Návrh a realizace Wi-Fi hotspotu v administrativním objektu

Bc. Petr Vavroušek

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. Petr Vavroušek**
Osobní číslo:	**A17354**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh a realizace Wi-Fi hotspotu v administrativním objektu**
Téma anglicky:	**The Design and Implementation of a Wi-Fi Hotspot for an Administration Building**

Zásady pro vypracování:

1. **V literární rešerši vypracujte přehled o technologii Wi-Fi a možnostech zabezpečení Wi-Fi sítí.**
2. **Zvolenými prostředky proveďte měření stávajícího signálu Wi-Fi s grafickým výstupem.**
3. **Navrhněte jednotlivé HW a SW komponenty hotspotu včetně jejich konfigurace.**
4. **Vytvořte webový informační přihlašovací portál.**
5. **Zpracujte výslednou mapu pokrytí signálem Wi-Fi v objektu a zhodnoťte funkčnost systému jako celku.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ZANDL, Patrick. Bezdrátové sítě WiFi: praktický průvodce. Brno: Computer Press, 2003. ISBN 80-722-6632-2.**
2. **PEREZ, Andre. Network security. Hoboken, NJ: ISTE Ltd/ Wiley, 2014. ISBN 978-1-848-21758-4.**
3. **CHANDRA, Praphul. Wireless networking. Boston: Elsevier/Newnes, c2008. ISBN 978-0-7506-8582-5.**
4. **BARKEN, Lee. Wi-Fi: jak zabezpečit bezdrátovou síť. Brno: Computer Press, 2004. ISBN 80-251-0346-3.**
5. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. Brno: CP Books, 2005. ISBN 80-251-0791-4.**

Vedoucí diplomové práce: **Ing. Ján Ivanka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **30. listopadu 2018**

Termín odevzdání diplomové práce: **17. května 2019**

Ve Zlíně dne 14. prosince 2018

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 17.5.2019

PETR VAVROUŠEK v.r.

.....

podpis diplomanta

ABSTRAKT

Diplomová práce se zabývá návrhem a realizací řešení hotspotu s informačním portálem pro návštěvníky administrativního objektu v Praze. V teoretické části shrnuje poznatky o bezdrátové technologii Wi-Fi se zaměřením zejména na možnosti zabezpečení. V praktické části je zpracována analýza stávajícího stavu pokrytí signálem Wi-Fi a průzkum lokality využitím softwarových a hardwarových nástrojů. Proveden návrh komponentů hotspotu včetně jejich konfigurace a navržen informační webový portál. Cílem diplomové práce je komplexní návrh a realizace zabezpečeného bezdrátového přístupu k síti Internet s integrovaným informačním a přihlašovacím portálem.

Klíčová slova:

Hotspot, Wi-Fi, Bezdrátová síť, Bezdrátové zabezpečení, WLAN, Průzkum lokality

ABSTRACT

This diploma thesis deals with design and implementation of hotspot solution with information portal for visitors of administrative building in Prague. The theoretical part summarizes the knowledge of Wi-Fi wireless technology with a particular focus on security options. In the practical part there is an analysis of the current state of Wi-Fi signal coverage and survey of the site by using software and hardware tools. Design of the components of the hotspot including their configuration and design of information web portal. The aim of the thesis is a complex design and implementation of secure wireless access to the Internet with an integrated information and login portal.

Keywords:

Hotspot, Wi-Fi, Wireless network, Wireless Security, WLAN, Site Survey

Na tomto místě bych rád poděkoval zejména rodině za jejich podporu při studiu a celému akademickému sboru Fakulty aplikované informatiky UTB ve Zlíně.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Obrovský nárůst používání bezdrátových technologií, především ke komunikaci s okolním světem, ať již mezi lidmi nebo mezi přístroji samotnými, vyžaduje nejen neustálé zrychlování a zkvalitňování připojení k bezdrátovým sítím, ale také jejich zabezpečení. Veřejných přístupových bodů k síti Internet (hotspotů) je dnes obrovské množství po celém světě a neustále přibývají. Přístup k jejich zabezpečení je různý, limitován je především vlastnostmi a funkcemi bezdrátových technologií. Bezdrátový přístup k síti Internet je dnes zcela běžnou záležitostí, jak v externím tak i interním prostředí objektů. Bezdrátové sítě využívají k přenosu dat rádiové vlny na určitých frekvencích, kvalita a úroveň vysílaného signálu je závislá nejen na použitých konstrukčních materiálech daného objektu, ale zejména na okolním prostředí s množstvím méně či více rušivých signálů. Pro analýzu prostředí a návrh řešení bezdrátových přístupových bodů se využívá specifických softwarových (dále jen SW) a hardwarových (dále jen HW) nástrojů.

Diplomová práce je členěna na teoretickou a praktickou část. V teoretické části se práce zaměřuje na historii, vývoj a standardizaci bezdrátové technologie Wi-Fi. Z větší části se zabývá především technologií Wi-Fi jako takové, zejména na jakém principu funguje a z jakých komponentů se skládá. Další kapitola teoretické části práce je zaměřena především na možnosti zabezpečení Wi-Fi. Detailněji jsou popsány možnosti zabezpečení a vlastnosti zabezpečovacích protokolů bezdrátových sítí. Praktická část práce se věnuje vlastnímu řešení hotspotu pro návštěvníky administrativního objektu. Od počáteční analýzy stavu bezdrátového prostředí v objektu pomocí SW a HW nástrojů, provedení prediktivního průzkumu objektu pomocí SW nástrojů, přes návrh jednotlivých SW a HW komponentů systému, jejich konfiguraci, nastavení a volbě zabezpečení. Následně provedení pasivního průzkumu před vlastním nasazením. Vytvoření vlastního webového portálu včetně prohlášení o ochraně osobních údajů. V závěru praktické části je proveden aktivní průzkum, ověření a zhodnocení funkčnosti systému, proměření úrovně signálu Wi-Fi s výslednou mapou pokrytí.

Cílem práce je návrh a realizace hotspotu pro administrativní objekt se zabezpečeným přístupem pro návštěvníky objektu. Součástí cíle je vytvoření vlastního informačního portálu, který poskytne návštěvníkům informace o objektu a interních bezpečnostních předpisech. Přínos práce spočívá v komplexním zpracování řešení systému hotspotu se zabezpečeným přístupem a zefektivnění informovanosti návštěvníků objektu prostřednictvím informačního portálu.

I. TEORETICKÁ ČÁST

1 WI-FI

V době kdy se začala vyrábět a následně na to hromadně používat mobilní zařízení (např. notebooky, netbooky, PDA…), bylo požadavkem a hlavně cílem propojení těchto zařízení pro vzájemnou komunikaci resp. jejich připojení k síti tak, aby nebyla degradována jejich hlavní vlastnost mobilita; tedy bezdrátově, což vedlo ke vzniku bezdrátové technologie nazývané Wi-Fi. Zařízení s podporou Wi-Fi jako notebook nebo mobilní telefon se může připojit k síti Internet, pokud se nachází v dosahu přístupového bodu neboli „access pointu". Oblast pokrytá jedním nebo několika přístupovými body se nazývá „hotspot". Hotspoty mohou pokrývat bezdrátovým signálem prostor o velikosti jedné místnosti až po rozsáhlé oblasti o několika kilometrech čtverečních. Wi-Fi lze také využít při vytváření bezdrátových lokálních sítí „WLAN", i rozsáhlé sítě bezdrátových sítí „Wireless mesh networks". Wi-Fi také umožňuje připojení v režimu klient-klient neboli „peer to peer", který umožňuje propojení zařízení přímo mezi sebou. [1]

1.1 Historie Wi-Fi

V časech kdy se Wi-Fi technologie začala komerčně prosazovat, se objevilo mnoho problémů s kompatibilitou a koncoví uživatelé si tak nemohli být jisti, že se jejich zakoupená zařízení k sobě vůbec připojí. Na základě odezvy koncových uživatelů se zformovala komunita nyní společnost Wi-Fi Alliance[1], která se snažila těmito problémy zabývat a umožnit tak této mladé technologii dospět. Aliance vytvořila značku „Wi-Fi CERTIFIED", která označuje, že výrobky jsou interoperabilní s jinými produkty, kterou jsou označeny logem Wi-Fi CERTIFIED. Wi-Fi využívá rádiovou technologii rozprostřeného spektra. Nelicencované rozprostřené spektrum bylo nejprve schváleno Federální komisí pro komunikace v roce 1985 (FCC – obdoba našeho ČTÚ) a následně FCC regulace a předpisy umožňující využívání této technologie přijaty většinou zemí. Na základě těchto regulací byla následně vyvíjena Wi-Fi i Bluetooth. Předchůdce Wi-Fi byla vynalezena v roce 1991 firmou NCR Corporation / AT & T (později Lucent & Agere System) v Nizozemsku v Nieuwegeinu. Původně

[1] Wi-Fi Alliance – v roce 1999 se spojilo několik vizionářských společností a vytvořilo globální neziskové sdružení s cílem popularizace bezdrátové technologie bez ohledu na značku. V roce 2000 přijala skupina oficiální název Wi-Fi pro svou technickou činnost a oznámila svůj oficiální název Wi-Fi Alliance. Počet členů se od založení aliance stále zvyšuje.

byla určena pro pokladní systémy; první bezdrátové produkty byly uvedeny na trh pod názvem WaveLAN o rychlostech 1-2Mbit/s. Vic Hayes[2], který byl primárním vynálezcem Wi-Fi, se podílel na navrhování standardů, jako jsou IEEE 802.11b, 802.11a a 802.11g. V roce 2003 společnost Agere Systems opustil a ta se následně pod tíhou silné konkurence rozhodla opustit trh Wi-Fi. [1]

Obr. 1. Volně použitelná Wi-Fi loga. [1]

1.2 IEEE 802.11

IEEE 802.11 je sada standardů pro bezdrátovou lokální síť (WLAN), počítačovou komunikaci, vytvořena IEEE LAN/MAN Standards Committee[3] pro frekvenční pásma 2.4Ghz a 5Ghz veřejného rádiového spektra. Sada 802.11 podporuje nebo používá bezdrátové modulační techniky pro komunikaci, které používají některé základní protokoly. Protokoly, které definují soubor pravidel. Nejznámější standardy jsou definovány protokoly IEEE 802.11b a IEEE 802.11g a jsou změnami původního standardu. Původní bezdrátový standard byl protokol IEEE 802.11a, ale široce akceptovaným protokolem se stal již zmíněný IEEE 802.11b následovaný protokoly IEEE 802.11g, IEEE 802.11n a IEEE 802.11ac. [2]

Původní verze standardu IEEE 802.11 byla vydána v roce 1997 a následně klarifikována v roce 1999. Specifikovala dva typy přenosových rychlostí dat, 1Mbps a 2Mbps, která mají být přenášena ve frekvenčním pásmu ISM (Industrial Scientific Medical) na frekvenci 2,4Ghz, ale velmi rychle byla nahrazena standardem IEEE 802.11b. Nejnověji certifikovaným standardem je IEEE 802.11ax označený „Wi-Fi Certified 6“ s přenosovou rychlostí až 10Gbps. [2]

---

[2] Victor „Vic“ Hayes – nar. 31/6/1941 v Indonésii, je bývalý vědecký pracovník na Delftské technologické univerzitě. Jeho úloha při vytváření a předsednictví pracovní skupiny standardů IEEE 802.11 pro bezdrátové lokální sítě vedla k tomu, že jej někteří označovali za „otce Wi-Fi“.

[3] IEEE – Institue of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství) založen 1963 v USA – mezinárodní nezisková organizace.

Tab. 1. Přehled standardů IEEE 802.11. [3] - upraveno Vavroušek 2019

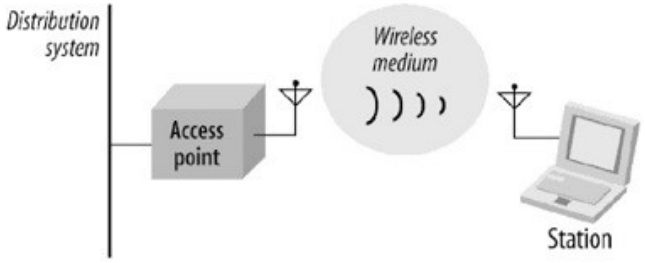
Standard	Rok vydání	Označení	Pásmo [GHz]	Maximální rychlost [Mbit/s]	Fyzická vrstva
původní IEEE 802.11	1997		2,4	2	DSSS a FHSS
IEEE 802.11a	1999	Wi-Fi 1	5	54	OFDM
IEEE 802.11b	1999	Wi-Fi 2	2,4	11	DSSS
IEEE 802.11g	2003	Wi-Fi 3	2,4	54	OFDM
IEEE 802.11n	2009	Wi-Fi 4	2,4 nebo 5	600	MIMO OFDM
IEEE 802.11y	2008		3,7	54	
IEEE 802.11ac	2013	Wi-Fi 5	2,4 a 5	1000	MU-MIMO OFDM
IEEE 802.11ad	2012		2,4, 5 a 60	7000	
IEEE 802.11ax	2018	Wi-Fi 6	2,4 a 5	10000	MIMO-OFDM

1.3 Technologie Wi-Fi

Bezdrátové sítě založené na protokolu 802.11 se skládají (*Obr. 2*) ze čtyř hlavních součástí. Těmito součástmi jsou:

- Distribuční systém (Distribution System)
- Přístupový bod (Access Point)
- Bezdrátové médium (Wireless Medium)
- Stanice (Station)

Sítě jsou určeny k přenášení dat mezi stanicemi. Stanice jsou počítačová zařízení, které obsahují bezdrátový síťový adaptér. Typicky jsou to zařízení jako mobilní telefony a notebooky, ale nutně nemusí jít jen o přenosná zařízení, k bezdrátové síti může být připojen nepřenosný desktopový systém, zabezpečovací systém, kamerový systém atp. Přístupové body zajišťují funkci jakéhosi „překladatele“ z bezdrátové sítě do sítě drátové, technicky se jedná

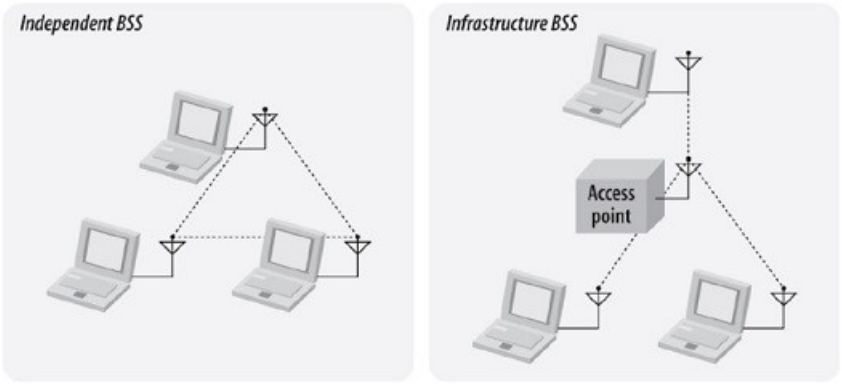


Obr. 2. Základní součásti bezdrátové sítě. [4]

o bridge, resp. přemostění. Přístupové body poskytují mnohé další funkce, ale funkce přemostění, je tou nejdůležitější. Abychom mohli ze stanice na stanici přenášet datové rámce, potřebujeme bezdrátové médium. Několik různých fyzických vrstev je definováno, architektura umožňuje vývoj několika fyzických vrstev, které podporují technologii 802.11. Původně dvě radiofrekvenční fyzické vrstvy a jedna infračervená byly standardizovány, dnes se používají převážně radiofrekvenční (dále jen RF). Při pokrytí velkých oblastí bezdrátovým signálem několika přístupovými body musí být zajištěna jejich vzájemná komunikace pro sledování pohybu mobilních zařízení, a k tomu slouží distribuční systém. Distribuční systém je logickou komponentou bezdrátových sítí 802.11, která se využívá pro doručování datových rámců do jejich destinací. [4] [5]

1.3.1 Síťová topologie

Základním stavebním kamenem bezdrátové sítě 802.11 je „Základní sada služeb“ resp. „Basic Service Set“ (BSS), zjednodušeně skupina stanic komunikujících vzájemně mezi sebou. Komunikace mezi nimi probíhá v neohraničené oblasti nazývané „Základní oblast služeb“ resp. „Basic Service Area“ (BSA), která je definována charakteristikou šíření bezdrátového média. Pokud se stanice nachází v BSA, může komunikovat s ostatními členy BSS. Rozeznáváme dva typy BSS, „Independent“ a „Infrastructure“. [4] [5]



Obr. 3. Nezávislý a Infrastrukturní BSS. [5]

1.3.1.1 Nezávislý BSS

Independent neboli nezávislý samostatný BSS (*Obr. 3*) též označovaný jako IBSS. Stanice v IBSS komunikují napřímo mezi sebou a tím pádem musí být v přímém komunikačním dosahu. Nejmenší možná 802.11 síť v IBSS má 2 stanice. Typicky se IBSS skládá z menšího počtu stanic připojených napřímo a na kratší časový úsek z nějakého specifického důvodu.

Jedním z důvodů může být např. dočasná bezdrátová síť složená z notebooků účastníků mítinku. Na začátku mítinku účastníci vytvoří IBSS pro sdílení dat, po ukončení mítinku je IBSS zrušen. Z důvodu délky trvání, malé velikosti a specifickému důvodu IBSS se někdy nazývají ad hoc BSS nebo též ad hoc sítě. [4] [5]

1.3.1.2 Infrastrukturní BSS

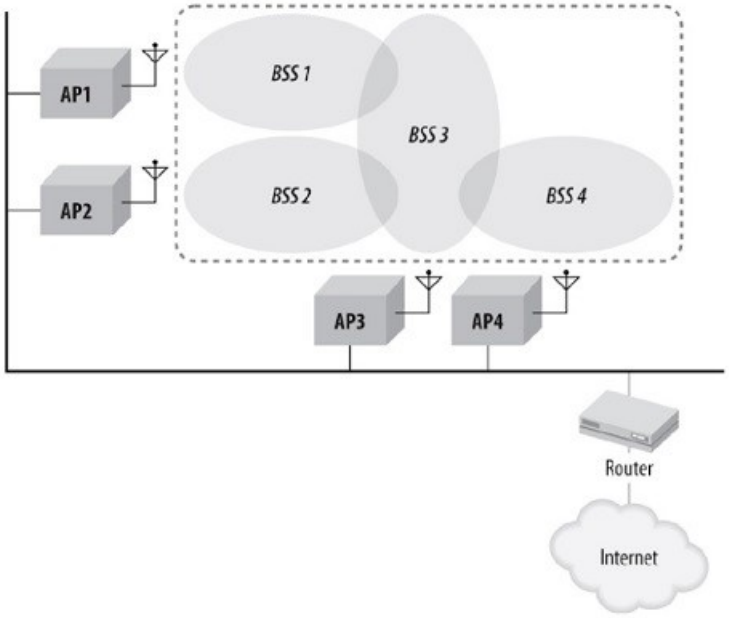
Infrastrukturní BSS (pozn. z důvodu stejného počátečního písmena nejsou nikdy infrastrukturní BSS nazývány IBSS) jsou význačné použitím přístupového nebo přístupových bodů. Přístupové body se používají pro veškerou komunikaci v infrastrukturních sítích, včetně mobilních uzlů ve stejné servisní oblasti. Pokud stanice v infrastrukturní síti potřebuje komunikovat s jinou stanicí, komunikace musí proběhnout ve dvou krocích. Nejdříve první stanice přenese rámec do přístupového bodu a následné přístupový bod přenese rámec do cílové stanice. Ačkoli tato dvou-kroková fáze přenosu rámce spotřebuje více přenosové kapacity než přímé odeslání rámce do cíle, má dvě zásadní výhody: [4] [5]

1) Infrastrukturní BSS je definován vzdáleností od přístupového bodu. Všechny stanice musí být v dosahu přístupového bodu, ale žádné restrikce, týkající se vzdálenosti mezi stanicemi, zde nejsou. Povolení přímé komunikace mezi stanicemi by sice ušetřilo přenosovou kapacitu, ale za cenu zvýšené složitosti fyzické vrstvy, protože stanice by musely udržovat „sousedské vztahy“ s ostatními stanicemi v BSA. [4] [5]
2) Přístupové body v infrastrukturních sítích jsou nápomocny mobilním stanicím, které se snaží ušetřit energii. Přístupový bod je schopen zaznamenat, když stanice vstoupí do úsporného režimu a jí určené rámce uložit do vyrovnávací paměti (bufferu). Zařízení pracující na baterie mohou bezdrátový adaptér vypnout a zapnout pouze pro přenos a příjem uložených rámců z přístupového bodu. [4] [5]

V infrastrukturní síti se musí stanice tzv. asociovat s přístupovým bodem pro získání přístupu k síťovým službám. Asociace je proces, kterým se mobilní stanice připojí k bezdrátové síti 802.11, z logiky věci lze srovnat s připojením síťového kabelu v Ethernetu. Nejedná se o symetrický proces, ale stanice vždy zahajuje asociační proces, a přístupový bod může takovou asociaci povolit nebo také zamítnout. Mobilní stanice může být v jeden okamžik asociována pouze s jedním přístupovým bodem. Množství mobilních stanic, které se mohou k přístupovému bodu připojit je dáno výrobcem přístupového bodu, reálně je však limitujícím faktorem relativně nízká propustnost bezdrátové sítě. [4] [5]

1.3.1.3 Rozšířená sada služeb

Extended service set (ESS) neboli „Rozšířená sada služeb“ poskytuje oproti BSS rozšíření resp. pokrytí větších oblastí. Protokol 802.11 umožňuje vytváření rozsáhlých bezdrátových sítí linkováním BSS v rozšířenou oblast služeb (ESS). ESS je vytvořen zřetězením více BSS



Obr. 4. ESS – Extended Service Set. [5]

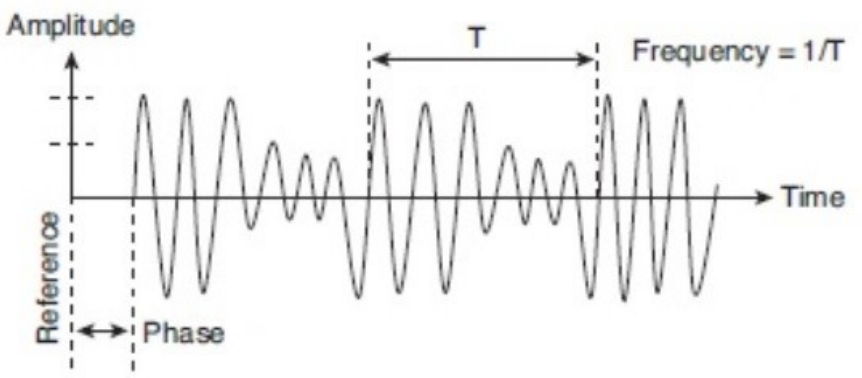
dohromady s páteřní sítí. Všechny přístupové body v ESS mají stejný identifikátor sady služeb resp. „service set identifier“, zkráceně SSID, které slouží uživatelům jako „název“ sítě. Stanice ve stejném ESS mohou komunikovat mezi sebou, i když se nachází v jiné BSA nebo se pohybují mezi různými BSA. Přístupové body fungují společně a umožňují externímu světu použít MAC adresu stanice ke komunikaci se stanicí, bez ohledu kde se v ESS nachází. Na *Obr. 4* router použije MAC adresu stanice jako cíl pro doručení rámce k mobilní stanici; pouze přístupový bod, ke kterému je mobilní stanice asociována doručí rámec. Router ignoruje umístění mobilní stanice a spoléhá se na přístupový bod, že rámec správně doručí do cíle. [4] [5]

1.3.2 Rádiová topologie

Laicky řečeno v bezdrátových sítích rádiové vlny přenášejí informace vzduchem z jednoho bodu do druhého. Při přenosu se rádiové vlny setkávají s různými překážkami, které mohou ovlivnit dosah a výkon, v závislosti na charakteristikách rádiové vlny. Navíc regulační pravidla vymezují použití a limity rádiových vln. [6]

1.3.2.1 Vlastnosti rádiových vln

Rádiová vlna je typ elektromagnetického signálu určeného k přenosu informací vzduchem na poměrně dlouhé vzdálenosti. Někdy jsou rádiové vlny označovány také jako radiofrekvenční signály (RF) z anglického „Radio Frequency“. Tyto signály oscilují velmi vysokou frekvencí, což umožňuje vlnám cestovat vzduchem, obdobě jako vlnám v oceánech. Rádiové vlny člověk využívá už mnoho let. Slouží jako prostředek např. pro přenos hudby do FM rádia a videa do televizorů. Kromě toho jsou rádiové vlny primárním prostředkem pro přenos dat po bezdrátové síti WLAN. Rádiová vlna má amplitudu, frekvenci a fázi (*Obr. 5*). [6]



Obr. 5. Rádiová vlna – amplituda, frekvence, fáze. [6]

1.3.2.2 Amplituda

Amplituda rádiové vlny indikuje její sílu. Měřítkem amplitudy je obecně výkon, jež můžeme analogicky přirovnat k množství úsilí, které musí člověk vynaložit k ujetí určité vzdálenosti na bicyklu. Obdobně, výkon ve smyslu elektromagnetických signálů představuje množství energie potřebné k přenosu signálu na určitou vzdálenost. Zvýšením výkonu se zvyšuje dosah. Rádiové vlny mají amplitudy reprezentovány jednotkou ve wattech a vyjadřují množství energie v signálu. Alternativně se používá jednotka dBm (decibel nad miliwattem) k vyjádření amplitudy rádiové vlny. Hodnota dBm vyjadřuje množství energie ve wattech vztažené k 1mW (0dBm = 1mW). Hodnoty dBm nabývají kladných hodnot nad 1mW a záporných hodnot pod 1mW. U mnoha přístupových bodů je hodnota vysílacího výkonu volitelná většinou krokově od -1dBm do 23dBm. [6]

1.3.2.3 Frekvence

Frekvence rádiové vlny je vyjádřena počtem opakování signálu za sekundu. Jednotkou frekvence je Hz (Hertz), což je počet cyklů vyskytujících se každou vteřinu. Bezdrátové sítě

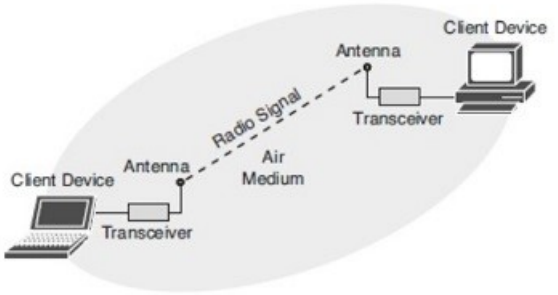
802.11 využívají rádiové vlny o frekvencích 2.4GHz a 5GHz, což znamená, že signál zahrnuje 2 400 000 000 cyklů za vteřinu resp. 5 000 000 000 cyklů za vteřinu. Signály pracující na těchto kmitočtech jsou příliš vysoké, aby je lidé mohli slyšet a příliš nízké, aby je mohli vidět. Frekvence ovlivňuje šíření rádiových vln. Teoreticky se signály s vyšší frekvencí šíří v kratším rozsahu než signály s nižší frekvencí. V praxi však může být rozsah různých frekvenčních signálů, nebo naopak signály o vyšší frekvenci se mohou šířit dál než signály s nižší frekvencí. Např. 5GHz signál přenášený při vyšším vysílacím výkonu může mít větší dosah než 2.4GHz signál vysílaný při nižším výkonu, zvláště pokud elektrický šum v oblasti ovlivňuje 5GHz část rádiového spektra méně než 2.4GHz část spektra. [6]

1.3.2.4 Fáze

Fáze rádiové vlny odpovídá vzdálenosti, odkud je signál posunut od referenčního bodu (např. určitého času nebo jiného signálu). Dle konvence je každý cyklus signálu v intervalu 360 stupňů. Např. signál může mít fázový posun o 90 stupňů, což znamená, že hodnota posunutí je jedna čtvrtina (90/360=1/4). [6]

1.3.3 Rádiové komponenty

Základní komponentou je RF systém (*Obr. 6*), který umožňuje šíření rádiových vln. Vysílač a anténa mohou být integrovány do klientského zařízení nebo mohou být externí komponen-

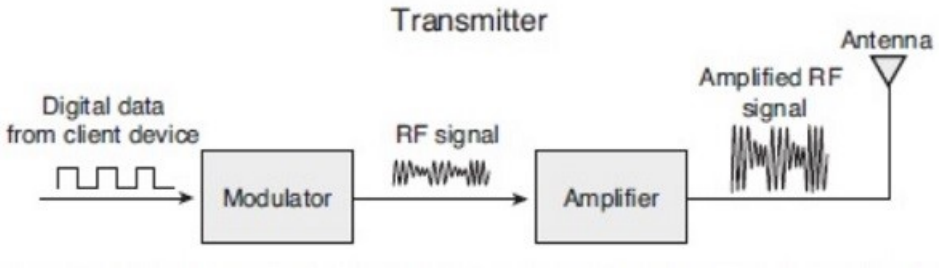


Obr. 6. RF Systém. [6]

tou. Přenosovým médiem je primárně vzduch, ale mohou zde existovat překážky, jako jsou zdi, nábytek, jiná elektronika atd. [6]

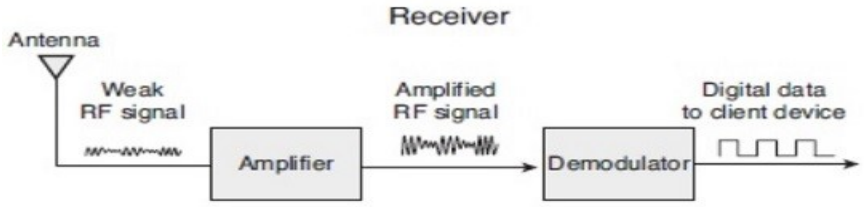
1.3.3.1 Transceiver

Klíčovou komponentou WLAN je RF transceiver, který se skládá z vysílače a přijímače. Vysílač vysílá rádiovou vlnu na jednom konci systému („zdroj“) a přijímač přijímá rádiovou vlnu na druhé straně („cíl“) systému. RF vysílač neboli transceiver se obecně skládá z hardwaru, který je součástí bezdrátového klientského rádiového zařízení, také označovaného jako klientský adaptér nebo karta. *Obr. 8* zobrazuje základní součásti vysílače. Proces známý jako modulace převádí elektrické digitální signály, které představují informace (datové bity, resp. 0 a 1) uvnitř počítače do rádiových vln s požadovanou frekvencí, které se šíří vzdušným médiem. Podrobněji bude modulace zmíněna v následujícím odstavci. Zesilovač zvětšuje amplitudu signálu rádiové vlny na požadovaný vysílací výkon před tím, než je přiveden do antény a dále šířen přes přenosové médium (sestává se ze vzduchu a různých překážek). Na



Obr. 8. Vysílač obsahuje modulátor, zesilovač a anténu. [6]

cílovém místě přijímač (*Obr. 7*) detekuje poměrně slabý RF signál a demoduluje jej do typů dat příslušících cílovému počítači. Rádiová vlna v přijímači musí mít amplitudu, která je nad minimální hladinou citlivosti přijímače, v opačném případě nebude přijímač schopen signál interpretovat, případně jej dekódovat. Minimální citlivost přijímače závisí na rychlosti přenosu dat. Předpokládejme například, že citlivost přijímače přístupového bodu je -68dBm pro 300 Mbps (802.11n) a -89dBm pro 1 Mbps (802.11b). Amplituda rádiové vlny na přijímači tohoto přístupového bodu musí být vyšší než -68dBm při rychlosti 300 Mbps nebo vyšší než -89dBm při rychlosti 1 Mbps dříve, než bude přijímač schopen dekódovat signál. [6]



Obr. 7. Přijímač obsahuje anténu, zesilovač a demodulátor. [6]

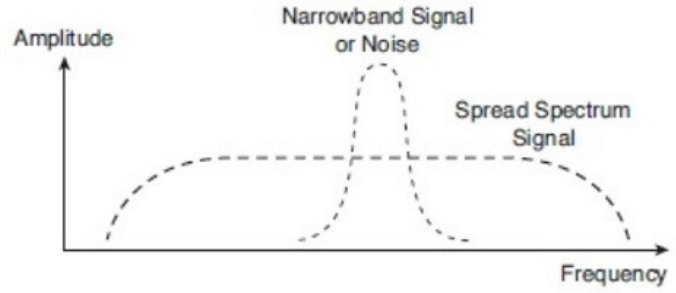
1.3.3.2 Modulace

RF modulace transformuje digitální data, například binární 0 a 1 představující emailovou zprávu z datové sítě do RF signálu vhodného pro přenos vzduchem. To zahrnuje převedení digitálního signálu představujícího data do analogového signálu. V rámci tohoto procesu modulace překrývá digitální datový signál nosným signálem, rádiovou vlnou se specifickou frekvencí. Modulace je nezbytná z důvodu nepraktičnosti přenášet data v jejich nativní podobě. Řekněme například, že Karel chce vyslat svůj hlas bezdrátově z Prahy do Brna, což je asi 200km. Jedním z přístupů je, aby Karel využil skutečně vysoce výkonný systém zesilovače zvuku, aby zvýšil hlas tak, aby byl slyšet v rozsahu 200km. Problémem s tímto přístupem je pravděpodobnost, že všichni v Praze a širokém okolí ohluchnou z důvodu velmi vysoké hlasitosti. Mnohem lepším přístupem je modulovat Karlovo hlas rádiovým nebo světelným nosným signálem, který je mimo dosah lidského sluchu a vhodný pro šíření vzduchem. Datový signál může měnit amplitudu, frekvenci nebo fázi nosného signálu a zesílení nosného signálu nebude omezovat člověka, protože bude mimo rozsah lidského sluchu. To je přesně to, co dělá modulace. Modulátor smíchává zdrojový datový signál s nosným signálem. Vysílač navíc spojuje modulované a zesílené signály s anténou, která je určena k přechodu signálu do vzduchu. Modulovaný signál následně opustí anténu a šíří se vzduchem. Anténa přijímací stanice spojí modulovaný signál s demodulátorem, který derivuje datový signál ze signálu nosného. Kromě amplitudové (ASK), frekvenční (FSK), fázové (PSK) modulace se dnes využívá nejvíce kvadraturní amplitudová modulace (QAM), která mění amplitudu zároveň s fází. Výhodou QAM je schopnost reprezentovat velké skupiny bitů jako jednu kombinaci amplitudy a fáze. Ve skutečnosti např. některé systémy založené na QAM využívají 64 různých fázových a amplitudových kombinací, což vede k reprezentaci 6 datových bitů na jeden symbol. Víceúrovňové kombinace fáze a amplitudy v QAM umožňuje standardům jako 802.11n a 802.11ac podporovat vyšší přenosové rychlosti. [6]

1.3.3.3 Rozprostřené spektrum

Po modulaci digitálního signálu do analogového nosného signálu pomocí FSK, PSK nebo QAM některé WLAN vysílače rozprostírají modulovaný nosný signál přes širší spektrum, tak aby splňovala regulační nařízení. Tento proces, nazývaný rozprostřené spektrum, významně snižuje možnost vnějšího a vnitřního rušení. V důsledku toho regulační orgány obecně nevyžadují, aby uživatelé rozprostřeného spektra vlastnili licenci. Rozprostřené spektrum (*Obr. 9*), původně vyvinuté pro armádní účely, rozprostírá sílu signálu skrze široký

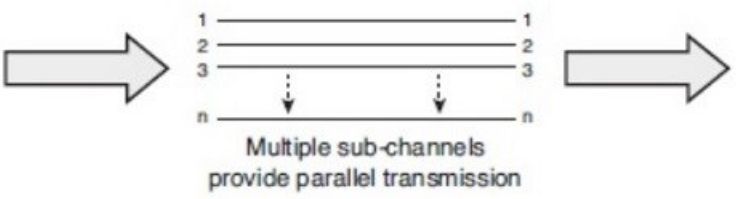
pás frekvencí. Rádiové komponenty rozprostřeného spektra používají modulační techniku přímého rozprostřeného spektra (DSSS) nebo modulační techniku přeskakování mezi frekvencemi (FHSS). [6]



Obr. 9. Rozprostřené spektrum. [6]

1.3.3.4 Ortogonální multiplex s frekvenčním dělením

Namísto využití rozprostřeného spektra, vysokorychlostní bezdrátové sítě WLAN využívají „Ortogonální multiplex s frekvenčním dělením“ (OFDM), což je technika širokopásmové modulace, která využívá frekvenční dělení kanálu. OFDM rozděluje signál modulovaný pomocí FSK, PSK a QAM na více subnosných signálů obsazujících určitý kanál. OFDM je



Obr. 10. OFDM. [6]

mimořádně efektivní a umožňuje tak poskytovat vyšší přenosové rychlosti. OFDM se využívá již delší dobu, podporuje globální standard pro asymetrickou digitální účastnickou linku (ADSL) a vysokorychlostní kabelový telefonní standard. [6]

1.4 Shrnutí

První kapitola pojednává o historii Wi-Fi, důvodu a potřebě jejího vzniku. Seznámili jsme se se sadou standardů IEEE 802.11 pro bezdrátovou lokální síť pro veřejná frekvenční pásma 2,4GHz a 5GHz. Další odstavec je věnován technologii Wi-Fi a jejím součástem. Následně je detailněji rozebrána síťová a rádiová topologie Wi-Fi.

2 ZABEZPEČENÍ WI-FI

Specifická opatření musí být přijata k udržení bezpečnosti v bezdrátové síti. Nicméně, ne každý přístup k zabezpečení funguje ve všech prostředích a různých situacích. Optimální řešení pro danou síť je závislé na mnoha faktorech např. požadované výši zabezpečení, velikosti sítě, zda je požadován přístup pro externí uživatele atp. Zabezpečení WLAN je zajištěno dvěma procesy: autentizací (authentication) a šifrováním (encryption). Ověření resp. autentizace je zde vnímáno jako verifikace autorizace stanice ke komunikaci s jinou stanicí. V infrastrukturním módu probíhá autentizace mezi AP a každou stanicí. Autentizace je nezbytnou podmínkou pro asociaci. Asociace je zřízení komunikačních služeb mezi AP a stanicí a mapování stanice do přístupovému bodu, aby mobilní uzel získal přístup do drátové sítě. Autentizace může být ve formě „Otevřeného systému“ (Open System) nebo „Sdíleného klíče“ (Shared Key). V Otevřeném systému může být jakékoliv žádající stanici uděleno ověření. Úspěch však není zaručen. Stanice, která žádost přijímá, může žádost o ověření odmítnout. V systému Sdíleného klíče pouze stanice, které znají sdílený klíč, mohou být autentizovány. Samozřejmě přenos Sdíleného klíče by mohl vést k jeho odposlechu neoprávněnými uživateli. Je tedy zašifrován ještě před vlastním šifrováním. [7]

2.1 Identifikátor sady služeb

SSID je zkratka pro identifikátor sady služeb. Laicky řečeno, SSID je název sítě Wi-Fi. Lidé se obvykle setkávají s SSID, když používají mobilní zařízení vybavené Wi-Fi adaptérem pro připojení k bezdrátové síti. Pokud na mobilním zařízení zapneme Wi-Fi adaptér, a pokusíme se připojit k bezdrátové síti, na obrazovce se zobrazí seznam SSID – to jsou názvy všech sítí, které jsou v dosahu mobilního zařízení resp. Wi-Fi adaptéru. [7] [8]

Obr. 11. SSID (zdroj: https://sfgov.org).

2.1.1 Nastavení SSID

SSID mohou mít délku až 32 alfanumerických znaků. Jsou také citlivé na velikost písmen; „MRACEK“ je jiná síť než „mracek“. Mnoho výrobců bezdrátových routerů nastavili zařízení tak, aby ve výchozím nastavení používali obecný název (často značka a model routeru nebo access pointu). Základním bezpečnostním pravidlem je změna výchozího názvu SSID a hesla. Toto základní zabezpečení znesnadní potenciální proniknutí do sítě a také snižuje pravděpodobnost, že dvě různé bezdrátové sítě se stejným SSID budou mezi sebou v dosahu. Nastavení SSID se provádí změnou v konfiguraci bezdrátového zařízení, přístupné většinou přes příkazovou řádku, webové rozhraní či softwarový konfigurátor. [7] [8]

2.1.2 Standardizace SSID

Standardy protokolu IEEE 802.11 určují, že SSID bude připojen k hlavičce paketů odeslaných přes lokální bezdrátovou síť (WLAN). To pomáhá zajistit, aby byla data přenášena do správné sítě a ze správné sítě. SSID odlišuje jednu WLAN od jiné, takže všechny přístupové body a všechna zařízení pokoušející se o připojení ke konkrétní síti WLAN musí používat stejné SSID, aby umožnily efektivní roaming. Jako součást procesu asociace musí mít bezdrátový adaptér stejné SSID jako přístupový bod, nebo nebude povoleno připojit se k základní sadě služeb (BSS). [7] [8]

2.1.3 Bezpečnost SSID

SSID je nutným základem pro „bezpečnou“ bezdrátovou síť, ale samo o sobě bezdrátovou síť bezpečnější neudělá. SSID může být zachyceno z paketu v textové podobě a většina přístupových bodů vysílá SSID několikrát za vteřinu uvnitř řídícího rámce („beacon frame“). Hacker tak může snadno identifikovat SSID pomocí nástroje pro analýzu 802.11. Někteří síťový administrátoři vypínají vysílání SSID ve snaze „skrýt“ síť, toto „zabezpečení“ však může mít zcela opačný důsledek, např. ve zvýšeném zájmu o napadení sítě. Administrátoři mohou přístupovému bodu přiřadit více než jedno SSID. Použití více SSID umožňuje uživatelům přístup k různým sítím, každý s různými bezpečnostními politikami a funkcemi (např. přístup pro zaměstnance a přístup pro hosty). [7] [8]

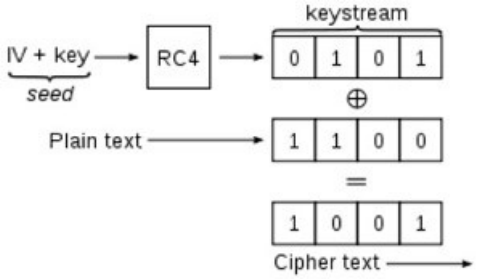
2.2 Filtrování MAC adres

Většina bezdrátových routerů a jiných přístupových bodů zahrnuje volitelnou funkcionalitu nazvanou filtrování MAC adres resp. filtrování hardwarových adres. Jedná se tedy o další

prvek zabezpečení ve smyslu omezení zařízení, která se mohou připojit k síti. Vzhledem k tomu, že MAC adresy mohou být falešné (podvržené), tak i přes tento fakt, je použití filtrování hardwarových adres jako další stupeň zabezpečení doporučeno. V typické bezdrátové síti se může jakékoli zařízení, která má příslušná pověření (zná SSID a heslo), ověřit pomocí směrovače a připojit se k síti, získat adresu IP a přístup např. k Internetu a jiným sdíleným prostředkům. Filtrování MAC adres přidává do tohoto procesu další vrstvu. Ještě předtím, než se zařízení připojí k síti, router zkontroluje adresu MAC zařízení podle interního seznamu schválených adres. Pokud se MAC adresa klienta shoduje s MAC adresou uvedenou v seznamu povolených MAC adres routeru, je přístup povolen; v opačném případě je zablokován. [8] [9]

2.3 Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) byl vyvinut pro bezdrátové sítě a schválen jako bezpečnostní standard Wi-Fi v září 1999. Wired Equivalent Privacy je doslovně: soukromí ekvivalentní drátovým sítím, bezpečnostní protokol pro bezdrátové lokální sítě (WLAN) definovaný ve standardu 802.11b. WEP je navržen tak, aby poskytoval stejnou úroveň zabezpečení jako kabelové sítě LAN. Sítě LAN jsou však ze své podstaty bezpečnější než sítě WLAN, protože sítě LAN jsou chráněny fyzickými vlastnostmi své struktury, které mají některé nebo všechny části sítě uvnitř budovy, kterou lze chránit před neoprávněným přístupem. WLAN, které jsou přes rádiové vlny, nemají stejnou fyzickou strukturu, a proto jsou zranitelnější. WEP si klade za cíl zajistit bezpečnost šifrováním dat přenášených přes rádiové vlny, tak aby byla chráněna při přenosu z jednoho koncového bodu k druhému. Bylo však zjištěno, že WEP není tak bezpečný, jak se dříve předpokládalo. WEP se používá ve dvou nejnižších vrstvách OSI modelu – datového spoje a fyzických vrstev; nenabízí proto komplexní zabezpečení. Crackeři přišli na to, jak WEP prolomit, jednoduše pomocí volně dostupných nástrojů. V roce 2004 Wi-Fi aliance oficiálně opustila WEP jako šifrovací standard. [8] [9]



Obr. 12. Základní WEP šifrování. [8]

2.4 Wi-Fi Protected Access

WPA je zkratkou pro Wi-Fi Protected Access doslovně: chráněný přístup k Wi-Fi a je bezpečnostní technologií pro sítě Wi-Fi. Byla vyvinuta v reakci na slabé stránky protokolu WEP a proto zlepšuje funkce ověřování a šifrování protokolu WEP. WPA poskytuje silnější šifrování pomocí jedné ze dvou standardních technologií: Temporal Key Integrity Protocol (TKIP) a Advanced Encryption Standard (AES). WPA také obsahuje vestavěnou podporu autentizace, kterou WEP nenabízí. 128bitový TKIP, který dynamicky vytváří nový klíč pro každý datový paket; WEP měl pouze menší 40bitový šifrovací klíč, který byl statický a musel být ručně zadáván na bezdrátových přístupových bodech (AP). TKIP byl navržen, aby fungoval i se staršími zařízeními podporujícími WEP s aktualizovaným firmwarem. [9] [10]

2.4.1 WPA-Personal

Neboli také WPA-Osobní je varianta WPA, určená pro použití v domácích sítích, se nazývá také WPA Pre Shared Key nebo WPA-PSK. U WPA-PSK, podobně jako u WEP, je nastaven statický klíč nebo heslo, ale používá se šifrovací protokol TKIP. WPA-PSK automaticky mění klíče v přednastaveném časovém intervalu, a je tak obtížnější pro potenciálního útočníka je odhalit a využít. [9] [10]

Obr. 13. Zabezpečení WPA-Personal. [10]

2.4.2 WPA-Enterprise

Neboli též WPA-Podnikové je varianta bezpečnostního bezdrátového mechanismu určeného pro malé až velké podnikové bezdrátové sítě. Jedná se o vylepšení bezpečnostního protokolu WPA s pokročilým ověřováním a šifrováním. WPA-Enterprise funguje obdobně jako WPA-Personal (WPA-PSK), ale vyžaduje, aby se každý uživatel sám autentizoval prostřednictvím např. serveru RADIUS. WPA-Enterprise funguje přiřazením dlouhého šifrovacího klíče každému připojenému zařízení. Tento klíč, který je sdílen s uživateli, není viditelný a automaticky se průběžně mění. Server RADIUS používá protokol IEEE 802.1x, ve kterém jsou

uživatelé ověřováni na základě jména a hesla, digitálních certifikátů, biometrických údajů atp. WPA-Enterprise využívá především šifrovací mechanismus AES, ale také podporuje protokol TKIP. [9] [10]

2.5 Wi-Fi Protected Access II

WPA a WPA2 jsou souběžné bezpečnostní standardy. WPA adresuje většinu z IEEE 802.11i standardu; certifikace WPA2 dosáhla plného souladu. Nicméně WPA2 nebude fungovat s některými staršími síťovými kartami, proto byla zachována souběžnost obou standardů. V dnešní době je doporučeno použít k zabezpečení Wi-Fi pouze standardu WPA2. Nejdůležitějším vylepšením WPA2 oproti WPA bylo použití pokročilého šifrovacího mechanismu využívající protokol „Counter Mode/CBC-MAC Protocol“ (CCMP) nazývaného „Advanced Encryption Standard“ (AES). Existují také dvě verze, stejně jako u WPA, Osobní (Personal) a Podnikové (Enterprise). Obě používají silnou šifrovací metodu AES-CCMP pro šifrování dat přenášených vzduchem. Hlavní rozdíl mezi těmito režimy zabezpečení je ve fázi ověřování. WPA2 Enterprise používá protokol 802.1x na úrovni podniku. WPA2 Personal používá předem sdílené klíče (PSK) a je určen pro domácí použití. WPA2 Enterprise byl navržen jako nejbezpečnější pro použití i ve velkých organizacích. [9] [10]

2.5.1 WPA2-Personal

V angličtině WPA2-Personal nebo WPA2-PSK. Jedná se o metodu zabezpečení předem sdíleného klíče (PSK), která byla navržena pro domácí použití bez využití podnikového autentizačního serveru (RADIUS). Heslová fráze pro WPA2-PSK může mít až 63 znaků. Šifrování WPA2-PSK zabezpečuje TKIP nebo CCMP-AES. Existuje pouze několik situací, ve kterých by mohl být WPA2-PSK nasazen. Prvním je případ, kdy síť má pouze několik zařízení, z nichž všechny jsou důvěryhodné, např. domácnost nebo malá kancelář. Dále jako možnost jak omezit příležitostným uživatelům přístup k otevřené síti, pokud není možno nasadit tzv. captive portál, např. internetová kavárna nebo síť pro hosty. Případně jako alternativní síť pro zařízení, která nejsou kompatibilní s 802.1x, jako např. herní konzole. [9] [10]

2.5.2 WPA2-Enterprise

WPA2-Enterprise je dostupné již od roku 2004 a je označován jako současný standard zabezpečení bezdrátových sítí. Nasazení WPA2-Enterprise vyžaduje server RADIUS, který zpracovává úlohu ověřování přístupu. Vlastní proces ověřování je založen na politice protokolu 802.1x a je poskytován v několika různých systémech označených EAP (Extensible

Authentication Protocol). Protože je každé zařízení před připojením ověřeno, je mezi zařízením a sítí efektivně vytvořen privátní tunel. To je důvodem, proč je WPA2-Enterpise označován také jako zabezpečené bezdrátové připojení. Další výhodou 802.1x je možnost nastavit sítě VLAN, která sdružují bezdrátová zařízení, jako by byla v osobní síti LAN. To může usnadnit správu politik a může optimalizovat síťový provoz. Ovšem WPA2-PSK i WPA2-Enterprise bezpečnostní standard má své slabiny a potenciální útočníci jich dokázali využít např. „KRACK attack“, bylo nutné vytvořit ještě bezpečnější mechanismus a tím je dnes WPA3. Veškerá moderní zařízení certifikovaná na Wi-Fi 6 podporují WPA3. [10] [11]

2.6 Wi-Fi Protected Access III

Wi-Fi Aliance v roce 2018 oznámila nový standard v bezdrátové síti, který se nazývá „Wi-Fi Certified WPA3“. WPA3 je navržen jako nástupce široce používaného WPA2 a přináší řadu základních vylepšení, která zlepšují ochranu zabezpečení a postupy integrace v rámci osobních, veřejných a podnikových sítí. WPA3 nahrazuje kryptografické protokoly náchylné k off-line analýze protokoly, které vyžadují interakci s infrastrukturou pro každé odhadované heslo, takže infrastruktura může časově omezit počet odhadů. Integrita dat je implementována použitím algoritmu SHA2, ve kterém jsou generovány různé hashovací funkce pro různé vstupy. To znamená, že nový WPA3-CNSA (EAP-TLS) využívá šifrovací sady Suite-B TLS a zároveň zavádí 192bitové zabezpečení, které se používá v kritických armádních, obranných a obdobných aplikacích. Tyto šifrovací sady kombinují všechny různé možnosti – režim šifrování, algoritmus hash, výměnu klíčů, metodu ověřování – do jednoho balíku, který zajišťuje konzistentní zabezpečení pro každé připojení uživatele. Stejně jako u WPA a WPA2 existují dva režimy zabezpečení WPA3-Osobní (Personal) a WPA3-Podnikové (Enterprise). Hlavní rozdíl mezi těmito dvěma režimy zabezpečení je ve fázi ověřování. [12]

2.6.1 Opportunistic Wireless Encryption

Z anglického „Opportunistic Wireless Encryption“ (OWE) je funkce ve WPA3, která nahrazuje „Open“ autentizaci, která je široce používána v hotspotech a veřejných bezdrátových sítích. Klíčovou myšlenkou je použití mechanismu pro bezpečnou výměnu klíčů pro šifrování veškeré komunikace mezi zařízením (klientem) a přístupovým bodem. Dešifrovací klíč pro komunikaci je odlišný pro každého klienta připojujícího se k přístupovému bodu. Žádné

FEATURES	WPA2	WPA3
STANDS FOR	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
WHAT IS IT?	Security protocol developed by the Wi-Fi Alliance for use in securing wireless networks.	Next generation of WPA2 and has better security features.
RELEASE YEAR	2004	2018
ENCRYPTION	WPA2 uses the Advanced Encryption Standard (AES) with CCMP standard.	AES-GCM encryption & Elliptical Curve Cryptography of CNSA Suit B.
SESSION KEY SIZE	128-bit	192-bit
HANDSHAKE PROTOCOL	Pre-Shared Key (PSK) exchange protocol.	Uses the Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange, with Forward Secrecy feature.
SECURITY MODES	WPA2 Personal: Pre-shared Keys (PSK) WPA2 Enterprise: IEEE 802.1X (Radius)	WPA3 Personal: 128-bit SAE (Optional 192-bit) WPA3 Enterprise: 192-bit SAE
AUTHENTICATION	Uses 802.11x Open Authentication & Extensible Authentication Protocol (EAP)	Opportunistic Wireless Encryption (OWE). OWE also protects open "unsecured" networks. e.g. Wi-Fi at libraries or cafes.
DATA INTEGRITY	CBC-MAC having 64-bit Message Integrity Code (MIC)	Secure Hash Algorithm-2 for each input.
WIRELESS CONNECTION PROTOCOL	Wi-Fi Protected Setup (WPS) – Vulnerable	Wi-Fi Easy Connect using Device Provisioning Protocol (DPP) – Secure.
PROTECTED MANAGEMENT FRAMES FOR IMPROVED RESILIENCY	Mandates support of PMF since early 2018. Older routers with unpatched firmware may not support PMF.	WPA3 mandates use of Protected Management Frames (PMF).
VULNERABLE TO KRACK ATTACKS	Yes.	No, due to SAE key exchange.
VULNERABLE TO OFFLINE DICTIONARY ATTACKS	Yes.	Blocks authentication after a certain number of failed log-in attempts.

Obr. 14 Porovnání WPA2 s WPA3. [12]

z ostatních zařízení v síti nemůže tuto komunikaci dešifrovat. WPA3 také blokuje ověřování

po určitém počtu neúspěšných pokusů o přihlášení a tím také poskytuje ochranu proti útoku brutální silou. Velkou výhodou OWE je, že připojení k otevřené síti Wi-Fi, je přenos mezi zařízením a přístupovým bodem šifrován. WPA3 také zavádí povinné testování řetězce certifikátů a povinnou ochranu řídícího rámce, která pomáhá zabezpečit zařízení před útokem, který se maskuje jako přístupový bod. [12]

2.6.2 Simultaneous Authentication of Equals

„Simultaneous Authentication of Equals“ (SAE) je nový bezpečnostní standard, který používá nový protokol výměny klíčů, známý jako systém výměny klíčů „Dragon Fly Exchange“. WPA3 definuje nový handshake, který poskytuje robustní ochranu i v případech použití méně složitých hesel. [12]

2.6.3 Forward Secrecy

WPA3 poskytuje „Forward Secrecy“, protokol, který je navržen tak, aby ani útočník vybavený síťovým heslem, nemohl odposlouchávat komunikaci mezi přístupovým bodem a jiným klientským zařízením. [12]

2.6.4 Easy Connect

WPA3 obsahuje funkci „Easy Connect“, která napomáhá ke zjednodušení procesu konfigurace zabezpečení pro zařízení, která mají omezenou nebo žádnou zobrazovací jednotku. Zjednodušeně např. mobilní telefon nebo tablet, může být použit ke správě všech zařízení, připojených k síti, z jednoho rozhraní. Pomocí protokolu DPP („Device Provisioning Protocol“) mohou uživatelé moci snadno připojit mini zařízení nebo IoT zařízení. DPP poskytuje těmto zařízením pověření podobné certifikátům a umožňuje důvěryhodnému zařízení zavést do sítě jiné zařízení, což se uplatní zejména v podnikových prostředích s velkým množstvím instalovaných zařízení. [12]

2.7 Shrnutí

V této kapitole jsme se seznámili s možnostmi zabezpečení bezdrátové sítě. Zabezpečení bezdrátové sítě je tedy zajištěno dvěma procesy; autentizací a šifrováním. Autentizace je mandatorní a může být ve dvou formách; Otevřený systém nebo Sdílený klíč. Základním nejnižším stupněm zabezpečení WLAN je změna názvu SSID a jeho případné skrytí. Dalším krokem může být použití filtru MAC adres. Je zmíněn dnes již nepoužívaný bezpečnostní standard WEP, a jeho nástupce WPA ve verzi WPA, WPA2, WPA3. Tyto bezpečnostní

standardy mohou být konfigurovány jako Private, určené pro domácí použití nebo malé kanceláře (tzv. SOHO) nebo jako Enterprise, určené pro firemní a komerční použití. Tak jako WEP, tak i WPA a dnes hojně využívané WPA2 mají své slabiny a budou postupně nahrazovány bezpečnějším WPA3 standardem.

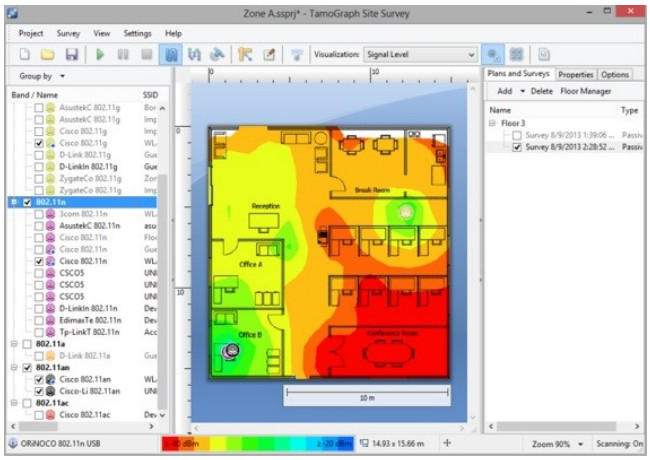
II. PRAKTICKÁ ČÁST

3 PRŮZKUM LOKALITY

Před vlastním návrhem jednotlivých komponent hotspotu je nutné zpracovat tzv. „Site Survey“ tedy průzkum lokality, resp. průzkum administrativního objektu pro nasazení a pokrytí signálem Wi-Fi. Pro tyto účely bude použit software Tamograph Site Survey a vybraný HW Wi-Fi adaptér. Na základě výsledků stávajícího stavu budou navrženy vlastní komponenty hotspotu, zejména jejich konfigurace, umístění atd. Průzkum a vlastní instalace hotspotu bude provedena v administrativním vícepodlažním objektu SouthPoint, Praha 4. Pokrytí signálem Wi-Fi je uvažováno v garáži, recepci a čtvrtém nadzemním podlaží. Jedná se o monolitickou železobetonovou konstrukci s prosklenými okenními a dveřními otvory. Vzdálenost ostatní zástavby od administrativní budovy je několik stovek metrů. V blízkém okolí se nachází jak bytová tak i komerční a veřejná zástavba. Vzdálenost těchto objektů je natolik dostačující, že by nemělo docházet ke vzájemnému rušení signálů Wi-Fi se sousedními objekty, ale stále je možné rušení od externích Wi-Fi v perimetru administrativního objektu. Ostatně detailní odpověď na tyto otázky poskytne níže provedený Site Survey.

3.1 Nástroje průzkumu

Software společnosti TamoSoft Ltd., Tamograph Site Survey, je profesionální, výkonná a uživatelsky intuitivní aplikace pro sběr a vizualizaci dat Wi-Fi. Nasazení a následná údržba bezdrátových sítí vyžaduje použití profesionálního radiofrekvenčního nástroje pro průzkum lokality, který ulehčuje jinak časově náročné a velmi složité úkoly, jako je průběžná analýza



Obr. 15. Tamograph Site Survey. [13]

a hlášení intenzity signálu, šumu a rušení, propustnosti TCP a UDP, alokace kanálů, rychlosti přenosu dat atd. Pomocí nástrojů pro Site Survey je dosaženo snížení celkového času a nákladů spojených s nasazením a údržbou bezdrátových sítí WLAN i zlepšení výkonu a

pokrytí sítě. Průzkumy jsou nezbytné, jelikož není jednoduché předvídat šíření bezdrátových vln, zvláště pak v uzavřených prostorech. Vzhledem ke všem proměnným, které mohou ovlivnit stav a výkon bezdrátové sítě je to prakticky nemožné. Měnící se podmínky, dokonce i taková drobnost, jako návštěvník s notebookem vybaveným starým bezdrátovým adaptérem, který se k hotspotu připojí, může ovlivnit výkon sítě WLAN. Kromě toho, vzhledem k širokému rozšíření bezdrátové infrastruktury, hrají velmi důležitou roli faktory jako rušení z okolních sítí WLAN. Doporučuje se provádět průzkumy lokality pravidelně nejen před, ale i po nasazení Wi-Fi sítě. [13]

3.2 Plánování průzkumů

- *Průzkum před-nasazením*: v této fázi je nutné provést průzkum na místě, aby se ověřilo, že plán sítě funguje v reálném prostředí. Umístění dočasných přístupových bodů (AP) a rychlý přehled o výsledných vlastnostech sítě WLAN umožňují projektantům jemné doladění umístění AP a antén, určit optimální počet a typy AP a vyhnout se zónám s nedostatečným pokrytím. Pomocí SW Tamograph je možné také před nasazením provést simulaci ve virtuálním prostředí. [13]
- *Průzkum po-nasazení*: po nasazení sítě WLAN je nutné provést kompletní ověření, aby bylo zajištěno, že výkon a pokrytí sítě WLAN budou splňovat požadavky návrhu. V této fázi je dokončeno umístění zařízení Wi-Fi a měl by být vygenerován report, aby bylo možné se vrátit k historickým záznamům v případě budoucí potřeby. [13]
- *Průzkum pravidelný*: udržení vysoké úrovně výkonu a pokrytí vyžaduje pravidelné průzkumy. Noví uživatelé, nové vybavení, rozšíření sítě, nové sousední sítě WLAN a další faktory mohou nepříznivě ovlivnit vaši síť WLAN. Mělo by to být pravidelně sledováno. [13]

3.3 Typy průzkumů

Tamograph poskytuje tři typy průzkumů – pasivní, aktivní a prediktivní.

- *Pasivní průzkum*: během tohoto typu průzkumu aplikace sbírá komplexní data z RF prostředí, informace o přístupových bodech (AP) a jejich charakteristikách, síla signálu, hladina šumu, rušení atd. Nazývá se pasivní, protože při tomto typu průzkumu aplikace pasivně naslouchá paketům a nepokouší se připojit k sítím WLAN. [13]

- *Aktivní průzkum*: nicméně, aby průzkum poskytl více informací o skutečném výkonu sítě WLAN, může Tamograph provádět tento typ průzkumů, během kterých se Wi-Fi adaptér připojí k bezdrátové síti (sítím) podle vlastního výběru pro změření skutečné propustnosti a několika dalších metrik. [13]
- *Prediktivní průzkum*: na rozdíl od pasivních a aktivních průzkumů se tento typ průzkumu neprovádí na místě. Jedná se o počítačovou simulaci, ve které jsou předvídány charakteristiky Wi-Fi pro model virtuálního prostředí vytvořeného uživatelem. Proces vytváření a úpravy virtuálního prostředí, výběr a umístění simulovaných přístupových bodů a analýza výsledné sítě WLAN se běžně označuje jako „RF plánování“. [13]

3.4 Spektrální analýza

Aplikace Tamograph Site Survey může provádět spektrální analýzu. Tato funkcionalita je dostupná pouze při použití speciálního HW vybavení (např. Wi-Spy dBx) určeného pro poslech a analýzu frekvenčních pásem zařízení Wi-Fi. Tato nelicencovaná veřejná frekvenční pásma jsou často sdílena s ostatními „ne-Wi-Fi“ zdroji RF signálu, například bezdrátové kamery, mikrovlnné trouby nebo bezdrátové telefony, které způsobují rušení. Účelem spek-

Obr. 16. Wi-Spy dBx. [13]

trální analýzy je detekovat a identifikovat takové zdroje rušení, eliminovat je a identifikovat kanály WLAN s minimálním rušením. Tamograph může provádět spektrální analýzu současně s pasivními průzkumy propojením s Wi-Spy, USB spektrálním analyzátorem od společnosti MetaGeek. Když je Wi-Spy zapojen, zobrazí se na centrálním panelu hlavní obrazovky TamoGraphu obraz živého spektra. Po provedení průzkumu, shromážděná data mohou být vložena do výstupních sestav ve formátu PDF nebo HTML. [13]

3.5 USB Wi-Fi adaptér

Pro účely provádění průzkumu softwarem Tamograph bude použit USB Wi-Fi adaptér Zyxel NWD6605, který podporuje teoretickou rychlost až 300Mbps pro 2.4GHz a 867Mbps pro 5GHz pásmo. Adaptér je dodáván se dvěma anténami, které umožňují poskytovat širší po-

Obr. 17. Zyxel NWD 6605. [14]

krytí a lepší bezdrátový výkon. Seznam doporučených USB Wi-Fi adaptérů pro provádění Site Survey se softwarem Tamograph lze dohledat na stránkách společnosti Tamos Ltd.

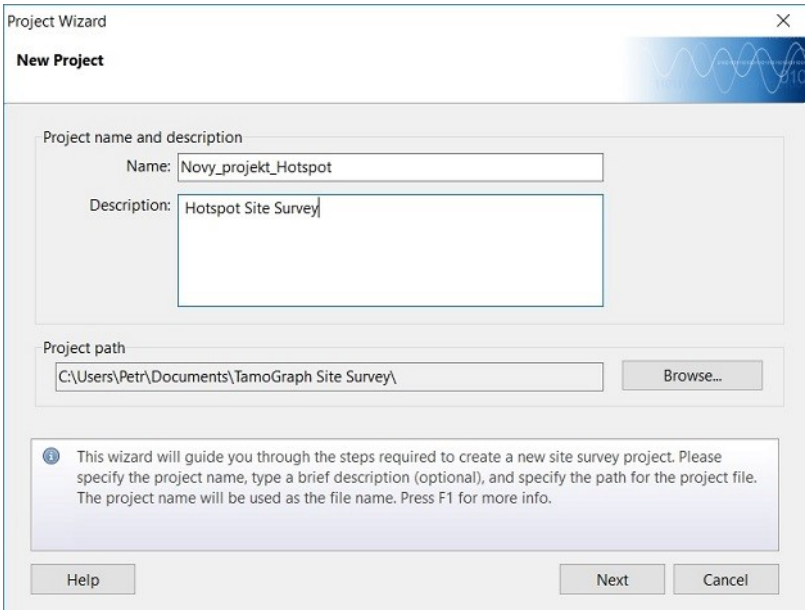
3.6 Prediktivní průzkum lokality

Prediktivní průzkum lokality je „virtuální prohlídka“ objektu nebo prostoru, který využívá příslušné informace o lokalitě pro plánování bezdrátové sítě. Obvykle to znamená, že půdorysy lokalit jsou načteny do příslušného softwaru pro prediktivní průzkum místa, aby se vytvořil návrh bezdrátové sítě. Nástroje pro prediktivní průzkum berou v úvahu stavební materiály, metry čtvereční, počet předpokládaných uživatelů, typy antén a aplikací a další proměnné, aby poskytly spolehlivý prediktivní bezdrátový plán pro danou lokalitu. Prediktivní průzkumy jsou efektivnější při předvídání přiřazení kanálů, nastavení výkonu a umístění přístupových bodů než fyzický průzkum.

3.6.1 Instalace softwarového nástroje

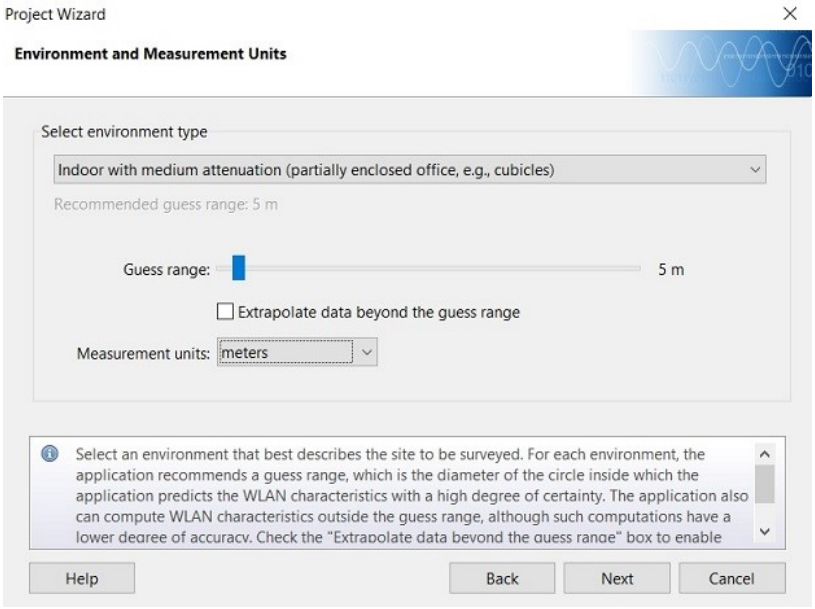
Software je ke stažení ze stránek společnosti TamoSoft (není v české lokalizaci) pro evaluační účely zcela zdarma, pro komerční využití je nutné zakoupit licenci. Po stažení instalačního archivu (tč. verze 6) do počítače se vlastní instalace provede spuštěním souboru

setup.exe. Software je kompatibilní s operačními systémy Windows nebo MacOS. V závěrečné fázi instalace softwaru je nutné nainstalovat specifický ovladač pro nalezený kompatibilní Wi-Fi adaptér. Tímto je instalace ukončena. Po spuštění aplikace je prvním nutným krokem vytvoření nového projektu a nahrání půdorysů zkoumané lokality. V hlavním menu



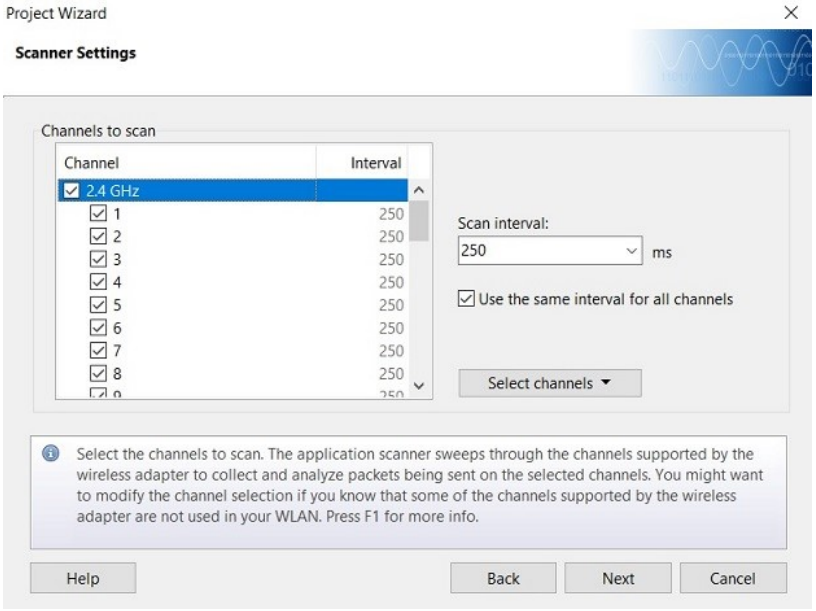
Obr. 18 Vytvoření nového projektu.

aplikace se vybere „New Project“, v prvním okně je možné zadat název projektu, popis a vybrat cestu kam bude projekt v počítači uložen. V následujícím okně po kliknutí na tlačítko



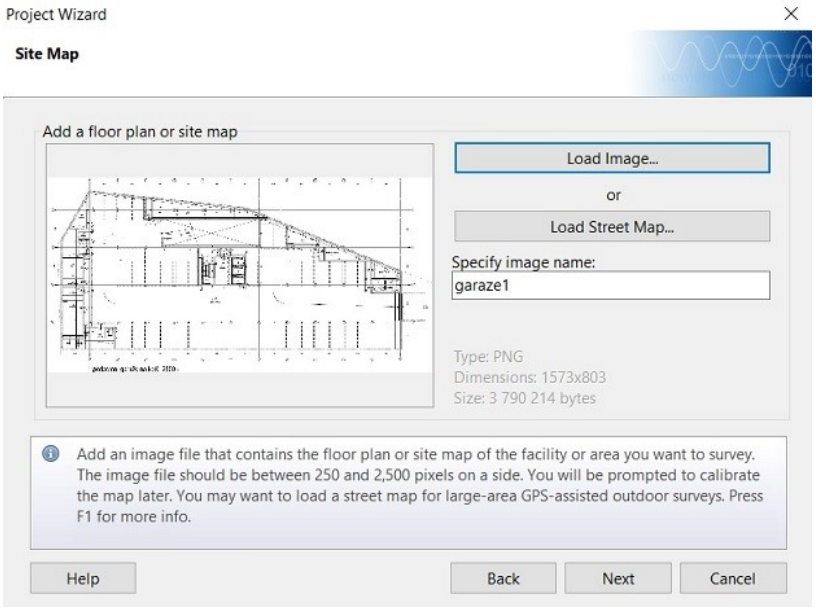
Obr. 19. Výběr typu prostředí.

„Next“ je nutné zvolit typ prostředí a měrné jednotky. Ve třetím kroku tvorby nového projektu se zvolí kanály pro skenování pro analýzu paketů. Po kliknutí na rozbalovací menu „Se-



Obr. 20. Volba kanálů.

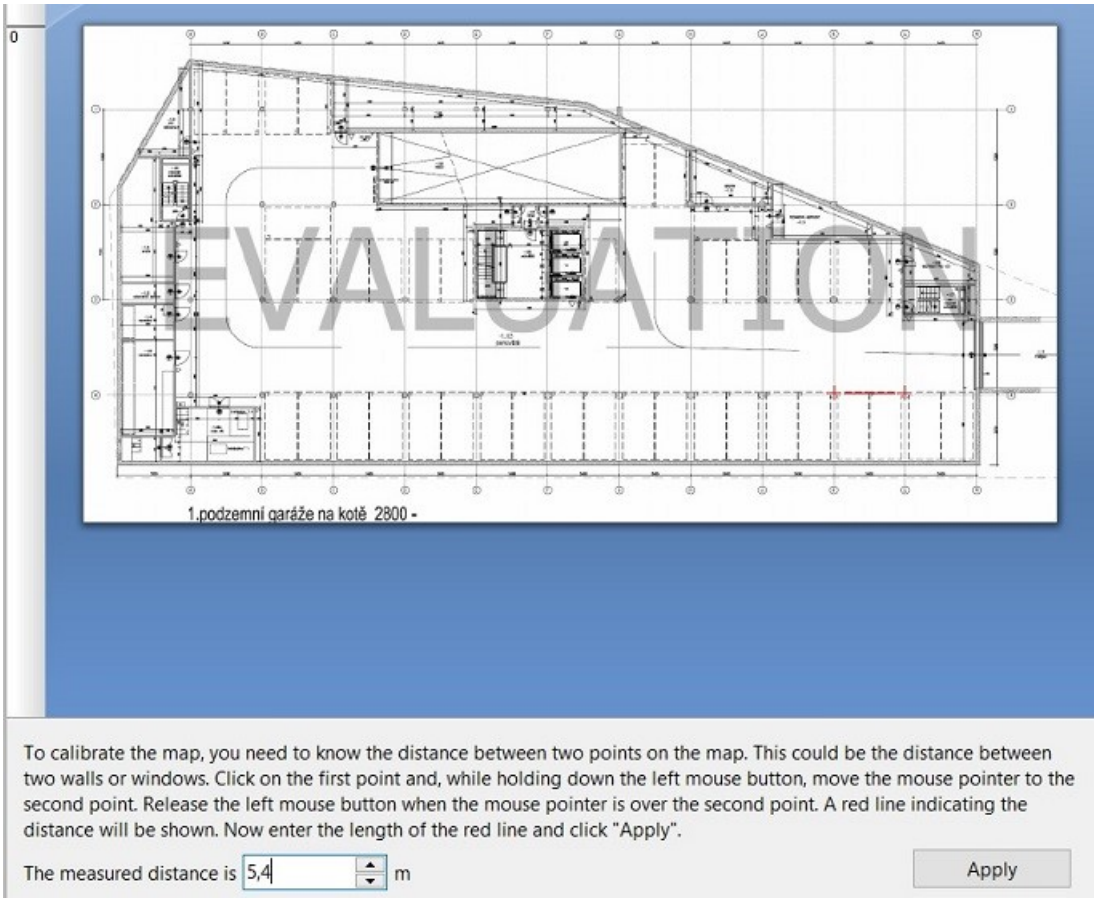
lect channels“ je možno zvolit přímo kanály pro Evropu. V předposledním kroku se nahraje půdorys lokality za souboru, podporovány jsou formáty jako jpg, bmp, pdf, dwg a další.



Obr. 21. Nahrání půdorysu.

V posledním kroku průvodce novým projektem je nutné provést kalibraci, kdy se uživatelsky definovaná vzdálenost v půdorysu promítne do skutečné vzdálenosti. Pro kalibraci je nutno

znát alespoň nějakou vzdálenost mezi dvěma body na mapě. To může být například vzdálenost mezi dveřmi, okny, zdmi atp. Tímto je průvodce ukončen a nový projekt pojmenovaný



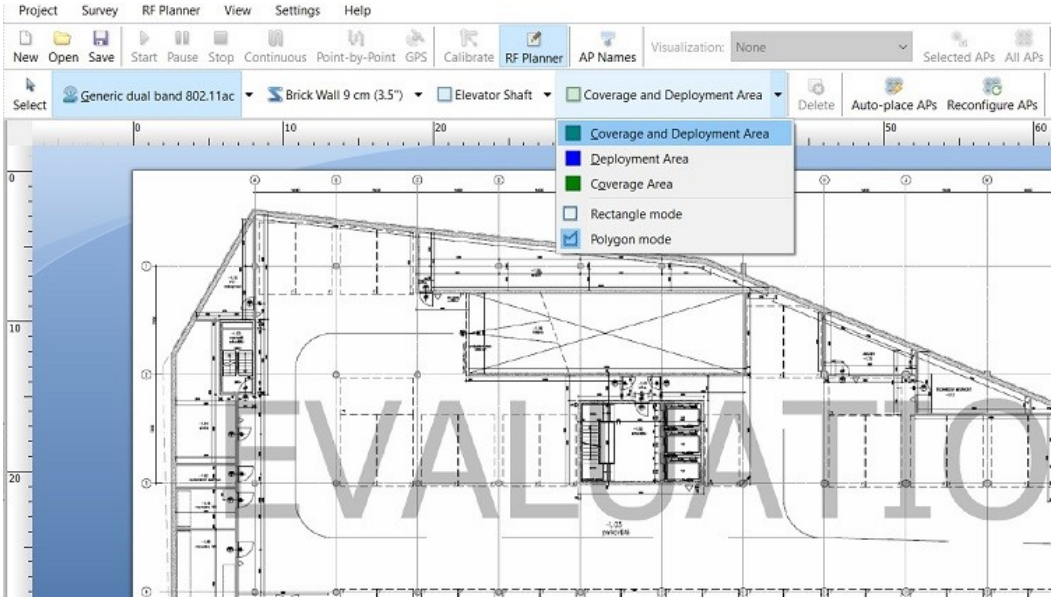
Obr. 22. Kalibrace mapy.

např. „Projekt Hotspotu“ je vytvořen, do projektu je dále možné přidávat další patra a jejich půdorysy, pokud se jedná o vícepatrový projekt resp. objekt.

3.6.2 Provedení prediktivního průzkum

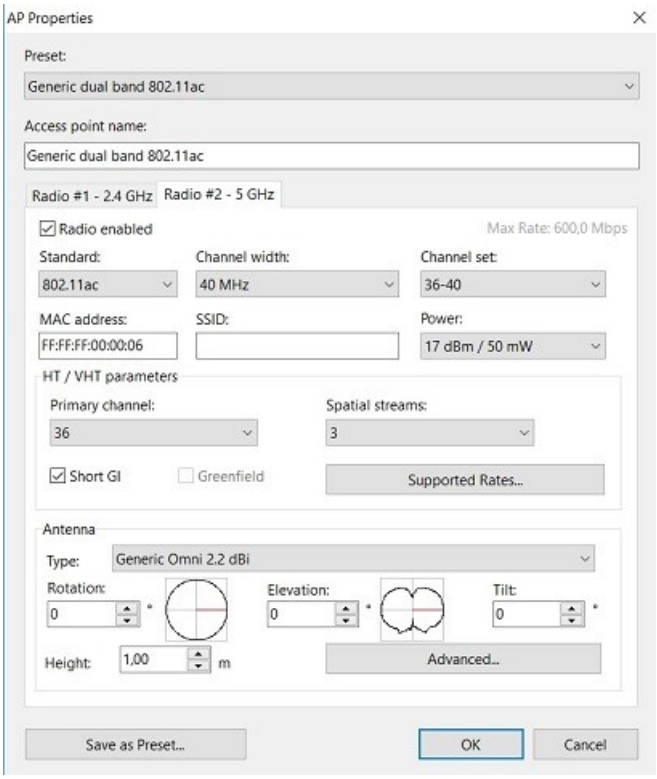
Prediktivní průzkum je překvapivě velmi přesný, když jsou použity co nejpřesnější hodnoty. V průběhu prediktivního průzkumu lokality je doporučováno navrhnout nastavení přístupových bodů na 50%, aby bylo možné další úpravy provádět přímo na místě. To umožňuje zvýšit nebo naopak i snížit sílu signálu v případě potřeby při instalaci v reálném prostředí. V aplikaci Tamograph Site Survey se prediktivní průzkum nachází pod tlačítkem „RF Planner“. Po kliknutí na tlačítko „RF Planner“ je zpřístupněna programová lišta s nabídkou vlastností konstrukce v nahraném půdorysu. Do půdorysu se pomocí vybraných materiálů zanesou typy zdí a příček, oken, dveří, stropu. Následně se do půdorysu vyznačí oblast pokrytí, tedy oblast kde je požadováno pokrytí signálem Wi-Fi. Je zde i možnost definovat oblast nasazení resp. instalace, oblast kde je uvažována fyzická montáž přístupových bodů. Finálně

pak klikneme na tlačítko „Auto-place APs“, kdy před vygenerováním virtuálních přístupových bodů můžeme definovat jejich vlastnosti a omezit jejich počet, následně dojde k auto-



Obr. 23. RF plánovač.

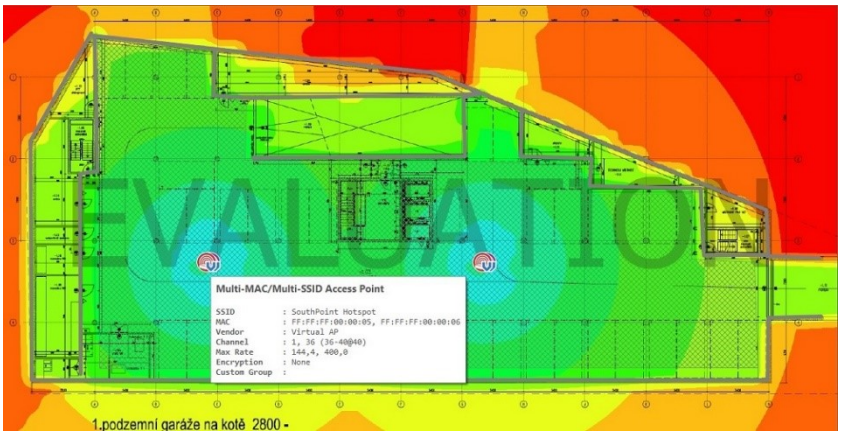
matickému vygenerování a rozmístění přístupových bodů. Pokud výsledek nesplňuje očekávání, je možné upravit hodnoty přístupových bodů, jejich vlastnosti, jako výkon, vysílací kanál, počet AP nebo vlastnosti antény atd. Na dalších obrázcích je výstup prediktivního



Obr. 24. Vlastnosti AP.

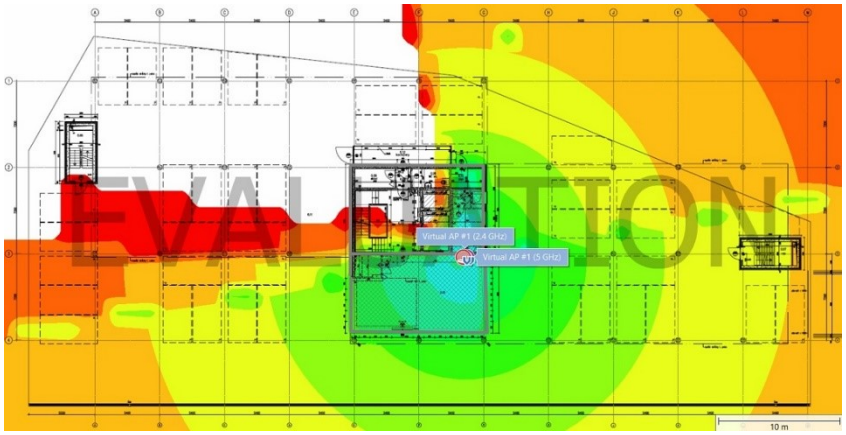
průzkumu pro jednotlivé lokality hotspotu s navrženými přístupovými body a jejich navržené umístění v objektu.

- Prediktivní průzkum: Hotspot Southpoint, lokalita „Garáže -1“



Obr. 25. Prediktivní průzkum „Garáže -1“.

- Prediktivní průzkum: Hotspot Southpoint, lokalita „Recepce“



Obr. 26. Prediktivní průzkum „Recepce“.

- Prediktivní průzkum: Hotspot Southpoint, lokalita „4. patro“

Obr. 27. Prediktivní průzkum „4. patro“.

3.7 Měření stávajícího stavu

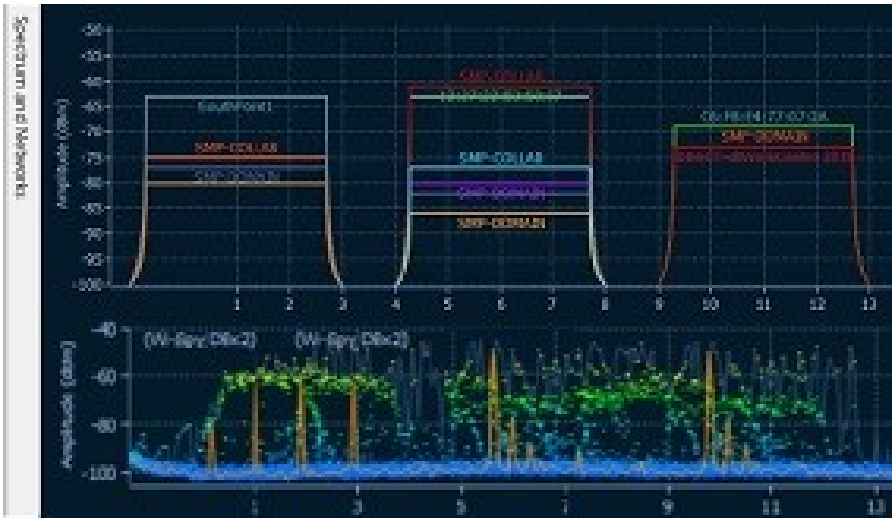
Pro měření a analýzu stávajícího stavu Wi-Fi signálu v objektu, v plánovaných lokalitách (Garáže -1, Recepce, 4. patro) umístění přístupových bodů, je použit software Tamograph Site Survey ve spojením s externím USB spektrálním analyzátorem „Wi-Spy DBx2“.

3.7.1 Stávající stav „Garáže -1“

Měření v podzemních garážích vykázalo nulovou úroveň signálu Wi-Fi na frekvencích 2.4GHz i na frekvenci 5GHz. Spektrální analýza vykázala slabý rušivý signál v jedné části lokality, v prostorech kde je instalována silnoproudá kabeláž. Na základě výsledků aktivního průzkumu bude přistoupeno k navýšení výkonu přístupového bodu, případně ke zkvalitnění odizolování prostor se silnoproudým vedením.

3.7.2 Stávající stav „Recepce“

V prostorech recepce v přízemí se vyskytuje větší množství signálů Wi-Fi na různých úrovních a taktéž na různých kanálech. Na vyšší úrovni byly naměřeny signály z již stávajících přístupových bodů. Větší množství signálů Wi-Fi bylo zjištěno především na frekvencích 2.4GHz a nepřekrývajících se kanálech 1, 6 a 11, zanedbatelné množství na frekvenci 5GHz.



Obr. 28. Spektrální a síťová analýza „Recepce“.

V prostorech recepce nelze příliš měnit umístění přístupového bodu, pokud by na základě aktivního průzkumu docházelo k výpadkům sítě, ztrátě paketů atp. bylo by řešením navýšení výkonu přístupového bodu v recepci, případně i snížení výkonu stávajících přístupových bodů. Vysílací kanál na přístupovém bodu by měl být nastaven na nepřekrývající se kanál např. 1, 6 nebo 11. Spektrální analýza nevykazuje žádné rušivé signály z jiných zdrojů než

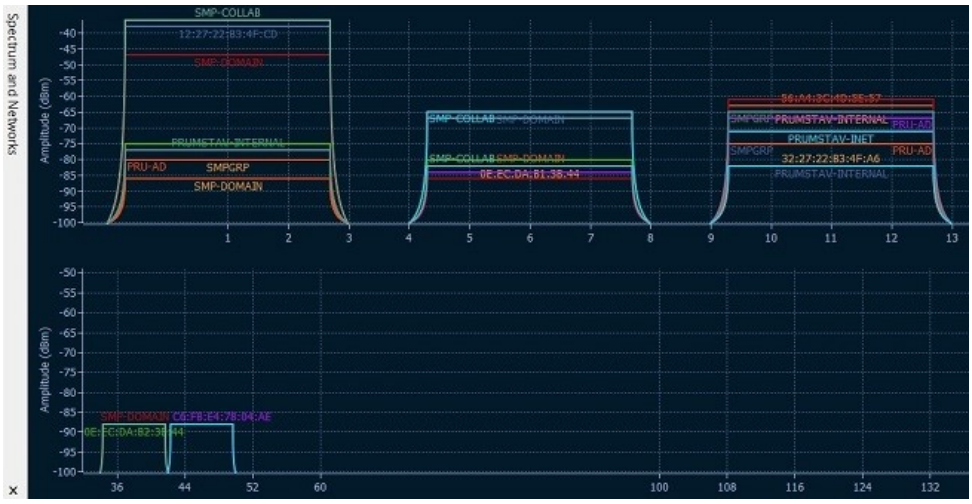
okolních Wi-Fi zařízení. Síťovou analýzou byla zjištěna stávající Wi-Fi zařízení, jejich seznam a zjištěné hodnoty jsou zobrazeny v následujícím grafickém přehledu.

Band / Name	SSID	Ch	Signal	Encryption	Max Rate	Spatial Streams	MAC Address
802.11g							
Unknown 802.11g	DIRECT-dtWorkCen...	11	-80	WPA2 (CCMP)	54,0	1	9E:93:4E:40:80:6A
802.11n (2.4 GHz)							
Ubiquiti 802.11n (2.4 GHz)	SMP-COLLAB	1	-73	WPA2 (CCMP)	144,0	2	00:27:22:B3:50:08
Ubiquiti 802.11n (2.4 GHz)	SMP-COLLAB	6	-80	WPA2 (CCMP)	144,0	2	00:27:22:B3:50:15
Ubiquiti 802.11n (2.4 GHz)	SMP-COLLAB	6	-61	WPA2 (CCMP)	144,0	2	00:27:22:B3:50:67
Unknown 802.11n (2.4 GHz)	SMP-DOMAIN	1	-77	WPA2 (CCMP)	144,0	2	02:27:22:B3:50:08
Unknown 802.11n (2.4 GHz)	SMP-DOMAIN	6	-82	WPA2 (CCMP)	144,0	2	02:27:22:B3:50:15
Unknown 802.11n (2.4 GHz)	SMP-DOMAIN	6	-61	WPA2 (CCMP)	144,0	2	02:27:22:B3:50:67
Unknown 802.11n (2.4 GHz)		1	-80	WPA2 (CCMP)	144,0	2	12:27:22:B3:50:08
Unknown 802.11n (2.4 GHz)		6	-82	WPA2 (CCMP)	144,0	2	12:27:22:B3:50:15
Unknown 802.11n (2.4 GHz)		6	-61	WPA2 (CCMP)	144,0	2	12:27:22:B3:50:67
Tp-LinkT 802.11n (2.4 GHz)	SouthPoint1	1	-63	WPA (TKIP),WPA2 (CCMP)	144,0	2	84:16:F9:7E:B5:CC
Ubiquiti 802.11n (2.4 GHz)	SMP-COLLAB	11	-71	WPA2 (CCMP)	144,0	2	B4:FB:E4:77:07:2A
Unknown 802.11n (2.4 GHz)	SMP-DOMAIN	11	-71	WPA2 (CCMP)	144,0	2	B6:FB:E4:77:07:2A
Unknown 802.11n (2.4 GHz)		11	-73	WPA2 (CCMP)	144,0	2	C6:FB:E4:77:07:2A
Unknown 802.11n (2.4 GHz)	SMP-DOMAIN	6	-86	WPA2 (CCMP)	144,0	2	FE:EC:DA:B1:3B:44
802.11ac							
Ubiquiti 802.11ac	SMP-COLLAB	36 (36-40...	-84	WPA2 (CCMP)	400,0	2	B4:FB:E4:78:07:2A
Unknown 802.11ac	SMP-DOMAIN	36 (36-40...	-84	WPA2 (CCMP)	400,0	2	B6:FB:E4:78:07:2A
Unknown 802.11ac		36 (36-40...	-84	WPA2 (CCMP)	400,0	2	C6:FB:E4:78:07:2A

Obr. 29. Přehled stávajících Wi-Fi zařízení „Recepce“.

3.7.3 Stávající stav „4. Patro“

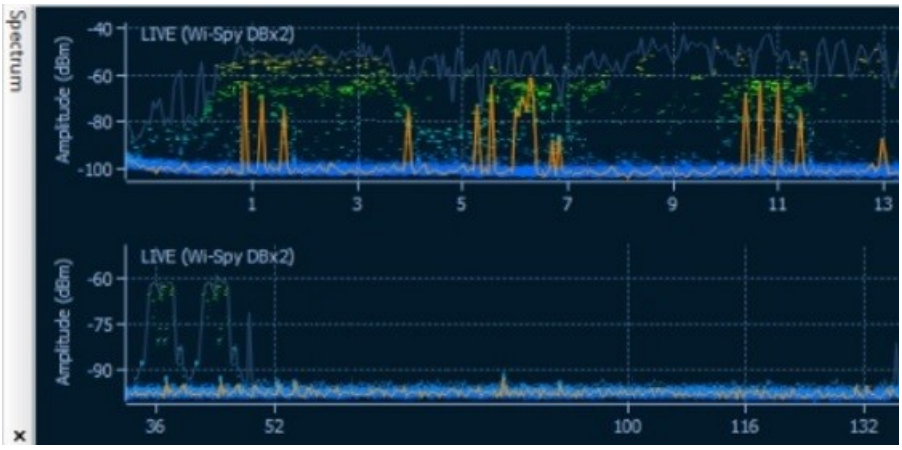
Ve 4. patře administrativního objektu bylo naměřeno větší množství zdrojů Wi-Fi signálu z blízkého okolí. Zdroje signálu s úrovní větší než -90dBm jsou ignorovány. V lokalitě umístění budoucích přístupových bodů se vyskytuje větší množství signálů Wi-Fi zejména na kanálech 1,6, 11 již stávajících Wi-Fi zařízení. Množství stávajících zařízení vysílající na



Obr. 30. Síťová analýza „4. patro“.

frekvenci 5GHz je zanedbatelné. Spektrální analýzou nebyly zjištěny žádné silnější nežádoucí rušivé signály z jiných zařízení než stávajících Wi-Fi. V objektu se nenachází významné zdroje nežádoucího rušení kromě silnoproudého vedení v podzemních podlažích. V dotčených lokalitách hotspotu se vyskytují zdroje rušivých signálů na minimální úrovni

především od uživatelských Bluetooth zařízení a bezdrátových setů klávesnic a myší. Mikrovlnná trouba instalovaná v kuchyňce v lokalitě „4. patro“ se nachází mimo uvažovanou oblast pokrytí signálem hotspotu.



Obr. 31. Spektrální analýza 2.4GHz a 5GHz „4. patro“.

3.8 Shrnutí

Tato kapitola pojednává o průzkumu lokality („Site Survey“) a jeho důležitosti pro vlastní návrh bezdrátové sítě Wi-Fi. Věnuje se plánování průzkumu před a po nasazení Wi-Fi a následným průběžným průzkumům. Jsou zmíněny jednotlivé typy průzkumů: prediktivní, pasivní a aktivní, které může doplňovat spektrální analýza, která pomůže zjistit ne-Wi-Fi zařízení, která by mohla interferovat s navrženým Wi-Fi systémem. Dále je představen zvolený softwarový nástroj Tamograph Site Survey a hardwarový spektrální analyzátor Wi-Spy, které byly zvoleny pro provedení průzkumu. Jsou popsány jednotlivé kroky instalace aplikace, přes vytvoření nového projektu, vložení a kalibrací mapy a následným grafickým zpracováním prediktivního průzkumu. Pasivnímu a aktivnímu průzkumu bude věnována pozornost v další kapitole. V závěru kapitoly je provedeno měření stávajícího stavu Wi-Fi prostředí a síťová a spektrální analýza jednotlivých lokalit.

4 NÁVRH A KONFIGURACE KOMPONENTŮ HOTSPOTU

Na trhu dnes existuje velké množství produktů, ze kterých je možné vybírat. Z důvodu dostupnosti a efektivnosti celého řešení proto nebudou vybrány high-endové produkty, které poskytují nejvyšší možnou kvalitu a zabezpečení, avšak na úkor velmi vysoké ceny a dalších ať již servisních nebo licenčních nákladů. Z množství dostupných produktů různých výrobců pro řešení hotspotu budou vybrány bezdrátové produkty Mikrotik, které poskytují velmi dobrou kvalitu, zabezpečení i univerzálnost, rozsáhlou a dostupnou technickou podporu dostupnou online a v neposlední řadě, zejména pro účely řešení hotspotu, integrovanou funkci hotspot serveru a RADIUS serveru. Zvolené komponenty poskytují i duální rádio a umožňují současně provoz na frekvenci 2.4Ghz i 5Ghz. V současnosti je na trhu pouze limitované množství produktů podporujících zabezpečení WPA3. Pro otevřený přístup k hotspotu 2.4GHz je zvoleno optimální zabezpečení formou RADIUS serveru, pro správu objektu pak zabezpečení WPA2-PSK pro 5GHz rádio. Celé řešení hotspotu bude obsahovat několik přístupových bodů rozmístěných dle prediktivního průzkumu s hlavní centrální jednotkou umístěnou společně s PoE switchem v uzamykatelné rackové skříni v místnosti „velína“ objektu. Tato místnost je uzamykatelná a pod 24hodinovým kamerovým dohledem se záznamem. Jednotlivé přístupové body budou připojeny do PoE switche kroucenou dvoulinkou UTP CAT6. Celý systém bude řízen centrální jednotkou, připojenou do PoE switche, s RADIUS serverem a funkcí hotspotu. PoE přepínač bude připojen do již stávajícího routeru, který umožňuje přístup do sítě Internet. Poslední komponentou bude stávající desktop PC s operačním systémem Microsoft Windows a nainstalovaným softwarem ReadyVoucher, který bude generovat a spravovat pověření pro autentizaci prostřednictvím webového přihlašovacího portálu. Centrální jednotka i přístupové body, PC a switch budou připojeny na stávající centrální záložní zdroj UPS, který zároveň poskytuje i funkci přepěťové ochrany.

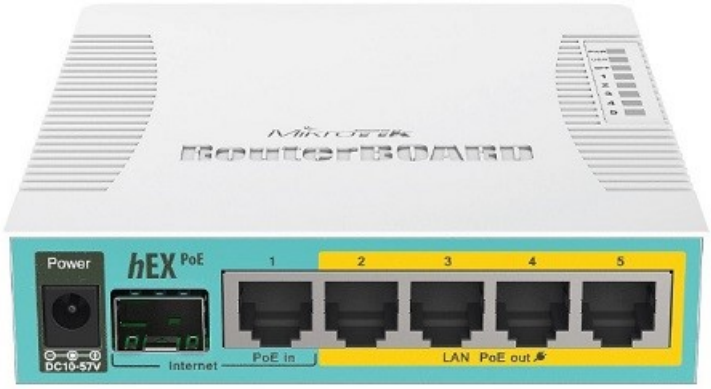
4.1 Hardwarové komponenty

Jednotlivé navržené hardwarové komponenty řešení hotspotu:

- Centrální jednotka – Mikrotik Routerboard 960PGS
- Přístupové body 2.4GHz a 5GHz – Mikrotik cAP ac
- Přístupové body 2.4GHz – Mikrotik cAP lite
- PoE Switch – TP-LINK TL-SG1005P

4.1.1 Centrální jednotka

Centrální jednotkou je navržen produkt Mikrotik RouterBoard 960PGS také uváděn pod názvem hEX PoE, je pětiportový gigabitový ethernetový router, který nemá integrovaný bezdrátový adaptér a může tak vykonávat pouze funkci centrální jednotky a funkci routeru pro přístup k síti Internet případně do jiných sítí. Součástí balení produktu je zdroj 24V DC,



Obr. 32. Mikrotik RB960PGS. [15]

avšak pro zprovoznění funkce napájení přes Ethernet (PoE) na tomto produktu musí být použit externí zdroj 48V DC.

Tab. 2. Specifikace produktu RB960PGS

Specifikace produktu	
Produktový kód	RB960PGS
Procesor	QCA9557
Frekvence procesoru	800 MHz
Počet jader procesoru	1
Paměť RAM	128 MB
Ethernetové porty 10/100/1000	5
PoE vstup	ANO, pasivní
Podporované vstupní napětí	12 - 57 V
PoE výstup	ANO, na portech 2-5
Teplotní senzor	ANO
Napěťový senzor	ANO
USB slot	ANO
Rozměry	114 x 137 x 29mm
Licenční úroveň	4
Operační systém	RouterOS
Maximální spotřeba	9 W

4.1.2 Duální přístupové body

Přístupový bod (AP) Mikrotik cAP ac bude umístěn ve třech lokalitách (recepce, garáž, a 5.NP). Jednotky budou připojeny kabelem UTP Cat6 do PoE switche a napájeny přes PoE

Obr. 33. Mikrotik cAP ac. [16]

porty a instalovány ve stropním podhledu. CAP ac je velmi schopný a výkonný přístupový bod, který lze montovat na strop nebo na stěnu. Souběžné dvoupásmové bezdrátové rádio podporuje 2.4GHz a 5GHz ve standardu 802.11ac i starších standardech a zajistí pokrytí v rozsahu 360 stupňů. Jednotka poskytuje pasivní PoE výstup pro připojení a napájení podružného přístupového bodu (cAP lite).

Tab. 3. Specifikace produktu cAP ac

Specifikace produktu		
Produktový kód	RBcAPGi-5acD2nD (EU)	
Procesor	4 jádra, IPQ-4018	
Frekvence procesoru	716 MHz	
Paměť RAM	128 MB	
Typ úložiště	Flash	
Velikost úložiště	16 MB	
10/100/1000 ether porty	2	
Wi-Fi	2.4 GHz	5 GHz
Protokoly	802.11b/g/n	802.11ac
Počet antén	2	2
Zisk antény	2 dBi	2.5 dBi
Napájení	PoE-in 802.3af/at, PoE-out (pasivní, ether port 2), 17-57 V	
Maximální spotřeba	13 W	
Licenční úroveň	4	
Operační systém	RouterOS	

4.1.3 Přístupové body

Přístupové body Mikrotik cAP lite jsou malé přístupové body, které jsou vhodné do nejrůznějších prostředí. Produkt cAP lite podporuje standard 802.11b/g/n a může být napájen přes

Obr. 34. Mikrotik cAP lite. [17]

PoE, může být připojen a napájen přes hlavní přístupový bod. Je vhodný zejména do prostor se sníženou kvalitou nebo slabým dosahem signálu hlavního přístupového bodu, jako extender („prodlužovač“) signálu Wi-Fi. Tak jako duální přístupový bod cAP ac tak cAP lite podporuje funkci Mikrotik CAPsMAN (řízený správce systému AP), ovládání všech přístupových bodů přes centrální jednotku. Jednotka cAP lite může být také použita jako samostatný přístupový bod a může tak fungovat zcela nezávisle.

Tab. 4. Specifikace produktu cAP lite

Specifikace produktu	
Produktový kód	cAP lite
Procesor	QCA9533
Frekvence procesoru	650 MHz
Počet jader procesoru	1
Paměť RAM	64 MB
10/100 ethernetové porty	1
Wi-Fi	Built-in 2.4 GHz 802.11b/g/n, dual-chain
Zisk antény	1.5 dBi
Šířka paprsku antény	360°
PoE vstup	ANO
Podporované napájení	5 V - 60 V (jack, 802.3af/at
Provozní teplota	-40°C +70°C testováno
Licenční úroveň	4
Operační systém	RouterOS

4.1.4 Ethernetový PoE switch

Je kompaktní stolní gigabitový ethernetový switch s pěti porty, z nichž čtyři porty mají PoE, resp. po jednom kabelu jde napájení i data. Switch dokáže napájet připojená zařízení, která

Obr. 35. Switch TL-SG1005P. [18]

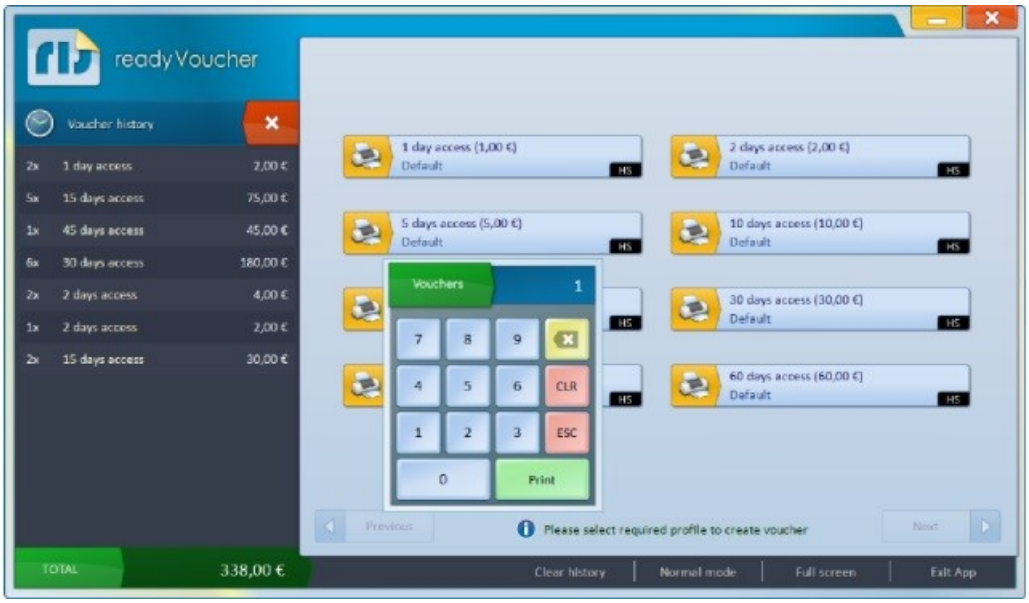
podporují protokol IEEE 802.3 af. Všech 5 portů ethernetového přepínače podporuje rychlosti 10, 100 a 1000Mbit/s. Tento switch nevyžaduje žádnou konfiguraci, obsahuje funkci přiřazení priorit pro ochranu systému v případě přetížení napájení. Celkově produkt podporuje PoE napájení do max. 55W dohromady na všech portech. Je nutné počítat se spotřebou jednotlivých připojených zařízení resp. přístupových bodů a případně zvolit výkonnější switch.

Tab. 5. Specifikace produktu TL-SG1005P

Specifikace produktu	
Produktový kód	TL-SG1005P
Rozhraní	5 10/100/1000Mbps RJ45 Portů AUTO Negotiation/AUTO MDI/MDIX
Síťové médium	1000BASE-T: UTP category 5, 5e, 6 nebo vyšší
Počet ventilátorů	bez ventilátorů
Spotřeba	63.31W (max. 56W PoE) 4.26W (žádné PoE připojení)
PoE porty RJ45	Standard: 802.3 af compliant PoE Porty: Port1- Port4 Zdroj: 56W
Vlastnosti produktu	Kompatibilní s IEEE 802.3af Funkce Priorit MAC Auto-učení a auto-zastarání IEEE802.3x Flow Control 802.1p/DSCP QoS IGMP Snooping

4.2 Softwarové komponenty

Software readyVoucher je navržen tak, aby jednoduše generoval regulérní uživatele hotspotu s přiřazeným profilem pro použití ve směrovačích Mikrotik. Produkt je určen k instalaci na



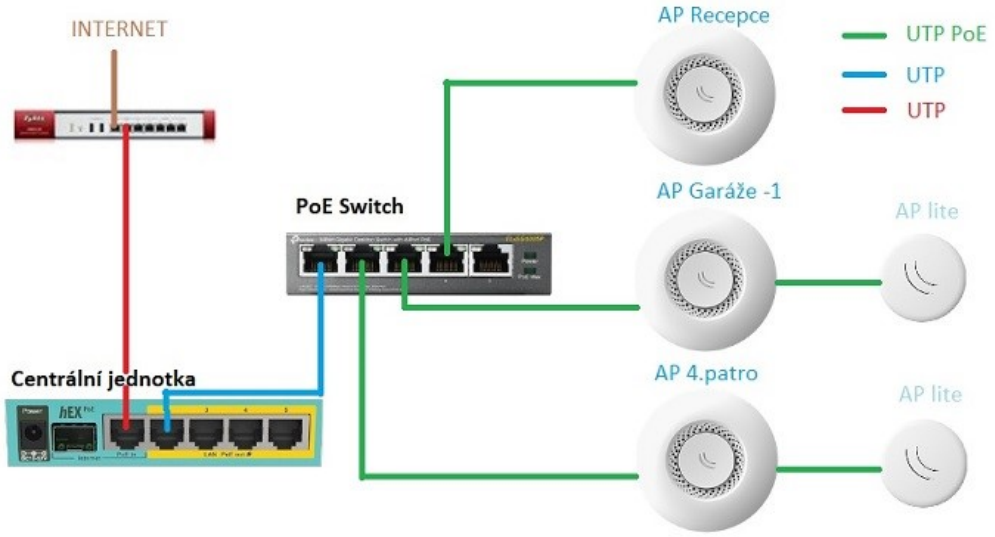
Obr. 36. Aplikace readyVoucher.

počítače s operačním systémem Microsoft Windows. Po instalaci software vytváří vouchery (poukázky) s přihlašovacími údaji pro uživatele hotspotu, které je možné vytisknout na připojené standardní tiskárně nebo přímo na štítkové, vstupenkové tiskárně. Software readyVoucher od firmy Ferrari E Hijos S. A. lze stáhnout z jejich webových stránek a používat zdarma. Jediným omezením oproti licencované verzi je jednotný design voucherů, u placené verze je pak možno tento design modifikovat. Pro potřeby řešení soukromého hotspotu je software dostačující, pro případné komerční účely může být vhodnější využití produktů českých dodavatelů softwarového řešení.

4.3 Konfigurace komponentů

Po navržení jednotlivých komponentů řešení hotspotu je nutná jejich konfigurace tak, aby celý systém správně fungoval. Hlavní součástí řešení Hotspotu je hardware společnosti Mikrotik, pro jehož konfiguraci se použije aplikace Winbox. Aplikaci je možné stáhnout ze stránek společnosti Mikrotik, toho času ve verzi 3.18. Aplikace se neinstaluje, po stažení se pouze spustí soubor „winbox.exe“. Pro používání aplikace WinBox existuje rozsáhlý uživatelský manuál, který je též dostupný na stránkách výrobce. Konfigurace a instalace softwaru

readyVoucher a vlastního hotspotu bude popsána samostatně. Prvotním krokem bude konfigurace centrální jednotky a přístupových bodů. Následující obrázek zobrazuje schéma zapojení jednotlivých komponentů celého systému hotspotu. Z ethernetového portu 1 centrální jednotky je kabelem UTP Cat6 připojen stávající router, který poskytuje připojení do Inter-

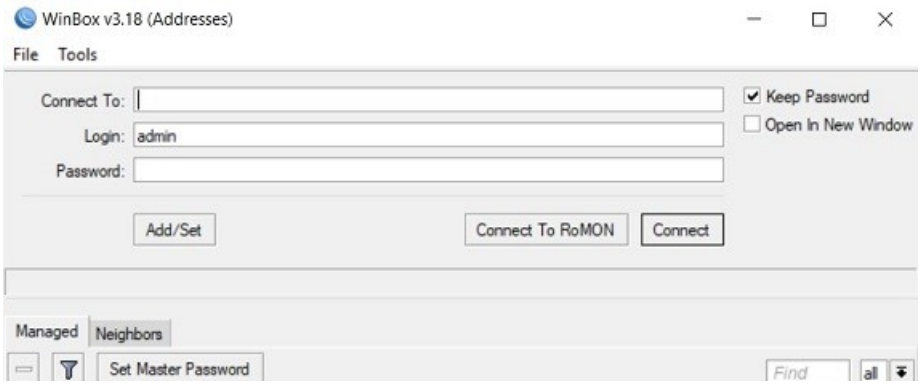


Obr. 37. Schéma zapojení komponentů.

netu. Do ethernetového portu 2 centrální jednotky je připojen kabelem UTP Cat 6 do portu LAN1 PoE switch TP-link. Do PoE portů switche, LAN2-4 jsou připojeny hlavní přístupové body. Do přístupových bodů pro lokalitu „Garáže -1“ a „4. patro“ jsou připojeny na výstupní PoE port vedlejší přístupové body.

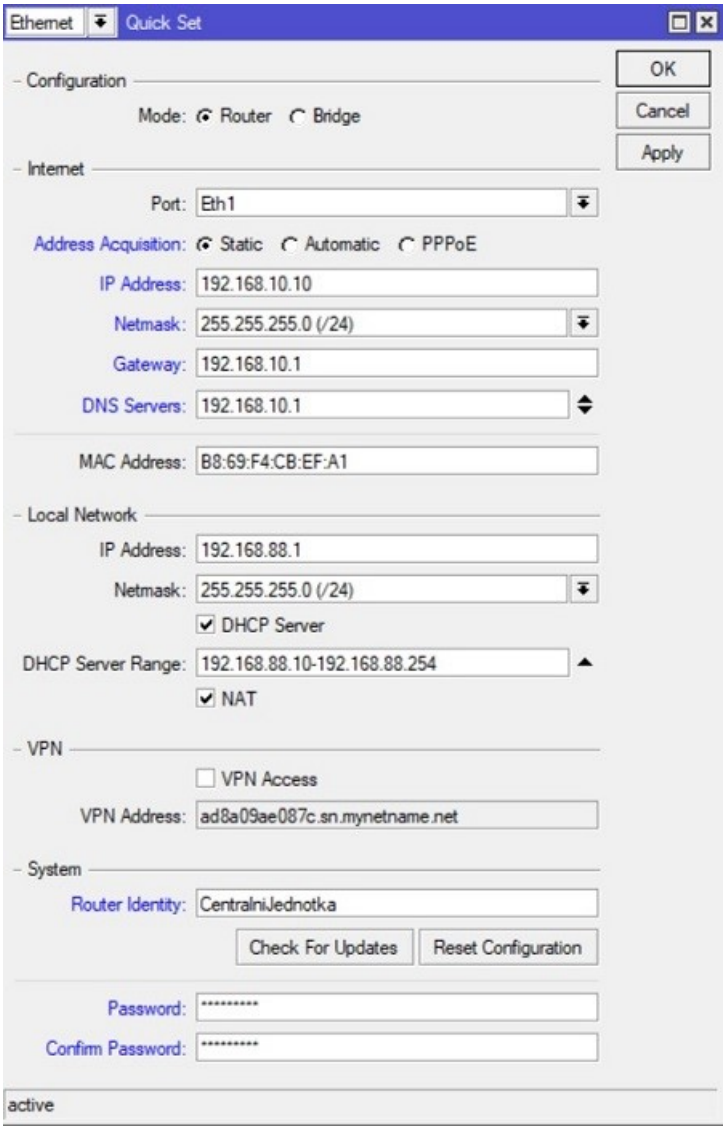
4.3.1 Konfigurace centrální jednotky

Centrální jednotka Mikrotik RB960PGS se připojí ke zdroji napájení a následně UTP kabelem ke stávajícímu routeru. Konektor RJ45 je připojen do portu 1. Dalším UTP kabelem se jednotka připojí k počítači jedním ze čtyř LAN portů na centrální jednotce. Již z výroby je produkt nastaven tak, aby po prvotním spuštění automaticky přiřadil IP adresu připojenému



Obr. 38. WinBox – Přihlašovací obrazovka.

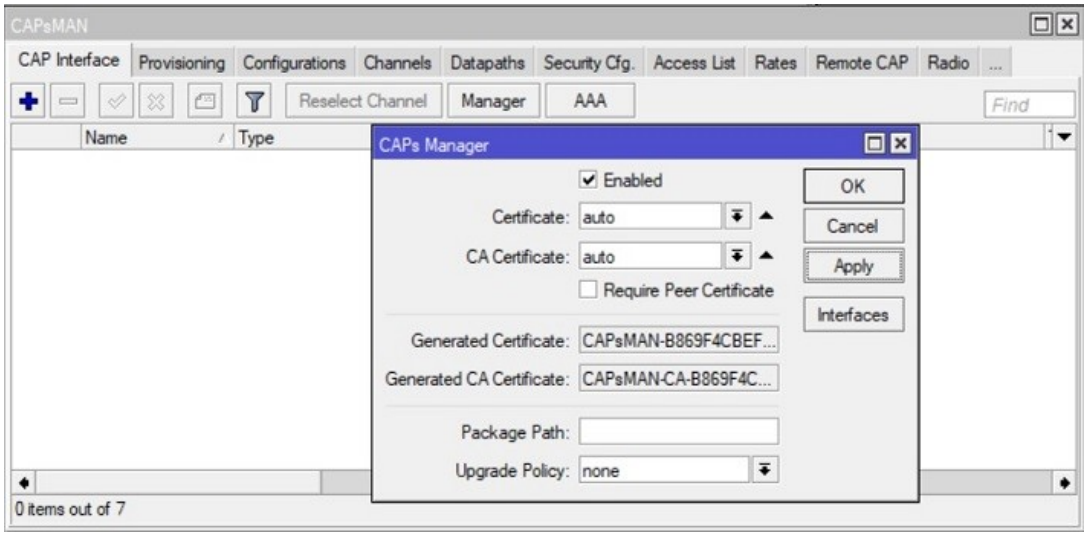
počítači, v tomto případě je adresa 192.168.88.254 a adresa routeru je 192.168.88.1, tyto informace lze nalézt v počítači ve vlastnostech síťového připojení. Po spuštění aplikace WinBox se do řádku „Connect to“ zadá adresa routeru, přihlašovací jméno, z výroby před-



Obr. 39. Quick Set – Základní nastavení.

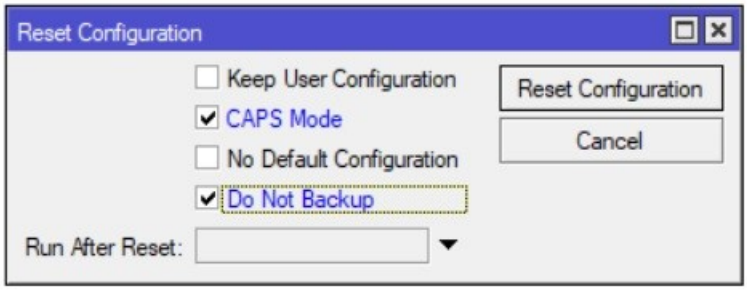
nastaveno „admin“ a stiskne se tlačítko „Connect“, tímto dojde k úspěšnému přihlášení a je možné začít zařízení konfigurovat. Jako první krok je potřeba nastavit v menu „System“ správné datum a čas. Po kliknutí na tlačítko „Quick Set“ se konfiguruje základní nastavení rozhraní IP adresa portu ether1 (rozhraní WAN připojené do Internetu), nastavení IP rozsahu sítě LAN, povolení DHCP serveru rozhraní ether2-ether5 pro automatické přidělování IP adres. Hodnoty síťových údajů poskytne místní správce sítě, případně jsou zvoleny dle potřeby. V neposlední řadě se nastaví systémový název jednotky a nové přístupové heslo pro administraci zařízení. V základní konfiguraci je mezi rozhraním LAN a WAN firewall povolen. Z bezpečnostního hlediska je však doporučeno přednastavené hodnoty překontrolovat

nebo změnit. Pokud jsou veškeré zadané údaje v pořádku, je v této fázi funkční přístup k síti Internet. Základní nastavení zařízení je tak hotovo a dalším krokem je konfigurace funkce CAPsMAN. Tato funkce umožňuje spravovat připojené přístupové body centrálně, veškerá konfigurace přístupových bodů bude prováděna z centrální jednotky. V hlavním menu se



Obr. 40. CAPsMAN – Nastavení.

vybere tlačítko CAPsMAN a v nově otevřeném okně se zvolí tlačítko „Manager“. V dalším okně se otevře CAPs Manager kde se zaškrtne položka „Enabled“ pro povolení. Certifikační autorita a certifikát se nastaví na hodnotu „auto“ a klikne se na tlačítko „Apply“ pro potvr-



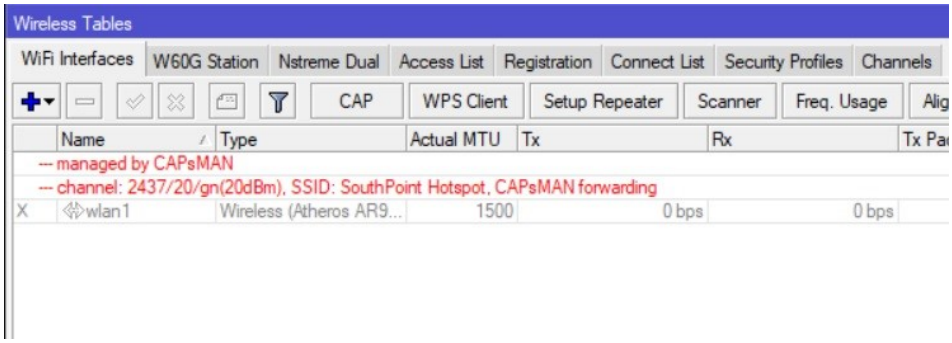
Obr. 41. Reset AP do CAPS módu.

zení. Připojené přístupové body obdrží od centrální jednotky při konfiguraci certifikát a tím je navázána důvěryhodná bezpečná komunikace mezi přístupovými body a centrální jednotkou.

4.3.2 Konfigurace přístupových bodů

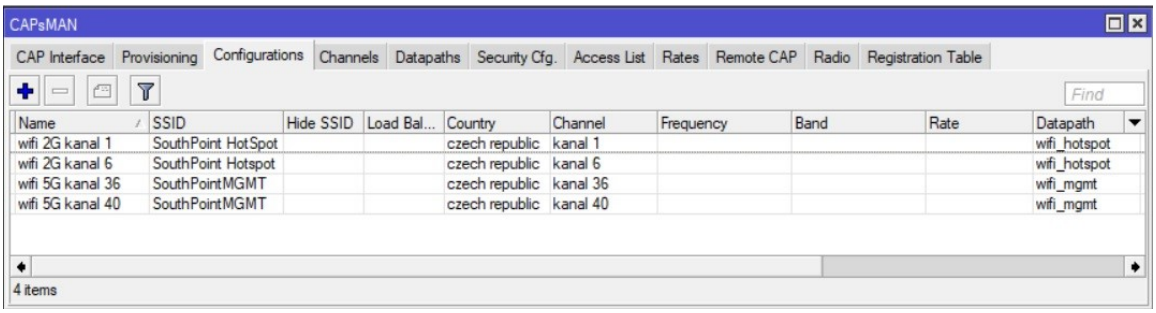
K připravené centrální jednotce se připojí všechny přístupové body přes jejich ethernetové rozhraní do portů PoE switche. Přístupové body získají IP adresu automatickým přidělením z DHCP serveru, který je nakonfigurován na síťový rozsah 192.168.33.0/24. Pro tento rozsah

je nastaven bridge nazvaný “caps_mgmt”. Po přihlášení k jednotlivým přístupovým bodům, stejným způsobem jako u základního přihlášení k centrální jednotce přes aplikaci WinBox se v hlavním menu zvolí „Systém“ a provede se reset konfigurace zaškrtnutím pole „ Do not backup“ a „Caps mode“ a potvrzení tlačítkem „Reset configuration“. Po restartu zařízení je



Obr. 42. AP nastaven na centrální správu.

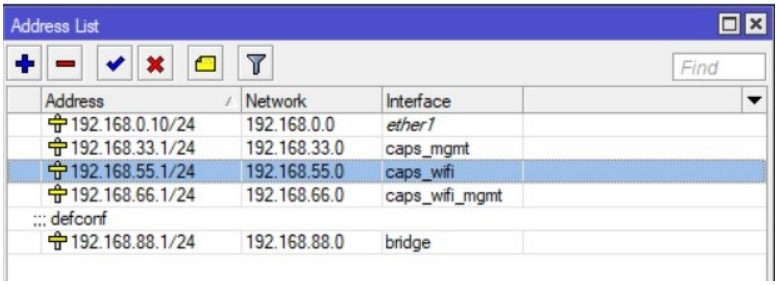
přístupový bod nastaven na centrální správu a je nyní možné veškerá nastavení přístupových bodů provádět z centrální jednotky. V centrální jednotce v menu „CAPSMAN“ se následně nakonfigurují nastavení jednotlivých profilů pro přístupové body. Každý profil může mít nastaven různé vlastnosti bezdrátového adaptéru jako je výkon, vysílací kanál, omezení



Obr. 43. Konfigurační profily pro AP.

rychlosti přenosu dat a mnoho dalších hodnot pro optimální provoz přístupového bodu. Jelikož se jedná o otevřený systém, veřejný přístupový bod, nebude prozatím nastaveno zabezpečení bezdrátového profilu, k tomuto dojde až v dalších krocích konfigurace celého hotspotu. Po nastavení jsou profily automaticky distribuovány do jednotlivých přístupových bodů a systém nyní již vysílá nastavené SSID a je připraven přijímat žádosti o připojení. Pro správu objektu je nastaven na 5GHz bezdrátové síti vlastní SSID s vlastním WPA2-PSK zabezpečením pro účely správy objektu a bezdrátovému přístupu k síti Internet. Bezdrátová

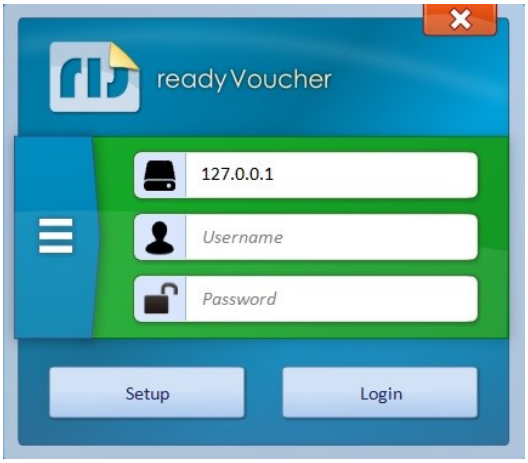
síť využívající pásmo 2.4GHz zabezpečuje primárně funkci hotspotu pro návštěvníky objektu. Pro distribuci IP adres klientům je nakonfigurován nový bridge „caps_wifi“, na kterém je povolen DHCP server v rozsahu 192.168.55.2-254/24.



Obr. 44. Adresa WLAN.

4.4 Instalace aplikace readyVoucher

Aplikace readyVoucher je volně ke stažení, dostupná na stránkách effesoftware.com. Po stažení a dekomprimaci archivu se aplikace spustí pomocí souboru „readyVoucher.exe“.



Obr. 45. Aplikace readyVoucher.

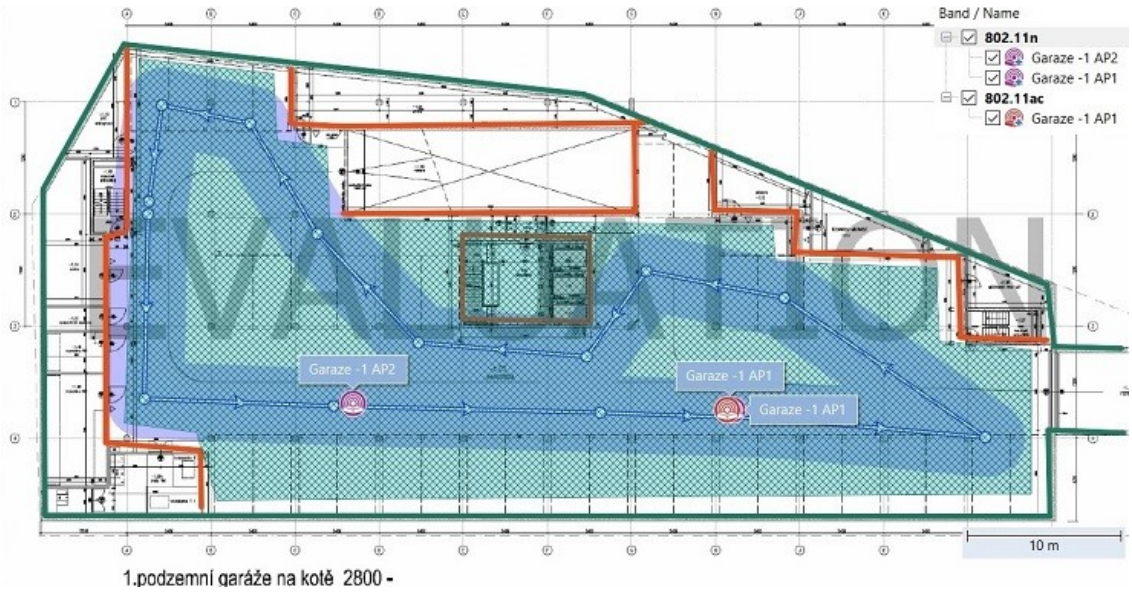
4.5 Pasivní průzkum lokality

Před vlastním nasazením celého systému je nutné provést pasivní průzkum lokality. Po instalaci vlastní kabeláže, připojení, montáži a umístění zvolených komponentů na základě prediktivního průzkumu přistoupit k pasivnímu průzkumu, který spočívá v měření a sběru informací Wi-Fi o bezdrátovém prostředí pro následné zhodnocení a optimalizaci. Výsledkem této fáze je přesné zmapování situace kam strategicky umístit vybrané přístupové body. Fáze „před nasazením“ ověřuje výkonnost přístupových bodů před vlastní fází nasazení celého systému. Pasivní průzkum je prováděn v případě, kdy zařízení provádějící průzkum není připojeno k žádné Wi-Fi síti a pouze „pasivně“ naslouchá prostředí Wi-Fi. Software

používaný pro tyto průzkumy je obvykle nakonfigurován pro skenování specifických kanálů a Wi-Fi sítí za účelem měření intenzity signálu a úrovní šumu.

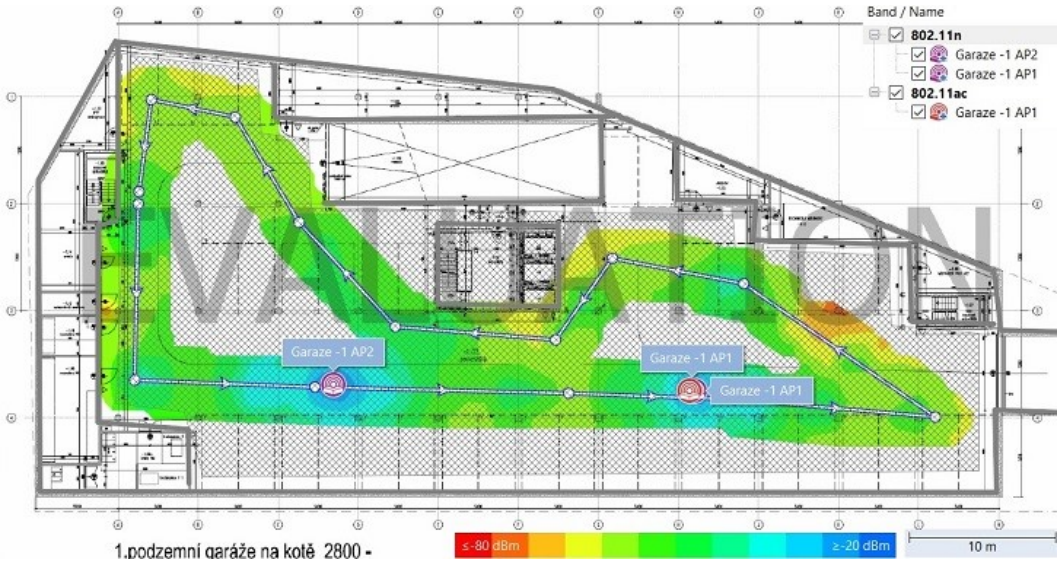
4.5.1 Pasivní průzkum lokality „Garáže -1“

V podzemních garážích jsou umístěny dle prediktivního průzkumu dva přístupové body s názvem „Garáže -1 AP1“, který vysílá současně na 2.4GHz a 5GHz, a „Garáže -1 AP2“, který vysílá pouze na frekvenci 2.4GHz. Na *Obr. 46. Pasivní průzkum Garáže -1: Vizualizace* je zobrazena vizualizace umístění přístupových bodů. V další fázi pasivního průzkumu byla



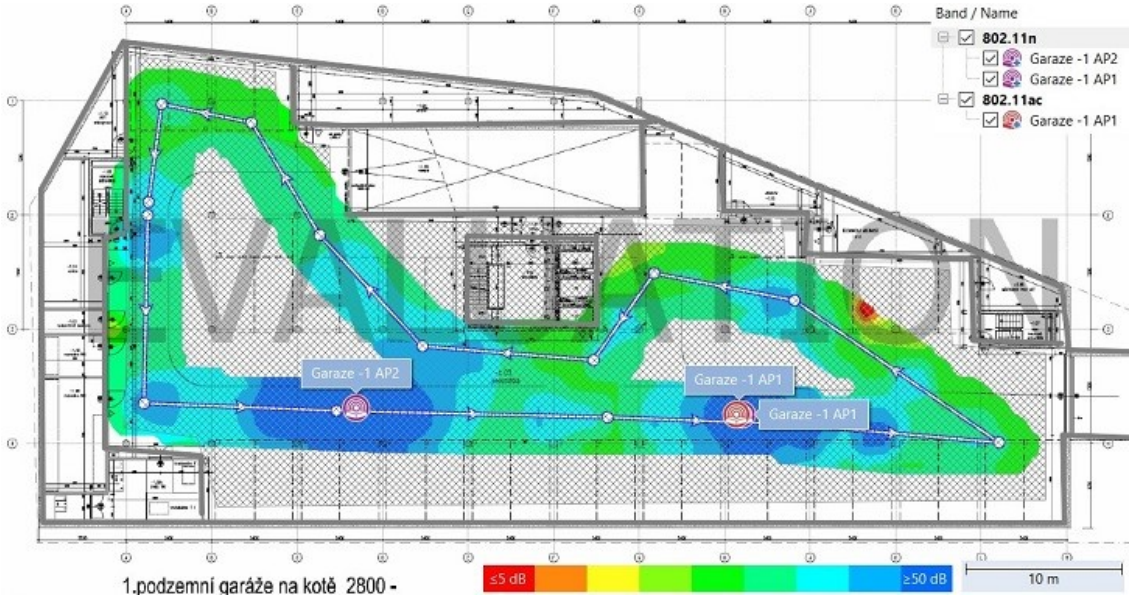
Obr. 46. Pasivní průzkum Garáže -1: Vizualizace.

„pasivně“, bez přihlášení k přístupovým bodům, měřena úroveň signálu vysílaného přístupovými body. V podzemních garážích je vysílaný signál na velice dobré úrovni, pouze



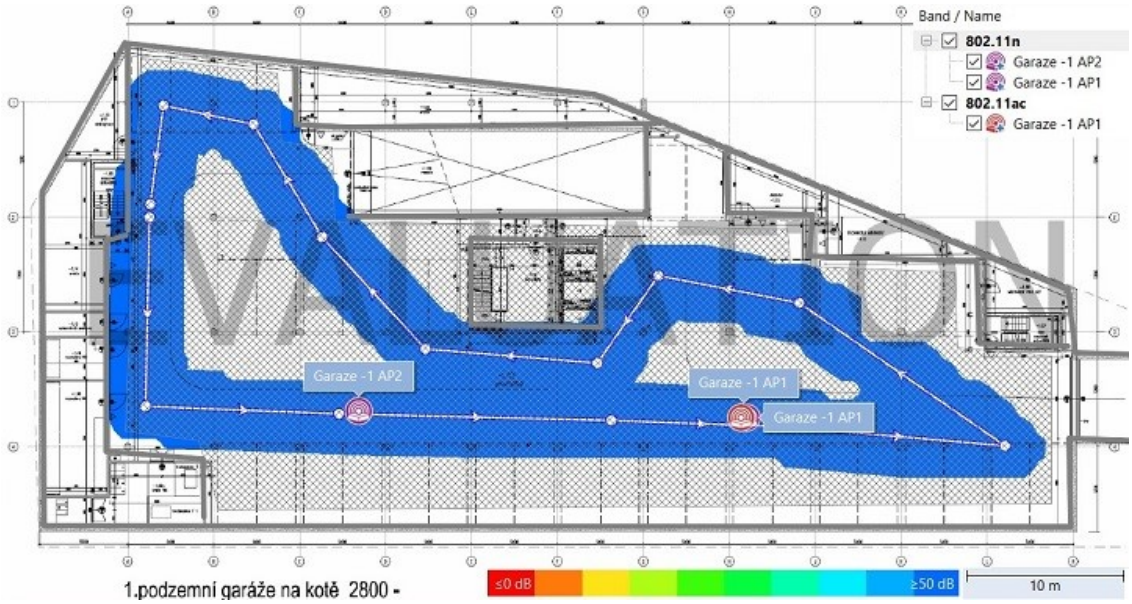
Obr. 47. Pasivní průzkum Garáže -1: Úroveň signálu.

v jedné části garáží je naměřena nižší úroveň signálu, bude tedy nutné upravit vysílací výkon přístupového bodu „Garáže -1 AP1“ na vyšší hodnotu. Další měřenou hodnotou je odstup



Obr. 48. Pasivní průzkum Garáže -1: Odstup signálu od šumu (SNR).

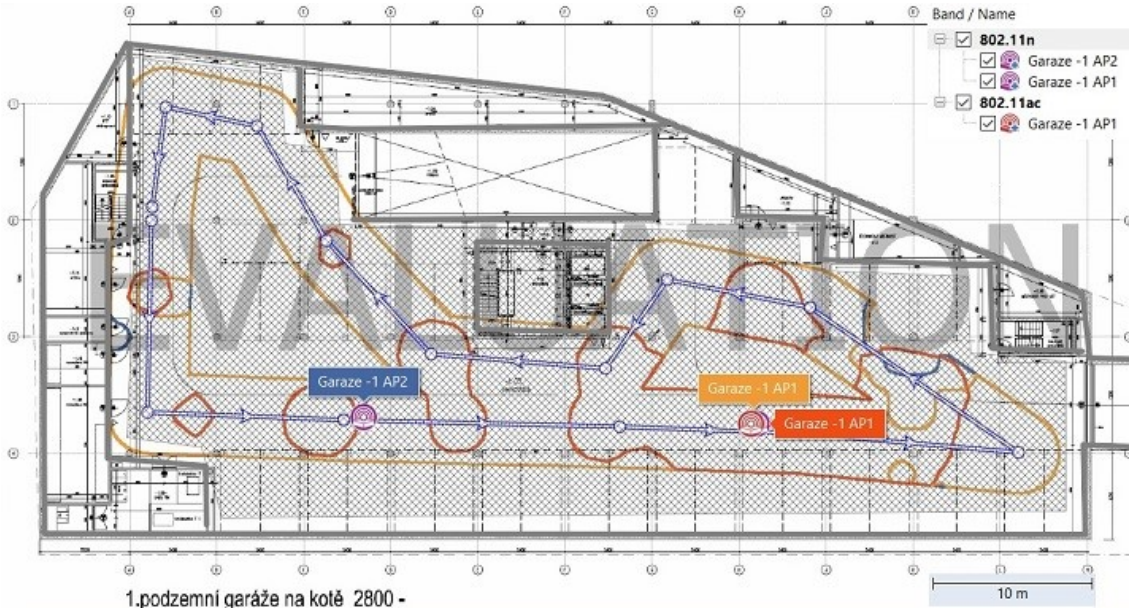
signálu od šumu (SNR), kde je zjišťován poměr žádoucího Wi-Fi signálu a signálů nežádoucích (šumu). Naměřen vyšší šum ve stejné části garáže jako v předchozím měření úrovně



Obr. 49. Pasivní průzkum Garáže -1: Poměr signálu k interferencím (SIR).

signálu, v tomto místě se nachází vedení silových kabelů. V posledním měření (*Obr. 49*) v lokalitě „Garáže -1“ je vyhodnocen poměr mezi vysílaným Wi-Fi signálem a cizími zdroji rušení (SIR). V podzemních garážích se nenachází žádný nežádoucí zdroj rušení signálu Wi-Fi. Na posledním obrázku je zobrazena, různými barvami, oblast pokrytí Wi-Fi signálem jednotlivých přístupových bodů. Výsledný pasivní průzkum vykazuje velmi dobré hodnoty

a kromě zvýšení výkonu jednoho přístupového bodu zůstane umístění a nastavení přístupových bodů beze změn.



Obr. 50. Pasivní průzkum Garáže -1: Oblast pokrytí Wi-Fi signálem.

4.5.2 Pasivní průzkum lokality „Recepce“

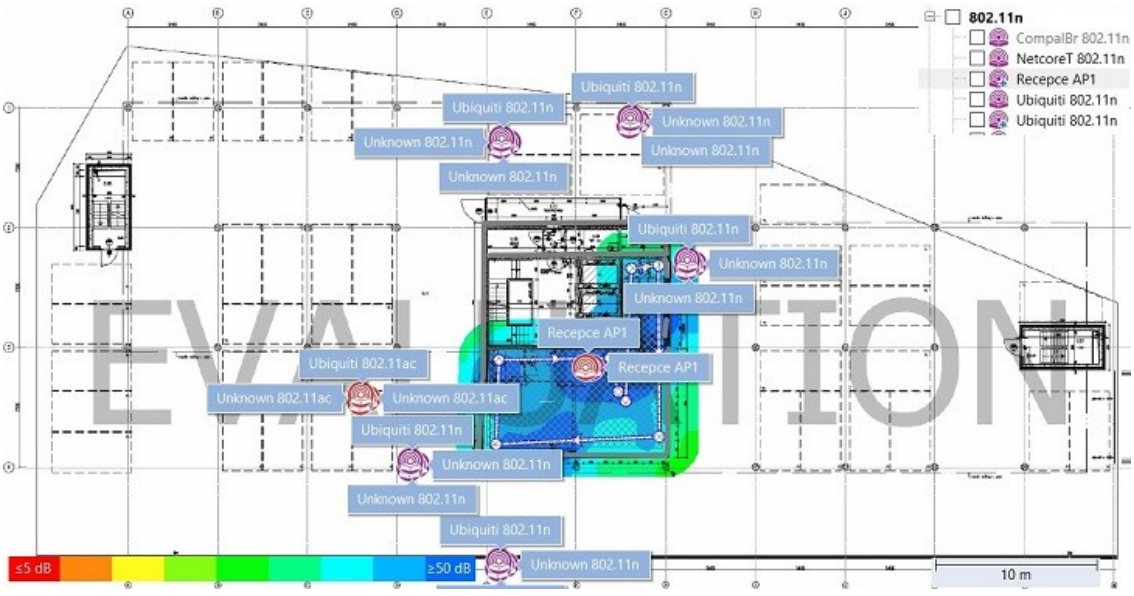
V recepci je umístěn dle prediktivního průzkumu jeden přístupové bod s názvem „Recepce AP1“, který vysílá současně na 2.4GHz a 5GHz. Na následujícím obrázku je zobrazena vizualizace umístění přístupového bodu na základě prediktivního průzkumu. Recepce je umístěna v přízemí objektu a celý prostor je prosklený. Přístupový bod je obklopen dalšími, již

Obr. 51. Pasivní průzkum Recepce: Vizualizace.

stávajícími přístupovými body, které vysílají pouze na frekvenci 2.4GHz, na nepřekrývajících se kanálech 1,6 a 11. Úroveň vysílaného signálu Wi-Fi na frekvenci 2.4GHz je dosta-

Obr. 52. Pasivní průzkum Recepce: Úroveň signálu.

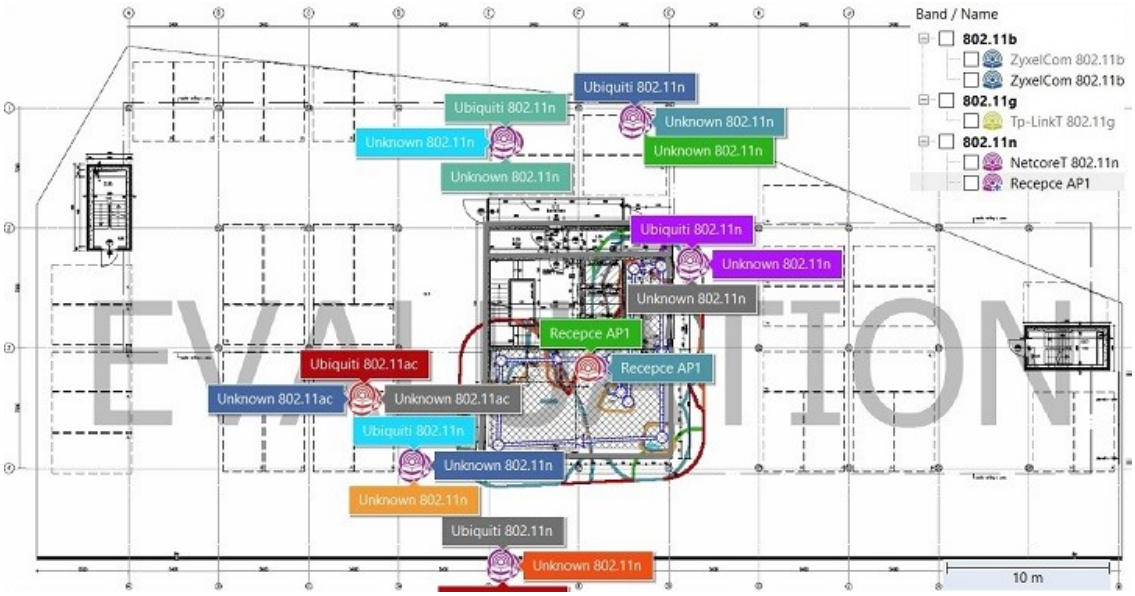
čující, AP bude nastaven na vyšší výkon. Úroveň signálu na frekvenci 5GHz je velmi dobrá. Další měřenou hodnotou je odstup signálu od šumu (SNR), kde je zjišťován poměr žádou-



Obr. 53. Pasivní průzkum Recepce: Odstup signálu od šumu (SNR).

cího Wi-Fi signálu a signálů nežádoucích (šumu). V prostorách recepce se nachází minimální množství zdrojů nežádoucího šumu. V posledním měření je vyhodnocen poměr mezi vysílaným Wi-Fi signálem a cizími zdroji rušení (SIR). V recepci se nachází menší množství nežádoucích zdrojů rušení signálu Wi-Fi na frekvenci 2.4GHz. Na vysílané frekvenci 5GHz se nenachází žádné blízké zdroje rušení. Rádio na 2.4GHz bude nastaveno na vyšší výkon a

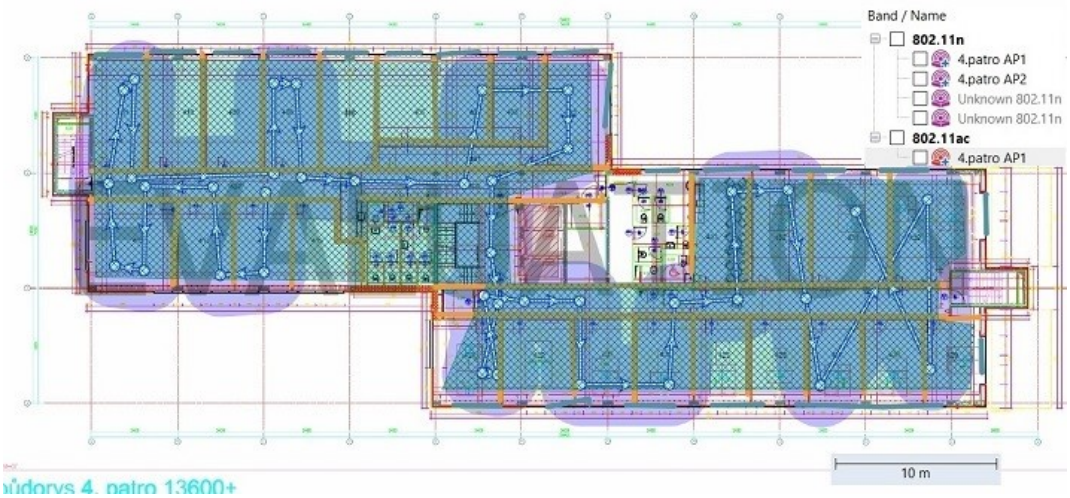
nastaveno na vysílací kanál 1, možné snížení vysílacího výkonu nejbližších stávajících přístupových bodů vysílajících na kanálu 1. Na posledním obrázku je zobrazena, různými barvami, oblast pokrytí Wi-Fi signálem duálního přístupového bodu. Výsledný pasivní průzkum vykazuje velmi dobré hodnoty a kromě zvýšení výkonu jednoho přístupového bodu zůstane umístění a nastavení přístupového bodu beze změn.



Obr. 54. Pasivní průzkum Recepce: Oblast pokrytí signálem Wi-Fi.

4.5.3 Pasivní průzkum lokality „4. patro“

Ve 4. patře objektu jsou umístěny dle prediktivního průzkumu dva přístupové body s názvem „4. patro AP1“, který vysílá současně na 2.4GHz a 5GHz, a „4. patro AP2“, který vysílá pouze na frekvenci 2.4GHz. Na obrázku níže je vizualizace umístění přístupových bodů. V dalším kroku pasivního průzkumu byla sledována hodnota úrovně signálu Wi-Fi, který je

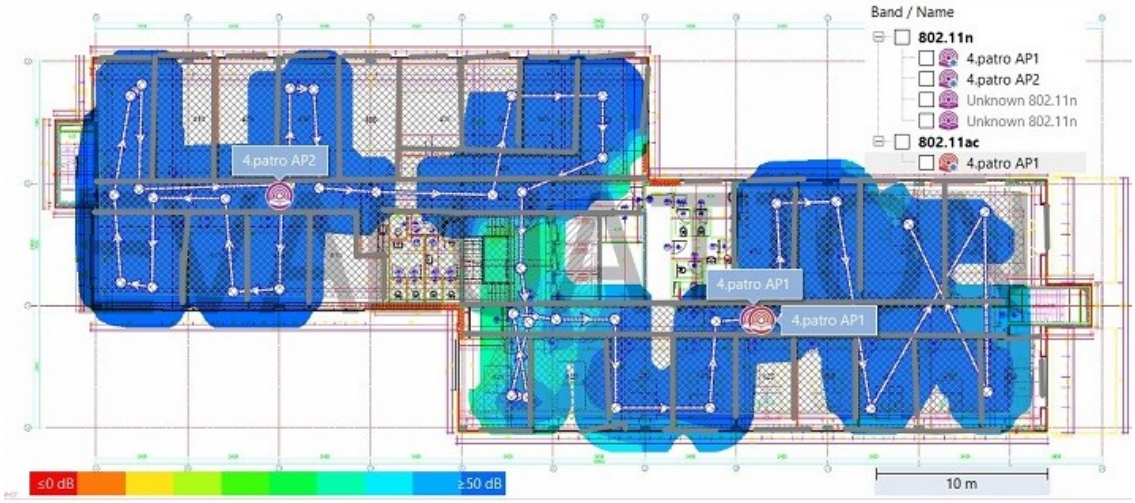


Obr. 55. Pasivní průzkum 4. patro: Vizualizace.

šířen přístupovými body s názvem „4. patro AP1“ a „4. patro AP2“. Umístění a nastavení přístupových bodu dle prediktivního průzkumu. Dle výsledků měření úrovně signálu se ob-

Obr. 56. Pasivní průzkum 4. patro: Úroveň signálu.

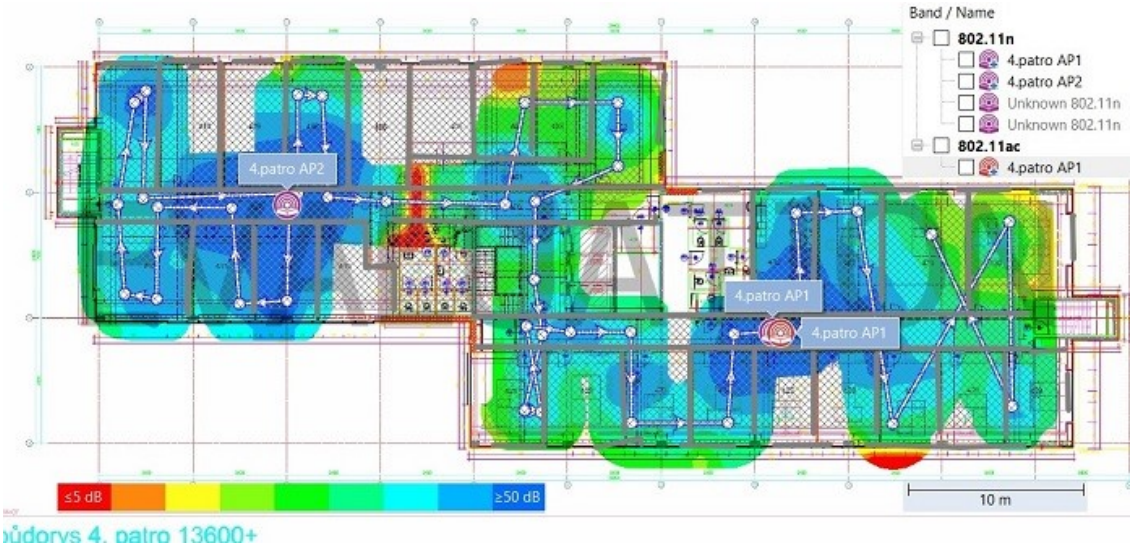
jevily dvě místa v objektu s nižší úrovní signálu, přístupové body budou v implementační fázi přesunuty blíže směrem k místům s nižší úrovní signály a mírně navýšen jejich výkon. Další měřenou hodnotou je odstup signálu od šumu (SNR), kde je zjišťován poměr žádoucího Wi-Fi signálu a signálů nežádoucích (šumu). Lehký šum naměřen zejména v okolí vý-



Obr. 57. Pasivní průzkum 4. patro: Odstup signálu od šumu (SNR).

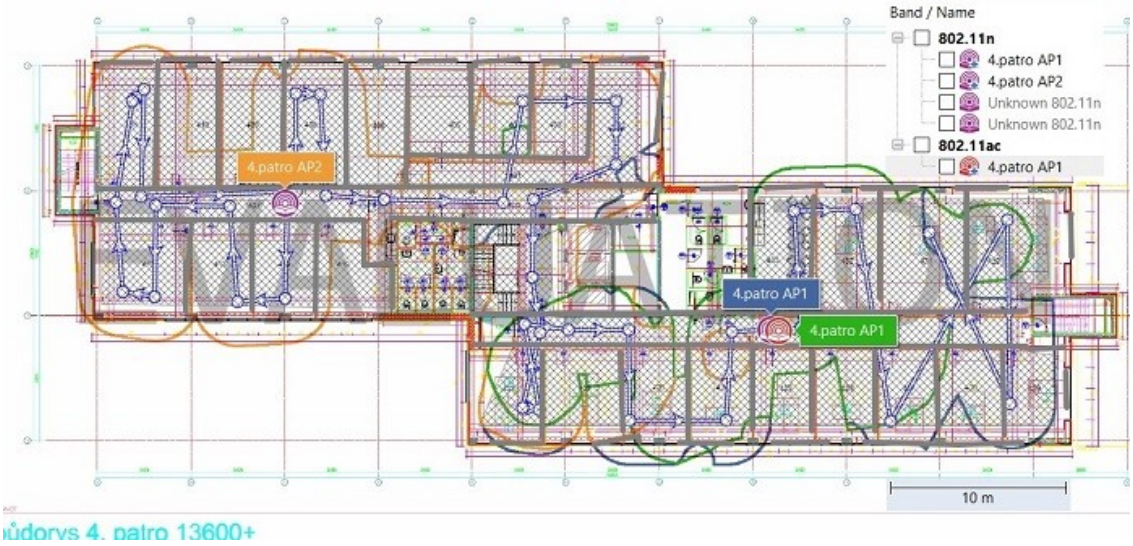
tahové šachty a kolem vedení silových kabelů, nejedná se však o extrémní hodnoty, a připojení na Wi-Fi síť by mělo být i v těchto místech stabilní. Stabilita připojení a datová propustnost bude otestována při fázi nasazení a aktivního průzkumu. Konstrukce 4. patra i ostatních nadzemních pater je z monolitického litého betonu s ocelovou výztuží a skleněnou výplní otvorů. V posledním měření je vyhodnocen poměr mezi vysílaným Wi-Fi signálem a cizími zdroji rušení (SIR). Ve 4. patře se nachází větší množství nežádoucích zdrojů rušení signálu

Wi-Fi. Externí zdroje rušení nedosahují extrémních hodnot. Vyšší mez rušení vykazují pouze již stávající instalované přístupové body v okolních patrech. Je nutné ověřit nastavení výkonu těchto přístupových bodů a případně jejich výkon snížit. Oblast pokrytí je zobrazena



Obr. 58. Pasivní průzkum 4. patro: Poměr signálu k interferencím (SIR).

různými barvami, oblast pokrytí Wi-Fi signálem jednotlivých přístupových bodů. Výsledný pasivní průzkum vykazuje dobré hodnoty a dojde při fázi nasazení k přemístění obou přístupových bodů a mírnému navýšení jejich výkonu.



Obr. 59. Pasivní průzkum 4. patro: Oblast pokrytí signálem Wi-Fi.

4.6 Shrnutí

V této kapitole je proveden a zdůvodněn výběr jednotlivých komponentů celého řešení hotspotu. Pozornost je věnována specifikaci jednotlivých komponentů a jejich funkci v systému. Zapojení jednotlivých komponentů zobrazuje schéma celého systému. V dalším odstavci je

postupně popsána konfigurace jednotlivých komponentů pomocí administrační aplikace WinBox. Vlastní zabezpečení komponentů je doporučeno provádět na nejvyšší úrovni dle ověřených postupů uváděných v technických manuálech jednotlivých produktů. Jde zejména o nastavení složitějšího hesla a omezení přístupu k administraci komponentů a taktéž i pravidelná aktualizace firmwaru komponentů. Podrobněji je popsána konfigurace centrální jednotky, nastavení centrální správy a připojení jednotlivých přístupových bodů k centrální jednotce. Dále je navržena softwarová aplikace readyVoucher, která přes podporu restAPI na produktech Mikrotik, zajišťuje kromě vytváření a odstraňování uživatelských profilů pro přístup k síti Internet, také jejich autentizaci a autorizaci, za využití vestavěného RADIUS serveru na centrální jednotce Mikrotik. Další část je věnována instalaci aplikace readyVoucher, její nastavení a konfigurace bude rozebrána v další kapitole. V závěrečné části kapitoly je nakonfigurovaná Wi-Fi část systému instalována, nastavena a umístěna dle provedeného prediktivního průzkumu v administrativním objektu. Poslední fází před vlastním nasazením celého systému je provedení pasivního průzkumu bezdrátového prostředí za použití softwarové aplikace Tamograph Site Survey a hw USB Wi-Fi klienta Zyxel NWD 6605 a verifikace konfigurace a nastavení provedených dle prediktivního průzkumu.

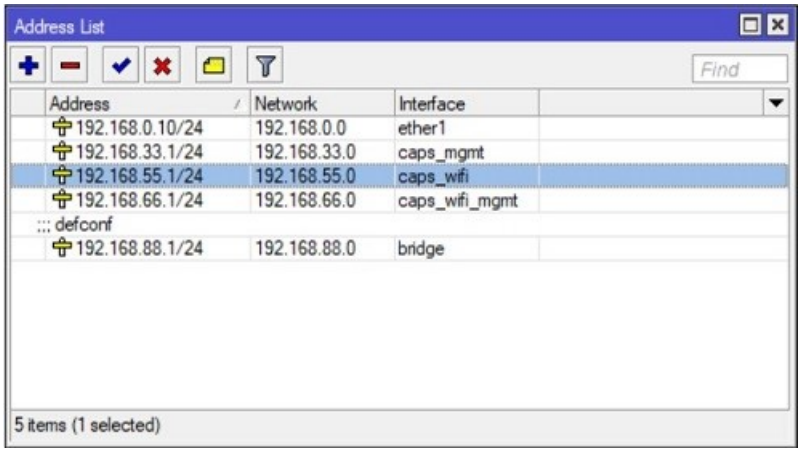
5 KONFIGURACE HOTSPOTU A READYVOUCHER

Jelikož je celý systém hotspotu navržen pro návštěvníky objektu, je nutné zabezpečit přístup k síti Internet, ke kterému budou využívat bezdrátový přístup přes vlastní bezdrátová mobilní zařízení. Z důvodu již více dostupných duálních resp. 5GHz adaptérů je systém provozován na obou nelicencovaných bezdrátových kanálech současně tedy 2.4GHz a 5GHz. Výraz „Hotspot“ označuje především veřejný přístupový bod k síti Internet. V současné době stále probíhá grantový program EU pro členské státy EU nazvaný „WiFi4EU“, jde o iniciativu na podporu volného přístupu k Wi-Fi konektivitě formou hotspotů pro občany ve veřejných prostorech, budovách, zdravotních zařízeních atd. Hotspot 2.0 je certifikovanou službou pro veřejný přístup k Internetu, založeném na standardu IEEE802.11u, který umožňuje odběrateli služby automatické přihlášení, odběr služeb na vyžádání a automatický roaming mezi dalšími Hotspoty 2.0. Jedná se tak o podporovanou, rozvíjenou a stále oblíbenou formu veřejného bezdrátového přístupu k Internetu se zvyšujícím se zabezpečením např. formou šifrované komunikace mezi klientem a hotspotem (viz. WPA3). Protokol WPA3 by měl být nasazen co nejdříve, jak jej začnou výrobci produktů podporovat např. formou aktualizace firmware zařízení. Pro potřeby „neveřejného“ administrativního objektu bude nasazen hotspot pro připojení k síti Internet integrovaný v centrální jednotce Mikrotik společně s aplikací readyVoucher, která zajišťuje správu přístupových údajů, které budou vyžadovány pro zabezpečené připojení k síti Internet.

5.1 Konfigurace hotspotu

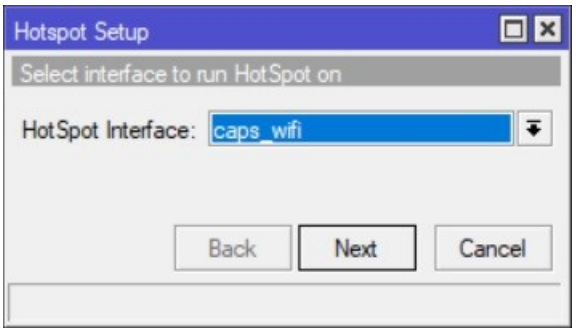
Vlastní konfigurace hotspotu se provádí na centrální jednotce, systém hotspotu je integrován v centrální jednotce Mikrotik formou vlastního balíčku, který je předinstalovaný, nebo je nutné jej stáhnout ze stránek výrobce a doinstalovat. Konfigurace hotspotu se může provádět z příkazové řádky nebo z aplikace WinBox. Po přihlášení do aplikace WinBox zadáním nastavených nebo přednastavených přihlašovacích údajů se do vlastní konfigurace hotspotu dostaneme přes hlavní menu volbou položky „IP“ a následně volbou „Hotspot“. Nejdůležitější součástí konfigurace hotspotu je zabezpečení přístupu, který je zprostředkován rodinou protokolů AAA (z anglického: Authentication, Autorization, Accounting). Centralizované zabezpečení síťového přístupu lze konfigurovat lokálně, využitím lokální databáze klientů nebo prostřednictvím RADIUS protokolu, využitím integrovaného RADIUS serveru. Nejoptimálnější volbou je použití RADIUS serveru, se kterým je plně podporován aplikací readyVoucher, která zprostředkovává vytvoření i odstranění uživatelských účtů pro autentizaci

bezdrátových klientů a další nastavení. Před vlastní konfigurací hotspotu je nutné vytvořit nový bridge nazvaný v tomto případě. „caps_wifi“ a pro tento bridge zvolit síťový rozsah, ze kterého budou následně přidělovány IP adresy bezdrátovým klientům DHCP serverem.



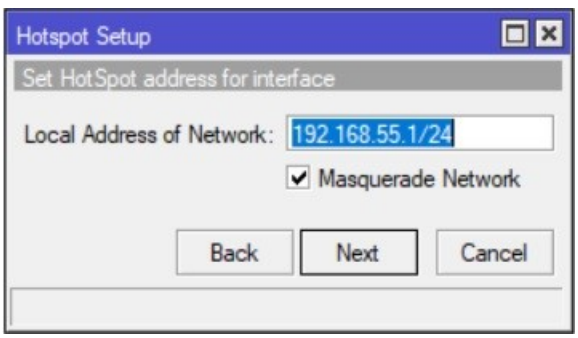
Obr. 60. Adresa rozhraní „caps_wifi“.

Následně se v otevřeném okně hotspotu na první záložce „Servers“ zvolí tlačítko „Hotspot Setup“. V prvním kroku se vybere vytvořené rozhraní pro hotspot „caps_wifi“. V dalším



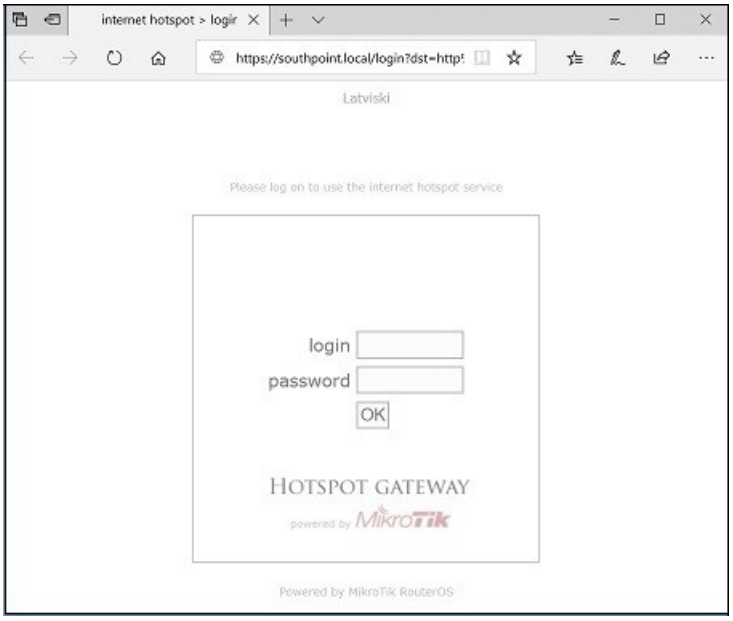
Obr. 61. Nastavení hotspotu 1.

kroku nastavení se zvolí adresa rozhraní hotspotu, která byla již dříve nastavena a přiřazena, dle předem zvoleného síťového subnetu, pro nově vytvořený bridge. V dalším nastavení je vybrán rozsah IP adres přidělovaným klientům např. 192.168.55.10-192.168.55.250. Ná-



Obr. 62. Nastavení hotspotu 2.

sledně se naimportuje certifikát vygenerovaný certifikační autoritou pro zabezpečení komunikace mezi klientem a hotspotem. Vyplní se IP adresy DNS serverů, které poskytne administrátor sítě případně poskytovatel internetového připojení. Dalším údajem, který je nutné vyplnit je doménové jméno lokálního serveru hotspotu. Tímto krokem je dokončeno základní nastavení hotspotu. Po přihlášení bezdrátového klienta k SSID „SouthPoint Hotspot" je automaticky zobrazena základní přihlašovací stránka hotspotu resp. kaptivní portál, který bude následně kustomizován do formy informačního a přihlašovacího portálu.

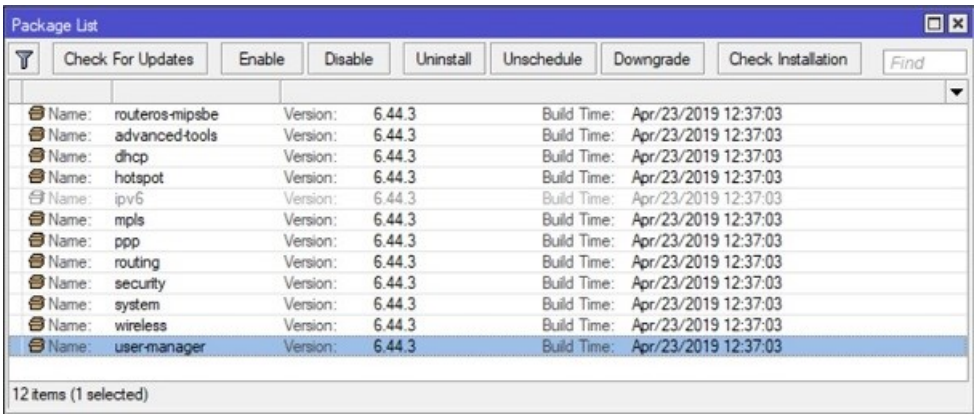


Obr. 63. Základní přihlašovací stránka hotspotu.

5.2 Konfigurace readyVoucher

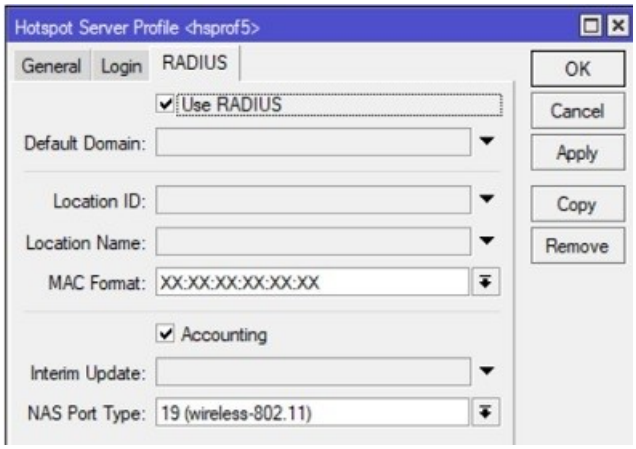
Pro správnou funkci aplikace je nutné ji nejdříve nakonfigurovat a připojit k centrální jednotce Mikrotik. Částečně se konfigurace provede přímo na centrální jednotce a zbývající část přímo v aplikaci readyVoucher. V prvním kroku se nastaví „user-manager" (správce uživatelů) v centrální jednotce, tak aby se žádosti uživatelů hotspotu dostali až ke správci uživatelů. Po tomto nastavení je možné přistoupit k vytvoření uživatelského profilu. Např. jako první se vytvoří profil, který vyprší, resp. jeho platnost se ukončí, za 1den. Nejprve se v menu centrální jednotky přesvědčíme, zda je nainstalován balíček „user-manager". Pokud balíček předinstalován není, je nutné jej doinstalovat. Před vlastní instalací balíčku se zkontroluje kompatibilita zařízení Mikrotik na stránkách výrobce, mimo jiné je vhodné zkontrolovat aktuálnost verze firmware a nainstalovat aktuální verzi, dle modelu zařízení se vybere správný archiv balíčků, který obsahuje i zmíněný „user-manager". Balíček se po stažení ze stránek výrobce dekomprimuje a přes administrační aplikaci WinBox nahraje do kořenového

adresáře centrální jednotky. Následně se provede restart zařízení a balíček by se měl objevit v menu „Systém“ položka „Packages“ jako nainstalovaný. V dalším kroku konfigurace sys-



Obr. 64. Seznam nainstalovaných balíčků.

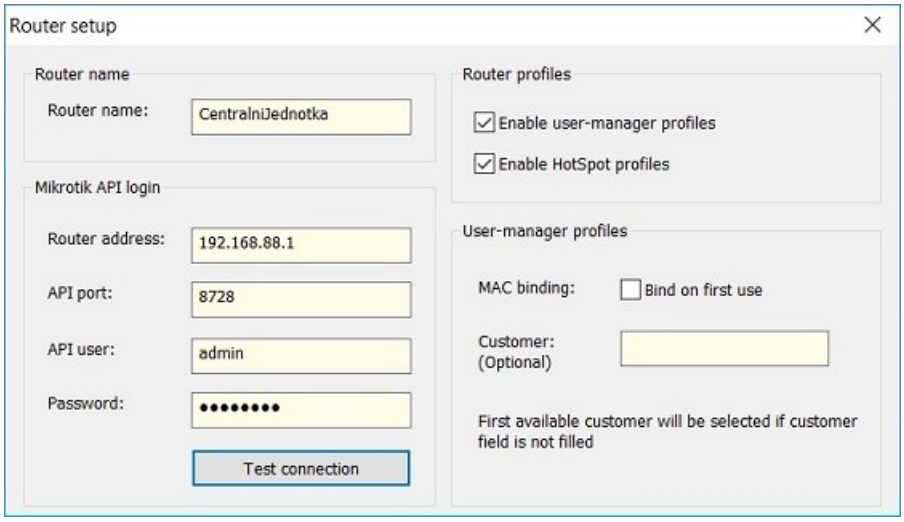
tému se provede nastavení profilu hotspot serveru. Po otevření položky „Hotspot“ se zvolí záložka „Server Profiles“ a zvolí se přiřazený profil k hotspotu. V záložce „RADIUS“ se



Obr. 65. Aktivace RADIUS serveru.

zaškrtne použití RADIUS. V následujícím kroku se vytvoří nový RADUIS server. V hlavním menu aplikace WinBox se vybere položka „RADIUS“ a v nově otevřeném okně se po kliknutí na tlačítko plus zobrazí okno pro vytvoření nového RADIUS serveru. V tomto okně se jako služba zaškrtne hotspot a vyplní se IP adresa pro lokálního hosta 127.0.0.1 a zvolí se heslo pro položku „Secret“. Následně se přes webové rozhraní aplikace „User-Manager“ nastaví základní údaje pro připojení k nově vytvořenému RADIUS serveru. Je vhodné z bezpečnostních důvodů nastavit nové heslo pro uživatele „admin“. Po nastavení údajů k připojení k RADIUS se vytvoří první testovací profil uživatele např. pro 24hodinový přístup. Po splnění těchto konfiguračních kroků je v této fázi možné přistoupit k vlastní konfiguraci aplikace readyVoucher. Aplikace se spustí poklepáním na ikonu readyVoucher.exe. Před započetím konfigurace je nutné zkontrolovat, že je povolena služba „API“, což je vlastní

rozhraní pro korektní komunikaci centrální jednotky a aplikace. V otevřené aplikaci ready-Voucher zvolíme záložku „Routers“ a vyplníme požadovaná pole. Nejdůležitější pole pro připojení k centrální jednotce jsou IP adresa routeru, port API, uživatel a heslo. Po vyplnění



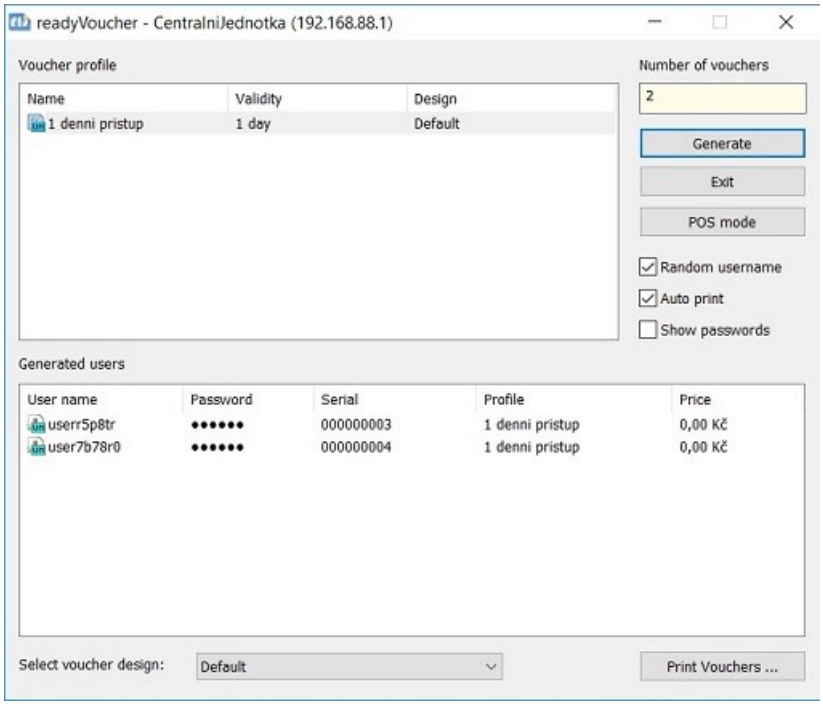
Obr. 66. Nastavení připojení k centrální jednotce.

údajů ověříme připojení k centrální jednotce kliknutím na tlačítko „Test connection“. V aplikaci se nastaví nové uživatelské jméno a heslo pro administrátora aplikace. Po dokončení nastavení nových uživatelských údajů je možné provést nové přihlášení do aplikace. Po při-

Obr. 67. Přihlašovací okno.

hlášení do aplikace by měl být zobrazen jeden tiket (voucher), který byl vytvořen v předchozí konfiguraci centrální jednotky, resp. tiket s přístupem na 1 den. Pro ověření můžeme zvolit 1denní voucher v počtu 2ks a kliknout na tlačítko „Generate“ a následně dojde k automatickému vygenerování voucherů, které obsahují uživatelské údaje a případně jiné údaje, které budou poskytnuty návštěvníkovi objektu pro připojení k hotspotu. Vygenerované údaje je

možné automaticky po jejich vygenerování vytisknout, případně jsou stále k dispozici v aplikaci. Pokud při přihlašování do aplikace zvolíme volbu „Setup“ namísto „Login“ , otevře se konfigurační část aplikace, ve které lze upravovat a vytvářet nové profily a nastavovat možnosti přístupu pro uživatele hotspotu dle potřeby.

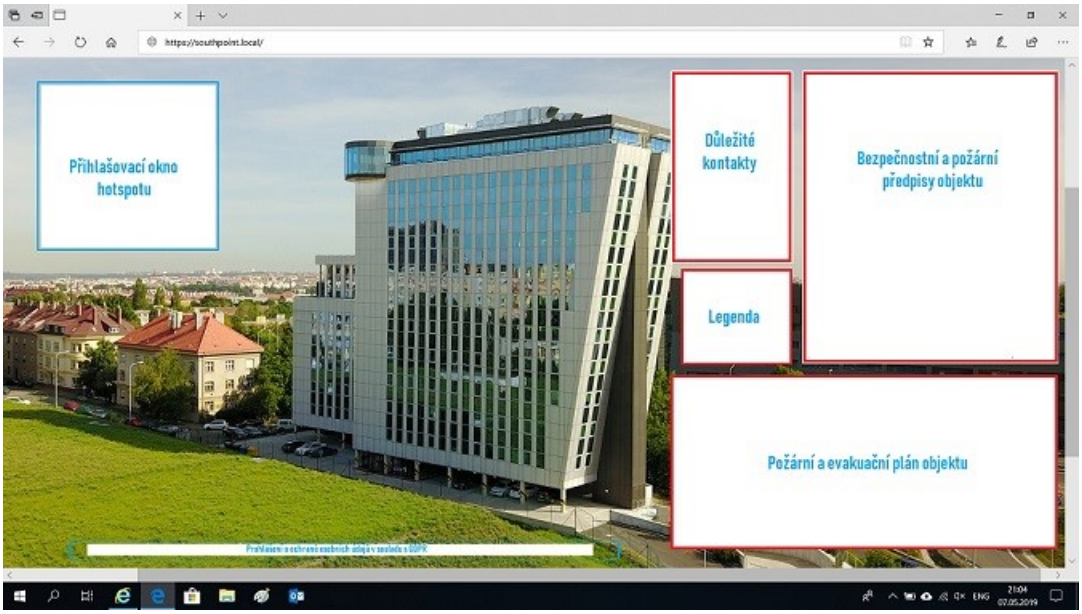


Obr. 68. Generování přístupových údajů.

5.3 Návrh a vytvoření informačního portálu

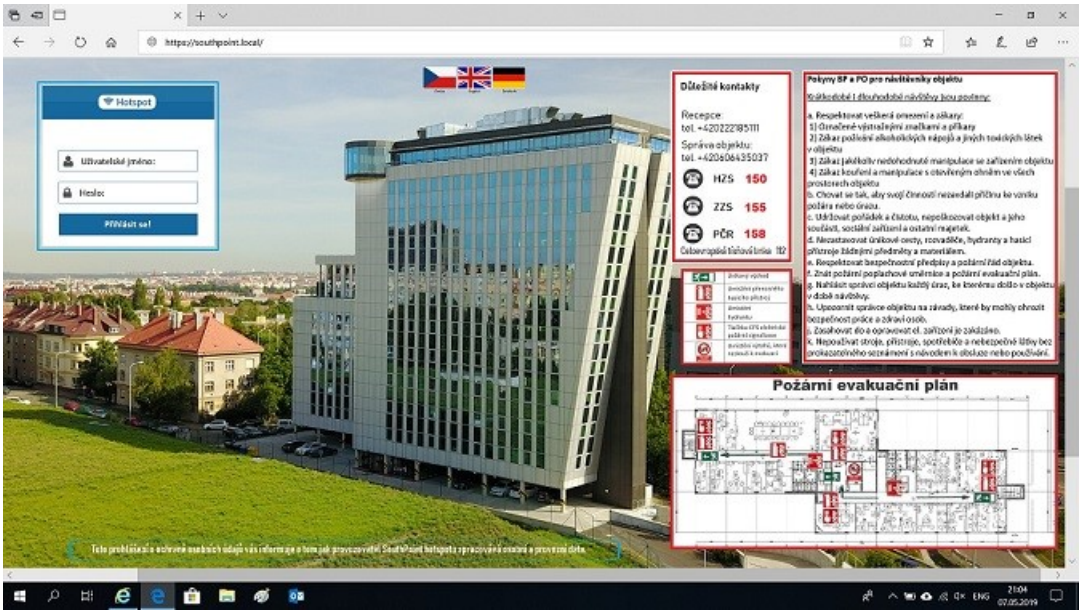
Integrovaný captive portál (přihlašovací webový portál) v zařízení Mikrotik je součástí hotspot serveru. Webový portál je možné bez omezení upravovat a základní stránka obsahuje pouze přihlašovací skript pro autentizaci uživatele a následnému přihlášení k síti Internet případně jiným sítím. Jednou ze základních vlastností je automatické načtení portálu ještě před vlastním přihlášením, je nutné se pouze připojit k Wi-Fi síti. Této vlastnosti je využito pro vytvoření informačního portálu pro návštěvníky objektu, který je volně přístupný bez nutnosti získání přístupových údajů, které jsou vygenerovány na základě žádosti v recepci objektu. Informační portál obsahuje zejména informace o objektu a vnitřních požárních a bezpečnostních předpisech a směrnicích. Na základě budoucích požadavků lze portál doplnit a upravit o další informace dle potřeby. Pro úpravu a vytvoření nového portálu je použit software Adobe Dreamweaver jako HTML editor, lze však využít jakéhokoli jiného dostupného HTML editoru. Původní verze přihlašovacího portálu, který se nachází v centrální jednotce, po přihlášení FTP klientem, ve složce \flash\hotspot bude nahrazena novou verzí portálu. V případě potřeby je portál vytvořen v různých jazykových mutacích pro potenciální

zahraniční návštěvníky objektu. Na *Obr. 69* je zobrazen základní návrh přihlašovacího a informačního portálu, který obsahuje důležité informace, které je možné kdykoliv upravovat a aktualizovat. Návrh portálu je vytvořen v aplikaci Adobe Dreamweaver ve formátu HTML



Obr. 69. Návrh informačního a přihlašovacího portálu.

pro zachování kompatibility s různými webovými prohlížeči. Mobilní verze portálu podporuje webové prohlížeče běžící na operačních systémech Android a MacOS. Následující zobrazení (*Obr. 70.*) zachycuje finální verzi vytvořeného informačního a přihlašovacího portálu administrativního objektu SouthPoint. Portál je uživateli zobrazen automaticky při připojení



Obr. 70. Informační a přihlašovací portál.

bezdrátové síti „SouthPoint Hotspot“, návštěvník objektu tak nutně nemusí disponovat přihlašovacími údaji k síti Internet a portál zůstává dostupný i bez přihlášení v celé oblasti pokryté signálem hotspotu. Vytvořený portál ve formátu HTML je následně nahrán přes vestavěný FTP server do centrální jednotky, složky /flash/hotspot/login.html.

5.4 Ochrana osobních údajů a GDPR

Směrnice o uchovávání údajů, která požadovala, aby provozovatelé hotspotů uchovávali statistická data resp. informace o uživatelích, po dobu 12 měsíců, byla zrušena Soudním dvorem Evropské unie v roce 2014. Směrnice a soukromí a elektronických komunikacích byla v roce 2018 nahrazena obecným nařízením o ochraně údajů (GDPR), které nařizuje jistá omezení při uchovávání údajů provozovatelům hotspotů. Součástí informačního a přihlašovacího portálu hotspotu je prohlášení o ochraně osobních údajů. Toto prohlášení zahrnuje zejména informace o provozovateli hotspotu, jaká statistická data jsou uchována při použití hotspotu, uživatelské údaje z voucherů, kontaktní informace provozovatele, informace o zabezpečení uchovávaných dat atd. Systém hotspotu je navržen tak, aby návštěvník objektu nemusel poskytovat žádné osobní údaje (např. jméno nebo telefonní číslo), přesto je však nutné zpracovávat a uchovávat údaje o použitém zařízení (např. MAC adresa) a další data v souladu s nařízením GDPR a zákony ČR.

5.5 Shrnutí

V této kapitole je objasněna konfigurace hotspot serveru v centrální jednotce. Dále je přehledně popsána konfigurace aplikace readyVoucher, která zabezpečuje generování přístupových uživatelských údajů za využití „User Manageru“, který je součástí centrální jednotky Mikrotik. Bezpečnost hotspotu, autentizaci a autorizaci uživatelů zajišťuje integrovaný RADIUS server. Další odstavec je věnován vygenerování přístupových údajů pro přihlášení k hotspotu. V další části kapitoly je navržen informační a přihlašovací portál, který je vytvořen ve formátu HTML v HTML editoru a následně nahrán přes FTP server do centrální jednotky. Závěrem kapitola zmiňuje legislativní požadavky na ochranu osobních údajů v souladu s evropským nařízením GDPR.

6 ZPRACOVÁNÍ MAPY POKRYTÍ A ZHODNOCENÍ SYSTÉMU

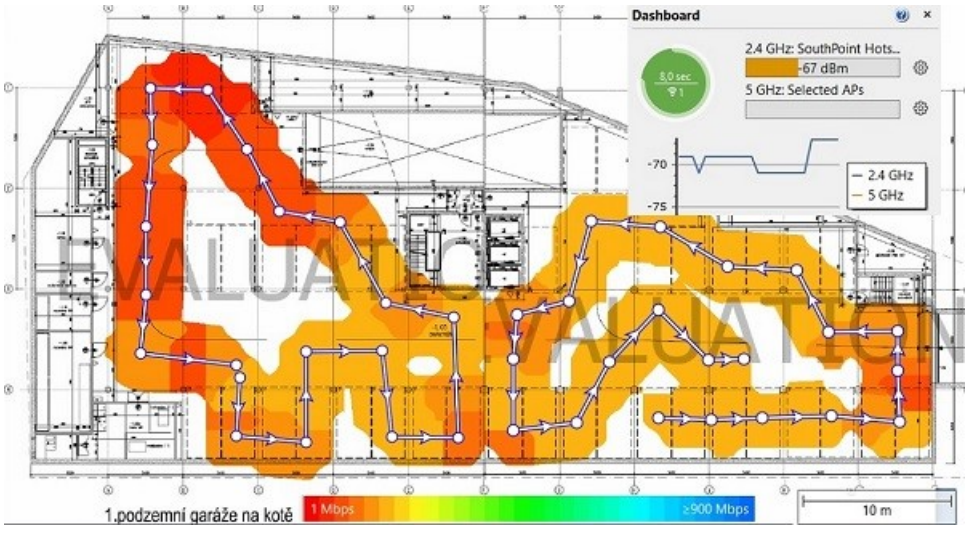
Závěrečná kapitola praktické části práce finalizuje řešení systému hotspotu provedením aktivního průzkumu lokalit a zpracováním mapy pokrytí signálem Wi-Fi v administrativní objektu. Součástí implementační fáze celého řešení je otestování funkčnosti hotspotu jednotlivými kroky od vygenerování přístupových údajů, přes přihlášení k hotspotu, až po ověření přístupu k síti Internet. V poslední části práce je zpracováno zhodnocení navrženého a realizovaného hotspotu včetně ekonomické náročnosti.

6.1 Aktivní průzkum lokality

Aktivní průzkum je proveden obdobně jako pasivní průzkum pomocí mobilního zařízení s bezdrátovým klientem Wi-Fi, v tomto případě notebook, SW Tamograph Site Survey a bezdrátový USB klient Zyxel. Po připojení k přístupovému bodu, provádí klient v módu aktivního průzkumu obdobné úlohy, jako standardně připojený Wi-Fi klient, což zahrnuje rychlost přenosu dat při změnách RF podmínek a opakování přenosů.

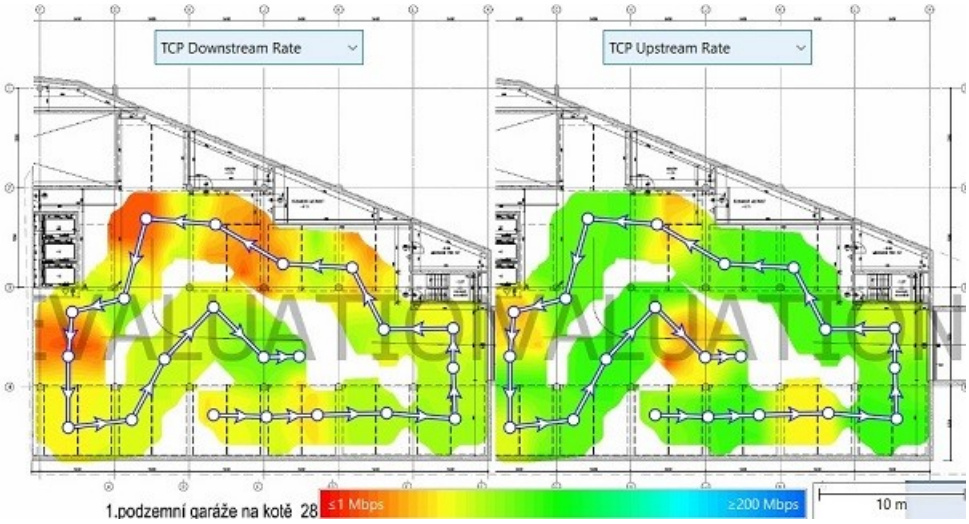
6.1.1 Aktivní průzkum lokality „Garáže -1“

V lokalitě podzemních garážích byly instalovány dva přístupové body. Bezdrátový klient se jednotlivě připojí k oběma přístupovým bodům. Před vlastním měřením je nutné nainstalovat na lokální server umístěný v síti LAN softwarový nástroj „TamoSoft Throughput Test Server“, testovací nástroj pro měření výkonosti bezdrátové nebo i drátové sítě. Aplikace je k dispozici volně ke stažení ze stránek výrobce. Naměřené aktuální přenosové hodnoty na obou



Obr. 71. Aktivní průzkum „Garáže -1“: Aktuální fyzická rychlost.

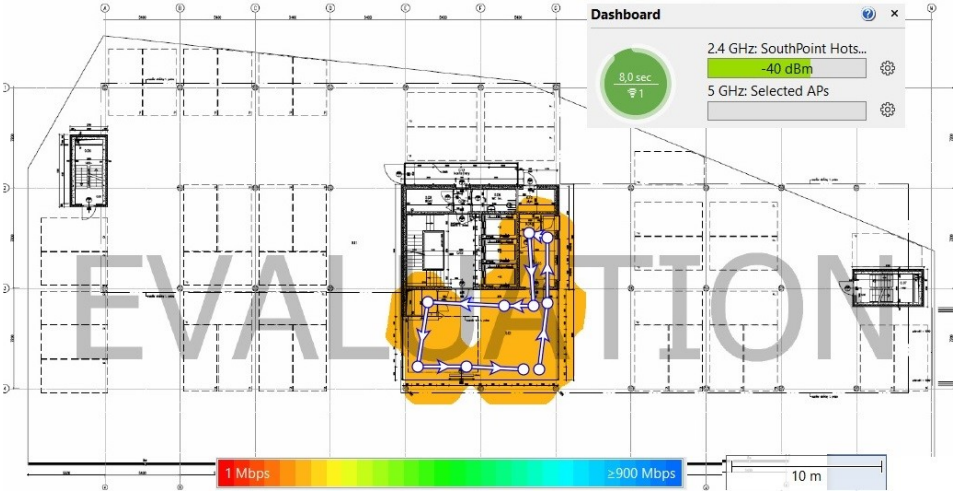
přístupových bodech dosahují rozmezí hodnot 50-144Mbit/s. Naměřené hodnoty propustnosti TCP dat (TCP downstream - propustnost směr server/klient a TCP upstream – propustnost směr klient/server) jsou zobrazeny na *Obr. 72*.



Obr. 72. Aktivní průzkum „Garáže -1“: Propustnost TCP.

6.1.2 Aktivní průzkum lokality „Recepce“

V lokalitě recepce je instalován jeden přístupový bod „Recepce AP1“, nejbližším bodě instalace infrastruktury, vykazuje měření hodnoty aktuální přenosové rychlosti 90-144Mbit/s. V dalším měření recepce jsou hodnoty propustnosti dat protokolu TCP , stejně jako u před-



Obr. 73. Aktivní průzkum „Recepce“: Aktuální fyzická rychlost.

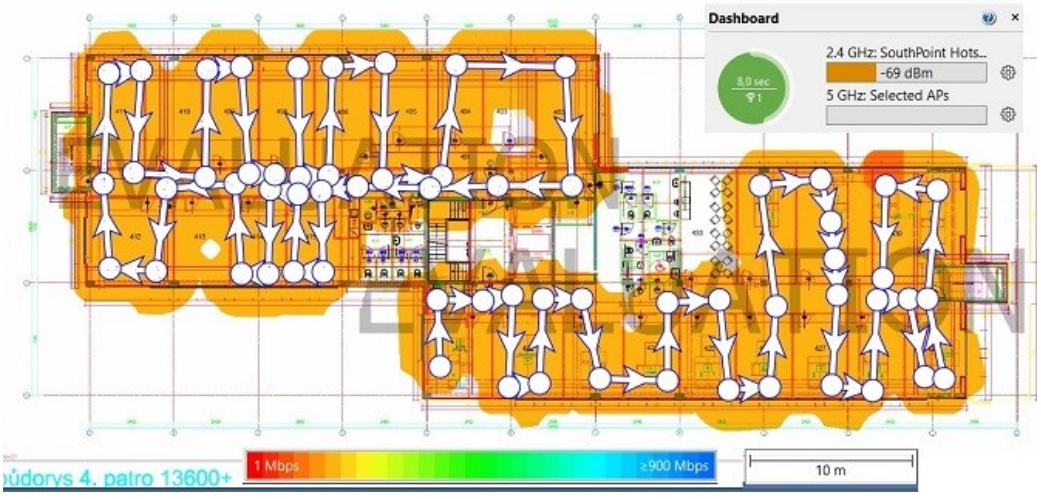
chozí lokality, „TCP downstream“ a „TCP upstream“. Umístění přístupového bodu a jeho konfigurace a nastavený výkon je pro tuto lokalitu optimální. Naměřené hodnoty propustnosti TCP dat jsou na velmi dobré úrovni. V této lokalitě je přístupový body umístěn a nakonfigurován optimálně a případná optimalizace konfigurace bude provedena po vyhodnocení budoucích výsledků průběžných průzkumů. Na následujícím *Obr. 74*. jsou zobrazeny

naměřené hodnoty propustnosti TCP v lokalitě „Recepce“, resp. hlavní vstup do prostor administrativního objektu kde návštěvník objektu, na vyžádání, obdrží přístupové údaje k hotspotu.

Obr. 74. Aktivní průzkum „Recepce“: Propustnost TCP.

6.1.3 Aktivní průzkum lokality „4. Patro“

V lokalitě „4. patro“ jsou instalovány dva přístupové body k hotspotu. Aktivní průzkum v této lokalitě je proveden jednotlivě připojením Wi-Fi klienta k přístupovému bodu. Naměřené hodnoty fyzické rychlosti tj. rychlosti mezi připojeným klientem a přístupovým bodem dosahují hodnot 90-144Mbit/s. V režimu aktivního průzkumu je k dispozici množství namě-



Obr. 75. Aktivní průzkum „4. patro“: Aktuální fyzická rychlost.

řených hodnot, nejen TCP downstream a TCP upstream, ale také propustnost protokolu UDP, ztráty paketů protokolu UDP, „Round Trip Time“, hodnoty v milisekundách, které vyjadřují čas za který je paket odeslán na server a zpět, nebo vlastní nastavení požadovaných

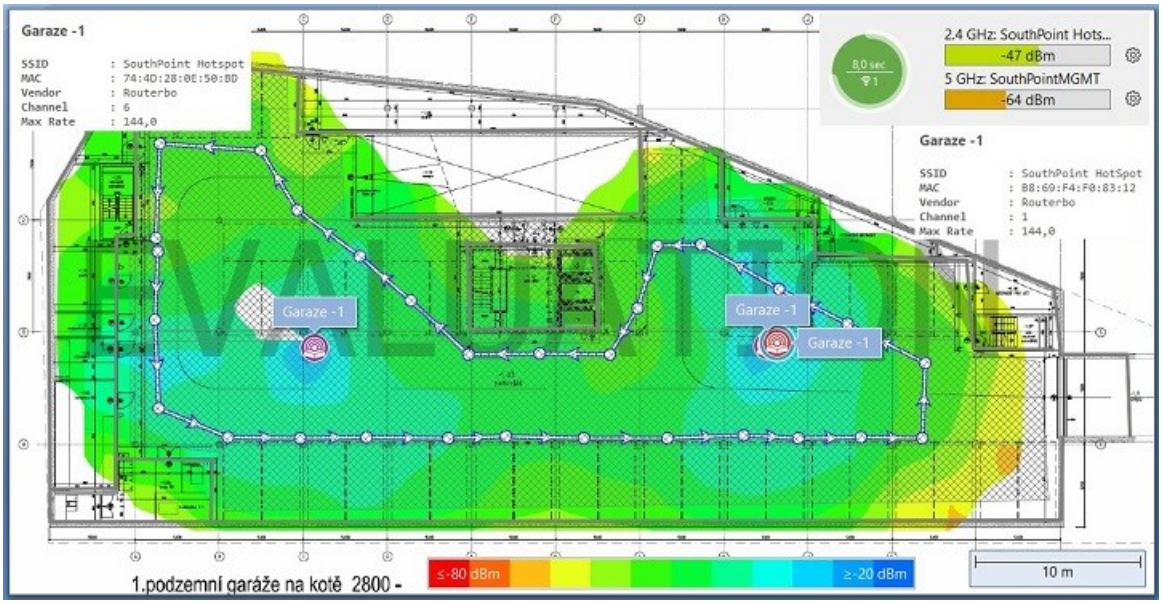
hodnot, podle kterých lze po průzkumu vyhodnotit zda nastavené podmíněné hodnoty jsou v souladu s hodnotami naměřenými.

6.2 Zpracování mapy pokrytí

Mapa pokrytí neboli „Wi-Fi heatmap“ je mapou pokrytí a úrovně bezdrátového signálu Wi-Fi v dané lokalitě. Mapa pokrytí zobrazuje skutečnou mapu místností včetně použitých konstrukčních materiálů anebo externího, venkovního prostoru pokrytého bezdrátovým signálem. Mapa pokrytí je zpracována v jednotlivých lokalitách měřením skutečného stavu po finálním umístění a konfiguraci všech přístupových bodů, které tvoří hotspot.

6.2.1 Mapa pokrytí lokality „Garáže -1“

Pro zpracování výsledné mapy pokrytí a měření je opět využit SW nástroj Tamograph Site Survey a HW USB adaptér Zyxel NWD 6605, půdorys lokality včetně vyznačených konstrukčních materiálů, které mají nebo mohou mít, vliv na šíření bezdrátového signálu Wi-Fi.



Obr. 76. Mapa pokrytí lokality „Garáže -1“.

V příloze této práce je pro názornost vložena zpracovaná mapa pokrytí ve vyšším rozlišení. Výsledné hodnoty měření úrovně signálu, propustnosti dat a přenosové rychlosti jsou velmi dobré a bezdrátové připojení k hotspotu je stabilní. Podmínky pro šíření bezdrátového signálu se mohou v čase měnit, ať již nově instalovanou technologií v objektu nebo změnou vnitřních konstrukčních materiálů, je doporučeno provádět pravidelné průzkumy lokality, případně využít některého z monitorovacích SW nástrojů pro analýzu stavu bezdrátové sítě a následnou úpravu či optimalizaci.

6.2.2 Mapa pokrytí lokality „Recepce“

V lokalitě „Recepce“ je zjištěn signál z většího množství stávajících přístupových bodů Wi-Fi na frekvenci 2.4GHz vysílajících na kanálech 1,6 a 11. Přístupový bod „Recepce“ bude vysílat na kanálu 1. Současně přístupový bod, kromě šíření signálu hotspotu na 2.4GHz, poskytuje signál Wi-Fi na 5GHz. Ve všech lokalitách je pro 5GHz rádio nastaveno SSID „SouthPoint MGMT“ a je vyhrazeno pro účely správy objektu.

Obr. 77. Mapa pokrytí lokality „Recepce“.

6.2.3 Mapa pokrytí lokality „ 4. patro“

Ve vyšším nadzemním podlaží se vyskytuje menší množství rušivých externích signálů Wi-Fi. Větší množství signálů na frekvenci 2.4GHz pochází ze stávajících zařízení Wi-Fi. V této lokalitě se nachází několik míst se sníženou úrovní signálu Wi-Fi, což způsobuje především

Obr. 78. Mapa pokrytí lokality „4. patro“.

členitost a uspořádání konstrukcí v prostoru a tím snížení dosahu bezdrátového signálu. V tomto případě je možným řešením instalace třech přístupových bodů namísto dvou.

6.3 Ověření funkčnosti systému

Ověření a testování bezdrátového připojení k hotspotu proběhlo ve všech lokalitách administrativní budovy, kde jsou přístupové body instalovány. Po příchodu do budovy je testovací uživatel (návštěvník) informován, verbálně na recepci nebo vývěskou v prostorech recepce, že je v daných lokalitách provozován hotspot s názvem „SouthPoint HotSpot“. Testovací uživatel se se svým bezdrátovým klientem připojí k Wi-Fi síti s názvem „SouthPoint HotSpot“. V jeho webovém prohlížeči se automaticky zobrazí informační a přihlašovací portál hotspotu, především s informacemi bezpečnostního charakteru, důležitými kontakty a prohlášením o ochraně osobních údajů. Vlastní přihlášení je zabezpečené a testovací návštěvník si musí vyžádat přihlašovací údaje v recepci. Na základě žádosti jsou vygenerovány přístupové údaje s časovým omezením na 24hodin. Testovací návštěvník vyplní přihlašovací údaje do přihlašovacího okna přihlašovacího portálu. Dojde k autentizaci a následné autorizaci přístupu k síti Internet. Testovací uživatel je úspěšně přihlášen. Otevřením webové stránky je ověřen přístup k Internetu. Otestování systému hotspotu proběhlo úspěšně, připojení k hotspotu je stabilní bez výpadků.

6.4 Zhodnocení funkčnosti systému

Na základě ověření a otestování celého systému lze zhodnotit navržený systém jako plně funkční. Navržené komponenty systému jsou vzájemně kompatibilní a plní svou funkci. Výsledná mapa pokrytí signálem Wi-Fi v lokalitě „Garáže -1“ vykazuje velmi dobrou úroveň signálu. V lokalitě „Recepce“ je dobré úrovně dosaženo navýšením výkonu přístupového bodu a vhodným umístěním. V lokalitě „4. patro“ se nachází několik míst se sníženou úrovní signálu, k optimálnímu pokrytí doporučuji instalovat tři přístupové body namísto dvou. Výhodou HW Mikrotik je rozhraní REST API, které využívá aplikace readyVoucher. Produkty Mikrotik disponují robustním managementem a množstvím integrovaných funkcí. Přístup k síti Internet je zabezpečen pomocí RADIUS serveru. Výhodou řešení je možnost definovat individuální uživatelské profily s časovým omezením přístupu, omezením rychlosti i množstvím přenesených dat. Komunikace klienta s webovým portálem je zabezpečena pomocí protokolu HTTPS. Webový informační a přihlašovací portál poskytuje důležité informace bez nutnosti autentizace, které lze upravovat dle potřeby. Další výhodou je dostupnost Wi-

Fi v podzemních garážích, kde je velmi nízká úroveň signálu GSM. Celý systém hotspotu je napojen na záložní zdroj UPS, který je společně s hlavními komponenty umístěn v uzamčené místnosti monitorované kamerovým systémem. Nevýhodou do budoucna by mohl být nárůst množství provozovaných Wi-Fi zařízení v objektu, vedoucí k nežádoucímu rušení signálu hotspotu. Nedílnou součástí zhodnocení navrženého systému je ekonomická náročnost, kterou shrnuje následující *Tab. 6*. V uvedené cenové kalkulaci není zahrnuta cena za provedený průzkum lokality s výsledky měření. Tato cena je obvykle stanovena individuálně dle náročnosti a rozsahu prací, v tomto případě se pohybuje v jednotkách tisíc korun.

Tab. 6. Cenová kalkulace

Produkt	**Množství**	**Jednotka**	**Cena za jednotku**	**Cena celkem bez DPH**
Mikrotik RB 960PGS	1	ks	1500,-	1500,-
TP-Link SG1005P	1	ks	1000,-	1000,-
Mikrotik cAP ac	3	ks	1200,-	3600,-
Mikrotik cAP lite	2	ks	500,-	1000,-
Kabel UTP CAT6	120	m		
Drobný instalační materiál			500,-	500,-
Montážní práce	10	h	650,-	6500,-
Webový portál	8	h	500,-	4000,-
Cena celkem bez DPH				**18 100 Kč**
Cena celkem s DPH				**21 901 Kč**
(Zkratky: ks - kus, m - metr, h - hodina)				

ZÁVĚR

V úvodu se diplomová práce věnuje historii bezdrátové technologie Wi-Fi a vzniku komunity, která se později formovala do společnosti s názvem Wi-Fi Alliance. Tato společnost sdružuje především zástupce z řad výrobců a vývojářů bezdrátových technologií Wi-Fi s neustále narůstajícím počtem členské základny. Pro společný postup při vývoji a výrobě Wi-Fi produktů, zejména z důvodu zachování kompatibility technologií, byla zavedena standardizace IEEE 802.11 pro bezdrátové sítě. Bezdrátové sítě mohou fungovat v tzv. nezávislém nebo infrastrukturním režimu. V nezávislém režimu bezdrátoví klienti komunikují přímo mezi sebou, oproti infrastrukturnímu režimu, který vyžaduje společný přístupový bod. Přístupový bod poskytuje přístup do bezdrátové sítě, typicky WLAN, a zprostředkovává její další služby např. přístup k síti Internet. Neveřejné přístupové body se zabezpečují pomocí bezpečnostních protokolů i šifrováním. U veřejných přístupových je jejich zabezpečení komplikovanější z důvodu otevřeného přístupu. Zabezpečení veřejných přístupových bodů je v současnosti řešeno obvykle prostřednictvím RADIUS serveru, jehož primární úlohou je autentizace uživatele a autorizace přístupu k bezdrátové síti. Obdobným způsobem je navržen zabezpečený přístup k internetu pro uvedený administrativní objekt. Návštěvník objektu se připojí k internetu, prostřednictvím hotspotu, pouze pomocí vygenerovaného uživatelského jména a hesla.

Cílem práce je návrh řešení a realizace navrženého řešení hotspotu pro administrativní objekt SouthPoint v Praze doplněný o vytvoření informačního přihlašovacího portálu. Před vlastním návrhem Wi-Fi komponentů byl zpracován pomocí SW nástroje prediktivní průzkum. Výsledkem tohoto průzkumu je představa o budoucím uvažovaném reálném stavu bezdrátových komponentů hotspotu ve zvolených lokalitách. Na základě prediktivního průzkumu byla vytvořena simulace jednotlivých Wi-Fi komponentů systému, jejich konfigurace i místo instalace. Před vlastním nasazením celého systému byl zpracován průzkum stávajícího stavu signálů Wi-Fi v objektu, zahrnující měření signálu a spektrální analýzu. Na základě výsledků tohoto průzkumu a především pasivního průzkumu došlo k upřesnění míst instalace a optimalizace vysílacího výkonu přístupových bodů. Po následné realizaci byl zpracován aktivní průzkum a měřeny reálné přenosové rychlosti a skutečná propustnost bezdrátové sítě. V závěrečné fázi realizace systému je zpracována mapa pokrytí pro jednotlivé lokality. Následně je celý hotspot ověřen a otestován. Z pozice návštěvníka je prověřen celý postup připojení k hotspotu. Proces zahrnuje vygenerování přístupových údajů a předání údajů návštěvníkovi objektu. Po připojení k SSID hotspotu je návštěvníkovi automaticky prezentován informační

a přihlašovací portál, s důležitými informacemi a především bezpečnostními předpisy objektu. Po zadání přístupových údajů v přihlašovacím okně portálu je povolen přístup k síti Internet.

Přínosem práce je komplexní návrh a realizace řešení zabezpečeného přístupu k internetu, prostřednictvím Wi-Fi hotspotu, pro návštěvníky administrativního objektu. Digitální formou informačního portálu, přístupného kdykoliv z různých typů mobilních bezdrátových zařízení, seznamuje návštěvníky s bezpečnostními předpisy administrativní budovy. Obdobné řešení je aplikovatelné i na jiné objekty, jako např. školy, nemocnice, obchodní centra atp.

SEZNAM POUŽITÉ LITERATURY

[1] NANNURI, Shalini. VILLANOVA UNIVERSITY. *What is WiFi* [online]. 2019 [cit. 2019-04-25]. Dostupné z: http://www.csc.villanova.edu/~nadi/csc8580/S11/ShaliniNannuri.pdf

[2] KAUSHIK, Shailandra. The Pennsylvania State University. *An overview of Technical aspect for WiFi Networks* [online]. 2019 [cit. 2019-03-07]. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.303.5672&rep=rep1&type=pdf

[3] Wikipedie: Otevřená encyklopedie. *IEEE 802.11* [online]. 2019 [cit. 2019-03-15]. Dostupné z: https://cs.wikipedia.org/wiki/IEEE_802.11

[4] BRISBIN, Shelly. *Wi-Fi: postavte si svou vlastní wi-fi síť*. Praha: Neocortex, 2003.

[5] GAST, Matthew. *802.11 wireless networks: the definitive guide*. 2. Farnham: O'Reilly, 2005.

[6] GEIER, James. *Designing and deploying 802.11 wireless networks: a practical guide to implementing 802.11n and 802.11ac wireless networks for enterprise-based applications*. 2. Indianapolis: Cisco Press, 2015.

[7] CHANDRA, Praphul. *Wireless networking*. Boston: Elsevier/Newnes, 2008.

[8] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. Brno: CP Books, 2005.

[9] ZANDL, Patrick. *Bezdrátové sítě WiFi: praktický průvodce*. Brno: Computer Press, 2003.

[10] BARKEN, Lee. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Brno: Computer Press, 2004.

[11] PEREZ, Andre. *Network security*. Hoboken, NJ: ISTE Ltd/ Wiley, 2014.

[12] GCS, Reliance. A Medium Corporation. *WPA3 Explained - Reliance GCS* [online]. 2018 [cit. 2019-04-10]. Dostupné z: https://medium.com/@reliancegcs/wpa3-explained-wi-fi-is-getting-major-security-update-2b6dca8f3aff

[13] TAMOSOFT, . Wired and Wireless Network Analysis Software by TamoSoft. *TamoGraph Site Survey* [online]. 2019 [cit. 2019-04-30]. Dostupné z: https://www.tamos.com/docs/tg_datasheet.pdf

[14] ZYXEL Communications corp. *Obrázek ve formátu JPG* [online]. 2019 [cit. 2019-04-26]. Dostupné z: https://www.zyxel.com/library/assets/products/nwd6605/img_nwd6605_main_600.jpg

[15] MikroTik. *Obrázek ve formátu JPG* [online]. 2019 [cit. 2019-03-05]. Dostupné z: https://i.mt.lv/cdn/rb_images/1220_l.jpg

[16] MikroTik. *Obrázek ve formátu JPG* [online]. 2019 [cit. 2019-03-05]. Dostupné z: https://i.mt.lv/cdn/rb_images/1449_l.jpg

[17] MikroTik. *Obrázek ve formátu JPG* [online]. 2019 [cit. 2019-03-05]. Dostupné z: https://i.mt.lv/cdn/rb_images/1277_l.jpg

[18] TP-Link. *TL-SG1005P Stolní switch s 5 gigabitovými porty* [online]. 2019 [cit. 2019-03-06]. Dostupné z: https://www.tp-link.com/cz/business-networking/unmanaged-switch/tl-sg1005p/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Wi-Fi	Obchodní značka standardu IEEE 802.11x
AP	Access Point (Přístupový bod)
WLAN	Wireless Local Area Network (Bezdrátová lokální síť)
RF	Radio Frequency (Rádiová frekvence, radiofrekvenční)
ASK	Amplitude-Shift Keying (Klíčování amplitudovým posuvem)
PSK	Phase-Shift Keying (Klíčování fázovým posuvem)
QAM	Quadrature Amplitude Modulation (Kvadraturní amplitudová modulace)
FSK	Frequency-Shift Keying (Klíčování frekvenčním posuvem)
IoT	Internet of Things (Internet věcí)
MAC	Media Access Control
dBi	Jednotka decibel na isotop
dBm	Jednotka decibel nad miliwattem
GHz	Jednotka Gigahertz
Mbit/s	Jednotka Megabit za sekundu
USB	Universal Seriál Bus
IEEE	Institute of Electrical and Electronics Engineers
GSM	Global System for Mobile Communications
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
SW	Software
HW	Hardware
BSS	Basic Service Set
ESS	Extended Service Set
SSID	Service Set Identifier

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Diplomová práce neobsahuje žádné přílohy.