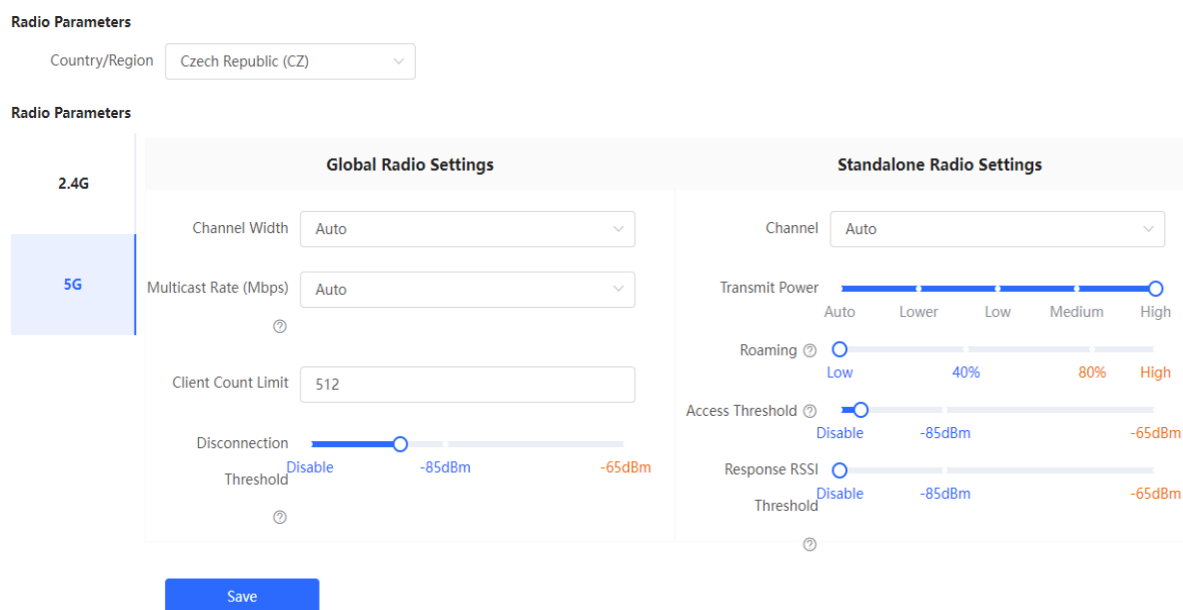
Položka „Channel“ byla nastavena také na Auto, protože mesh systém přepíná kanály automaticky, aby dosáhl co nejmenšího rušení v závislosti na prostředí. Alternativně lze ručně nastavit na každém jednotlivém AP požadovaný kanál.

V modelovém příkladě byla nastavena „Transmit Power“ na medium/high, protože větší vysílání výkon znamená vyšší pokrytí, avšak přináší nadměrné rušení okolním bezdrátovým zařízením. V případě, že by byla hustota AP ve firmě ještě větší, doporučuje se nižší úroveň vysílacího výkonu.

Roamingová citlivost je hodnota, při které koncové zařízení změní připojení na jiný AP s dostatečným signálem. Hodnota byla nastavena na low, jelikož ve firmě nejsou žádné AP velmi blízko u sebe. Vyšší hodnota se používá například ve větších prostorech nebo halách, kde je potřeba více AP, která jsou blízko sebe a koncové zařízení se mezi nimi často přepojuje.

„Access Threshold“ byl nastaven na -93 dBm. Jedná se o hodnotu, kdy koncové zařízení uvidí Wi-Fi síť v dosahu a bude se možné připojit. Hodnota byla zvolena na základě doporučení výrobce, který poskytuje stanovené rozsahy doporučených hodnot pro optimální fungování.

„Response RSSI Threshold“ byl ponechán na hodnotě disable.



Obrázek 28 – Nastavení parametrů vysílání

Zdroj: Vlastní

V položce menu „LimitSpeed“ lze nastavit omezení rychlosti downloadu a uploadu. A to buď na všechna zařízení globálně, anebo na konkrétní zařízení dle MAC adresy. Na obrázku 79 v příloze je zobrazeno omezení konkrétního zařízení na rychlost 10/10 Mbit/s. Omezení se používají zejména tehdy, kdy je vysoký počet připojených zařízení a je třeba zabezpečit dostatečnou rychlost připojení pro všechna tato zařízení. V případě, že by nebylo nastaveno žádné omezení a některé ze zařízení by abnormálně využívalo stanovenou šířku pásma, tak by mohlo dojít k výraznému poklesu rychlosti připojení všech ostatních připojených zařízení.

Dále bylo možné nastavit rychlostní omezení dle jednotlivých SSID, jak zobrazuje obrázek 80 v příloze. V modelové situaci bylo omezení dle SSID ponecháno bez limitu. Poté bylo třeba v nastavení v položce „Reyee Mesh“ zapnout podporu mesh. Po připojení dalších AP do sítě byla automaticky přidána do Reyee Mesh a následně na ně byla přenesena veškerá potřebná nastavení. Nastavení statické IP adresy dle schématu bylo možné již vzdáleně, pouze stačí být připojený ve stejné síti a není tak nutné se připojovat do GUI rozhraní.

AP je možné přidat také ručně na úvodní obrazovce, kde lze vybrat „Add AP“, poté zařízení naskenuje další AP v síti a automaticky jim přepoše veškerá nastavení. Toto nastavení je zobrazeno na obrázku 81 v příloze.

V položce „Online Clients“ se přehledně zobrazují veškerá připojená zařízení. Zařízení si lze pojmenovat, je možné zjistit typ připojení, IP adresu, MAC adresu a také informace o připojení na bezdrátovou síť, včetně nastaveného limitu. Zařízení lze přidat na blacklist, který funguje na principu blokování konkrétní MAC adresy. Tyto zařízení jsou zobrazena na obrázku 82 v příloze. Také lze volitelně AP připojit k Ruijie Cloud, který umožňuje vzdálenou správu, i když se administrátor nachází mimo síť. Přidání sítě probíhá na základě zobrazeného QR kódu a následně funguje plně v cloudu. Výhodou je základní diagnostika a správa sítě bez nutnosti připojení do místní sítě.

Po nastavení se bylo možné vrátit na úvodní obrazovku, kde byl již zobrazen pracovní mód AP a dále zde byly zobrazeny stavové informace konkrétního AP. Tato úvodní obrazovka je zobrazena na obrázku 83 v příloze.

Protože se veškerá nastavení implementují na všechny ostatní připojená AP, tak není třeba nově připojená zařízení znovu konfigurovat obdobným způsobem. Pouze bylo potřeba nastavit konkrétní statickou IP dle připraveného schématu sítě. Nyní byla dokončena konfigurace sítě s využitím AP Reyee. Obdobný postup lze aplikovat na veškerá zařízení s operačním systémem Reyee OS 2.0 a novější a tento postup lze využít univerzálně.

## 5 EKONOMICKÉ NÁKLADY A ZHODNOCENÍ PŘÍNOSU

Poslední kapitola diplomové práce se zaměřuje na přínos nasazení moderních bezdrátových technologií ve firmě, mezi které v tomto případě patří nově nasazené 60 GHz příjmové antény a Wi-Fi 6/6E přístupové body.

V následující tabulce 9 jsou uvedeny veškeré výdaje za hardware, součástí kalkulace není částka za spotřební materiál a za provedenou práci. Ceny jsou uvedeny vč. DPH a jsou vypočítány z průměrných nebo nejnižších uvedených cen na trhu.

Tabulka 9 – Ekonomické náklady

<b>Sdílené síťové prvky</b>			
<b>Zařízení</b>	<b>Název</b>	<b>Počet</b>	<b>Cena vč. DPH</b>
Rozvaděč	XtendLan WS-15U-64-BLACK-U	1	2 457 Kč
Router	MikroTik RB1100AHx2	1	4 720 Kč
Switch	TP-Link TL-SG2428P	1	7 360 Kč
UPS	ADLER záložní zdroj UPS 400W 230V	1	2 518 Kč
Baterie	SSB olověná baterie AGM 12V 55Ah	1	3 937 Kč
Vyvazovací panel	Masterlan vyvazovací panel 1U	2	358 Kč
Patch kabel	Masterlan patch kabel UTP, Cat5e	30	300 Kč
Rozvodný panel	Masterlan 19" rozvodný panel 8x 230V	1	687 Kč
Osvětlovací panel	EuroLan osvětlovací panel 1U LED	1	439 Kč
Záslepka	TRITON Záslepka 1U, černá	4	348 Kč
<b>Celkem:</b>			<b>23 124 Kč</b>
<b>I. modelová varianta</b>			
<b>Zařízení</b>	<b>Název</b>	<b>Počet</b>	<b>Cena vč. DPH</b>
Příjmová anténa	MikroTik Wire nRAY 60 GHz	1	3 250 Kč
Wi-Fi 6 síť	TP-Link EAP610	7	16 800 Kč
<b>Celkem vč. sdílených síťových prvků:</b>			<b>43 174 Kč</b>
<b>II. modelová varianta</b>			
<b>Zařízení</b>	<b>Název</b>	<b>Počet</b>	<b>Cena vč. DPH</b>
Příjmová anténa	UBNT UISP Wave Nano 60 GHz	1	7 950 Kč
Wi-Fi 6E síť	Ubiquiti UniFi U6 Enterprise	7	50 463 Kč
<b>Celkem vč. sdílených síťových prvků:</b>			<b>81 537 Kč</b>
<b>III. modelová varianta</b>			
<b>Zařízení</b>	<b>Název</b>	<b>Počet</b>	<b>Cena vč. DPH</b>
Příjmová anténa	UBNT UISP Wave Nano 60 GHz	1	7 950 Kč
Wi-Fi 6 síť	Reyee RG-RAP2260(G)	7	24 612 Kč
<b>Celkem vč. sdílených síťových prvků:</b>			<b>55 686 Kč</b>

*Zdroj: Vlastní*

Každá z variant nabízí kompletní vysokorychlostní bezdrátové pokrytí modelové firmy. Modelové varianty se pak liší zejména v ceně, v podpoře výrobce zařízení, v možnostech nastavení a v reálné kapacitě bezdrátově připojených klientů.

Výrazně nejlevněji vychází I. modelová varianta, kde jsou náklady celkem 43 174 Kč, a to zejména kvůli nasazení nižší cenové kategorie síťových prvků. Mezi nevýhody tohoto řešení patří přijímová anténa, která využívá pouze frekvenční pásmo 60 GHz a nemá možnost zálohy pásma 5 GHz, což snižuje spolehlivost sítě v případě deště nebo sněžení.

Nejdražší byla II. modelová varianta, kde vychází náklady na 81 537 Kč. Jedná se o síťové prvky Ubiquiti. Tato společnost se zaměřuje na výrobu firemních síťových prvků, které jsou určeny na vysoké počty připojených bezdrátových zařízení. Nevýhodou je vyšší cena hardware.

Střední cestou je využití III. modelové varianty, kde jsou náklady 55 686 Kč. Byla zde použita stejná přijímová anténa jako v předchozím případě. Pro Wi-Fi síť bylo využito řešení od společnosti Ruijie Networks. Vzhledem k tomu, že společnost do Evropy teprve proniká, tak je jejich cenová politika nasazena níže než v případě zbytku světa.

Veškeré modelové varianty jsou plně využitelné pro široké spektrum nasazení a nabízejí dobrý poměr cena a výkon. Jejich výhodou je modularita při využití technologie mesh. Veškeré konfigurační postupy lze využít univerzálně, jelikož zařízení ze stejné produktové řady pracují na stejném operačním systému. Nasazení Wi-Fi 6/6E ve firemním prostředí přináší řadu výhod oproti Wi-Fi 5. První výhodou je zvýšená rychlost a kapacita sítě. Ve firemním prostředí, kde se nachází vysoký počet síťových zařízení připojených k bezdrátové síti, je rychlá a spolehlivá konektivita důležitá pro chod společnosti. Vyšší rychlost a vyšší šířka pásma pak znamená, že veškerá zařízení mohou přistupovat k datům rychleji, a to i v případě vysokého provozu v síti.

Další významnou výhodou je efektivnější využití pásma a řízení provozu v sítích s více připojenými zařízeními. Wi-Fi 6/6E zavádějí a vylepšují technologie jako je OFDMA a MU-MIMO, které umožňují lépe rozložit a spravovat provoz mezi různými síťovými zařízeními, což vede k vyšší efektivitě a výkonu sítě.

Nižší latence je důležitá zejména pro aplikace, které vyžadují rychlou odezvu. Mezi tyto aplikace patří například videokonference nebo cloudové aplikace. Firmy často využívají virtualizaci. Nižší latence tak přináší vyšší plynulost komunikace. Virtualizační prostředí se ve firmách využívá čím dál častěji zejména kvůli možnosti práce na dálku z domova.

Wi-Fi 6E přináší ještě další výhody, a to díky nově využívanému frekvenčnímu pásmu 6 GHz. Toto nové pásmo poskytuje další nezarušený prostor pro bezdrátovou komunikaci, což zvyšuje celkovou kapacitu sítě a snižuje interferenci s ostatními zařízeními v již existujících pásmech 2.4 GHz a 5 GHz.

Celkově lze konstatovat, že přechod na Wi-Fi 6/6E přináší výrazné zlepšení výkonu, spolehlivosti a efektivity bezdrátových sítí. Tyto nové technologie jsou klíčem k podpoře stále rostoucího počtu připojených zařízení a moderních aplikací, které vyžadují vysokou rychlost, nízkou latenci a stabilitu připojení.

## ZÁVĚR

Cílem diplomové práce bylo vytvořit návrh bezdrátové datové sítě pro modelový subjekt v několika variantách s využitím moderních vysokorychlostních technologií.

V úvodní kapitole se práce zabývala analýzou současného stavu bezdrátových sítí v České republice a představila strukturu přístupu k internetu. V této kapitole práce také souhrnně prezentovala legislativní požadavky na využívání konkrétních frekvenčních pásem.

Druhá část práce popisuje teoretické poznatky, které jsou následně využívány v praktické části. V teoretické části byly představeny frekvenční pásma bezdrátových sítí a jejich nejnovější standardy IEEE. Poté byly detailně popsány jednotlivé technologie využívané ve standardu IEEE 802.11ax. Dále v této části byla popsána topologie sítě mesh, protokoly IPv4 a IPv6 nebo také zabezpečení bezdrátových sítí pomocí firewallu nebo standardu WPA3. Nakonec se kapitola věnovala několika případovým studiím, kde byly aplikovány bezdrátové vysokorychlostní technologie v různých regionech světa. Motivací vypracování této diplomové práce bylo mimo jiné také představení výhod těchto bezdrátových technologií, které jsou již ve světě široce využívány.

Ve třetí kapitole diplomové práce byla popsána výchozí situace v modelové firmě, předvedeny důvody výběru jednotlivých síťových prvků a vytvořeno schéma sítě.

V empirické části byl proveden návrh bezdrátové počítačové sítě, kde bylo nejprve detailně navrženo osazení rozvaděče a vybrány síťové prvky. Praktická část byla rozdělena na tři modelové varianty, z nichž každá využívala jiný typ přístupových bodů a přijímové antény. Následně proběhla konfigurace veškerých síťových prvků, mezi které patřil router, switch, přijímová anténa a přístupové body.

Poslední kapitola obsahuje zhodnocení nasazení jednotlivých modelových variant a bylo také provedeno jejich ekonomické srovnání.

Celkově tato diplomová práce přináší ucelený přehled o možnosti využití nejnovějších bezdrátových technologií ve firmách a poskytuje komplexní přehled konfigurace těchto síťových zařízení.

## POUŽITÁ LITERATURA

- [1] Zpráva o vývoji trhu elektronických komunikací se zaměřením na rok 2022. online. In: *Český telekomunikační úřad*. 2022. Dostupné z: [https://www.ctu.cz/sites/default/files/obsah/stranky/472017/soubory/zovt\\_2022.pdf](https://www.ctu.cz/sites/default/files/obsah/stranky/472017/soubory/zovt_2022.pdf). [cit. 2024-01-05].
- [2] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. Všeobecné oprávnění č. VO-S/1/08.2020-9. In: *§ 150 odst. 2 zákona č. 127/2005 Sb.* Praha, 2020. Dostupné také z: <https://www.ctu.cz/sites/default/files/obsah/stranky/36864/soubory/vos1final.pdf>.
- [3] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *Všeobecná oprávnění*. online. 2023. Dostupné z: <https://www.ctu.cz/vseobecna-opravneni>. [cit. 2024-01-05].
- [4] U-NII Wi-Fi / WLAN Bands & Frequencies. online. In: *Electronicsnotes*. Dostupné z: <https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/unii-wifi-wlan-bands-spectrum-frequencies.php>. [cit. 2024-01-05].
- [5] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. Všeobecné oprávnění č. VO-R/12/11.2021-11 k využívání rádiových kmitočtů a k provozování zařízení pro širokopásmový přenos dat v pásmech 2,4 GHz až 71 GHz. online. In: *§ 150 odst. 2 zákona č. 127/2005 Sb.* Praha, 2021. Dostupné také z: [https://www.ctu.cz/sites/default/files/obsah/vo-r\\_12-112021-11.pdf](https://www.ctu.cz/sites/default/files/obsah/vo-r_12-112021-11.pdf).
- [6] 60GHz v České republice legálně od 15.1.2020. online. In: *DISCOMP networking solutions*. 2020. Dostupné z: [https://www.discomp.cz/60ghz-v-ceske-republice-legalne-od-15-1-2020-\\_w502.html](https://www.discomp.cz/60ghz-v-ceske-republice-legalne-od-15-1-2020-_w502.html). [cit. 2024-01-06].
- [7] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *Informace k vydání všeobecného oprávnění VO-R/12/12.2019-10, kterým se stanoví podmínky využívání pásma 60 GHz*. 2019. Dostupné také z: <https://www.ctu.cz/sites/default/files/obsah/ctu/vseobecne-opravneni-c.vo-r/12/12.2019-10/obrazky/informace-k-vo-r12.pdf>.
- [8] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *ČTÚ RLAN portál*. online. 2024. Dostupné z: <https://rlan.ctu.cz/cs/stanice/092986>. [cit. 2024-01-06].
- [9] ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD. *Registrace v 60 GHz, 5,8 GHz a 5,2 GHz*. online. 2020. Dostupné z: <https://rlan.ctu.cz/cs/regulatorni-podminky-v-pasmu-60-ghz>. [cit. 2024-01-06].



- [10] EUROPEAN COMMISSION. Commission makes more spectrum available for better and faster Wi-Fi. online. In: EUROPEAN COMMISSION. 2021, 16 December 2022. Dostupné z: <https://digital-strategy.ec.europa.eu/en/news/commission-makes-more-spectrum-available-better-and-faster-wi-fi#z1v3>. [cit. 2024-01-06].
- [11] CARROLL, Brandon. *Bezdrátové sítě Cisco: autorizovaný výukový průvodce*. 1. Samostudium. Brno: Computer Press, 2011. ISBN 978-80-251-2884-8.
- [12] SLÍŽEK, David. ČTÚ uvolnil pásmo 60 GHz, které může změnit bezdrátový trh. online. In: *Lupa.cz*. Internet Info, s.r.o, 2019. Dostupné z: <https://www.lupa.cz/aktuality/ctu-uvolnil-pasmo-60-ghz-ktere-muze-zmenit-bezdratovy-trh/>. [cit. 2024-02-19].
- [13] FOROUZAN, Behrouz A. a CHUNG FEGAN, Sophia. *Data Communications and Networking*. online. Fourth. Huga Media, 2007. ISBN 9780072967753. Dostupné z: [https://books.google.it/books?id=bwUNZvJbEeQC&pg=PA1&hl=cs&source=gbs\\_selected\\_pages&cad=1#v=onepage&q&f=false](https://books.google.it/books?id=bwUNZvJbEeQC&pg=PA1&hl=cs&source=gbs_selected_pages&cad=1#v=onepage&q&f=false). [cit. 2024-02-19].
- [14] GAST, Matthew S. 802.11ac: *A Survival Guide: Wi-Fi at Gigabit and Beyond*. 1st edition. USA: O'Reilly Media, Inc., 2013. ISBN 978-1449343149.
- [15] Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements. online. *TEKTRONIX*. 2016. Dostupné z: [https://download.tek.com/document/37W-29447-2\\_LR.pdf](https://download.tek.com/document/37W-29447-2_LR.pdf). [cit. 2024-02-19].
- [16] GOLD, Jon. Nový standard Wi-Fi 802.11ad: vyšší frekvence, ale menší dosah. online. In: *CIO Business World*. 2024. Dostupné z: <https://www.cio.cz/clanky/802-11ad-je-nejrychlejsi-wi-fi-ktere-ale-mozna-nikdy-nevyuzijete/>. [cit. 2024-02-20].
- [17] SCHULZ, Bernhard. 802.11ad - WLAN at 60 GHz A Technology Introduction. online. *Rohde & Schwarz GmbH & Co. KG*. 2017. Dostupné z: [https://scdn.rohde-schwarz.com/ur/pws/dl\\_downloads/dl\\_application/application\\_notes/1ma220/1MA220\\_3e\\_WLAN\\_11ad\\_WP.pdf](https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_application/application_notes/1ma220/1MA220_3e_WLAN_11ad_WP.pdf). [cit. 2024-02-20].
- [18] COLEMAN, David a MILLER, Lawrence C. *802.11ax for Dummies: Aerohive Special Edition*. online. 1. John Wiley & Sons, For Dummies, Special, 2018. ISBN 978-1-119-52800-5. Dostupné z: [https://www.alternetivo.cz/info/KUV/802.11ax\\_For\\_Dummies\\_Aerohive\\_Special\\_Edition\\_9781119528029.pdf](https://www.alternetivo.cz/info/KUV/802.11ax_For_Dummies_Aerohive_Special_Edition_9781119528029.pdf). [cit. 2024-02-20].
- [19] BREINBAUER, M. HINTS FOR IEEE 802.11BE EVM MEASUREMENTS. online. *Rohde & Schwarz*. 2022. Dostupné z: <https://scdn.rohde->

- schwarz.com/ur/pws/dl\_downloads/dl\_application/application\_notes/1ef114/1EF114\_e\_802\_11be\_EVM.pdf. [cit. 2024-02-20].
- [20] MICHALEC, Libor. První čipy pro WiFi7. online. In: *Vyvoj.hw.cz*. 2023. Dostupné z: <https://vyvoj.hw.cz/prvni-cipy-pro-wifi7.html>. [cit. 2024-02-20].
- [21] KHOROV, Evgeny; KIRYANOV, Anton; LYAKHOV, Andrey a BIANCHI, Giuseppe. A Tutorial on IEEE 802.11ax High Efficiency WLANs. online. 2019, roč. 21, č. 1, s. 197-216. ISSN 1553-877X. Dostupné z: <https://doi.org/10.1109/COMST.2018.2871099>. [cit. 2024-02-20].
- [22] LEE, Kyu-Haeng. Using OFDMA for MU-MIMO User Selection in 802.11ax-Based Wi-Fi Networks. online. *IEEE Access*. 2019, roč. 7, s. 186041-186055. ISSN 2169-3536. Dostupné z: <https://doi.org/10.1109/ACCESS.2019.2960555>. [cit. 2024-02-20].
- [23] EMMERLING, Friedrich a BEHMKE, Michael. Wi-Fi 6: Key Innovations and their Contributors -Part 2-. online. In: *Braun-Dullaesus Pannen Emmerling Patent- und Rechtsanwälte*. Munich: Juve Patent, 2024. Dostupné z: <https://www.juve-patent.com/sponsored/braun-dullaesus-pannen-emmerling-patent-rechtsanwalte/wi-fi-6-key-innovations-and-their-contributors-part-2/>. [cit. 2024-02-20].
- [24] SELINIS, I.; KATSARO, K. a VAHID, S. Damysus: A Practical IEEE 802.11ax BSS Color Aware Rate Control Algorithm. online. *Int J Wireless Inf Networks*. 2019, č. 26, s. 285–307. Dostupné z: <https://doi.org/https://doi.org/10.1007/s10776-019-00439-6>. [cit. 2024-02-20].
- [25] REJZEK, Jakub. Wi-Fi 6 přichází. Co je pod pokličkou nového standardu?. online. In: *Lupa.cz*. 2019. Dostupné z: <https://www.lupa.cz/clanky/wi-fi-6-prichazi-co-je-pod-poklickou-noveho-standardu/>. [cit. 2023-10-17].
- [26] HYNČICA, Ondřej. Bezdrátové sítě typu mesh. online. *Automa – časopis pro automatizační techniku*. 2005, roč. 2005, č. 12. Dostupné z: [https://automa.cz/cz/casopis-clanky/bezdratove-site-typu-mesh-2005\\_12\\_30826\\_1141/](https://automa.cz/cz/casopis-clanky/bezdratove-site-typu-mesh-2005_12_30826_1141/). [cit. 2024-02-21].
- [27] KIZZA, Joseph Migga. *Guide to computer network security*. Fourth edition. Cham, Switzerland: Springer-Verlag, 2017. ISBN 978-3-319-55605-5.
- [28] BENYAMINA, Djohara; HAFID, Abdelhakim a GENDREAU, Michel. Wireless Mesh Networks Design — A Survey. online. 2012, roč. 14, č. 2, s. 299-310. ISSN 1553-877X. Dostupné z: <https://doi.org/10.1109/SURV.2011.042711.00007>. [cit. 2024-02-21].

- [29] KUROSE, James F. a ROSS, Keith. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.
- [30] SATRAPA, Pavel. *IPv6: internetový protokol verze 6*. 4. aktualizované a rozšířené vydání. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-43-0.
- [31] *Google IPv6 Statistics*. online. In: Google. 2024. Dostupné z: <https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption>. [cit. 2024-02-24].
- [32] JAKUBOVÁ, Veronika. IPv6: v čem je lepší než IPv4 a proč jeho nasazení v Česku zaostává?. online. In: *MasterDC*. 2021. Dostupné z: <https://www.master.cz/blog/ipv6-v-cem-je-lepsi-nez-ipv4-proc-jeho-nasazeni-v-cesku-zaostava/>. [cit. 2024-02-24].
- [33] SUMMERS, Wayne C. a BOSWORTH, Edward. Password Policy: The Good, The Bad, and The Ugly. online. *Columbus State University*. 2004. Dostupné z: [https://www.researchgate.net/profile/Wayne-Summers-2/publication/234799064\\_Password\\_policy\\_The\\_good\\_the\\_bad\\_and\\_the\\_ugly/links/54f204310cf2f9e34eff3d50/Password-policy-The-good-the-bad-and-the-ugly.pdf](https://www.researchgate.net/profile/Wayne-Summers-2/publication/234799064_Password_policy_The_good_the_bad_and_the_ugly/links/54f204310cf2f9e34eff3d50/Password-policy-The-good-the-bad-and-the-ugly.pdf). [cit. 2024-02-26].
- [34] HALBOUNI, Asmaa; ONG, Lee-Yeng a LEOW, Meng-Chew. Wireless Security Protocols WPA3: A Systematic Literature Review. online. *IEEE Access*. 2023, roč. 11, s. 112438-112450. ISSN 2169-3536. Dostupné z: <https://doi.org/10.1109/ACCESS.2023.3322931>. [cit. 2024-02-26].
- [35] HOWARD, . *WEP vs. WPA vs. WPA2 vs. WPA3*. online. In: FS.com. 2021, Updated on Sep 29, 2021. Dostupné z: <https://community.fs.com/article/wep-vs-wpa-vs-wpa2-vs-wpa3.html>. [cit. 2024-02-26].
- [36] Augmented Reality Market Size Worth \$340.16 Billion By 2028 | CAGR: 43.8%: Grand View Research, Inc. online. In: *PR Newswire*. 2021. Dostupné z: <https://www.prnewswire.com/news-releases/augmented-reality-market-size-worth-340-16-billion-by-2028--cagr-43-8-grand-view-research-inc-301228121.html#:~:text=SAN%20FRANCISCO%2C%20Feb.,43.8%25%20from%202021%20to%202028>. [cit. 2024-02-26].
- [37] From Home Office to HQ: Consumerization of Wi-Fi 6E. online. In: *Network Computing*. 2022. Dostupné z: <https://www.networkcomputing.com/wireless-infrastructure/home-office-hq-consumerization-wi-fi-6e>. [cit. 2024-02-26].

- [38] WOOD, Steve. Why Wi-Fi 6E matters for today's digital enterprises. online. In: *Futurecio*. 2021. Dostupné z: <https://futurecio.tech/why-wi-fi-6e-matters-for-todays-digital-enterprises/>. [cit. 2024-02-26].
- [39] Non-profit University in the UAE Equips New Administrative Office Building With Fast, Reliable Wi-Fi. online. In: *EnGenius*. 2022. Dostupné z: <https://www.engeniustech.com/wp-content/uploads/2022/03/American-University-of-Sharjah-Case-Study.pdf>. [cit. 2024-02-26].
- [40] KERRAVALA, Zeus. Wi-Fi 6E Is Critical to Healthcare Modernization. online. In: *EWeek*. 2022. Dostupné z: <https://www.eweek.com/networking/wi-fi-6e-healthcare-modernization/>. [cit. 2024-02-26].
- [41] HOROWITZ, Brian T. San Francisco Giants Deploy Fully Wi-Fi 6E-Ready Network With Comcast, Extreme Networks: April 20, 2023. online. In: *Network Computing*. Dostupné z: <https://www.networkcomputing.com/network-security/san-francisco-giants-deploy-fully-wi-fi-6e-ready-network-comcast-extreme-networks>. [cit. 2024-02-26].
- [42] CISCO. Customer Case Study: BEXCO, a major exhibition and convention center, has adopted Wi-Fi 6 to provide a next-generation high-speed mobile network environment. online. In: CISCO. 2020. Dostupné z: [https://www.cisco.com/c/dam/en\\_us/about/case-studies-customer-success-stories/cisco-bexco-wifi6-casestudy.pdf](https://www.cisco.com/c/dam/en_us/about/case-studies-customer-success-stories/cisco-bexco-wifi6-casestudy.pdf). [cit. 2024-02-26].
- [43] *60 GHz cnWave Connects Hundreds of Campers at the North Sea*. Online. In: CAMBIUM NETWORKS, INC. [Cambiumnetworks.com](https://www.cambiumnetworks.com). 2022. Dostupné z: <https://www.cambiumnetworks.com/wp-content/uploads/Cambium-Networks-Wireless-Portfolio-of-Solutions-Connects-Hundreds-of-Campers-at-the-North-Sea.pdf>. [cit. 2024-03-05].
- [44] MIKROTIK. *Mikrotik RB1100AHx2*. online. In: . 2024. Dostupné z: <https://mikrotik.com/product/RB1100AHx2>. [cit. 2024-01-17].
- [45] UBIQUITI INC. EdgeRouter datasheet. Online. UI.com. 2020. Dostupné z: [https://dl.ubnt.com/datasheets/edgemax/EdgeRouter\\_DS.pdf](https://dl.ubnt.com/datasheets/edgemax/EdgeRouter_DS.pdf). [cit. 2024-03-14].
- [46] Cisco 1000 Series Integrated Services Routers Data Sheet. Online. CISCO SYSTEMS, INC. Cisco. 2023. Dostupné z: <https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-739512.html>. [cit. 2024-03-14].

- [47] TP-LINK CORPORATION LIMITED. *TL-SG2428P*. online. 2024. Dostupné z: <https://www.tp-link.com/cz/business-networking/smart-switch/tl-sg2428p/>. [cit. 2024-01-18].
- [48] UBIQUITI INC. Switch 24 PoE – Ubiquiti Store. Online. UBIQUITI INC. UI.com. 2024. Dostupné z: <https://eu.store.ui.com/eu/en/collections/unifi-switching-standard-power-over-ethernet/products/usw-24-poe>. [cit. 2024-03-14].
- [49] HPE Aruba Instant On 1930 24G PoE 4SFP/SFP+. Online. 100MEGA DISTRIBUTION S.R.O. 100MEGA Distribution. 2024. Dostupné z: <https://b2b.100mega.cz/cs/252872-hpe-aruba-instant-on-1930-24g-poe-4sfp-sfp>. [cit. 2024-03-14].
- [50] *Draw.io*. Online. 2024. Dostupné z: <https://www.drawio.com/>. [cit. 2024-03-04].
- [51] I4WIFI. *Rozvaděč XtendLan WS-15U-64-BLACK-U*. online. In: . Dostupné z: [https://www.i4wifi.cz/cs/181759-xtendlan-15u-600x450-na-zed-jednodilny-rozlozeny-sklenene-dvere-cerne?gad\\_source=1&gclid=CjwKCAiA44OtBhAOEiwAj4gpOZYqAv-VVo6mRZTwtDyp1exMqXBX18Ara0peAAcmdxh8riQXK1VWVhoCP98QAvD\\_BwE](https://www.i4wifi.cz/cs/181759-xtendlan-15u-600x450-na-zed-jednodilny-rozlozeny-sklenene-dvere-cerne?gad_source=1&gclid=CjwKCAiA44OtBhAOEiwAj4gpOZYqAv-VVo6mRZTwtDyp1exMqXBX18Ara0peAAcmdxh8riQXK1VWVhoCP98QAvD_BwE). [cit. 2024-01-17].
- [52] DISCOMP. *EuroLan osvětlovací panel 1U LED*. online. 2024. Dostupné z: [https://www.discomp.cz/eurolan-osvetlovaci-panel-1u-led\\_d54839.html?action=setcur&curid=14](https://www.discomp.cz/eurolan-osvetlovaci-panel-1u-led_d54839.html?action=setcur&curid=14). [cit. 2024-01-17].
- [53] DISCOMP. *Masterlan vyvazovací panel 1U, 24 mezer, plastový*. online. 2024. Dostupné z: [https://www.discomp.cz/masterlan-vyvazovaci-panel-1u-24-mezer-plastovy\\_d25940.html](https://www.discomp.cz/masterlan-vyvazovaci-panel-1u-24-mezer-plastovy_d25940.html). [cit. 2024-01-17].
- [54] DISCOMP. *TRITON Záslepka 1U (výška 4,5 cm), černá*. online. 2024. Dostupné z: [https://www.discomp.cz/triton-zaslepka-1u-vyska-4-5-cm-cerna\\_d56908.html](https://www.discomp.cz/triton-zaslepka-1u-vyska-4-5-cm-cerna_d56908.html). [cit. 2024-01-17].
- [55] BUBENÍČEK, Jaroslav. Jaké jsou typy záložních zdrojů – UPS?. online. *ElektroPrůmysl.cz*. 2021. ISSN 2571-0761. Dostupné z: <https://www.elektroprumysl.cz/elektricke-a-zalozni-zdroje-energie/jake-jsou-typy-zaloznich-zdroju-ups>. [cit. 2024-01-17].
- [56] DISCOMP. *ADLER záložní zdroj UPS 400W 230V, 12V*. online. 2024. Dostupné z: [https://www.discomp.cz/adler-zalozni-zdroj-ups-400w-230v-12v\\_d87870.html](https://www.discomp.cz/adler-zalozni-zdroj-ups-400w-230v-12v_d87870.html). [cit. 2024-01-17].

- [57] DISCOMP. *SSB olověná baterie AGM 12V 55Ah, životnost 10-12let, M6 konektor*. online. 2024. Dostupné z: [https://www.discomp.cz/ssb-olovena-baterie-agm-12v-55ah-zivotnost-10-12let-m6-konektor\\_d76584.html](https://www.discomp.cz/ssb-olovena-baterie-agm-12v-55ah-zivotnost-10-12let-m6-konektor_d76584.html). [cit. 2024-01-17].
- [58] SSB Battery SBL 66-12HR. online. In: *TME*. 2020. Dostupné z: <https://www.tme.eu/Document/af5f4b29089ffd0b5ab16f09fca31ba7/ACCU-SBL-66-12HRS.pdf>. [cit. 2024-01-17].
- [59] MIKROTIK. *Building Your First Firewall*. online. In: . Dostupné z: <https://help.mikrotik.com/docs/display/ROS/Building+Your+First+Firewall>. [cit. 2024-02-05].
- [60] MIKROTIK. *Wireless Wire nRAY*. Online. Dostupné z: [https://mikrotik.com/product/wireless\\_wire\\_nray](https://mikrotik.com/product/wireless_wire_nray). [cit. 2024-03-04].
- [61] *EAP653 - Přístupový bod AX3000 WiFi 6 pro montáž na strop*. online. In: TP-Link. 2024. Dostupné z: <https://www.tp-link.com/cz/business-networking/ceiling-mount-ap/eap653/>. [cit. 2024-02-27].
- [62] UBIQUITI INC. *60 GHz client Wave Nano*. online. In: Ubiquiti Unifi. 2024. Dostupné z: <https://store.ui.com/us/en/collections/uisp-60ghz-client-compact>. [cit. 2024-02-07].
- [63] UBIQUITI. *UISP Design Center Unifi*. online. In: . Dostupné z: <https://ispdesign.ui.com/#>. [cit. 2024-02-07].
- [64] *Tech Specs U6 Enterprise*. online. In: Ubiquiti UniFi. 2024. Dostupné z: <https://techspecs.ui.com/unifi/wifi/u6-enterprise#datasheet>. [cit. 2024-03-02].
- [65] RUIJIE NETWORKS. *O Ruijie Networks*. online. In: . 2024. Dostupné z: <https://www.ruijie.cz/clanek/9/o-ruijie-networks/>. [cit. 2024-02-01].
- [66] DISCOMP. *Reyee RG-RAP2260(G) Access point*. online. In: DISCOMP. 2024. Dostupné z: [https://www.discomp.cz/reyee-rg-rap2260-g-access-point\\_d121720.html](https://www.discomp.cz/reyee-rg-rap2260-g-access-point_d121720.html). [cit. 2024-02-01].
- [67] RUIJIE NETWORKS. *Ruijie Reyee RG-RAP Series Access Points Web-based Configuration Guide, ReyeeOS 1.206 (V1.0)*. online. In: Ruijie Networks. 2022. Dostupné z: <https://www.ruijienetworks.com/resources/preview/77372>. [cit. 2024-02-01].

## **PŘÍLOHY**

Příloha A – seznam příkazů konfigurace routeru MikroTik.....	80
Příloha B – konfigurační obrazovky sdílených síťových prvků .....	82
Příloha C – seznam příkazů konfigurace antény MikroTik .....	91
Příloha D – konfigurační obrazovky I. modelové varianty .....	92
Příloha E – konfigurační obrazovky II. modelové varianty.....	101
Příloha F – konfigurační obrazovky III. modelové varianty .....	108

## Příloha A – seznam příkazů konfigurace routeru MikroTik

Zdroj: [59]

### Odebrání konfigurace:

```
system reset-configuration no-defaults=yes
```

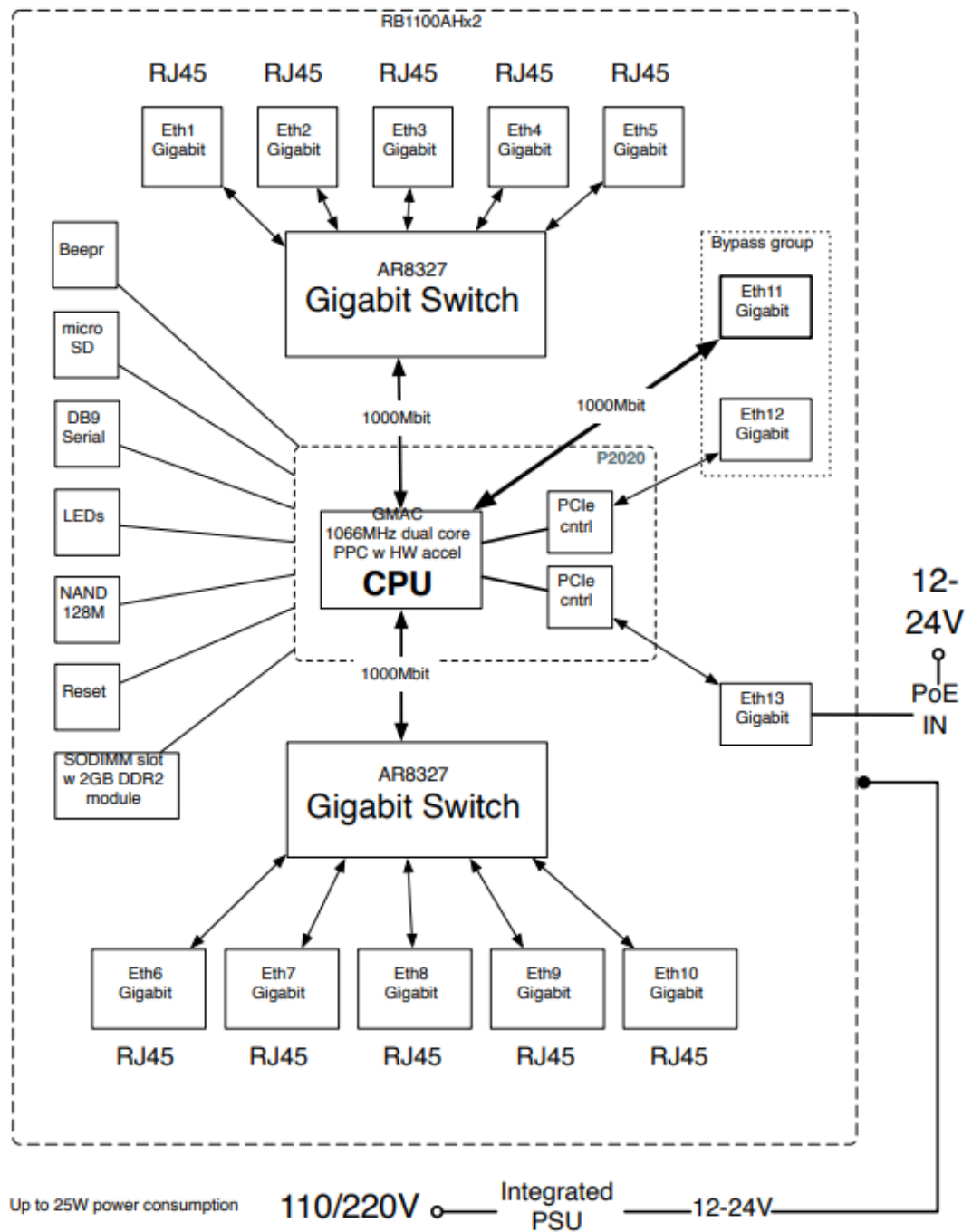
### Seznam příkazů konfigurace:

```
/interface bridge
add name=bridge
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=dhcp_pool0 ranges=192.168.0.100-192.168.15.254
/ip dhcp-server
add address-pool=dhcp_pool0 disabled=no interface=bridge
lease-time=1h name=dhcp1
/interface bridge port
add bridge=bridge interface=ether1
add bridge=bridge interface=ether6
add bridge=bridge interface=ether7
add bridge=bridge interface=ether8
add bridge=bridge interface=ether9
add bridge=bridge interface=ether10
/ip address
add address=10.100.7.4/24 comment=WAN interface=ether11
network=10.100.7.0
add address=192.168.0.1/20 comment="LAN (SW + AP)"
interface=bridge network=192.168.0.0
/ip dhcp-server network
add address=192.168.0.0/20 dns-
server=10.254.253.250,8.8.8.8,8.8.4.4 gateway=192.168.0.1
/ip dns
set servers=10.254.253.250,8.8.8.8,8.8.4.4
/ip firewall address-list
add address=192.168.0.2-192.168.15.255 list=allowed_to_router
/ip firewall filter
add action=accept chain=input comment="default configuration"
connection-state=established,related
add action=accept chain=input src-address-
list=allowed_to_router
add action=accept chain=input protocol=icmp
add action=drop chain=input
add action=fasttrack-connection chain=forward
comment=FastTrack connection-state=established,related
add action=accept chain=forward comment="Established, Related"
connection-state=established,related
add action=drop chain=forward comment="Drop invalid"
connection-state=invalid log=yes log-prefix=invalid
add action=drop chain=forward comment="Drop incoming packets
that are not NAT`ted" connection-nat-state=!dstnat connection-
state=new in-interface=ether11 log=yes log-prefix=!NAT
```



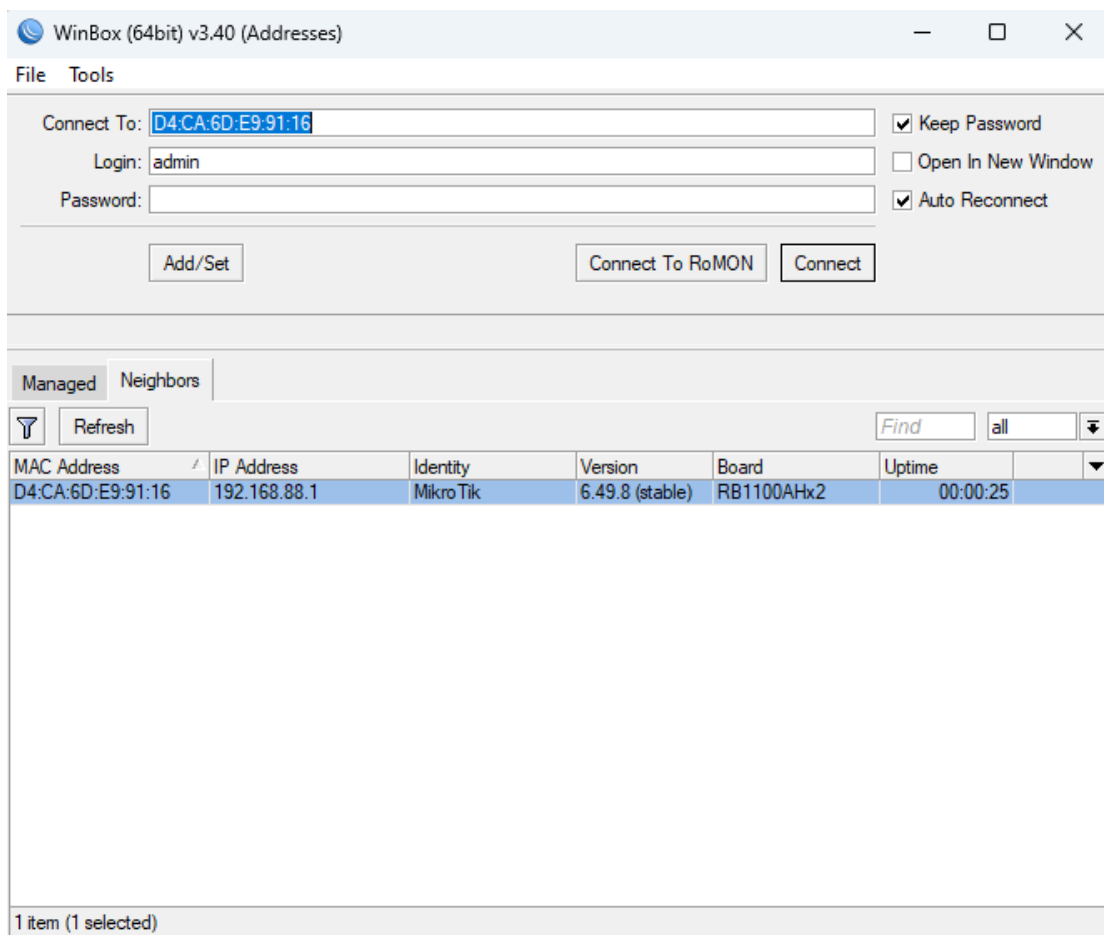
```
add action=jump chain=forward comment="jump to ICMP filters"
jump-target=icmp protocol=icmp
add action=drop chain=forward comment="Drop packets from LAN
that do not have LAN IP" in-interface=bridge log=yes log-
prefix=LAN_!LAN src-address=!192.168.0.0/20
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether11
/ip route
add distance=1 gateway=10.100.7.1
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set api disabled=yes
set api-ssl disabled=yes
/system identity
set name=Router-MikroTikRB1100
/system ntp client
set enabled=yes primary-ntp=195.113.144.201 secondary-
ntp=195.113.144.238
```

Příloha B – konfigurační obrazovky sdílených síťových prvků



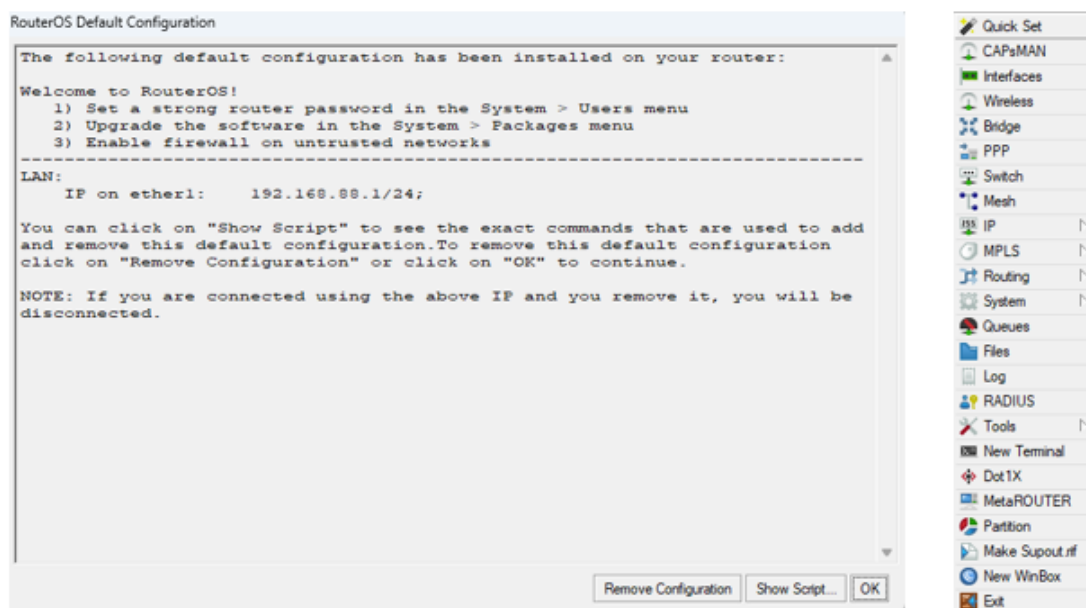
Obrázek 29 – Blokové schéma RB1100AHx2

Zdroj: [44]



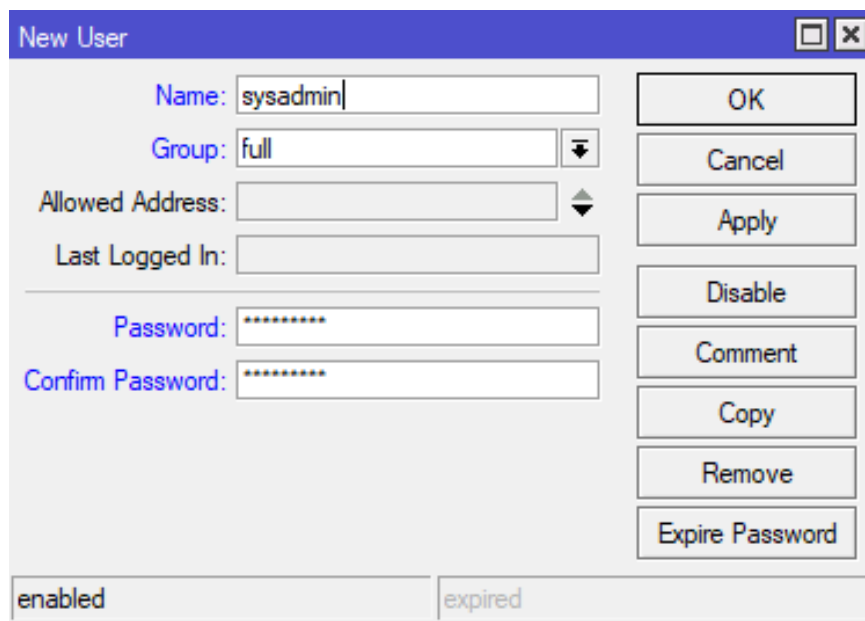
Obrázek 30 – Připojení k routeru v aplikaci WinBox

*Zdroj: Vlastní*



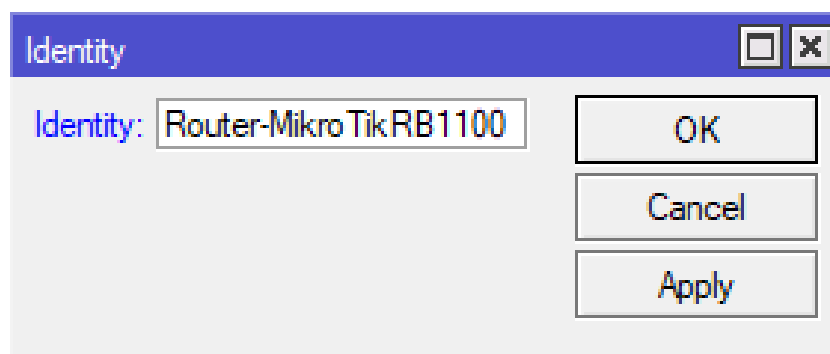
Obrázek 31 – Úvodní informace o nastavení a menu WinBox

*Zdroj: Vlastní*



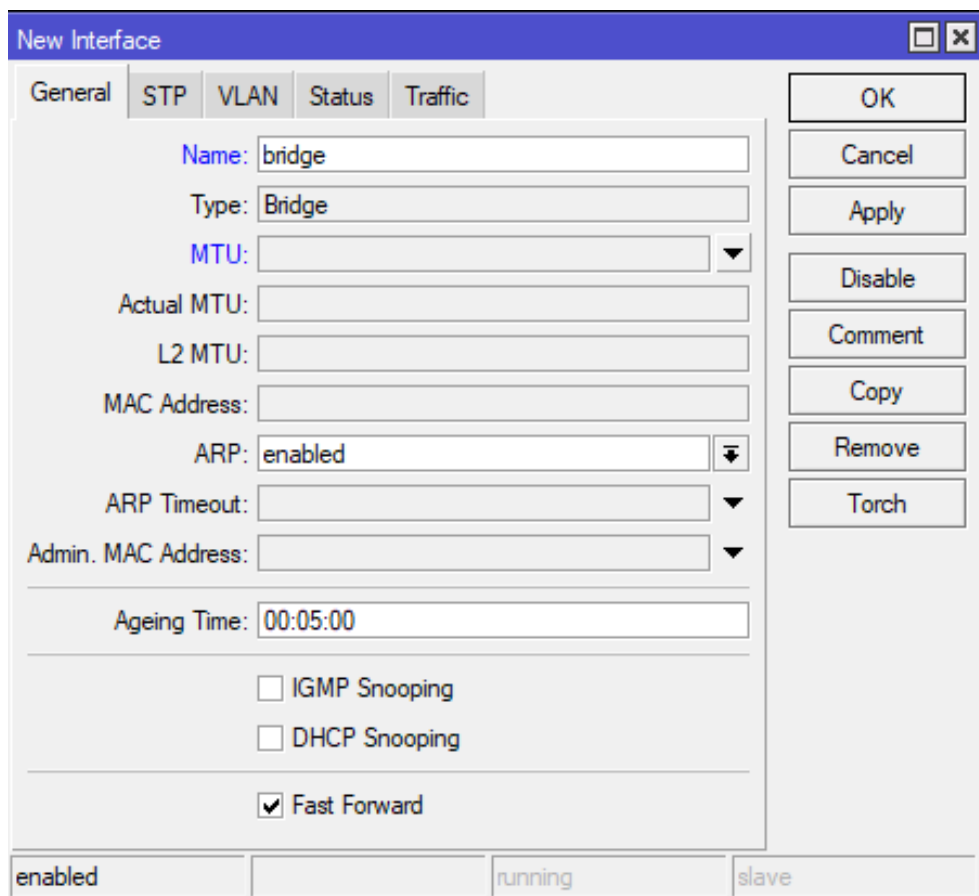
Obrázek 32 – Nastavení uživatele

*Zdroj: Vlastní*



Obrázek 33 – Nastavení názvu zařízení

*Zdroj: Vlastní*



Obrázek 34 – Vytvoření rozhraní bridge

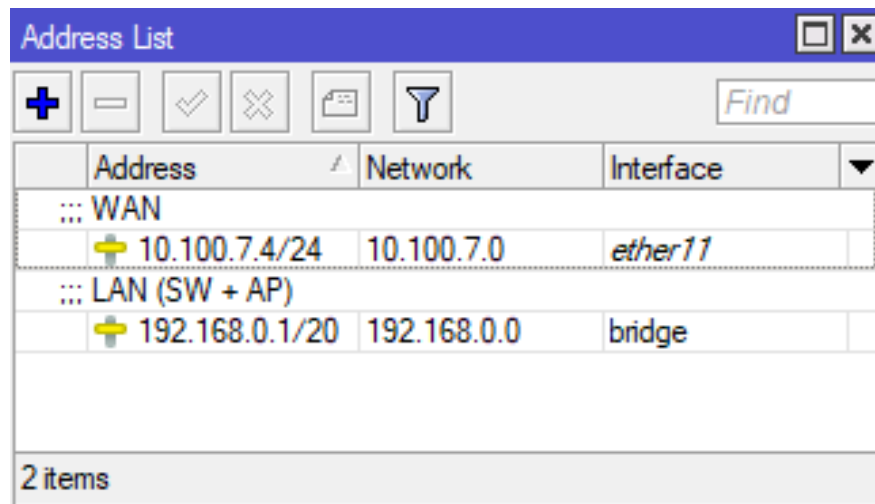
*Zdroj: Vlastní*

#	Interface	Bridge	Horizon	Trusted	Priority (h...)	Path Cost	Role	Root Pat...
0 H	ether1	bridge		no	80	10	designated port	
1 IH	ether6	bridge		no	80	10	disabled port	
2 IH	ether7	bridge		no	80	10	disabled port	
3 IH	ether8	bridge		no	80	10	disabled port	
4 IH	ether9	bridge		no	80	10	disabled port	
5 IH	ether10	bridge		no	80	10	disabled port	

6 items

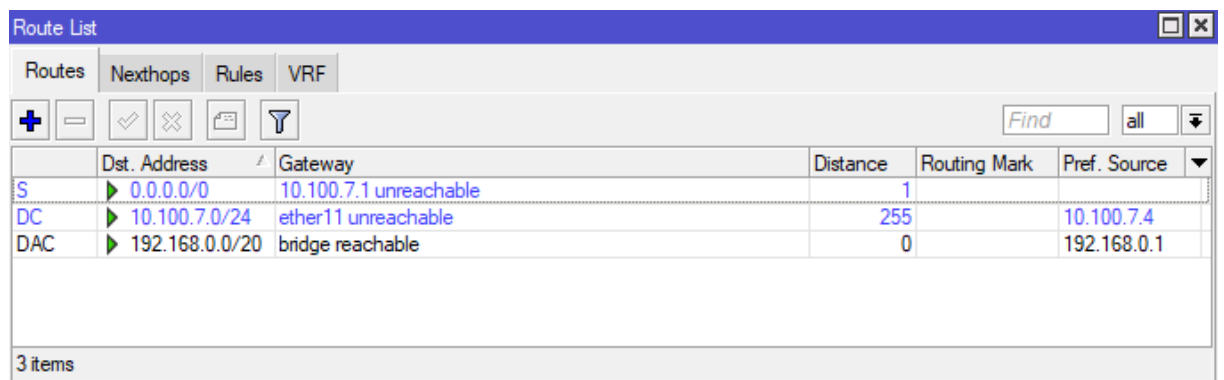
Obrázek 35 – Přidání rozhraní do bridge

*Zdroj: Vlastní*



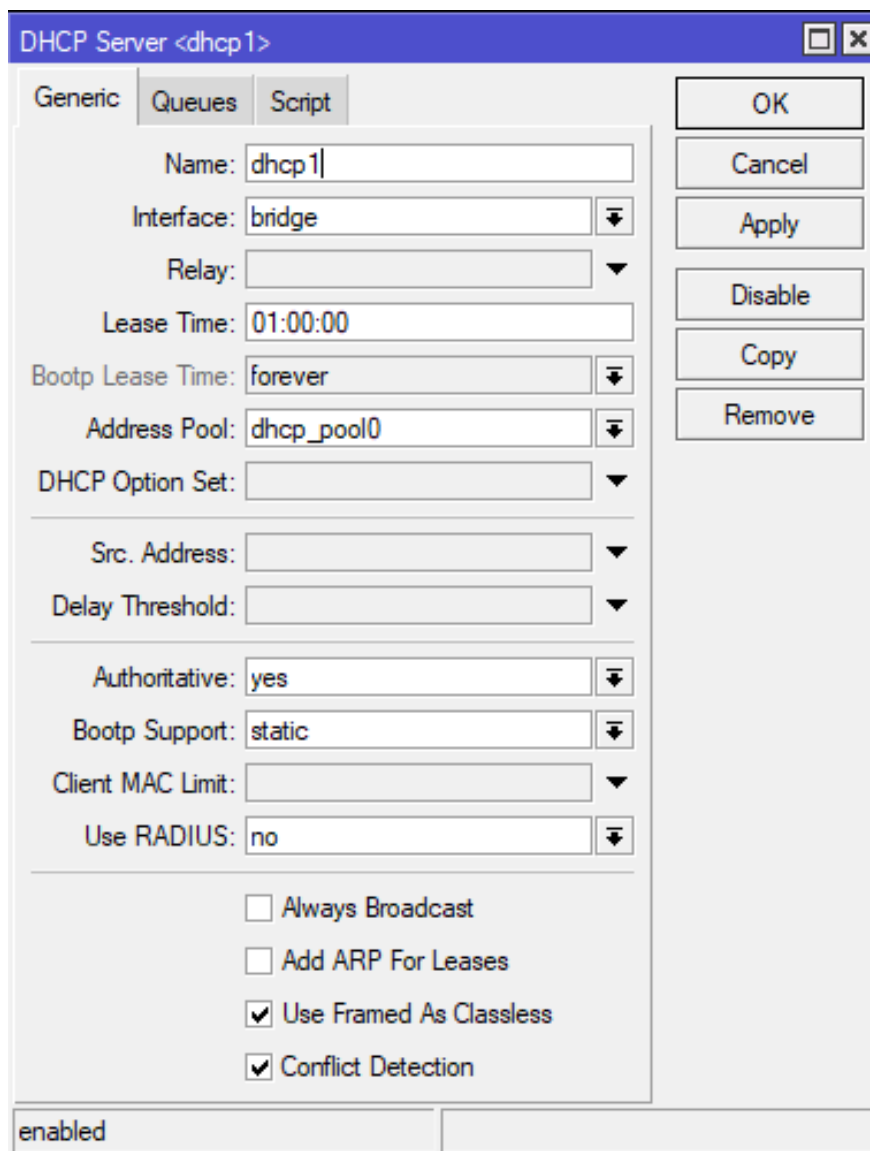
Obrázek 36 – Nastavení IP adres

Zdroj: Vlastní



Obrázek 37 – Nastavení výchozí brány

Zdroj: Vlastní



Obrázek 38 – Nastavení DHCP serveru

*Zdroj: Vlastní*

	Name	Port	Available From	Certificate	TLS Version
X	api	8728			
X	api-ssl	8729		none	any
X	ftp	21			
	ssh	22			
X	telnet	23			
	winbox	8291			
X	www	80			
X	www-ssl	443		none	any

8 items

Obrázek 39 – Nastavení služeb

*Zdroj: Vlastní*

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Address List	Dst. Ad...	Bytes	Packets
0	passthrough	forward												0 B	0
::: default configuration															
1	accept	input										allowed_to_router		241.3 KiB	3 189
2	accept	input												0 B	0
3	accept	input			1 (icmp)									0 B	0
4	drop	input												41.5 KiB	278
::: FastTrack															
5	fasttrack connection	forward												0 B	0
::: Established, Related															
6	accept	forward												0 B	0
::: Drop invalid															
7	drop	forward												0 B	0
::: Drop incoming packets that are not NATted															
8	drop	forward							ether11					0 B	0
::: jump to ICMP filters															
9	jump	forward			1 (icmp)									0 B	0
::: Drop packets from LAN that do not have LAN IP															
10	drop	forward	!192.168.0.0/20						bridge					0 B	0

Obrázek 40 – Nastavení firewallu

Zdroj: [59]

DNS Settings	
Servers:	10.254.253.250
	8.8.8.8
	8.8.4.4
Dynamic Servers:	
Use DoH Server:	
<input type="checkbox"/>	Verify DoH Certificate
<input type="checkbox"/>	Allow Remote Requests
Max UDP Packet Size:	4096
Query Server Timeout:	2.000 s
Query Total Timeout:	10.000 s
Max. Concurrent Queries:	100
Max. Concurrent TCP Sessions:	20
Cache Size:	2048 KiB
Cache Max TTL:	7d 00:00:00
Cache Used:	25 KiB

Obrázek 41 – Nastavení DNS

Zdroj: Vlastní



Obrázek 42 – Nastavení NTP serveru

*Zdroj: Vlastní*

Interface ID: VLAN1

Admin Status:  Enable

Interface Name:  (Optional. 1-128 characters)

IP Address Mode:  None  Static  DHCP  BOOTP

IP Address:  (Format: 192.168.0.1)

Subnet Mask:  (Format: 255.255.255.0)

Obrázek 43 – Nastavení IP adresy switche

*Zdroj: Vlastní*

Destination:  (Format: 10.10.10.0)

Subnet Mask:  (Format: 255.255.255.0)

Next Hop:  (Format: 192.168.0.2)

Distance:  (Optional. range: 1-255)

Obrázek 44 – Nastavení výchozí brány switche

*Zdroj: Vlastní*

UNIT1									
<input type="checkbox"/>	Port	PoE Status	PoE Priority	Power Limit	Power Limit Value (0.1-30.0 W)	Time Range	PoE Profile	Power (W)	Current
		Disable ▾	Low ▾	Class4 ▾	30	No Limit ▾	None ▾		
<input checked="" type="checkbox"/>	1	Disabled	Low	Class4	30	No Limit	None	0	
<input type="checkbox"/>	2	Enabled	Low	Class4	30	No Limit	None	0	
<input type="checkbox"/>	3	Enabled	Low	Class4	30	No Limit	None	0	
<input type="checkbox"/>	4	Enabled	Low	Class4	30	No Limit	None	0	
<input type="checkbox"/>	5	Enabled	Low	Class4	30	No Limit	None	0	
<input type="checkbox"/>	6	Enabled	Low	Class4	30	No Limit	None	0	
<input type="checkbox"/>	7	Enabled	Low	Class4	30	No Limit	None	0	
<input type="checkbox"/>	8	Enabled	Low	Class4	30	No Limit	None	0	
<input checked="" type="checkbox"/>	9	Disabled	Low	Class4	30	No Limit	None	0	
<input checked="" type="checkbox"/>	10	Disabled	Low	Class4	30	No Limit	None	0	

Obrázek 45 – Nastavení PoE portů switche

Zdroj: Vlastní

Configure Manually   
 Get Time from NTP Server   
 Synchronize with PC's Clock

Time Zone:

Primary NTP Server:  (Format: 192.168.0.1 or 2001::1 or domain)

Secondary NTP Server:  (Format: 192.168.0.1 or 2001::1 or domain)

Update Rate:  hours (1-24)

Obrázek 46 – Nastavení NTP serverů switche

Zdroj: Vlastní

## Příloha C – seznam příkazů konfigurace antény MikroTik

```
/interface bridge
add name=bridge1 port-cost-mode=short
/interface lte apn
set [ find default=yes ] ip-type=ipv4 use-network-apn=no
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=Antena-prijem-
MikroTik
/routing bgp template
set default disabled=no output.network=bgp-networks
/interface w60g
set [ find ] disabled=no isolate-stations=no name=wlan60-1
put-stations-in-bridge=*3 ssid=60G-Firma-ISP
/interface bridge port
add bridge=bridge1 ingress-filtering=no interface=wlan60-1
internal-path-cost=10 path-cost=10
add bridge=bridge1 ingress-filtering=no interface=ether1
internal-path-cost=10 path-cost=10
/ipv6 settings
set max-neighbor-entries=8192
/interface ovpn-server server
set auth=sha1,md5
/ip address
add address=10.100.7.3/24 interface=bridge1 network=10.100.7.0
/ip dns
set servers=10.254.253.250,8.8.8.8,8.8.4.4
/ip route
add disabled=no dst-address=0.0.0.0/0 gateway=10.100.7.1
/ipv6 address
add address=fd06:be7d:83ca:fe53::98fa interface=bridge1
/routing bfd configuration
add disabled=no interfaces=all min-rx=200ms min-tx=200ms
multiplier=5
/system identity
set name=Antena-prijem-MikroTik
/system leds
set 0 leds=led1,led2,led3,led4
/system note
set show-at-login=no
/system ntp client
set enabled=yes
/system ntp client servers
add address=195.113.144.201
add address=195.113.144.238
```

Příloha D – konfigurační obrazovky I. modelové varianty

New User

Name: sysadmin

Group: full

Allowed Address:

Last Logged In:

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

OK

Cancel

Apply

Disable

Comment

Copy

Remove

enabled

Obrázek 47 – Nastavení uživatele

*Zdroj: Vlastní*

Identity

Identity: Antena-prijem-Mikro Tik

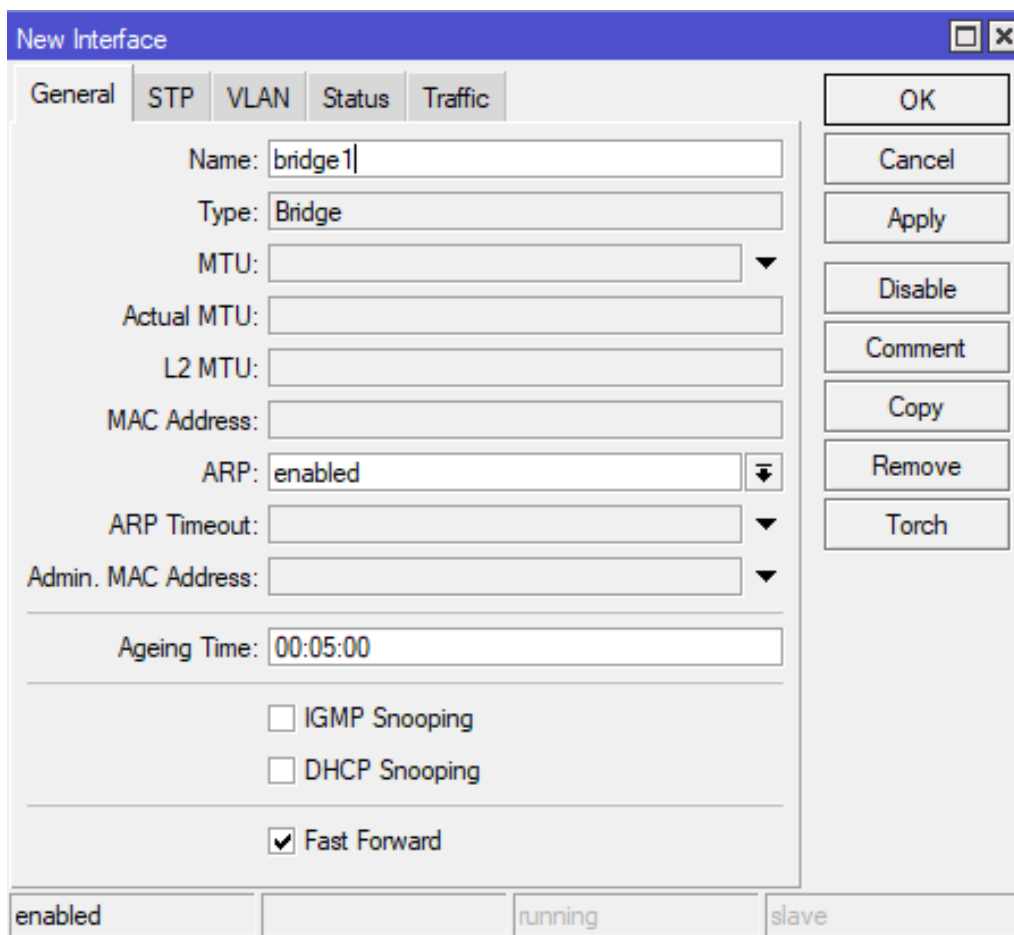
OK

Cancel

Apply

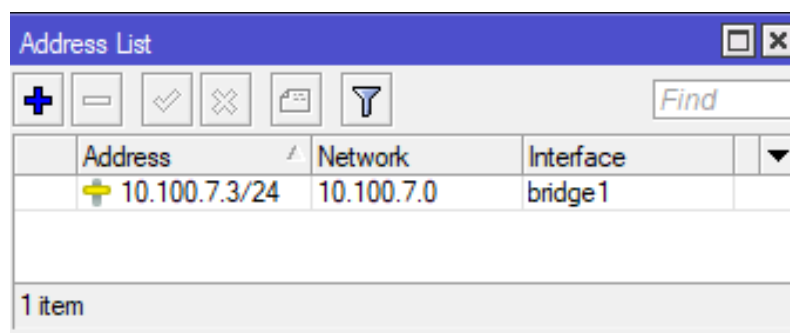
Obrázek 48 – Nastavení názvu zařízení

*Zdroj: Vlastní*



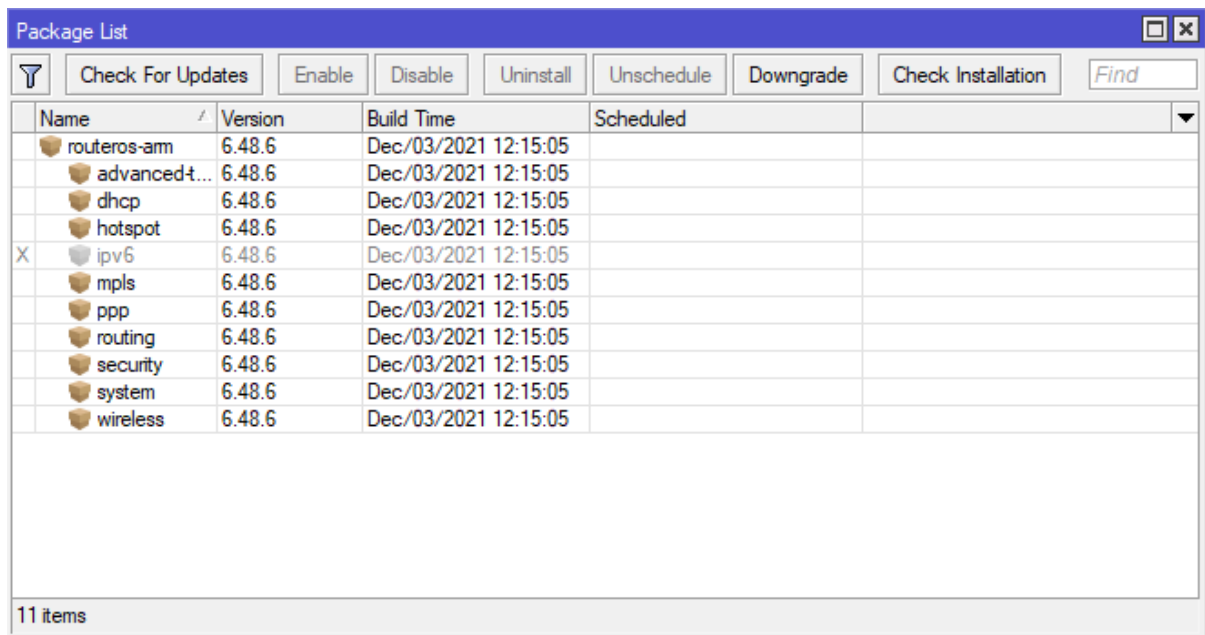
Obrázek 49 – Vytvoření rozhraní bridge

*Zdroj: Vlastní*



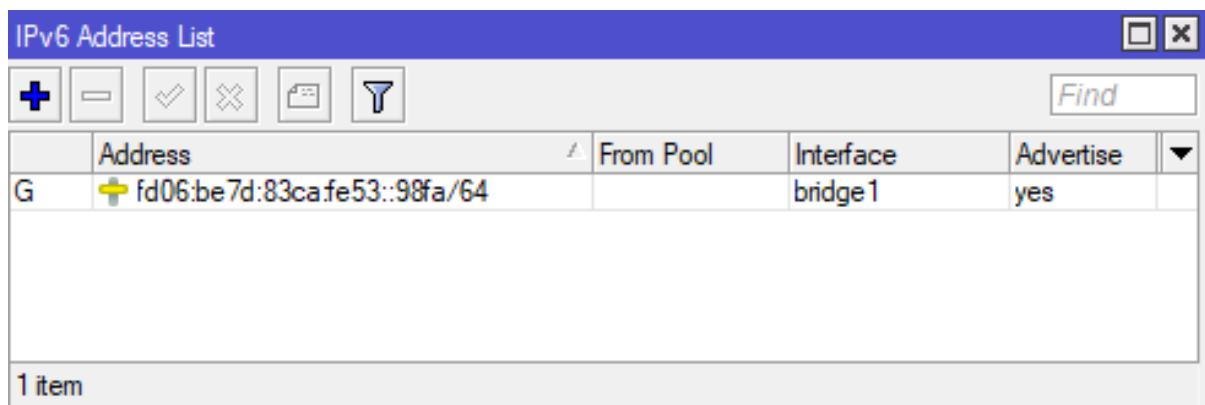
Obrázek 50 – Nastavení IPv4 adresy

*Zdroj: Vlastní*



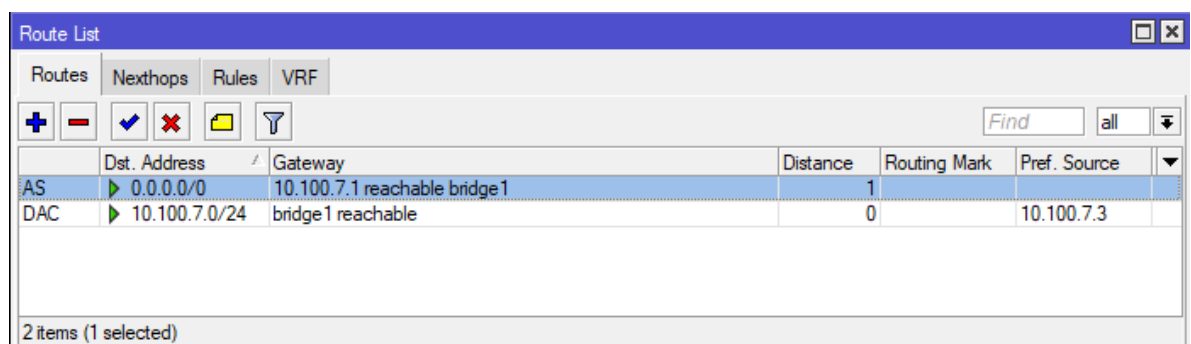
Obrázek 51 – Povolení balíčku IPv6

Zdroj: Vlastní



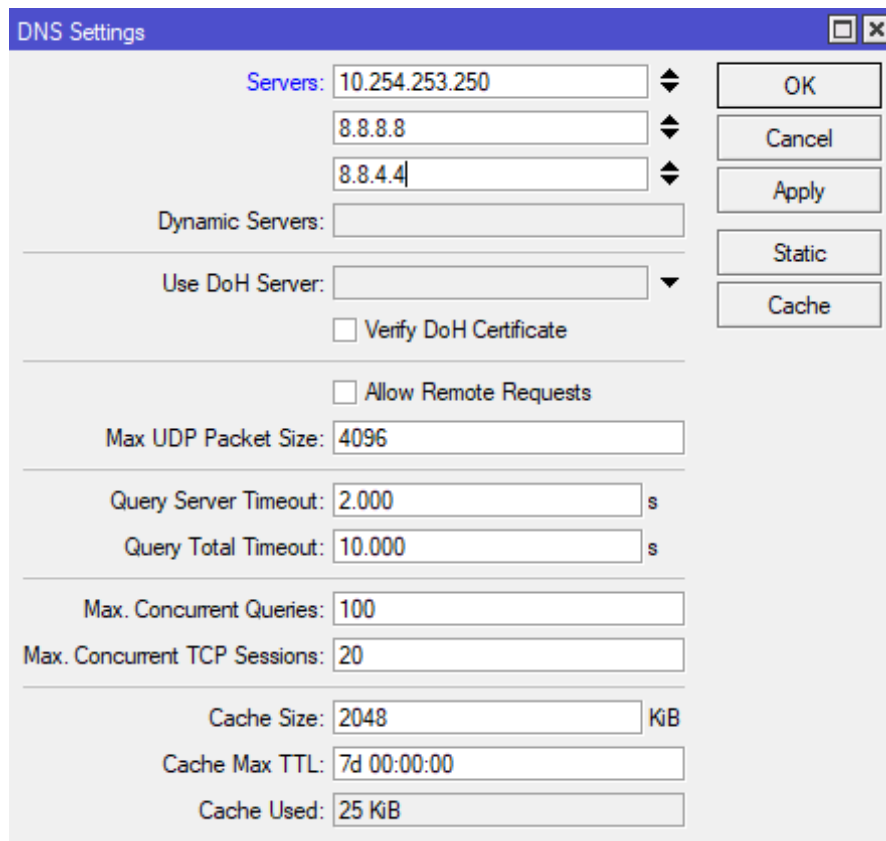
Obrázek 52 – Nastavení IPv6 adresy

Zdroj: Vlastní



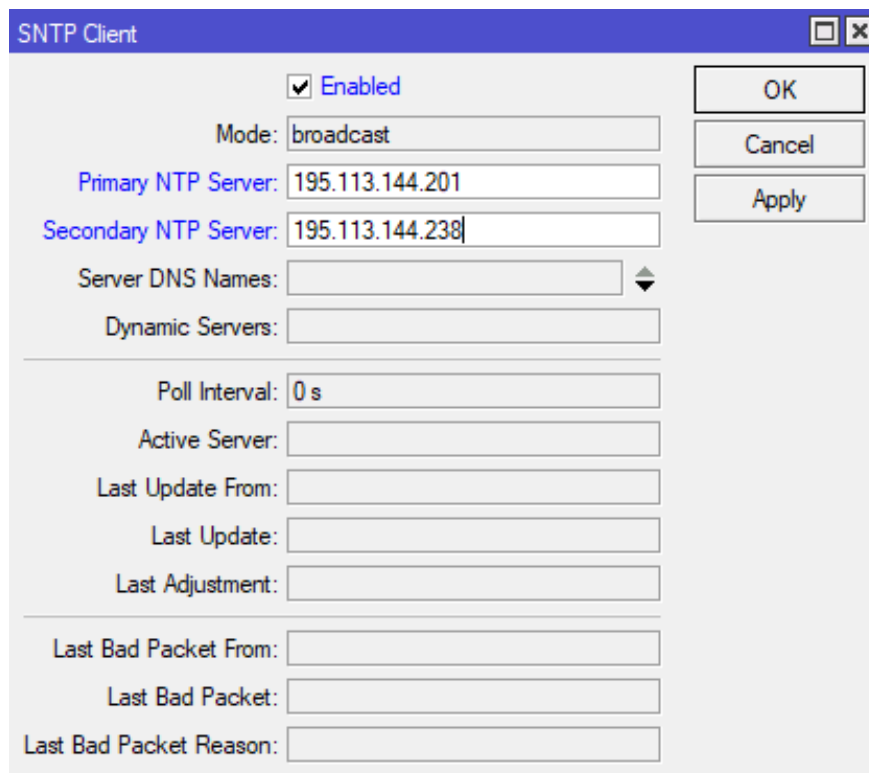
Obrázek 53 – Nastavení výchozí brány

Zdroj: Vlastní



Obrázek 54 – Nastavení DNS serverů

*Zdroj: Vlastní*



Obrázek 55 – Nastavení NTP serverů

*Zdroj: Vlastní*

Signal:	90
MCS:	8
PHY Rate:	2.3 Gbps
RSSI:	-55 dB

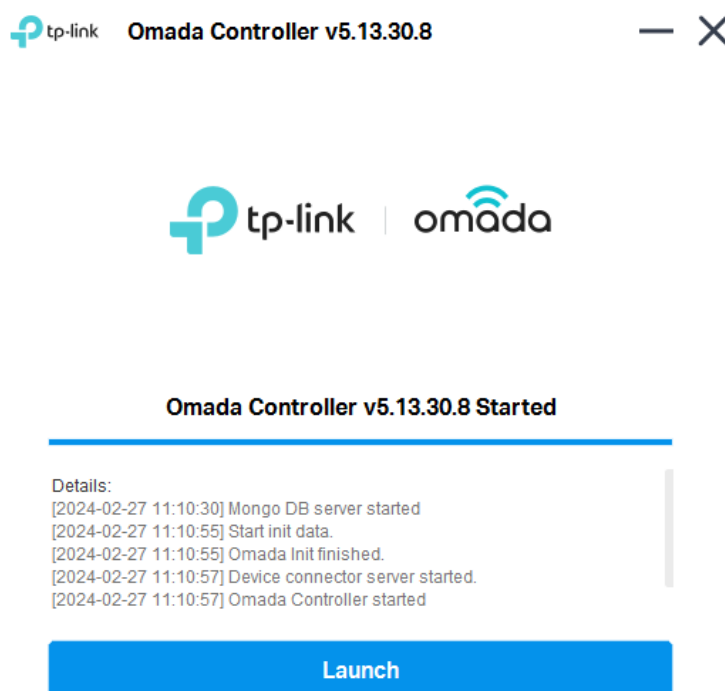
Obrázek 56 – Bezdrátové hodnoty připojení

*Zdroj: Vlastní*

Factory Firmware:	6.48.6
Current Firmware:	7.13.4
Upgrade Firmware:	7.13.4

Obrázek 57 – Update firmware zařízení

*Zdroj: Vlastní*



Obrázek 58 – Omada Software Controller

*Zdroj: Vlastní*



## Controller Access

Create an administrator name and password for local login to Omada Controller.

### Controller Main Administrator

Administrator Name:  Enter the username with letters (case-sensitive), numbers, underscores, or hyphens.

Email:  ⓘ

Password:  ⓘ  
Strength: High

Confirm Password:  ⓘ

To enjoy Omada Cloud Service, you can log in and bind your TP-Link ID to your controller.

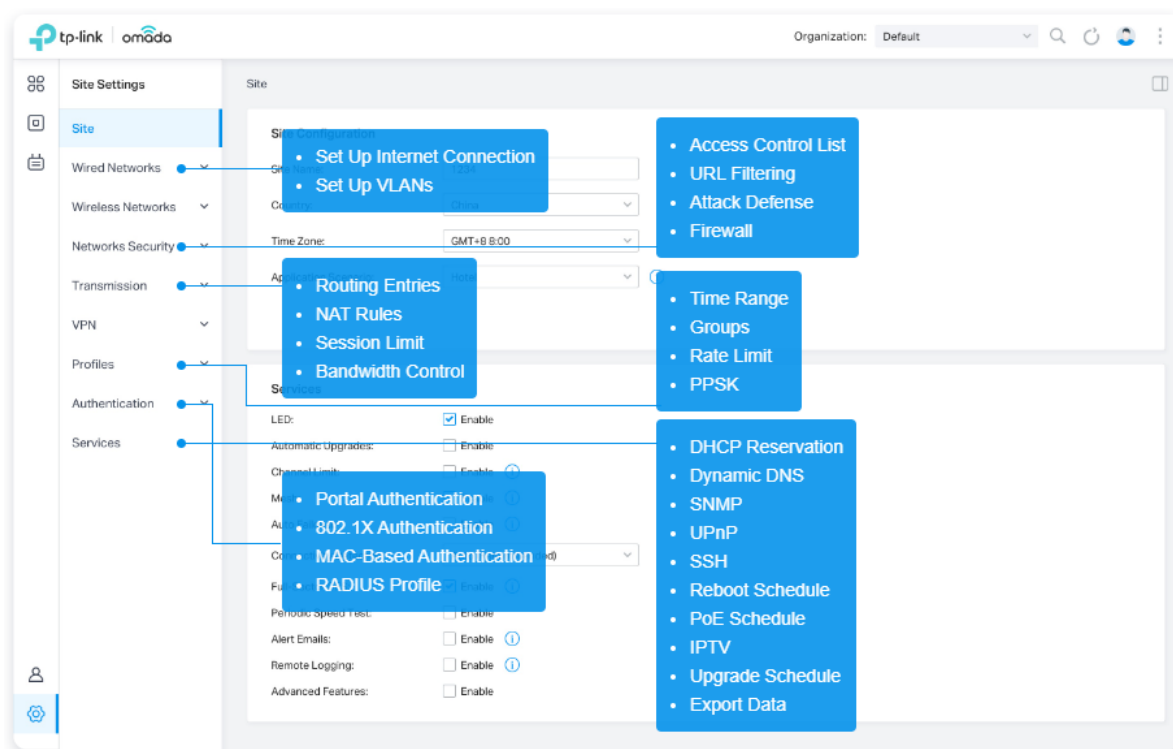
Cloud Access:

### Terms

I accept the [Terms of Use](#) and confirm that I have fully read and understood the [Privacy Policy](#).

Obrázek 59 – Nastavení přihlašovacích údajů

Zdroj: Vlastní



Obrázek 60 – Popis záložek nastavení Omada

Zdroj: Vlastní

1 Omada Setup Wizard — 2 Create Site — 3 Configure Devices — 4 Configure WAN Settings Overrides — 5 Configure Wi-Fi — 6 Summary

### Omada Setup Wizard

Controller Name:

Controller Country/Region:

Controller Timezone:

Controller Update Notification:  ⓘ

Devices Update Notification:  ⓘ

**Join User Experience Improvement Program**

By joining this program, you have fully read and understood our [User Experience Improvement Program Policy](#). You can opt out of the program at any time.

Obrázek 61 – Nastavení kontroleru

*Zdroj: Vlastní*

## Edit Wireless Network

Network Name (SSID):

Band:  2.4 GHz  5 GHz  6 GHz [i](#)

Guest Network:  Enable [i](#)

Security:

Security Key:  [i](#)

**Advanced Settings**

SSID Broadcast:  Enable

VLAN:  Enable

WPA Mode:

PMF: [i](#)  Mandatory  Capable  Disable

Group Key Update Period:  Enable GIK rekeying every   [v](#) (30-86400)

802.11r:  Enable [i](#)

Client Rate Limit Profile:  [i](#)

Download Limit:  Enable   [v](#) (1-10485760)

Upload Limit:  Enable   [v](#) (1-10485760)

SSID Rate Limit Profile:  [i](#)

Download Limit:  Enable

Upload Limit:  Enable







**WLAN Schedule**

**802.11 Rate Control**

**MAC Filter**

Obrázek 62 – Nastavení karty Wireless Networks

Zdroj: Vlastní

10-27-F5-BE-2F-	192.168.1.79	CONNECTED	EAP610(EU) v1.0	1.0.1	0 days 00:14:49	 
10-27-F5-BE-2F-	--	PENDING 	EAP610 v1.0	--	--	
10-27-F5-BE-2F-	--	PENDING 	EAP610 v1.0	--	--	

Obrázek 63 – Přidání AP do kontroleru

*Zdroj: Vlastní*

### IP Settings

#### IPv4

Mode:

DHCP

Static

IP Address:

192 . 168 . 0 . 3

IP Mask:

255 . 255 . 240 . 0

Gateway:

192 . 168 . 0 . 1

Primary DNS Server:

10 . 254 . 253 . 250 (Optional)

Secondary DNS Server:

8 . 8 . 8 . 8 (Optional)

**Apply**

Cancel

Obrázek 64 – Nastavení IP adresy AP

*Zdroj: Vlastní*

## Příloha E – konfigurační obrazovky II. modelové varianty

60 GHz Radio Settings

Channel Width: 2160 MHz

Frequency: 64800 MHz

Enable GPS Sync

5 GHz Backup Radio Settings

Channel Width: 20 MHz

Frequency: 5240 MHz

Obrázek 65 – Nastavení frekvencí a šířky kanálu

*Zdroj: Vlastní*

Network Mode:  Bridge  Router

Management Network Settings

Management IP Address:  DHCP  Static

IP Address: 10.100.7.3

Netmask: 255.255.255.0

Gateway IP: 10.100.7.1

MTU: 1500

Management VLAN:

IPv6 Address:  Local  Static  SLAAC

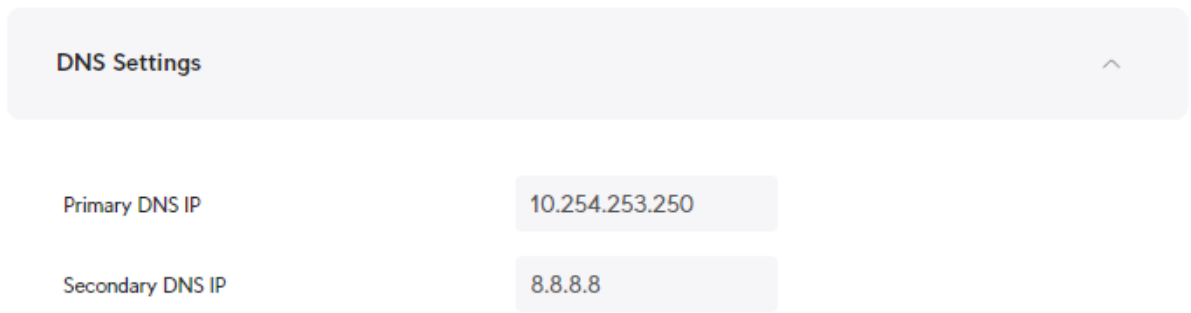
IPv6 Address: fd06:be7d:83ca:fe53::98fa

IPv6 Netmask: 64

IPv6 Gateway: fd06:be7d:83ca:fe53:ffff:ffff:ffff:ffff

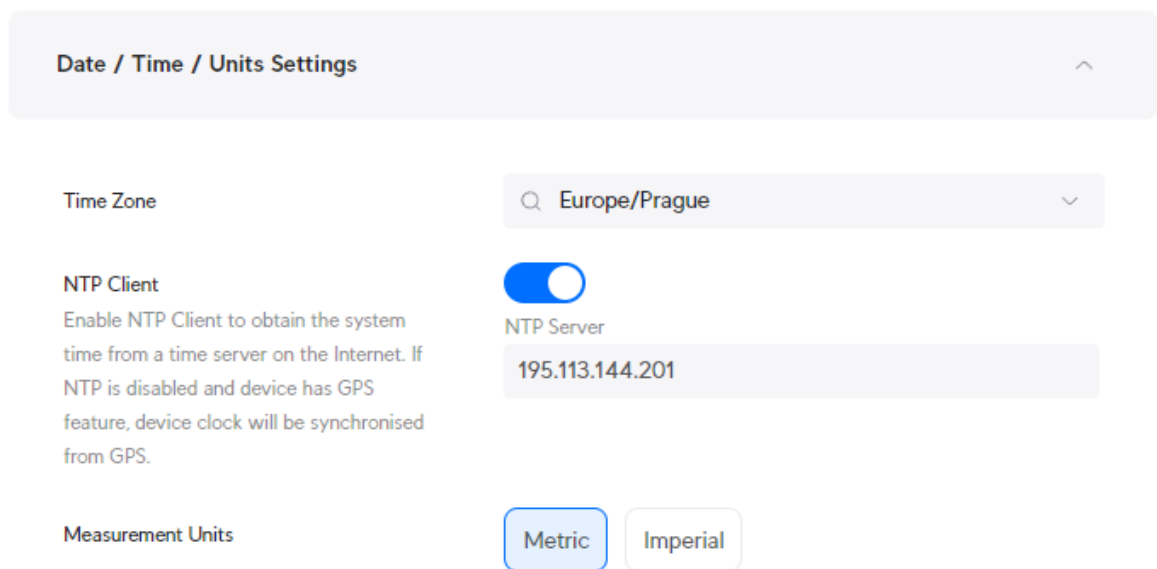
Obrázek 66 – Síťová nastavení

*Zdroj: Vlastní*



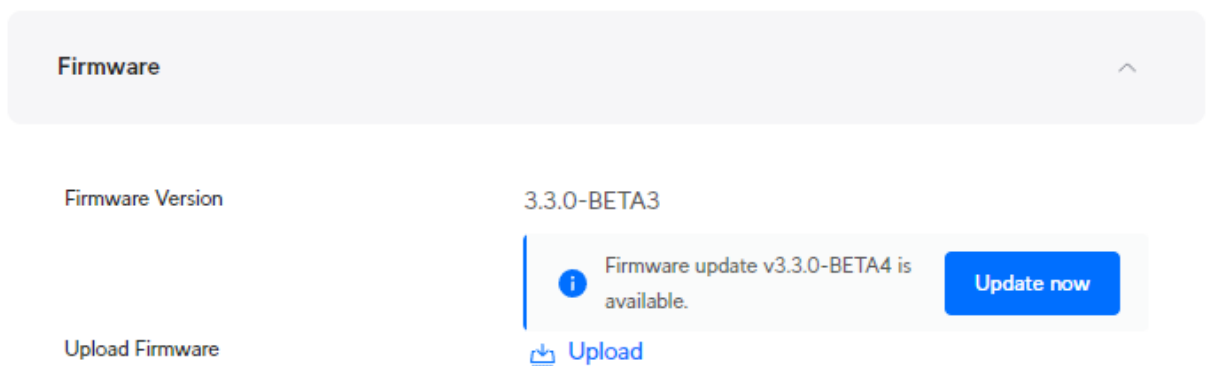
Obrázek 67 – Nastavení DNS

*Zdroj: Vlastní*



Obrázek 68 – Nastavení NTP serveru

*Zdroj: Vlastní*



Obrázek 69 – Aktualizace firmware

*Zdroj: Vlastní*

**Port Management** Beta

**Auto Port**

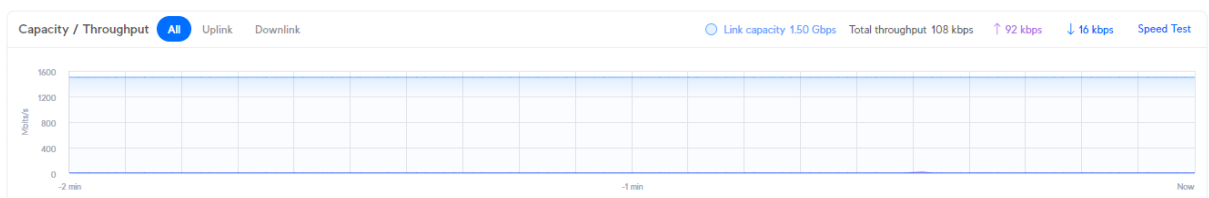
Automatically disables data on Ethernet ports in case the SFP+ is active

■ 10/100 Mbps
 ■ 1 Gbps
 ■ 2.5 Gbps
 ■ 5 Gbps
 ■ 10 Gbps
 ■ Not Connected
 ⚡ PoE

Port	Name	Status	Current Speed	Type	Actions
<span style="color: green;">⚡</span> 1	Ethernet Port	Enabled	1000-FDX (Auto)	Ethernet	<a href="#">Edit</a>

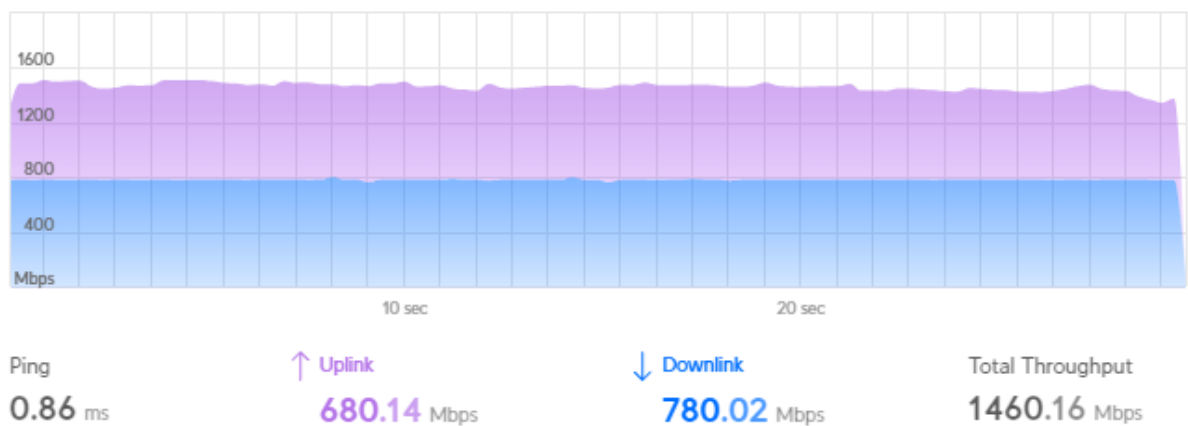
Obrázek 70 – Port Management

Zdroj: Vlastní



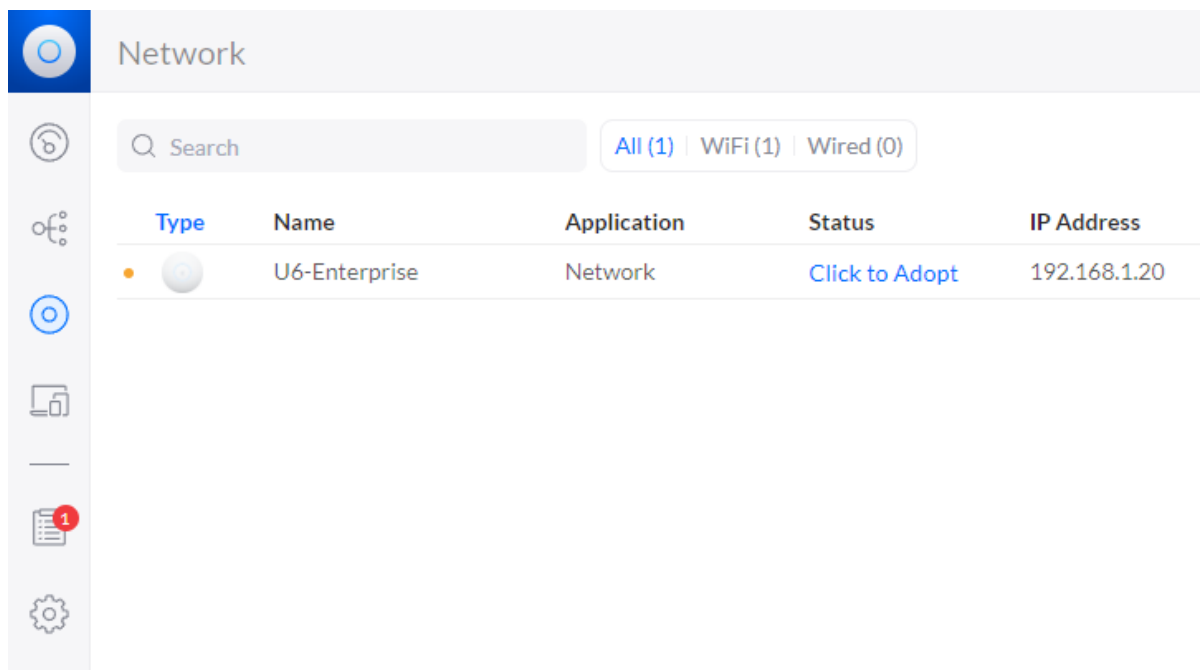
Obrázek 71 – Kapacita rádii

Zdroj: Vlastní



Obrázek 72 – Test rychlosti

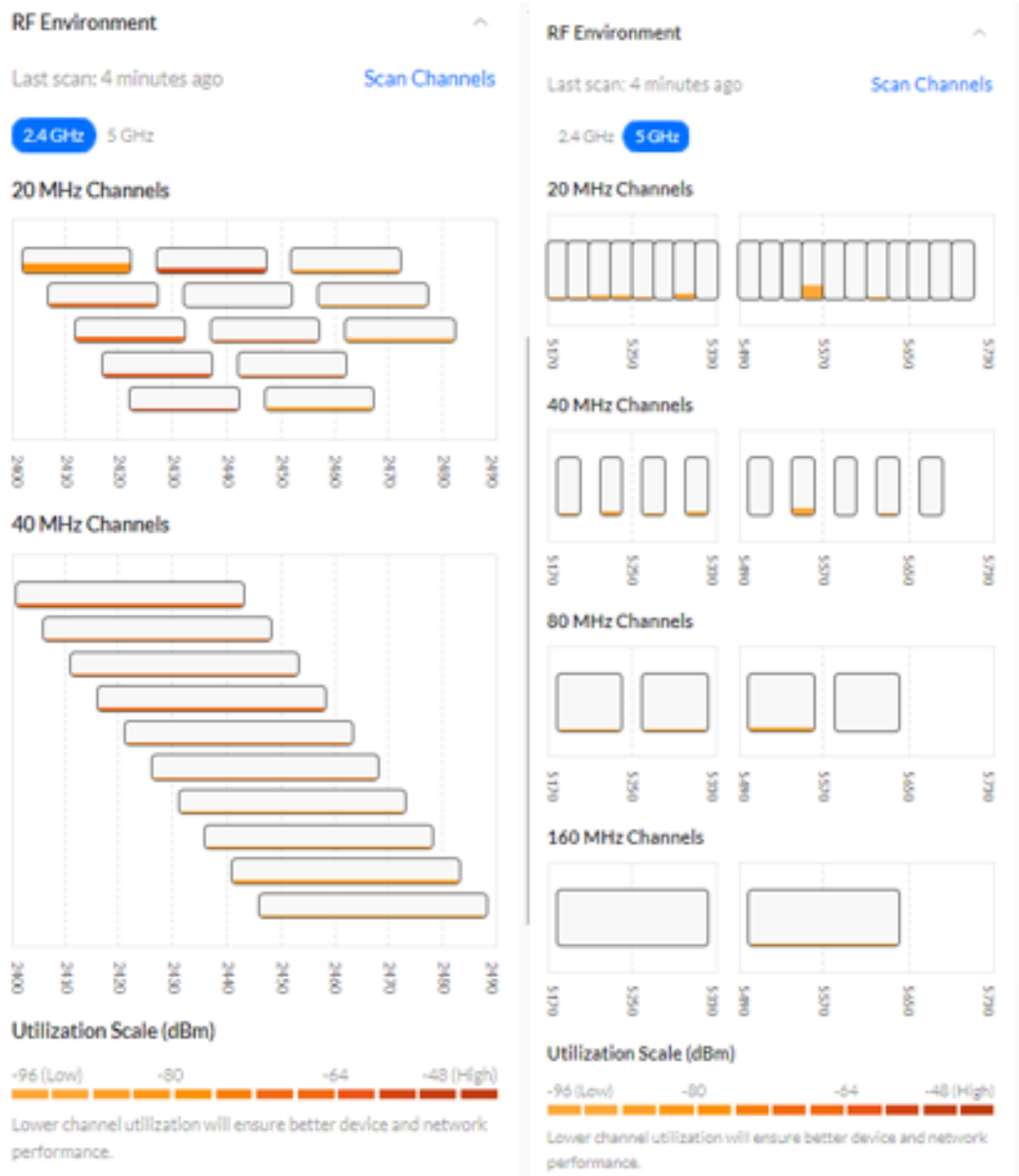
Zdroj: Vlastní



Obrázek 73 – Seznam zařízení UniFi

*Zdroj: Vlastní*





Obrázek 74 – Skenování kanálů

Zdroj: Vlastní

Auto  Manual

---

**Band Steering** ^

Off  Prefer 5 GHz  Balanced

---

**IP Settings** ^

IP Configuration

DHCP  Static

IP Address	Preferred DNS
192.168.0.3	10.254.253.250
Subnet Mask	Alternate DNS
255.255.240.0	8.8.8.8
Gateway	DNS Suffix
192.168.0.1	

---

**Manage** ^

LED

SNMP

Low Performance Mode ⓘ

Obrázek 75 – Nastavení sítě

*Zdroj: Vlastní*

WiFi Band ⓘ	<input checked="" type="checkbox"/> 2.4 GHz <input checked="" type="checkbox"/> 5 GHz <input checked="" type="checkbox"/> 6 GHz	Minimum Data Rate Control ⓘ	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Band Steering ⓘ	<input checked="" type="checkbox"/>	MAC Address Filter ⓘ	<input type="checkbox"/>
Hide WiFi Name	<input type="checkbox"/>	RADIUS MAC Authentication ⓘ	<input type="checkbox"/>
Client Device Isolation ⓘ	<input type="checkbox"/>	Security Protocol ⓘ	WPA3
Proxy ARP ⓘ	<input type="checkbox"/>	PMF ⓘ	<input checked="" type="radio"/> Required <input type="radio"/> Optional <input type="radio"/> Disabled
BSS Transition ⓘ	<input checked="" type="checkbox"/>		<small>⚠ WPA3 is a new security standard that has been known to cause connectivity issues with certain WiFi devices. Please implement with caution.</small>
UAPSD ⓘ	<input type="checkbox"/>	Group Rekey Interval ⓘ	<input type="checkbox"/> 0 Sec
Fast Roaming ⓘ	<input type="checkbox"/>	SAE Anti-clogging	5
WiFi Speed Limit ⓘ	<input type="checkbox"/>	SAE Sync Time	5
Multicast Enhancement ⓘ	<input type="checkbox"/>	WiFi Scheduler ⓘ	<input checked="" type="radio"/> Off <input type="radio"/> On
Multicast and Broadcast Control ⓘ	<input type="checkbox"/>		
802.11 DTIM Period ⓘ	<input checked="" type="checkbox"/> Auto <input type="checkbox"/> 2.4 GHz 1 <input type="checkbox"/> 5 GHz 3 <input type="checkbox"/> 6 GHz 3		

Obrázek 76 – Nastavení Wi-Fi

*Zdroj: Vlastní*

Příloha F – konfigurační obrazovky III. modelové varianty

The image shows a network configuration interface. At the top, there is a field for '\* Network Name' with the value 'Firma'. Below this is a section titled 'Network Settings'. Inside this section, there are radio buttons for 'Internet', 'DHCP', and 'Static IP', with 'Static IP' selected. A 'Current IP' button is next to it. Below the radio buttons are several input fields: '\* IP' (192.168.0.3), '\* Subnet Mask' (255.255.240.0), '\* Gateway' (192.168.0.1), '\* DNS Server' (8.8.8.8), and '\* SSID' (@Firma). At the bottom of the 'Network Settings' section, there are radio buttons for 'Wi-Fi Password' with 'Security' selected and 'Open' unselected. Below these is a password input field with a masked password '.....' and a visibility toggle icon.

Obrázek 77 - Síťová nastavení

*Zdroj: Vlastní*

## Wi-Fi Settings Device Group: Default

Up to 8 SSIDs can be added.

**Default**  
**@Firma**  
Default VLAN  
Band:2.4G+5G

**@IT\_oddeleni**  
Default VLAN  
Band:2.4G+5G

**@ucetni\_oddeleni**  
Default VLAN  
Band:2.4G+5G

+ Add Guest Wi-Fi

+ Add Wi-Fi

\* SSID

Band  2.4G  5G

Encryption  Open  Security  802.1x (Enterprise)

\* Security

\* Wi-Fi Password

Expand

Save

Obrázek 78 – Nastavení Wi-Fi

Zdroj: Vlastní

## Add



\* Client MAC

Uplink Rate  Mbps

Limit Current: **10240** Kbps. Range: 1-1700000 Kbps

Downlink Rate  Mbps

Limit Current: **10240** Kbps. Range: 1-1700000 Kbps

Remarks

Cancel

OK

Obrázek 79 – Omezení rychlosti koncového zařízení

Zdroj: Vlastní

SSID-based Rate Limiting Device Group: Default

[Are you sure you want to add a Wi-Fi? Click to go.](#)

SSID	Uplink Rate Limit	Downlink Rate Limit	Action
@Firma	No Limit	No Limit	<a href="#">Edit</a> <a href="#">Disable</a>
@IT_oddeleni	No Limit	No Limit	<a href="#">Edit</a> <a href="#">Disable</a>
@ucetni_oddeleni	No Limit	No Limit	<a href="#">Edit</a> <a href="#">Disable</a>

Obrázek 80 – Omezení rychlosti dle SSID

Zdroj: Vlastní

After Reyee Mesh is enabled, the devices that support Reyee Mesh can be paired through wireless or wired connection to set up a Mesh network. Auto link optimization is supported in the Mesh network.

**i** Mesh link optimization algorithm: The algorithm not only covers signal strength, wireless mode, antenna streams and bandwidth parameters, but also considers the attenuation of Mesh hops. The Mesh system will select the optimal uplink automatically for the AP based on the link optimization algorithm.

Enable

[Save](#)

Obrázek 81 – Reyee Mesh

Zdroj: Vlastní

**Online Clients**  
The client going offline will not disappear immediately. Instead, the client will stay in the list for three more minutes.

**Online Clients**

All (1) | Wired (0) | Wireless (1) | User not connected (0)

Search by IP/MAC/Username

Device Name	Type	Access Location	IP Address/MAC Address	Wi-Fi	LimitSpeed	Action
<a href="#">Click to edit</a>	2.4G	CAR60X9046157	192.168.0.219 ea:01:6f:10:4d:19	Channel:6 RSCP:-52 Duration:8 minutes 8 seconds Negotiation Rate:86M SSID:@IT_oddeleni	Uplink Rate:10Mbps Downlink Rate:10Mbps	<a href="#">Add to Blocklist</a>

1 / 10/page Total 1

Obrázek 82 – Připojená zařízení

Zdroj: Vlastní

**Device Info**

Memory Usage: 36%

Online Clients: 1

Connection Status: Online  
Uptime: 45 minutes 5 seconds  
System Time: 2024-01-30 20:13:35

**Device Details**

Device Model: RAP2260(G) | Device Name: [Rujjie](#) | SN: CAR60X9046157  
 MAC Address: 54:16:51:46:EE:11 | Working Mode: [AP](#) | Role: Master AP  
 Hardware Version: 1.11 | Software Version: ReyeeOS 2.262.0.2404

**Wi-Fi**

Primary Wi-Fi: @Firma Security: Yes | Guest Wi-Fi: Security: No

**Ethernet status**

Connected | Disconnected

WAN 192.168.0.3 | LAN

Obrázek 83 – Úvodní obrazovka nastaveného AP

Zdroj: Vlastní