Optimalizace internetové konektivity objektu U2 se zohledněním požadavků místních přístupových bodů

Bc. Jan Křepelka

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jan Křepelka**
Osobní číslo:	**A19427**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Optimalizace internetové konektivity objektu U2 se zohledněním požadavků místních přístupových bodů**
Téma práce anglicky:	**Optimization of the Internet Connectivity of the U2 Building, taking into Account the Requirements of Local Access Points**

Zásady pro vypracování

1. Proveďte literární rešerši tématu přístupových bodů a internetové konektivity.
2. Analyzujte stávající situaci konektivity objektu U2 s ohledem na pokrytí míst se zvláštními požadavky a určením.
3. Navrhněte vhodné řešení zajišťující požadavky bezpečnosti na dostupnost a výkon.
4. Navržené řešení dle možností realizujte a ověřte.
5. Vyhodnoťte formou kritické diskuse výstupy práce.

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

Seznam doporučené literatury:

1. BEČVÁŘ, Zdeněk, Pavel MACH a Ivan PRAVDA. *Mobilní sítě* [online]. V Praze: České vysoké učení technické, [2013] [cit. 2017-02-22]. ISBN 9788001053058.
2. KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.
3. *ManagementMania: profesionální dynamická znalostní síť* [online]. Wilmington USA: MANAGEMENTMANIA.COM, © 2011-2020 [cit. 2020-11-20]. ISSN 2327-3658. Dostupné z: https://managementmania.com
4. ORR, Ruby Ashby. *Sto a jedna věc co dělat, když wifi nefunguje*. Ilustroval Kenny PITTOCK, přeložil Kateřina NEJEDLÁ. Praha: Ikar, 2020. Esence. ISBN 978-80-249-4280-3.
5. SOMMERVILLE, Ian. *Software engineering*. Tenth edition. Boston: Pearson, [2016]. ISBN isbn-978-0133943030.

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **15. ledna 2021**
Termín odevzdání diplomové práce: **17. května 2021**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

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

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

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 práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- 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 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 18.5.2021

Bc. Jan Křepelka v.r.
podpis diplomanta

ABSTRAKT

Cílem diplomové práce je navrhnout a realizovat optimalizaci internetové konektivity na budově U2, což je sídlo Fakulty managementu a ekonomiky Univerzity Tomáše Bati ve Zlíně. V teoretické části práce pojednává o principu fungování bezdrátových sítí, modulačních metodách, standardizačních a regulačních organizacích a také o negativních vlivech, které se mohou v oblasti bezdrátových sítí vyskytnout. Dále jsou v teoretické části přiblíženy možnosti zabezpečení bezdrátových sítí, autentizační metody a protokoly. Praktická část práce se zaměřuje na analýzu aktuálního stavu internetové konektivity pomocí vybraných hardwarových a softwarových prostředků. Dále se práce zabývá návrhem a realizací změn, které vychází z provedené analýzy. Práce se poté zaměřuje na analýzu stavu po provedení změn a přibližuje dopady optimalizace v zájmových prostorách. Nedílnou součástí praktické části práce je také analýza zabezpečení bezdrátové sítě.

Klíčová slova: bezdrátové sítě, internetová konektivita, přístupové body, optimalizace, bezpečnost

ABSTRACT

The aim of the diploma thesis is to optimize and realize Internet connectivity in the building U2, which is residence of the Faculty of Management and Economics of Tomas Bata University in Zlín. The theoretical part concentrates on the principle of operation of wireless networks, modulation methods, standardization and regulatory organizations, as well as the negative effects that may occur in the field of wireless networks. Furthermore, the theoretical part describes the security options of wireless networks, authentication methods and protocols. The practical part of the work focuses on analyzing the current state of Internet connectivity using selected hardware and software tools. Moreover, the work deals with the idea and implementation of changes based on the analysis. The work then concentrates on studying the state after the changes and depicts the effects of optimization in the areas of interest. An integral part of the practical section of the work is also the analysis of wireless network security.

Keywords: wireless networks, Internet connectivity, access points, optimization, security

Tímto bych chtěl poděkovat panu prof. Mgr. Romanu Jaškovi, Ph.D., DBA, za cenné rady a odborné vedení při zpracování této diplomové práce.

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

OBSAH

ÚVOD **9**

I TEORETICKÁ ČÁST **11**

1 BEZDRÁTOVÉ SÍTĚ **12**

1.1 HISTORIE BEZDRÁTOVÝCH SÍTÍ 12

1.2 RADIOVÉ FREKVENCE 12

1.3 FREKVENČNÍ PÁSMA 14

1.3.1 Frekvenční pásmo 2,4 GHz 14

1.3.2 Frekvenční pásmo 5 GHz 14

1.3.3 Frekvenční pásmo 60 GHz 14

1.4 MODULAČNÍ TECHNIKY 15

1.4.1 Modulační technika DSSS 15

1.4.2 Modulační technika OFDM 15

1.4.3 Technologie MIMO 15

1.5 REGULAČNÍ ORGÁNY A STANDARDIZAČNÍ ORGANIZACE 16

1.5.1 Regulační orgány 16

1.5.1.1 Agentura FCC 16

1.5.1.2 Organizace ETSI 17

1.5.2 Standardizační organizace 17

1.5.2.1 Organizace IEEE 17

1.5.2.2 Wi-Fi Alliance 17

1.6 CHARAKTERISTIKY BEZDRÁTOVÝCH SÍTÍ 18

1.6.1 Model Free Path Loss 18

1.6.2 Absorpce 18

1.6.3 Odraz 18

1.6.4 Vícecestnost 19

1.6.5 Rozptyl 19

1.6.6 Lom 19

1.6.7 Zorná přímka 19

1.7 STANDARDY 802.11 20

1.7.1 Původní standard 802.11 20

1.7.2 Standard 802.11a 20

1.7.3 Standard 802.11b 20

1.7.4 Standard 802.11g 21

1.7.5 Standard 802.11n 21

1.7.6 Standard 802.11ac 21

1.7.7 Standard 802.11ax 21

1.8 ŘADIČE BEZDRÁTOVÉ SÍTĚ 22

1.9 ROAMING 23

1.9.1 Roaming vrstvy 2 24

1.9.2 Roaming vrstvy 3 24

2 ZABEZPEČENÍ A AUTENTIZACE **26**

2.1 AUTENTIZACE 26

2.1.1 Jednoduchá autentizace 26

2.1.2 Centralizovaná autentizace 26

2.1.3 Standard 802.1X 27
2.1.3.1 Autentizační server 28
2.2 METODY EAP 28
2.2.1 Protokol EAP 29
2.2.2 Metoda EAP-TLS 29
2.2.3 Metoda EAP-FAST 30
2.2.4 Protokol PEAP 32
2.3 OVĚŘOVACÍ PROTOKOLY 34
2.3.1 Protokol PAP 34
2.3.2 Protokol CHAP 35
2.3.3 Protokol MS-CHAPv1 a MS-CHAPv2 35
2.3.4 GTC 35
2.4 METODY ZABEZPEČENÍ 36
2.4.1 Zabezpečení WEP 36
2.4.2 Zabezpečení WPA 36
2.4.3 Zabezpečení WPA2 39
2.4.4 Zabezpečení WPA3 40
II PRAKTICKÁ ČÁST 41
3 STÁVAJÍCÍ STAV KONEKTIVITY NA BUDOVĚ U2 42
3.1 HISTORICKÝ VÝVOJ INTERNETOVÉ KONEKTIVITY NA BUDOVĚ U2 42
3.1.1 Metalická datová infrastruktura 42
3.1.2 Bezdrátová síť 43
3.2 POUŽITÉ PROSTŘEDKY 44
3.2.1 Softwarové prostředky 44
3.2.2 Hardwarové prostředky 45
3.3 ANALÝZA ROZMÍSTĚNÍ PŘÍSTUPOVÝCH BODŮ A IDENTIFIKACE MÍST SE ZVLÁŠTNÍMI POŽADAVKY 46
3.3.1 Plán prvního podzemního podlaží 47
3.3.2 Plán prvního nadzemního podlaží 48
3.3.3 Plán druhého nadzemního podlaží 49
3.3.4 Plán třetího nadzemního podlaží 49
3.3.5 Plán čtvrtého nadzemního podlaží 50
3.3.6 Plán pátého nadzemního podlaží 50
3.3.7 Analýza budovy a míst se zvláštním určením 51
3.4 POUŽÍVANÉ TYPY AP 52
3.4.1 Cisco AIR CAP1602I 52
3.4.2 Cisco AIR CAP1702I 53
3.4.3 Cisco AIR CAP1832I 53
3.5 NASTAVENÍ BEZDRÁTOVÉHO ŘADIČE 54
3.5.1 Nastavení bezdrátového řadiče pro 2,4 GHz frekvenci 54
3.5.2 Nastavení bezdrátového řadiče pro 5 GHz frekvenci 55
3.6 MODEL STÁVAJÍCÍHO STAVU POKRYTÍ 56
3.7 MĚŘENÍ POKRYTÍ 57
3.7.1 Výsledky měření signálu v prvním podzemním podlaží 58
3.7.2 Výsledky měření signálu v prvním nadzemním podlaží 59
3.7.3 Výsledky měření signálu ve druhém nadzemním podlaží 60

3.7.4 Výsledky měření signálu ve třetím nadzemním podlaží 61
3.7.5 Výsledky měření signálu ve čtvrtém nadzemním podlaží 61
3.7.6 Výsledky měření signálu v pátém nadzemním podlaží 62
3.7.7 Analýza aktuálního stavu 62
4 OPTIMALIZACE INTERNETOVÉ KONEKTIVITY 63
4.1 OPTIMALIZAČNÍ MODEL 63
4.2 NÁVRHY NA PŘENASTAVENÍ BEZDRÁTOVÉHO ŘADIČE 64
4.2.1 Nastavení bezdrátového řadiče pro 2,4 GHz frekvenci 64
4.2.2 Nastavení bezdrátového řadiče pro 5 GHz frekvenci 65
4.3 DISLOKAČNÍ NÁVRHY 66
4.3.1 Plán prvního podzemního podlaží po provedení změn 66
4.3.2 Plán prvního nadzemního podlaží po provedení změn 67
4.3.3 Plán druhého nadzemního podlaží po provedení změn 68
4.3.4 Plán třetího nadzemního podlaží po provedení změn 69
4.3.5 Plán čtvrtého nadzemního podlaží po provedení změn 69
4.3.6 Plán pátého nadzemního podlaží po provedení změn 70
4.3.7 Souhrn změn a jejich účel 71
4.4 MĚŘENÍ SIGNÁLU PO REALIZACI ZMĚN 72
4.4.1 Výsledky měření prvního podzemního podlaží po realizaci 72
4.4.2 Výsledky měření druhého nadzemního podlaží po realizaci 74
4.4.3 Výsledky měření třetího nadzemního podlaží po realizaci 75
4.4.4 Výsledky měření čtvrtého nadzemního podlaží po realizaci 76
4.4.5 Výsledky měření pátého nadzemního podlaží po realizaci 77
4.5 ANALÝZA CELKOVÉHO STAVU PO OPTIMALIZACI 78
4.6 ZABEZPEČENÍ BEZDRÁTOVÉ SÍTĚ 79
ZÁVĚR 82
SEZNAM POUŽITÉ LITERATURY 84
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 88
SEZNAM OBRÁZKŮ 91
SEZNAM TABULEK 93
SEZNAM PŘÍLOH 94

ÚVOD

S bezdrátovými sítěmi se dnes setkáváme každý den, protože jsou všudypřítomné a všichni z nás je již považují za standard. Sítě každý z nás využívá téměř každý den ať již pro práci, studium či zábavu. Vyskytují se v dopravních prostředcích, parcích, obchodních domech, školách nebo úřadech a na mnoha dalších místech, což ilustruje, jak jsou pro nás důležité. Jde o odvětví, které proniklo do našich každodenních životů a stále se rozvíjí a zdokonaluje a život bez nich si dnes mnoho lidí nedokáže představit.

Tématem diplomové práce je optimalizace internetové konektivity na budově U2, což je sídlo Fakulty managementu a ekonomiky Univerzity Tomáše Bati ve Zlíně. Cílem této práce je vhodným způsobem navrhnout a provést optimalizaci internetové konektivity s důrazem na bezpečnost a kontinuitu provozu bezdrátových sítí. K dosažení cíle je nejprve nutné provést analýzu aktuálního stavu internetové konektivity na fakultě a poté vytvořit a realizovat návrhy, které povedou k celkové optimalizaci konektivity. Nakonec bude nutné analyzovat dopady provedených změn a ověřit tak dopady optimalizace.

Teoretická část práce se zabývá problematikou bezdrátových sítí jako celku a přibližuje především princip fungování bezdrátových sítí. V této části se práce věnuje historii bezdrátových sítí, frekvenčním pásmům a modulačním technikám. Dále se také zabývá regulačními orgány a standardizačními organizacemi, které se bezdrátovými sítěmi zabývají. V této části budou také přiblíženy negativní faktory, které je nutné brát v úvahu při správě a návrhu bezdrátových sítí. Také je nutné přiblížit standardy používané v bezdrátových sítích a dále řadiče bezdrátových sítí a síťový roaming. Ve druhé polovině teoretické části se práce věnuje zabezpečení bezdrátových sítí. Práce přiblíží obecné metody autentizace a také jednotlivé používané metody autentizace, používané protokoly a metody zabezpečení.

Praktická část práce je rozdělena do tří logických fází. V první fázi je nutné provést analýzu aktuálního stavu internetové konektivity v budově Fakulty managementu a ekonomiky. V této části práce zkoumá historický vývoj síťové infrastruktury v budově a přibližuje technické prostředky, které jsou použity k optimalizaci. Také dojde k analýze aktuálního rozmístění přístupových bodů v budově a jejich aktuální konfigurace. Dále dojde k identifikaci míst, které mají zvláštní určení a k jejich rozdělení do kategorií dle požadavků na kvalitu připojení. Dále bude vytvořen model budovy, který bude co nejpřesněji reflektovat skutečnost a bude použit k simulaci prováděných změn a jejich dopadům. Poté se práce zaměří na měření signálu ve všech prostorách budovy a získané výsledky budou

porovnány s vytvořeným modelem. Druhou fází praktické části práce bude příprava scénářů, jejichž účelem bude optimalizace internetové konektivity v celé budově. Vytvořený model a výstupy z analýz z předchozí fáze práce se použijí k optimalizaci míst, kde je identifikováno nedostatečné pokrytí. Optimalizace se bude provádět dislokačními změnami a úpravou konfigurace jednotlivých přístupových bodů. Po vytvoření scénářů dojde k jejich aplikaci. Poslední fází praktické části bude opětovné měření všech prostor v budově za účelem analýzy reálných dopadů provedených změn. Nakonec dojde k analýze všech dat, výstupů a zjištěných skutečností jejichž účelem bude shrnout jaké měly provedené změny dopady a jakými metodami jich bylo dosaženo.

I. TEORETICKÁ ČÁST

1 BEZDRÁTOVÉ SÍTĚ

V této kapitole bude rozebrána problematika bezdrátových sítí. Nejprve bude popsán historický vývoj, dále používaná pásma, modulační techniky a regulační orgány. Poté práce přiblíží negativní vlivy, které se mohou v bezdrátových sítích vyskytnout. Bude zde také popsán vývoj norem, které se vztahují k bezdrátovým sítím. Bude také přiblížen princip roamingu a řadičů bezdrátových sítí.

1.1 Historie bezdrátových sítí

V roce 1990 začalo docházet k pronikání bezdrátové technologie na trh, ovšem technologie bezdrátového přenosu byla popsána již v roce 1800. Tato technologie byla objevena v roce 1800 a to Wiliemem Herschelem, který při svých pokusech objevil infračervené světlo, které je nemožné spatřit. Michael Faraday a André-Marie Ampére prováděli výzkumy, z nichž vycházel James Maxwell. Tyto výzkumy poté vedly k teorii elektromagnetických vln. Na základě Maxwellových výzkumů bylo Heinrichem Hertzem dokázáno, že elektromagnetické vlny jsou schopné přenášet elektřinu a pohybují se rychlostí světla.

Souvislost mezi bezdrátovými sítěmi a těmito objevy je více než jasná. Bez těchto objevů by nebylo možné bezdrátový přenos realizovat. V síti LAN (Local Area Network) dochází k přenosu dat, které jsou ve formě elektrických signálů pomocí kabelů. Učiněné objevy znamenaly, že tato data je možné přenášet ve formě elektrických signálů i vzduchem. Tato forma přenosu se označuje jako RF (rádiová frekvence) a vděčíme za ni objevům Herchela, Maxwella, Ampéra a Hertze. Tento typ sítí je označován jako WLAN (Wireless LAN), tedy síť LAN bez využití kabelů.

Radiové frekvence se využívají pro bezdrátové přenosy, ať už se jedná o jakýkoli typ přenosu (televizní vysílání, rádiové vysílání, mobilní síť). Na přenos pomocí RF jsou kladeny stejné požadavky jako na klasické přenosy, tj. posílání co největšího objemu dat, co možná nejvyšší rychlostí a na co největší vzdálenost. U bezdrátových přenosů ovšem existují mnohé negativní faktory, které mají velký vliv na výše zmíněné požadavky u bezdrátových přenosů a je nutné je zohlednit. [1, 2]

1.2 Radiové frekvence

Radiová frekvence je úzce spjatá s elektromagnetickým spektrem. Elektromagnetické spektrum začíná u extrémně nízkých frekvencí označovaných jako ELF (Extreme Low

Frequency) a jde o kmitočty 3-30 Hz, až po extrémně vysoké frekvence označované jako EHF (Extreme High Frequency) kde jde o kmitočty 30-300 GHz. Provoz WLAN sítí neprobíhá v těchto frekvencích, ovšem je využíváno frekvenčních pásem 900 MHz (pouze v USA), 2,4 GHz, 5 GHz a také 60 GHz. V těchto pásmech probíhá provoz Wi-Fi sítí a internetový bezdrátový provoz. Tato pásma se označují jako nelicencovaná pásma. Standardní měrnou jednotkou je jednotka hertz, která udává počet cyklů za vteřinu.

Všechny frekvenční pásma jsou spravovány organizacemi, které zajišťují jejich rozdělení a správu. Dále definují, jaký typ provozu bude v jednotlivých pásmech probíhat. V USA spravuje frekvenční pásma organizace FCC (Federal Communications Commission), v Evropě organizace ETSI (European Telecommunications Standards Institute). Tyto organizace budou blíže přiblíženy v kapitole 1.5. Toto rozdělení dané organizací musí každý výrobce a uživatel zařízení striktně dodržovat. Organizace FCC navíc definuje také úrovně výkonu WLAN zařízení, jaké je možné využít přenosové technologie a také místa, kde mohou být WLAN zařízení nasazena. Tyto organizace spolupracují, což znamená, že frekvenční pásma jsou definovány pro celý svět podobně. Existují jen malé rozdíly v rozdělení a povolených frekvenčních pásmech. Tato spolupráce znamená, že při cestování po světě je každé zařízení schopné se připojit k libovolné WLAN síti, jelikož provoz probíhá na stejných frekvencích v Evropě, v USA i v Asii.

Pro odesílání a přijímání dat jsou definovány standardy 802.11, které definovala organizace IEEE (Institute of Electrical and Electronics Engineers). Tyto standardy definují half-duplexový provoz s využitím stejné frekvence. Tyto standardy musí být v souladu s pravidly dané organizací FCC, i přesto, že nepotřebují licenci. K odesílání a příjmu dat pomocí bezdrátového signálu je ovšem zapotřebí upravit data tak, aby bylo možné z nich vytvořit RF signál. K tomu je využívána modulační technika. Modulace je vlastně přidání dat k přenosovému signálu. [3, 4]

Obrázek 1 Radiové spektrum [4]

1.3 Frekvenční pásma

Všechny frekvence radiového spektra jsou rozděleny do frekvenčních pásem. Frekvenční pásmo udává rozsah použitelných frekvencí. Pro WLAN sítě jsou definovány frekvenční pásma 900 MHz (využíváno pouze v USA), a dále se pro provoz WLAN sítí používají frekvenční pásma 2,4 GHz, 5 GHz a také 60 GHz.

1.3.1 Frekvenční pásmo 2,4 GHz

Šlo o nejpoužívanější frekvenční pásmo ve WLAN sítích a využívají jej standardy IEEE 802.11, 802.11b, 802.11g, 802.11n a 802.11ax. Rozsah využitelných frekvencí v tomto pásmu začíná na 2,4 GHz a končí na 2,483 GHz. V tomto rozsahu je využíváno 11 kanálů o šířce kanálu 22 MHz. Zde ovšem mohou vznikat problémy, jelikož se některé kanály překrývají s ostatními. Proto se využívá nejvíce kanálů 1, 6 a 11, jelikož se nepřekrývají. Díky tomu je možné, aby v jednom prostoru pracovali tři nepřekrývající se kanály, jelikož se kanály vzájemně neruší. Ovšem nová zařízení umožňují nastavit šířku kanálu, což sice snižuje počet využitelných kanálů, ovšem pokud je kanál širší, tak při použití vhodné modulační techniky vznikne mnohem více pomocných nosných vln a rychlost přenosu tak narůstá. [5]

1.3.2 Frekvenční pásmo 5 GHz

V dnešní době se jedná o velmi používané frekvenční pásmo, jelikož podporuje mnohem vyšší přenosové rychlosti než frekvenční pásmo 2,4 GHz. První zařízení, které podporovalo standard 802.11a, který využíval frekvenci 5 GHz bylo na trhu dostupné až v roce 2001. V tomto frekvenčním pásmu jsou dnes využívány standardy 802.11a, 802.11n, 802.11ac a 802.11ax. I toto pásmo je rozděleno na několik kanálů, přičemž existuje 23 nepřekrývajících se kanálů. V jednom prostoru tedy může pracovat až 23 různých kanálů, aniž by se vzájemně rušily. [5]

1.3.3 Frekvenční pásmo 60 GHz

V posledních letech bylo podporováno přijetí tzv. multi-gigabitové bezdrátové technologie. Sdružení Wireless Gigabit Alliance byla zahrnuta pod organizaci Wi-Fi aliance v roce 2013. Toto pásmo podporuje mnohem vyšší přenosové rychlosti než pásma 2,4 GHz a 5 GHz. Je proto ideální na venkovní bezdrátové spoje. Vznikl také standard 802.11ad, který v tomto

pásmu pracuje. V lednu roku 2020 byla vydána všeobecná oprávnění českým telekomunikačním úřadem která umožňují využívat toto pásmo v ČR. [6]

1.4 Modulační techniky

Jak již bylo řečeno, modulace je ve skutečnosti přidání dat k přenosovému signálu, a to pozměněním signálu. Pomocí modulace jsou tedy odesílána data bezdrátově s pomocí rádiového signálu. Pozměňuje se jedna ze tří částí modulované vlny. Může jít o amplitudu, fázi a frekvenci signálu. Různé standardy bezdrátových sítí používají různé modulační techniky.

1.4.1 Modulační technika DSSS

DSSS (Direct Sequence Spread Spectrum) je modulační technikou přímého rozloženého spektra. Tento signál se rozprostírá v celém frekvenčním spektru. Pokud tedy přístupový bod bude přenášet data na kanálu 1, signál se rozloží napříč 22 MHz kanálem v rozsahu 2,401-2,423 GHz. Při přenosu je každý bit nahrazen sekvencí bitů, jenž se označují jako čipy a které mají pseudonáhodný charakter. Tyto sekvence bitů se vytváří například Barkerovými kódy. Modulační technika DSSS je využívána standardy 802.11 a 802.11b. [7]

1.4.2 Modulační technika OFDM

OFDM (Orthogonal Frequency Division Multiplexing) není považována za technologii rozprostřeného spektra, přesto je však využívána pro modulaci signálu v bezdrátových sítích. Jde spíše o širokopásmovou modulaci, která využívá frekvenční dělení kanálu. Každý kanál a jeho frekvenční rozsah je rozdělen na několik pomocných nosných vln, které mají menší šířku pásma. Pomocné nosné vlny mají šířku 300 kHz, což znamená, že v jednom kanálu je k dispozici 50 pomocných nosných vln. Každá z těchto vln má nízkou rychlost přenosu, ovšem tím, že jsou data odesílána paralelně všemi pomocnými vlnami najednou je možné dosáhnout mnohem vyšších přenosových rychlostí než u modulační techniky DSSS. Navíc je přenosový signál odolnější vůči poškození dat interferencemi. Pomocné vlny je také možná dále modulovat dalšími technikami jako je QPSK nebo QAM. Tuto modulační techniku využívají standardy 802.11a, 802.11g, 802.11n a 802.11ac. [5]

1.4.3 Technologie MIMO

MIMO (Multiple-Input Multiple-Output) není přímo modulační technika, ale jde o technologii, která se v posledních letech velmi prosazuje v bezdrátových přenosech

a zařízeních. Tato technologie pracuje s abstraktním matematickým modelem a využívá několik antén. Využívá se označení 3x3 MIMO nebo ekvivalent, kdy čísla značí počet antén využívaných pro odesílání a pro příjem signálu. V případě 3x3 MIMO jsou v zařízení tři antény pro odesílání a tři antény pro příjem signálu. Tato technologie tedy výrazně navyšuje přenosovou rychlost mezi bezdrátovými zařízeními a to tak, že jedním kanálem je odesíláno více datových proudů. Tato technologie je zpětně kompatibilní, může tedy komunikovat i se zařízeními, která MIMO nepodporují. V dnešní době je možné se setkat s termínem MU-MIMO. MU-MIMO (Multi-User MIMO) funguje stejně jako technologie MIMO, ovšem pro více uživatelů současně. Přístupový bod, podporující technologii MU-MIMO vysílá datové toky několika zařízením současně, což zvyšuje celkovou kapacitu sítě. S technologií MIMO pracují standardy 802.11n, 802.11ac a 802.11ax. [2, 8]

1.5 Regulační orgány a standardizační organizace

Jak již bylo zmíněno, existují různé regulační orgány, které mají na starost rozdělování a správu frekvenčních pásem, definují maximální výkony antén, použitelné přenosové technologie a umístění WLAN zařízení. Existují však i další organizace, které nejsou zaměřeny na regulace, ale vytváří standardy nebo kontrolují kompatibilitu a dodržování vydaných regulací a standardů.

1.5.1 Regulační orgány

Regulační organizace nastavují pravidla, dle kterých se musí výrobci a uživatelé řídit. Tyto organizace mohou mít působnost v daném státě, ale také existují globální komise, které nastavují globální pravidla. Tato pravidla a jejich dodržování jsou nutná a díky nim je možné se se stejným zařízením připojit k bezdrátové síti kdekoli na světě. Pokud by tato pravidla nebyla zavedena globálně a každý kontinent měl svá pravidla, došlo by k nekompatibilitě mezi zařízeními a v každé zemi bychom museli používat zařízení, která by splňovala pravidla země, ve které se nacházíme. [1, 9]

1.5.1.1 Agentura FCC

Nezávislá agentura FCC má působnost v USA. Vznikla v roce 1934 a vydává pravidla pro více než 50 států. Poskytuje také spolupráci, vedení a dohled podobným organizacím v severní Americe. Jde o agenturu přímo se zodpovídající kongresu a má na starost nelicencované frekvenční rozsahy, zabývá se také různými typy zařízení a udává maximální vysílací výkony. Tato agentura se nezabývá jen pravidly pro bezdrátové technologie, ale

v její působnosti je i kabelová a satelitní televize, rádiové vysílání, telefonní služby a další. [1, 9]

1.5.1.2 Organizace ETSI

ETSI je nezávislou organizací, která provádí standardizaci v telekomunikačním průmyslu především v Evropě, ovšem má celosvětový dosah. Tato organizace vznikla v roce 1988 a je oficiálně uznávaná Evropskou komisí. ETSI má 740 členů v 62 zemích v Evropě i mimo ni. Zabývá se standardizací informačních a telekomunikačních technologií, kam patří telekomunikace, rádiové vysílání, rozhlasové vysílání a také inteligentní dopravou a lékařskou elektronikou. [1]

1.5.2 Standardizační organizace

Mimo regulační organizace, které nastavují všeobecná pravidla pro státy a vytváří globální pravidla, existují také další organizace, které se zabývají standardy, jež se využívají v bezdrátových technologiích. Tyto standardy zohledňují vydaná pravidla od regulačních orgánů.

1.5.2.1 Organizace IEEE

Organizace IEEE je neziskovou profesní organizací. Tato organizace vznikla v roce 1963 a sdružuje více než 400 000 členů ve 175 zemích. Vizí této organizace je stát se lídrem v oblasti mezioborových inovací, přenosu technologií, reálných aplikací ve světě a vzdělávání v oblasti výpočetní inteligence. Organizace provádí údržbu a vyvíjí další standardy, kdy uzavřela více než 900 platných standardů a dalších 500 má ve vývoji. Mezi hlavní standardy patří rodina standardů 802, která se zabývá LAN/WAN sítěmi a zahrnuje standardy 802.3, což jsou standardy pro Ethernet a dále 802.11, což je rodina standardů, které se zabývají bezdrátovými technologiemi. [10]

1.5.2.2 Wi-Fi Alliance

Jedná se o obchodní sdružení, které kontroluje, zda zařízení a další produkty splňují určité normy. Vznikla v roce 1999 a od počátku se zaměřovala na testování a kontroly zařízení, jelikož organizace IEEE neměla žádné stanovy, jakým způsobem testovat, zda zařízení odpovídají jeho standardům. Jelikož první produkty 802.11 měli interoperační potíže a neexistovala společnost, která by kontroly prováděla, vznikla Wi-Fi Alliance. Většina výrobců byla v roce 2012 členy této aliance a čítala tak více než 550 členů. Tato společnost

vlastní a vydává certifikát, který uděluje těm zařízením, která prošla jejich testy a splňuje normy a standardy. Ne všechny zařízení jsou však u Wi-Fi Alliance testována, jde o rozhodnutí výrobce, jelikož certifikační proces je poměrně drahý. [11]

1.6 Charakteristiky bezdrátových sítí

Jelikož bezdrátové přenosy probíhají bez kabelů pouze vzduchem, jsou velmi často ovlivňovány různými vlivy prostředí. Tyto vlivy jsou vesměs negativní. Tato kapitola poskytuje přehled nejčastěji se vyskytujících negativních vlivů, které bezdrátové přenosy ovlivňují. [1, 12]

1.6.1 Model Free Path Loss

Tento jev je dán způsobem šíření signálu. Vysílač, jakožto zdroj signálu vysílá signál prostorově okolo sebe. Čím dále se ovšem signál dostane, tím je rozptýlenější a tudíž slabší. Tento signál tedy nemůže cestovat na libovolnou vzdálenost, jelikož během šíření dochází k energetickým ztrátám a po určité vzdálenosti se signál rozptýlí tak moc, že zanikne. Dosah jakéhokoli zařízení je vždy vázán na určení energetických ztrát, které jsou zase závislé na vzdálenosti. Pokud jsme příliš vzdáleni od zdroje, nejsme schopni přijmout žádný signál a tento jev je nazýván jako Free Path Loss. [1]

1.6.2 Absorpce

Absorpce je jev, který se většinou váže k prostředí, ve kterém se signál šíří. Jde vlastně o pohlcování signálu prostředím. Pokud je signál pohlcen úplně, zastaví se. Tento jev tedy snižuje vzdálenost, na kterou se signál může šířit. Pro lepší představu je možné si představit jakýkoli zvuk. Zvuk je pohlcován okolím úplně stejně jako signál. Zavřením okenic se sníží hluk jdoucí z venkovního prostředí. Okenice absorbují část tohoto hluku a ten se pak nešíří na takovou vzdálenost. Příčinou pohlcování je cokoli od zdí přes lidská těla až po koberce, tohle všechno může signál pohlcovat neboli absorbovat. [1]

1.6.3 Odraz

Dalším negativním jevem, se kterým je možné se setkat je odraz. Stejně tak, jak se odráží světlo od různých předmětů a ploch je odrážen i signál. Signál se odráží pod stejným úhlem, pod jakým dopadl na odrazivou plochu. Odražený signál se dále šíří jiným směrem, než byl vyslán. K tomuto jevu dochází i v kancelářském prostředí, kde se vyskytuje mnoho objektů, které mají odrazové vlastnosti a může díky nim docházet k odrazům signálu. Mohou to být

monitory, zrcadla nebo i obrazy zarámované ve skle. Existují ovšem frekvence, které netrpí na odrazy tak moc jako jiné. Odraz je tedy závislý na frekvenci signálu, jelikož objekty mohou modifikovat odražený signál na určité frekvenci více, než modifikují odražený signál na frekvenci jiné. [1]

1.6.4 Vícecestnost

Vícecestnost je úzce spjatá s jevem odrazu. Pokud dojde k odrazu, signál se poté šíří jiným směrem a může do cíle dorazit v jiném pořadí, než byl vyslán. Může se také stát, že přijímač dostane části signálu vícekrát, což způsobuje problémy. Velmi zde záleží na vlnové délce signálu a umístění přijímače. [1]

1.6.5 Rozptyl

Tento jev má také velký vliv na signál, protože jej rozptýlí do více směrů. Tento jev se může vyskytnout ve chvíli, kdy signál prostupuje objektem, který má sice reflexní povrch, ale nemá ostré hrany. Pro lepší představu je možné si představit prudký déšť, kdy padají velké kapky. Velké kapky jsou totiž schopné odrazu, takže když jimi prochází signál, kapky jej odrazí do mnoha směrů, což je označováno jako rozptyl. Výsledkem rozptylu je slabší signál a působí především na signál s kratší vlnovou délkou. [1]

1.6.6 Lom

Lom je jev, který se vyskytuje spíše ve venkovním prostředí. Lom je vlastně změna směru, nebo ohyb signálu, který prochází prostředím s různou hustotou. Dojde tak k tomu, že je část signálu odražena a část signálu projde objektem, ovšem změní se směr jeho šíření. Například sucho může způsobit lom směrem od země, a naopak vlhko způsobuje lom směrem k zemi. [1]

1.6.7 Zorná přímka

Tento jev se projevu především při přenosu na velké vzdálenosti. Jelikož se signál ve směru od vysílače rozšiřuje kolem středového bodu a poté zužuje ve směru k přijímači, může docházet k negativním vlivům na tento signál. Samotná skutečnost, že je cesta zdánlivě čistá, pokud se díváme od vysílače na přijímač, ještě nic neznamená. Tato cesta se nazývá jako vizuální zorná přímka. Nejsou v ní žádné zřejmé překážky, ovšem samotná země je překážkou. V praxi je tedy překážkou samotné zakřivení země, hory, stromy a mnoho dalších překážek, které mohou mít vliv na signál. I v případě, že se cesta jeví přímá

a bez překážek, je nutné mít na paměti, že signál se rozšiřuje a tím na něj mohou působit překážky, které nejsou na první pohled zřejmé. [1]

1.7 Standardy 802.11

Organizace IEEE tvoří a vydává standardy, které standardizují bezdrátové sítě. Jde o rodinu standardů 802.11. Samotný standard 802.11 vznikl v roce 1997 a jde o samostatný standard, který se využíval. Každý vydaný standard měl nové označení a doplňoval nové technologie a poskytoval další výhody. Tyto standardy, označované také jako protokoly umožňují fungování bezdrátových sítí a definují rychlosti, možné metody modulace a další parametry. [1, 2]

1.7.1 Původní standard 802.11

Tento standard vznikl v roce 1997 a byl prvním vydaným standardem. O tomto standardu je možné mluvit jako o začátku rozvoje bezdrátových sítí. Tento standard se dnes již nepoužívá, jelikož poskytoval rychlosti pouze 1 a 2 Mbit/s. Standard také popisuje modulační metodu DSSS, která podporuje také jen rychlosti 1 a 2 Mbit/s a byla používána pouze u tohoto původního standardu. Tento standard pracoval pouze s frekvenčním rozsahem 2.4 GHz. [1, 2]

1.7.2 Standard 802.11a

Standard 802.11a byl vydán v roce 1999 a pracuje s frekvenčním pásmem 5 GHz. Jelikož pracuje na této frekvenci, není rušen zařízeními bluetooth, mikrovlnnými troubami ani zařízeními, které podporují protokoly pracující ve frekvenčním rozsahu 2,4 GHz. Standard také popisuje modulační techniku OFDM a podporuje rychlost až 54 Mbit/s. Standard je označován také jako Wi-Fi 1. [1, 2]

1.7.3 Standard 802.11b

Standard 802.11b byl vydán také v roce 1999 a pracuje s frekvenčním pásmem 2,4 GHz. Jde o doplněk původního protokolu 802.11 a přináší vyšší přenosovou rychlost a to až 11 Mbit/s. Je zpětně kompatibilní s předchozím standardem, kdy využívá modulační techniku DSSS pro rychlosti 1 a 2 Mbit/s, ovšem v režimu rychlostí 5,5 a 11 Mb/s se uplatňuje modulace QPSK. Tento standard je také označován jako Wi-Fi 2. [1, 2]

1.7.4 Standard 802.11g

Standard 802.11g byl vydán v roce 2003 a pracuje s frekvenčním pásmem 2,4 GHz. Došlo k navýšení maximální rychlosti až na 54 Mbit/s, čímž se vyrovnal rychlostem standardu 802.11a, ovšem ve 2,4 GHz pásmu. Je zpětně kompatibilní se standardem 802.11b, kdy pro rychlosti tohoto standardu využívá stejnou modulační metodu, ovšem pro rychlosti vyšší využívá modulační metodu OFDM, kterou uplatňuje i standard 802.11a. Tento standard je také označován jako Wi-Fi 3. [1, 2]

1.7.5 Standard 802.11n

Standard 802.11n byl vydán v roce 2009 a pracuje s frekvenčním pásmem 2,4 GHz i 5 GHz. Cílem bylo upravit fyzickou vrstvu a část linkové vrstvy tak, aby bylo možné dosáhnout rychlosti přenosu vyšší než 100 Mbit/s. Maximální rychlost při využití tohoto standardu je až 600 Mbit/s, ovšem pouze při použití technologie 4x4 MIMO. Technologie MIMO byla poprvé zahrnuta v tomto standardu. Standard je kompatibilní se standardem 802.11g. Standard využívá modulační metodu OFDM. Tento standard je také označován jako Wi-Fi 4. [1, 2]

1.7.6 Standard 802.11ac

Standard 802.11ac byl vydán v roce 2014 a pracuje s frekvenčním pásmem 5 GHz. Tento standard dále vylepšuje a rozšiřuje koncepty, které byly zavedeny se standardem 802.11n a tím dosahuje přenosových rychlostí vyšších než 1 Gbit/s, uváděno je až 6,4 Gbit/s. Podporuje také více prostorových kanálů a MU-MIMO technologii. Standard využívá modulační metodu OFDM. Tento standard je také označován jako Wi-Fi 5. [13, 14]

1.7.7 Standard 802.11ax

Tento standard je nejnovějším z celé rodiny standardů 802.11. Standard 802.11ax byl vydán v roce 2021 a jde o přímého nástupce standardu 802.11ac. S tímto standardem bude možné dosáhnout rychlosti až 9,6 Gbit/s, ovšem standard zůstává kompatibilní se standardy 802.11a/g/n/ac. Standard využívá modulační metodu OFDMA, která seskupuje subnosné vlny do bloků, které pak přiděluje dynamicky uživatelům. Tento standard také využívá technologii MU-MIMO, navíc ovšem přináší další technologie, které jsou v tomto standardu využívány poprvé. Jde o technologii BSS a TWT. Technologie BSS (Basic Service Set) dokáže označit určitou barvou komunikaci v rámci jedné BSS a komunikaci mimo tuto BSS barvou jinou. Dík tomu dokáže detekovat komunikaci na stejném kanále a případně

ignorovat komunikaci jiné barvy. Technologie TWT (Target Wake Time) dokáže definovat pro jednotlivé klienty čas nebo sadu časů, ve kterém mohou klienti komunikovat, což minimalizuje spotřebu energie u mobilních zařízení. [13, 14]

1.8 Řadiče bezdrátové sítě

Na počátku, kdy se začali bezdrátové sítě nasazovat fungovaly přístupové body v tzv. autonomním režimu. Přístupovým bodům v tomto režimu se říká také silné přístupové body. Ovšem s vývojem bezdrátových sítí a nasazováním stále většího množství přístupových bodů bylo nutné implementovat společnou správu těchto bodů. Autonomní přístupové body jsou totiž konfigurovány jednotlivě. Při větším počtu bodů se stává jejich správa značně obtížnou záležitostí. Autonomní přístupový bod je totiž nutné konfigurovat, spravovat a sledovat jeho stav samostatně, čímž může docházet k nekonzistenci mezi jednotlivými body. Dalším problémem je, že se prostředí, ve kterém se body nachází neustále mění a na tyto změny je potřeba reagovat, jelikož ovlivňují pokrytí bezdrátovým signálem. Při těchto změnách a následné korekci se tedy museli body konfigurovat opět samostatně, což není tolik praktické.

Bylo tedy nutné přinést způsob, jak konfiguraci a správu centralizovat, a proto vznikly bezdrátové řadiče. Bezdrátové řadiče ovšem nespravují autonomní přístupové body ale tzv. lehké přístupové body. Nejvýhodnější je, převést co největší počet přístupových bodů do lehkého režimu a spravovat je pomocí bezdrátového řadiče, jehož nasazení přinese mnoho výhod. Přístupový bod, který je připojený k řadiči získává svou konfiguraci přímo z řadiče. Pokud dojde k změnám v prostředí, řadič dokáže dynamicky aktualizovat přístupové body bez vnějšího zásahu. Tyto možnosti přinesla jako první společnost Cisco systémem nazvaným CUWN (Cisco Unified Wireless Network) a zahrnuje několik funkčních oblastí kam patří především klienti bezdrátových sítí, přístupové body, sjednocení sítě, správa sítě a síťové služby.

Do oblasti klientů bezdrátových sítí spadají všechna zařízení, která se k dané síti připojují. Oblast přístupových bodů pokrývá celou problematiku konfigurace, správy a dynamických aktualizací přístupových bodů. Do oblasti sjednocení sítě spadají bezdrátové řadiče s možnostmi, jak přístupové body dělit do kategorií a skupin. Oblast správy sítě zahrnuje pokročilé možnosti správy jak přístupových bodů, tak celé bezdrátové sítě. Oblast síťových služeb pokrývá podpůrná zařízení jako jsou přepínače, směrovače atp.

Přístupové body v systému CUWN musí být v lehkém režimu, k jehož řízení se používá WLC (Wireless LAN Controller). S tímto řadičem přístupová bod komunikuje přes protokol LWAPP (Lightweight Access Point Protocol). Přes tento protokol jsou mezi řadičem a přístupovým bodem vyměňovány informace o pokrytí, rušení, přidružení klientů a konfiguraci. Komunikace přes LWAPP je šifrována a v hlavičkách rámců mohou být odesílána i klientská data. Pokud jsou přenášena i klientská data, kromě výše zmíněných informací má řadič k dispozici i RSSI (Recieved Signal Strenght Indicator) a také SNR (Signal to Noise Ratio) kdy na základě těchto dat může řadič provádět aktualizaci konfigurace přístupových bodů za účelem zlepšení pokrytí či výkonu.

V systému CUWN má lehký přístupový bod připojený k řadiči na starosti následující činnosti:

„*Výměna rámců a navázání komunikace mezi klienty, přenos rámců typu maják, ukládání do vyrovnávací paměti a přenos rámců pro klienty v režimu úspory energie, odesílání odpovědí na sondovací požadavky z různých klientů v síti, předávání oznámení o přijatých sondovacích požadavcích řadiči, podávání aktuálních informací o kvalitě signálu řadiči, sledování šumu a rušení všech kanálů.*“ [1, s.178]

Řadič má na starosti všechny ostatní funkce, mezi které patří přidružení, změna přidružení, autentizace, překlad rámců a přemostění rámců. [1, 15]

1.9 Roaming

Z uživatelského hlediska by měl být roaming nepostřehnutelný a většina uživatelů ani neví, že k roamingu došlo. Jako roaming se označuje přechod klienta od jednoho přístupového bodu k jinému bez přerušení spojení. Pojem roaming se úzce váže k pojmu mobilní skupina. Mobilní skupina se nastavuje na řadiči, přičemž samotný řadič se definuje jako člen této skupiny. Do stejné mobilní skupiny může patřit i více řadičů. Všechny řadiče, připojené ke stejné mobilní skupině mezi sebou sdílí informace o klientech, které roamují. Aby ovšem bylo možné na řadiči nastavit mobilní skupinu, je nutné provést konfiguraci mobilní domény. Pokud má roaming správně fungovat, měla by být mobilní doména jen jedna. V této mobilní doméně ovšem může fungovat více mobilních skupin a v každé z těchto skupin může být více řadičů, ovšem roaming bude fungovat jen za předpokladu, že řadiče v různých mobilních skupinách jsou součástí stejné mobilní domény. To znamená, že roaming bude fungovat i pokud existuje více mobilních skupin, protože řadiče jsou připojené ke stejné

mobilní doméně, a tudíž jsou schopné spolu komunikovat a zajistit plynulý přechod klienta mezi různými přístupovými body.

„*Chceme-li u svých řadičů zajistit podporu roamingu, je nutné splnit tyto požadavky:*

- *Řadiče musí patřit do stejné mobilní domény.*
- *Řadiče musí používat stejnou verzi kódu.*
- *Řadiče musí fungovat ve stejném režimu protokolu LWAPP.*
- *Přístupové seznamy musí být vždy stejné.*
- *Musí se shodovat identifikátor SSID.*“ [1, s.217]

Roaming může také fungovat ve dvou režimech. Roaming se dělí na roaming na vrstvě 2 a roaming na vrstvě 3. Rozdílem je, že u roamingu vrstvy 2 si klient při přechodu ponechá svou IP adresu. Roaming vrstvy 3 nastává, pokud klient při přechodu na jiný přístupový bod přechází i do jiné podsítě, přičemž se shoduje identifikátor SSID. [1]

1.9.1 Roaming vrstvy 2

Jako roaming vrstvy 2 se označuje přechod klienta od jednoho přístupovému bodu ke druhému, pokud jsou tyto body připojeny ke stejnému řadiči. Označuje se také jako roaming v rámci řadiče. Při přechodu klienta od jednoho přístupového bodu k jinému je novému bodu odeslán požadavek k autentizaci, který jej předá řadiči. Řadič poté zjistí, že klient již je autentizován pomocí jiného přístupového bodu a klient je v řadiči označen jako roamující. Klient není nijak upozorněn, že k roamingu dochází, je mu ponechána stejná IP adresa a všechny relace zůstanou aktivní.

Jako roaming vrstvy 2 je označován také případ, kdy se v síti nachází více řadičů. Pokud dojde k přechodu klienta od přístupového bodu, který je připojen k řadiči 1 k přístupovému bodu, který je připojen k řadiči 2, je tento přechod označován jako roaming mezi řadiči. Řadiče musí být ovšem součástí stejné mobilní skupiny a klient musí zůstat ve stejné VLAN síti. Řadiče si při přechodu vymění mobilní zprávy a klient je přesunut mezi databázemi řadičů. [16]

1.9.2 Roaming vrstvy 3

Roaming vrstvy 3 funguje velmi podobně jako roaming vrstvy 2, ovšem v tomto případě je více řadičů v různých podsítích. I zde si při přechodu mezi přístupovými body klient

ponechává svou IP adresu, a i když jsou řadiče v různých podsítích je provoz tunelován k původnímu řadiči a z hlediska sítě se předstírá, že roaming vůbec nenastal. [17]

2 ZABEZPEČENÍ A AUTENTIZACE

V této kapitole se práce zaměří na možnosti autentizace uživatelů. Vždy je nutné uvažovat o tom, kteří uživatelé mají mít povolený přístup k síti. K ověřování uživatelů vzniklo mnoho metod, díky kterým je možné uživatele autentizovat a zajistit jim šifrovanou komunikaci. Vznikají stále nové metody, protože většina aktuálně dostupných metod byla prolomena, ovšem prolomení aktuálního zabezpečení je složité.

2.1 Autentizace

Autentizace se dělí na jednoduchou a centralizovanou. Jednoduchá autentizace je prosté připojení k přístupovému bodu, kdy není nijak dokazována identita uživatele ani sítě. Centralizovaná autentizace se používá pro podnikové sítě a dle kritérií na bezpečnost sítě je možné vybrat mezi několika různými metodami. Práce se zaměřuje především na centralizovanou autentizaci a možnosti zabezpečení podnikové bezdrátové sítě.

2.1.1 Jednoduchá autentizace

Jde o nejjednodušší případ. Pojem autentizace je v tomto případě použit zcela volně, jelikož k faktické autentizaci nedochází. Jde o součást přidružení. Klient vyšle sondovací požadavek a přístupový bod na něj zareaguje a zaregistruje klienta. Poté odešle požadavek na přidružení a potvrzení. Tento typ autentizace je často využíván v hotspotech. [1]

2.1.2 Centralizovaná autentizace

Centralizovaná autentizace vznikla pro systematické zabezpečení bezdrátových sítí. Využívá se především ve firemním prostředí, jelikož je zde kladen mnohem větší důraz na bezpečnost přenášených dat a zároveň kontrolu nad uživateli, kteří se připojují k bezdrátové síti. Zde se pracuje s PKI (Public Key Infrastructure), která využívá certifikáty podepsané důvěryhodnou třetí stranou. Důvěryhodná třetí strana je certifikační autorita neboli CA. Certifikátem se tedy ověřuje identita jeho držitele a tato identita je považována za důvěryhodnou. CA tedy vydá certifikát CA a certifikát serveru. Zařízení, které se snaží autentizovat ověří pomocí certifikátu CA podpis certifikátu druhé strany. Pokud jsou tyto podpisy shodné, je autentizace úspěšná. Certifikáty slouží pro autentizaci 802.1X, což je centralizovaná metoda autentizace a autentizace probíhá různými metodami, které poskytuje protokol EAP. [18, 19]

„*Certifikát obsahuje následující informace:*

- *informace o majiteli (vlastníkovi) certifikátu.*
- *informace o vydavateli certifikátu.*
- *dobu platnosti.*
- *veřejný klíč.*“ [19]

2.1.3 Standard 802.1X

Tento standard slouží k autentizaci uživatele a jde o centralizovanou autentizaci. Jeho princip spočívá v otevření nebo uzavření portu do chvíle, než je ověřena identita uživatele a autentizace se provádí pomocí různých metod protokolu EAP. Tento standard je tedy pouze rámec, protože neřeší způsob odeslání uživatelových údajů, pouze vyžaduje jejich odeslání. Tato metoda autentizace funguje na principu klient-server. Proto je důležité rozlišovat tři typy zařízení, která se na autentizaci podílejí. Prvním z nich je klient, což je jakékoli zařízení, které se snaží připojit k síti. Na tomto zařízení musí být spuštěn tzv. supplicant, což je software schopný žádat o autentizaci. Tento standard používá RADIUS (Remote Autentization Dial-In User Servise), což je autentizační server, který obsahuje databázi všech uživatelských účtů, pomocí které provádí autentizaci. Druhým ze zařízení je nazvané autentizační klient, což je přepínač nebo přístupový bod. Autentizační klient kontroluje fyzické připojení k síti dle autentizačního stavu. Autentizační klient je vlastně prostředníkem mezi klientem a autentizačním serverem. Třetím zařízením je autentizační server, který ověřuje klientovu identitu. Po ověření identity předá autentizačnímu klientovi informaci, zda má klient oprávnění přistupovat k síti. Výměna zpráv mezi těmito zařízeními probíhá přes protokol EAPoL (EAP over LAN) v případě, že autentizační klient je přepínač a přes protokol EAPoWLAN (EAP over WLAN) v případě, že se jedná o přístupový bod. [1, 20]

Proces autentizace začíná nejprve přidružením klienta k přístupovému bodu.

„*Proces autentizace zahrnuje následující kroky:*

1. *Klient se přidruží k přístupovému bodu.*
2. *Klient přijme autentizační požadavek.*
3. *Klient vrátí autentizační odpověď.*
4. *Klient přijme požadavek na přidružení.*
5. *Klient odešle odpověď přidružení.*“ [1, s.335]

Po přidružení klienta může libovolná strana zahájit proces 802.1X. Port je dále blokován, protože nedošlo k úspěšné autentizaci ale pouze přidružení. Následující algoritmus přibližuje proces autentizace při použití jednorázového hesla. Během samotné autentizace probíhají následující děje:

1. Klient zahájí proces autentizace.
2. Autentizační klient požádá klienta o identitu a po obdržení odpovědi ji předá autentizačnímu serveru.
3. Autentizační server identitu potvrdí a odešle odpověď autentizačnímu klientovi a klientovi.
4. Autentizační klient požádá o jednorázové heslo a po jeho obdržení je odešle autentizačnímu serveru.
5. Autentizační server dle své databáze udělí nebo zamítne přístup a odpověď odešle autentizačnímu klientovi a klientovi.
6. Autentizační klient na základě odpovědi odblokuje port a klient je připojen do sítě.

Tento proces je ovšem závislý především na použité metodě protokolu EAP. Výše popsaný proces pouze v jednoduchosti přibližuje koncepci, pomocí které dochází k autentizaci klienta. [20]

2.1.3.1 Autentizační server

Nejdůležitější součástí centralizované autentizace je autentizační server, nazývaný také jako AAA (Authentication, Authorization, Accounting) server, který provádí samotnou autentizaci. Autentizační server může být externí a může jít o ACS server nebo o server RADIUS. Nezáleží přitom na tom, jaký typ serveru je použit. Server pouze musí být kompatibilní s metodou EAP, kterou využívá řadič, autentizační klient a klient. Na řadiči se nastavuje metoda EAP a také umístění autentizačního serveru, přičemž stačí znát IP adresu serveru a správný sdílený tajný klíč. [21]

2.2 Metody EAP

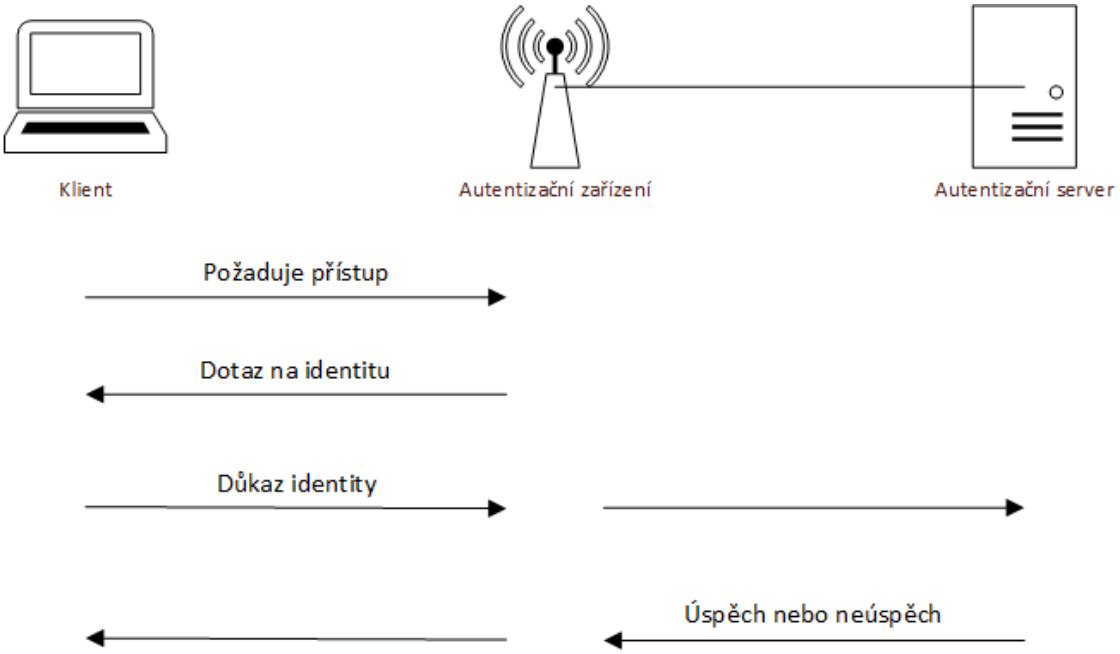
Následující část popisuje EAP metody a přibližuje jejich fungování. Jde o přehled nejznámějších metod, se kterými bylo možné se setkat, ale existuje jich ještě mnohem více. Metody ověření se stále vyvíjejí se snahou dosáhnout vyšší bezpečnosti bezdrátových sítí.

2.2.1 Protokol EAP

Tento protokol je využíván standardem 802.1X a slouží k definování, jakým způsobem bude probíhat odeslání uživatelských údajů. Protokol EAP (Extensible Authentication Protocol) zahrnuje několik metod, které je možné implementovat a u jakékoli metody bude postupováno prakticky stejně. Proces EAP autentizace je přiblížen na obrázku 2.

„*Postup zahrnuje následující kroky:*

1. *Klient požádá o přístup.*
2. *Autentizační zařízení se klienta dotáže na jeho identitu.*
3. *Klient poskytne identitu.*
4. *Klient dostane odpověď od serveru.*“ [1, s.336]



Obrázek 2 Proces EAP [1] (Vlastní zpracování)

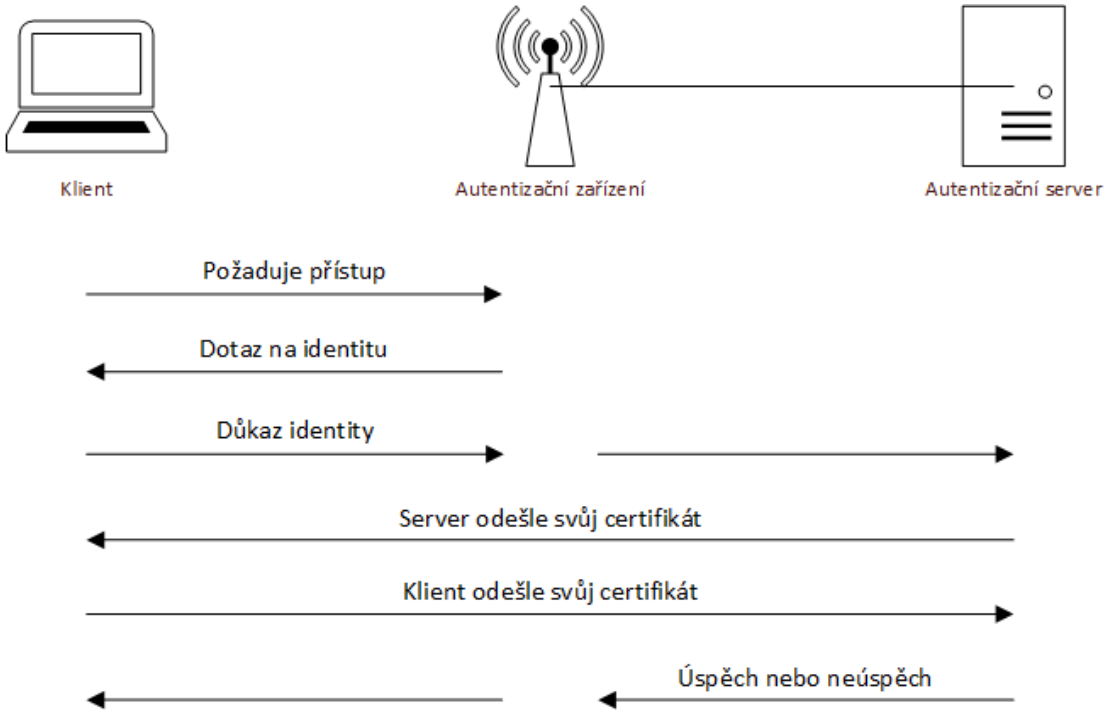
2.2.2 Metoda EAP-TLS

EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) je velmi používanou metodu, jelikož se jedná o jednu z nejbezpečnějších metod. To je dáno tím, že pracuje s certifikáty jak na straně serveru, tak na straně klienta. Do klientova zařízení musí být nainstalován certifikát žadatele podepsaný důvěryhodnou CA. Z tohoto důvodu se tato metoda považuje za nadstandardně bezpečnou. Komunikace pomocí této metody je podobná

jako šifrování SSL, ovšem TLS protokol se považuje za jeho nástupce. Proces EAP-TLS autentizace je přiblížen na obrázku 3.

Proces autentizace u metody EAP-TLS vypadá následovně:

1. Klient se přidruží k autentizačnímu zařízení a požaduje přístup.
2. Autentizační zařízení se dotáže na identitu klienta.
3. Klient poskytne svou identitu, kterou autentizační zařízení pošle autentizačnímu serveru.
4. Autentizační server odešle klientovi svůj certifikát a klient jej ověří.
5. Klient odešle autentizačnímu serveru svůj certifikát a server jej ověří.
6. Pokud je vzájemně prokázána identita vytvoří se symetrické klíče relace.
7. Autentizační server odešle hlavní klíč relace přístupovému bodu a ten jej použije při šifrování WEP, WPA nebo WPA2 pro komunikaci s klientem. [22, 23]



Obrázek 3 Proces EAP-TLS [22] (Vlastní zpracování)

2.2.3 Metoda EAP-FAST

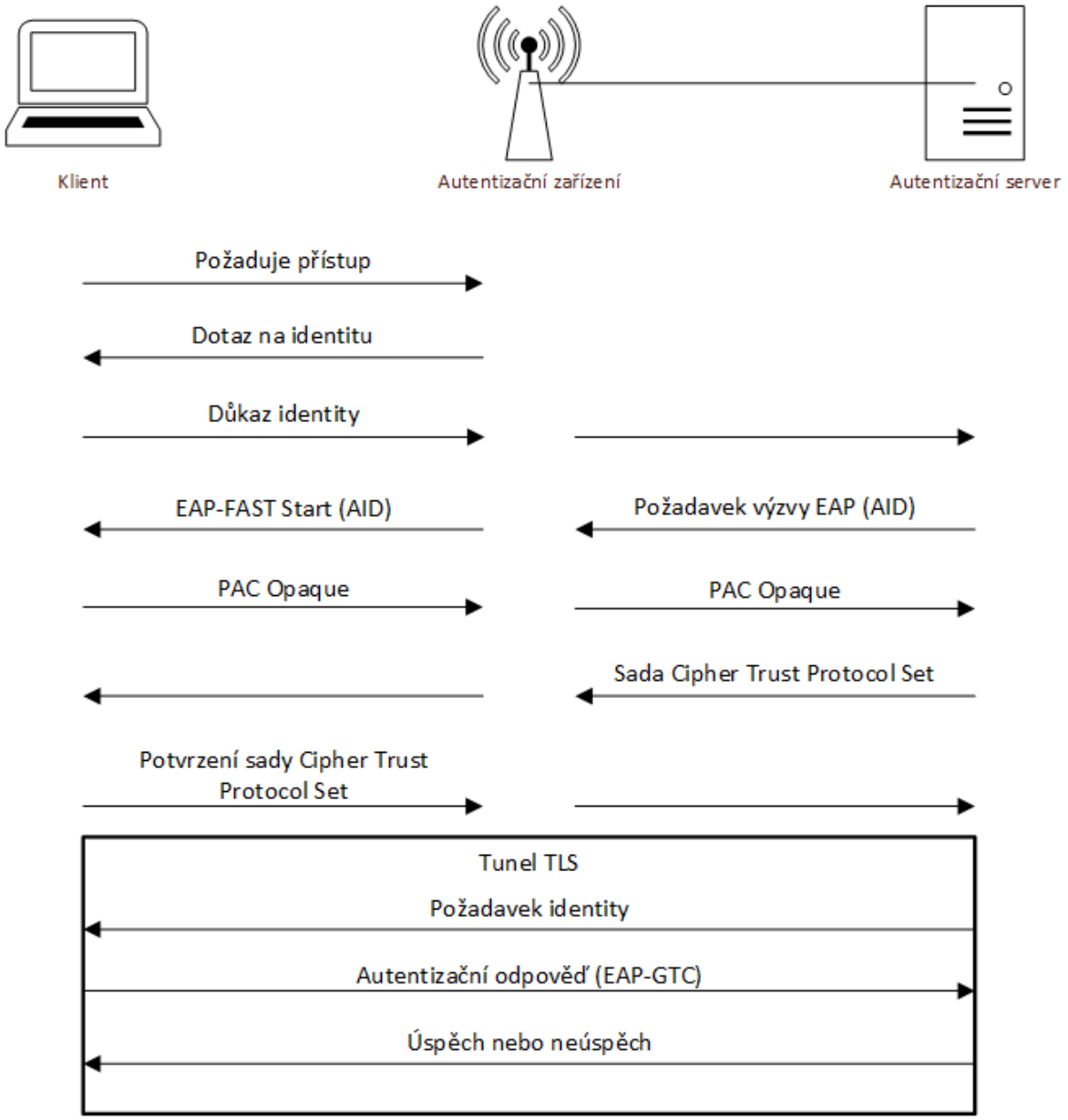
Tato metoda byla vyvinuta společností Cisco jako náhrada za protokol LEAP. Celý název metody je Extensible Authentication Protocol – Flexible Authentication via Secure Tunnel. Z tohoto názvu vyplývá, že je podobný jako EAP-TLS, ovšem používá silný sdílený tajný klíč zvaný PAC (Protected Access Credential), který je jedinečný. Proces autentizace touto

metodou je rozdělen na 2 fáze, ale výměna PAC klíče probíhá již ve fázi 0. Teprve po výměně klíče PAC začíná fáze 1, která po ověření klíče PAC mezi serverem a klientem vytvoří TLS tunel. Po vytvoření tunelu přechází autentizace do fáze 2 při které dochází k samotné autentizaci uživatele pomocí jiné metody EAP. Proces EAP-FAST autentizace je přiblížen na obrázku 4.

Průběh autentizace u metody EAP-FAST probíhá následovně:

1. Klient se přidruží k autentizačnímu zařízení a požaduje přístup.
2. Autentizační zařízení se dotáže na identitu klienta.
3. Klient poskytne svou identitu autentizačnímu zařízení, které ji přepošle autentizačnímu serveru.
4. Autentizační server klientovi odešle zprávu EAP-FAST Start, ve které je zahrnuto ID autority (A-ID).
5. Klient odešle PAC klíč, jenž je založený na hodnotě A-ID a dále odešle tzv. PAC Opaque, což je hodnota, kterou dokáže interpretovat jen autentizační server. Tato hodnota kontroluje pověření klienta.
6. Server dešifruje hodnotu PAC Opaque hlavním klíčem a odešle zprávu EAP-TLS Server Hello společně se sadou Cipher Trust Protocol Set.
7. Při shodě klíčů je navázán tunel TLS a klient odešle potvrzení.
8. V rámci TLS tunelu se server dotáže na identitu klienta libovolnou metodou EAP (v tomto případě metodou EAP-GTC).
9. Klient poskytne svou identitu autentizačnímu serveru.
10. Po ověření identity autentizační server odešle odpověď, čímž umožní nebo neumožní klientovi přenášet data.

Na obrázku 4 je znázorněn postup výměny zpráv mezi klientem, autentizačním zařízením a autentizačním serverem. [1]



Obrázek 4 Proces EAP-FAST [1] (Vlastní zpracování)

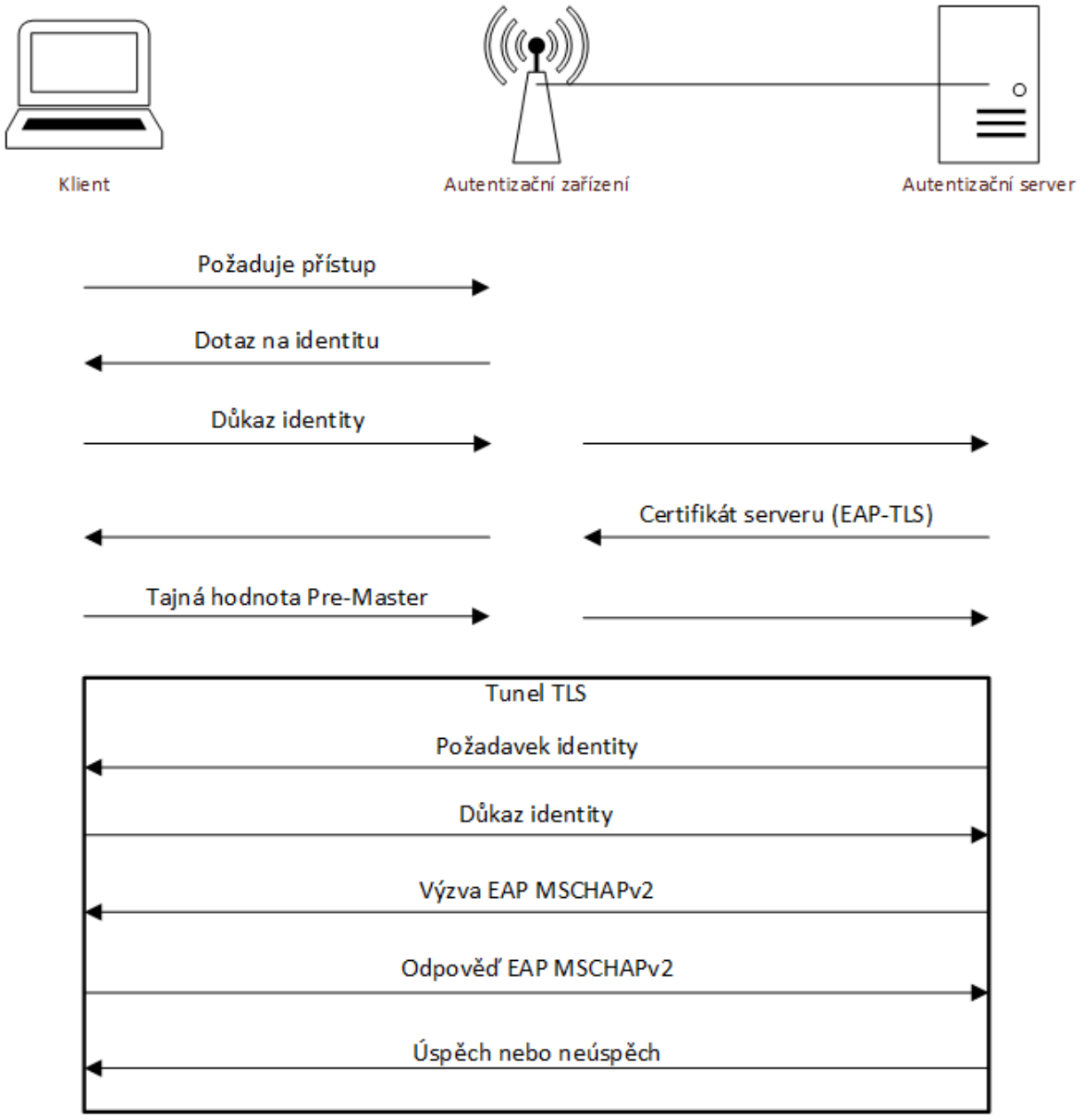
2.2.4 Protokol PEAP

PEAP (Protected Extensible Authentication Protocol) se řadí mezi nejvíce používané, protože nepožaduje certifikát na straně klienta, ovšem požaduje certifikát serveru, díky kterému je možné vytvořit TLS tunel a autentizace uživatele probíhá v rámci tohoto tunelu. Pro autentizaci v TLS tunelu využívá protokol MS-CHAPv2 nebo GTC. Protokol je navržený tak, že na straně serveru je možné využít zabezpečení EAP-TLS a na straně klienta použít jinou ověřovací metodu.

Průběh autentizace u metody PEAP probíhá následovně:

1. Klient se přidruží k autentizačnímu zařízení a požaduje přístup.
2. Autentizační zařízení se dotáže na identitu klienta.
3. Klient odešle svou identitu autentizačnímu zařízení, které ji přepošle autentizačnímu serveru.
4. Autentizační server odešle svůj certifikát klientovi a začne vytvářet TLS tunel.
5. Klient po ověření podpisu certifikátu odešle odpověď s tajnou hodnotou Pre-Master.
6. TLS tunel mezi autentizačním serverem a klientem je navázán.
7. Server se dotáže na identitu klienta.
8. Klient poskytne svou identitu autentizačnímu serveru.
9. Server odešle výzvu EAP-MS-CHAPv2.
10. Klient na výzvu odpoví zadáním pověření do připravené zprávy a odešle jako odpověď EAP-MSCHAPv2.
11. Po ověření identity autentizační server odešle odpověď, čímž umožní nebo neumožní klientovi přenášet data.

Na obrázku 5 je znázorněn postup výměny zpráv mezi klientem, autentizačním zařízením a autentizačním serverem. [23]



Obrázek 5 Proces PEAP [23] (Vlastní zpracování)

2.3 Ověřovací protokoly

2.3.1 Protokol PAP

Ověřovací protokol PAP (Password Authentication Protocol) je jednoduchý protokol používaný k autentizaci v protokolu PPP (Point to Point Protocol). Je založen na výměně uživatelského jména a hesla a následném ověření údajů na serveru. Tento protokol ovšem odesílá údaje v nešifrované formě, a proto není bezpečný, jelikož je možné údaje snadno přečíst po jejich odposlechnutí. PAP využívá tzv. two-way handshake, což je dvoufázová výměna údajů. Komunikace probíhá tak, že klient odešle požadavek k autentizaci se svými

údaji a server tyto údaje ověří a pokud jsou údaje správné provede autentizaci uživatele a výsledek autentizace odešle zpět uživateli. [24]

2.3.2 Protokol CHAP

Tento protokol je již zastaralý, ovšem na jeho základě byly vyvinuty další protokoly, které jsou hojně využívány. CHAP (Challenge Handshake Authentication Protocol) se využívá k autentizaci v protokolu PPP. Tento protokol využívá tzv. three-way handshake. Dochází tedy k třífázové výměně údajů. Klient i autentizační server sdílí šifrovací klíč. Autentizace pak probíhá následovně:

1. Autentizační server odešle tzv. Challenge, což je výzva klientovi, která obsahuje náhodný řetězec.
2. Klient přijatý řetězec spojí se šifrovacím klíčem a výslednou hodnotu zašifruje. Tuto hodnotu pak odešle autentizačnímu serveru.
3. Autentizační server zašifruje původní hodnotu, kterou odeslal stejným způsobem jako to udělal klient a porovná ji s hodnotou přijatou od klienta.

Autentizační server provádí opětovnou autentizaci v průběhu komunikace v náhodných intervalech, přičemž se opakují všechny kroky autentizace. [24]

2.3.3 Protokol MS-CHAPv1 a MS-CHAPv2

Tyto autentizační protokoly vychází z protokolu CHAP, ovšem Microsoft jej převzal a provedl úpravy původního protokolu. Od příchodu operačního systému Vista se již nepoužívá, jelikož již v tomto systému není podporován. MS-CHAPv1 oproti původnímu protokolu využívá jiný způsob šifrování a dále umožňuje šifrování dat. Protokol MS-CHAPv2 je nástupcem protokolu MS-CHAPv1 a přinesl možnost změny hesla a jinou metodu šifrování. Tato možnost znamená, že pokud autentizační server oznámí klientovi, že platnost jeho hesla vypršela, může klient heslo změnit. [25]

2.3.4 GTC

GTC (Generic Token Card) je autentizační metoda, která je založená na autentizaci založené na certifikátu nebo kartě tokenu. Jednou z možností protokolu je možnost skrytí uživatelského jména do chvíle, než je vytvořen TLS tunel. Proces autentizace není nijak šifrován, během autentizace se ovšem používají jednorázové tokeny, které generuje karta. Z tohoto důvodu je tato metoda považována za bezpečnou. [25]

2.4 Metody zabezpečení

2.4.1 Zabezpečení WEP

WEP (Wired Equivalent Privacy) je protokol, který ověřuje, zda má uživatel, který chce navázat připojení správný klíč. U tohoto protokolu neprobíhá autentizace uživatele v pravém slova smyslu, jelikož se neověřuje uživatelova identita.

Existují 2 možnosti autentizace při použití tohoto protokolu. Buď je možné použít otevřenou autentizaci, při které klient neposkytuje své údaje. Zde nedochází k žádné autentizaci, může se tak připojit libovolný klient bez nutnosti znát klíč.

Druhou možností autentizace je autentizace sdíleným klíčem. Při použití této možnosti protokol šifruje pouze text výzvy. Klíč může mít délku 40 bitů, 104 bitů nebo 128 bitů. Jde ovšem o zavádějící hodnoty, jelikož klíč se dále kombinuje s inicializačním vektorem o délce 24 bitů. Inicializační vektor se přidá ke klíči, čímž vytvoří unikátní šifrovací klíč. Tento protokol využívá k šifrování algoritmus RC4.

„*Proces autentizace WEP vypadá takto:*

1. *Klient odešle autentizační požadavek.*
2. *Přístupový bod odešle autentizační odpověď, která obsahuje nezašifrovaný text výzvy.*
3. *Klient na základě přijatého textu odpoví zašifrovaným autentizačním paketem. Šifrování je založeno na jednom ze statických klíčů WEP.*
4. *Přístupový bod porovná hodnotu přijatou od klienta se svou vlastní hodnotou, kterou vypočítal na základě statických klíčů WEP. Pokud se hodnoty shodují, klient přejde do fáze přidružení.*“ [1, s.331]

Otevřená autentizace je považována za silnější metodu zabezpečení, než je metoda sdíleného klíče. Je to z toho důvodu, že u zabezpečení sdíleným klíčem útočník může zachytit nezašifrovaný text výzvy a poté i zašifrovanou odpověď, čímž je možné snadno odvodit statický klíč WEP. WEP protokol byl prolomen v roce 2001. [2, 26, 27]

2.4.2 Zabezpečení WPA

Tento standard vznikl v roce 2002 po prolomení zabezpečení WEP. WPA (Wi-Fi Protected Access) používá stejnou šifrovací metodu jako WEP. Je tedy využit algoritmus RC4. WPA ovšem přináší i se stejnou šifrovací metodou výrazně vyšší zabezpečení než WEP.

Po prolomení zabezpečení WEP byla potřebná rychlá reakce na tuto skutečnost a byl proto použit algoritmus RC4. Bylo důležité, aby bylo možné zabezpečení WPA použít u veškerých hardwarových zařízení. Změna zabezpečení měla být možná bez výměny zařízení pouhou aktualizací firmwaru těchto zařízení a aktualizací softwaru na klientských zařízeních. Data jsou tedy šifrována stále stejnou metodou, jakou využíval WEP. Zvýšení bezpečnosti komunikace bylo docíleno implementací protokolu TKIP (Temporal Key Integrity Protocol), který umožňuje dynamickou správu šifrovacích klíčů. U zabezpečení WPA je možné šifrovat komunikaci šifrováním AES, které je považováno za velmi bezpečné, ovšem v případě jeho použití bylo nutné provést výměnu zařízení z důvodu vyšších požadavků na výkon zařízení. WPA pracuje s protokolem TKIP a také delším inicializačním vektorem a je tedy odolnější proti útokům hrubou silou. Další metodou, která přispěla zvýšení bezpečnosti je MIC (Message Integrity Code), která obsahuje počítadlo rámců. Díky kódu MIC je možné chránit se před útoky, které opakují předchozí odposlechnutou komunikaci.

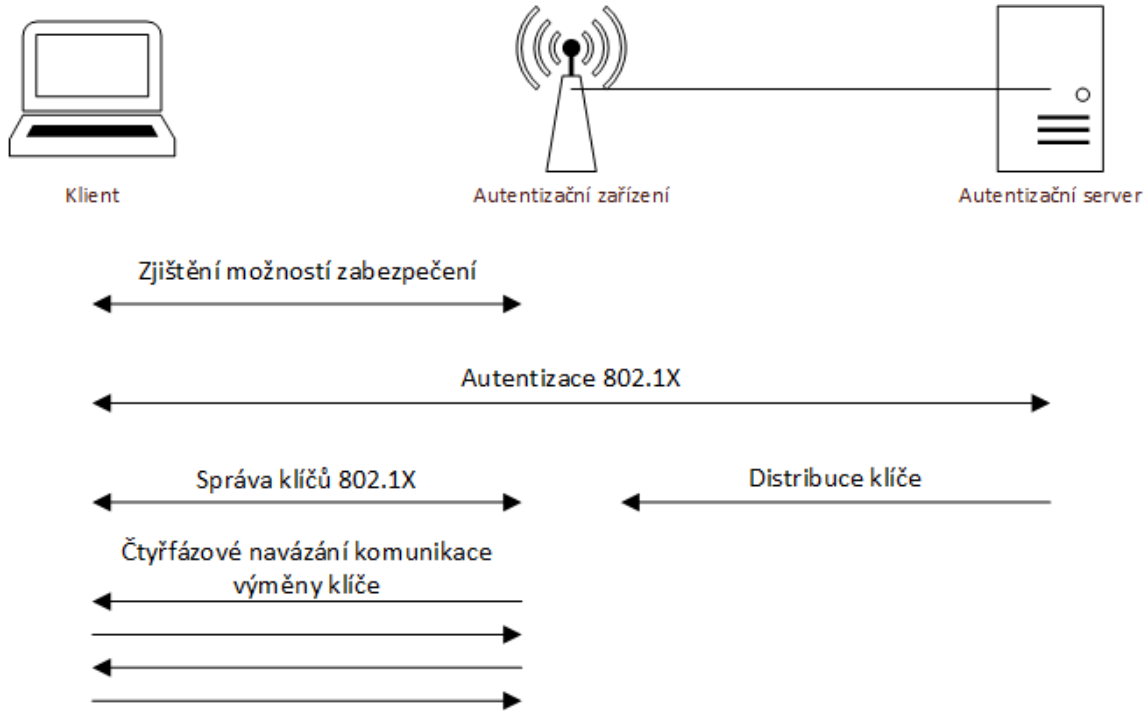
WPA také poskytuje 2 režimy autentizace. Jde o autentizaci osobní (WPA-Personal) a o autentizaci centralizovanou (WPA-Enterprise). U osobní autentizace se nevyužívá autentizační server a využívá pouze tajný sdílený klíč. Tento klíč je uložen na přístupovém bodu a u klienta. Po zadání správného klíče je klient připojen do sítě.

V režimu centralizované autentizace je vyžadován autentizační server a podpora protokolu 802.1X. Dále je možné použití některé z metod EAP autentizace.

Proces autentizace WPA je následující:

1. Klient a autentizační zařízení se shodnou na zabezpečení.
2. Začne proces 802.1X, který provede autentizaci uživatele definovanou metodou EAP.
3. Pokud je autentizace úspěšná tak autentizační server odvodí hlavní klíč, který odešle přístupovému bodu. Stejný klíč odvodí i klient. Klient i autentizační zařízení disponují stejným klíčem PMK (Pairwise Master Key).
4. Za pomoci čtyřfázové komunikace mezi klientem a autentizačním zařízením je vytvořen klíč PTK (Pairwise Transient Key).
5. Za pomoci dvoufázové komunikace je vytvořen klíč GMK (Group Master Key) a poté se vytvoří náhodné číslo skupiny. Číslem skupiny se vytvoří klíč GTK (Group Temporal Key), který dešifruje komunikaci mezi klientem a autentizačním zařízením.

Princip zabezpečení WPA je přiblížen na obrázku 6.

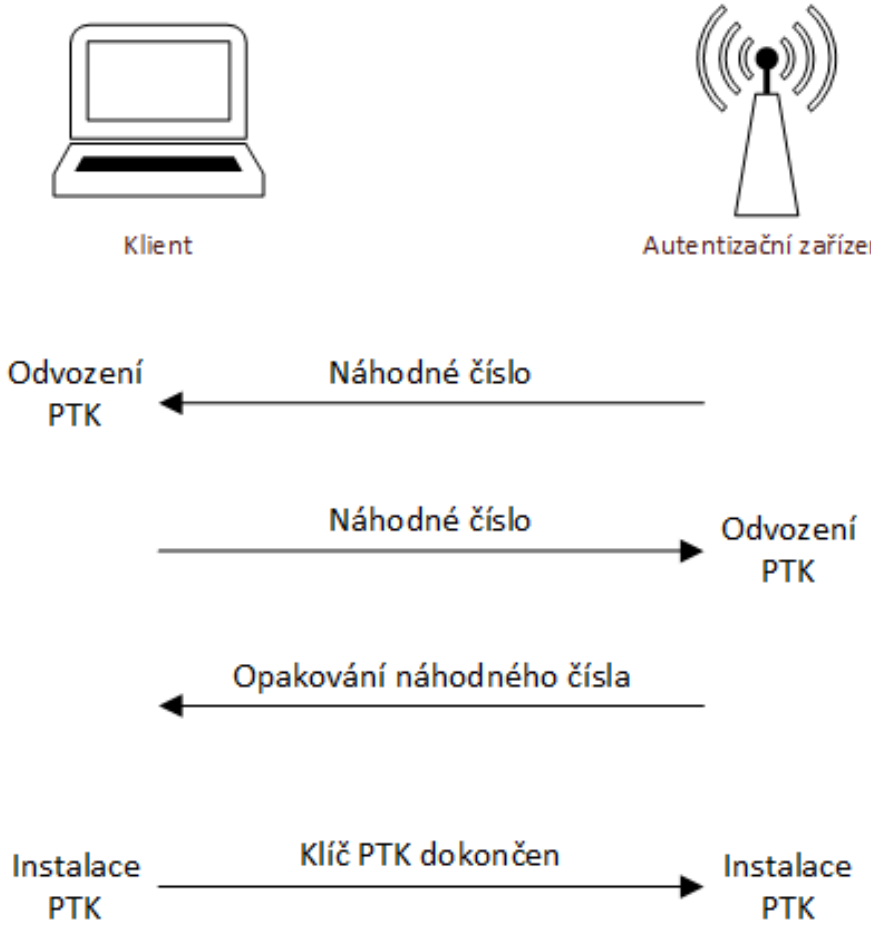


Obrázek 6 Autentizace WPA [1] (Vlastní zpracování)

Zabezpečení WPA využívá k výměně klíčů čtyřfázovou komunikaci, která probíhá následovně:

1. Autentizační zařízení vygeneruje náhodné číslo a odešle jej klientovi.
2. Klient pomocí společného klíče a přijatého čísla odvodí klíč, který použije k šifrování dat, které odesílá autentizačnímu zařízení. Klient poté vygeneruje náhodné číslo a společně s hodnotou MIC jej odešle autentizačnímu zařízení.
3. Autentizační zařízení odvodí klíč, kterým bude šifrovat data odesílaná klientovi. Poté autentizační zařízení znovu odešle náhodné číslo zašifrované odvozeným klíčem klientovi.
4. Klient odešle autentizačnímu zařízení oznámení, že je použit stejný odvozený klíč.

Čtyřfázovou komunikaci mezi klientem a autentizačním zařízením přibližuje obrázek 7. [2, 26, 27]



Obrázek 7 Čtyřfázová komunikace WPA [1] (Vlastní zpracování)

2.4.3 Zabezpečení WPA2

WPA2 je nástupcem zabezpečení WPA a byl schválen roku 2004. Zabezpečení WPA2 vychází ze standardu 802.11i, který podporuje více metod 802.1X a šifrování AES-CCMP. Z tohoto důvodu už nebylo možné WPA2 nasadit na starý typ hardwarových zařízení jako tomu bylo u WPA, ale musel být pořízen nový hardware. WPA2 již nepoužívá proudovou šifru RC4, ale využívá blokovou šifru AES (Advanced Encryption Standard). Šifra AES využívá šifrovací protokol CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol). Šifrování AES je považováno za velmi bezpečné a doposud nebylo prolomeno.

I toto zabezpečení je rozděleno na osobní WPA2-Personal a podnikový WPA2-Enterprise mód. Tyto módy pracují stejně jako u WPA.

Proces autentizace probíhá stejně jako u WPA a tento proces je zobrazen na obrázku 6 a obrázku 7. WPA2 pouze používá jiné šifrování, proces autentizace a připojení je ovšem shodný. [27]

2.4.4 Zabezpečení WPA3

WPA3 bylo schváleno a vydáno v roce 2018. Celých 14 let po vydání WPA2. Cílem WPA3 je ještě více zvýšit zabezpečení sítí a odstranit známe problémy, které má WPA2. WPA3 zachovává možnost vybrat mezi osobním WPA3-Personal a podnikovým WPA3-Enterprise módem. Navíc WPA3 přináší třetí mód nazvaný Wi-Fi Easy Connect, což je mód, který má co nejvíce zjednodušit proces připojení pro IoT zařízení, které jsou v posledních letech stále více rozšířené. Nasazení přístupového bodu se má stát ještě snadnějším pro nezkušené uživatele.

Změnou prošel WPA3-Personal mód, který nahrazuje PSK klíč (Pre-Shared Key) za metodu SAE (Simultaneous Authentication of Equals). Tato změna velmi ztěžuje útoky hrubou silou a slovníkové útoky. Jde vlastně o přidání další vrstvy mezi komunikující zařízení.

I podnikový WPA3-Enterprise prošel změnou a nyní požaduje 192-bitové šifrovací klíče a místo SAE se zde používá mechanismus Suite-B. Jde opět o přidání vrstvy mezi komunikující zařízení.

Proces autentizace u WPA3 probíhá totožně jako u WPA a WPA2 a je zobrazen na obrázku 6 a obrázku 7. [28]

II. PRAKTICKÁ ČÁST

3 STÁVAJÍCÍ STAV KONEKTIVITY NA BUDOVĚ U2

V této kapitole bude analyzován aktuální stav internetové konektivity na budově U2, což je budova Fakulty managementu a ekonomiky, která je součástí Univerzity Tomáše Bati ve Zlíně. Nejprve bude přiblížen historický vývoj síťové infrastruktury, kde bude zkoumán vývoj metalických datových rozvodů a vývoj bezdrátové sítě. Poté práce přiblíží technické prostředky, které byly využity pro sběr dat a jejich následné zpracování. V další části kapitoly se práce zaměří na identifikaci umístění přístupových bodů a jejich aktuální konfiguraci. V poslední části této kapitoly bude pomocí technických prostředků měřen a analyzován aktuální stav pokrytí bezdrátovým signálem na budově U2.

3.1 Historický vývoj internetové konektivity na budově U2

Tato kapitola se zaměřuje na historický vývoj internetové konektivity v budově U2. Tato analýza je nutná k pochopení vývojových fází a k identifikaci problematických oblastí.

3.1.1 Metalická datová infrastruktura

Budova U2 byla dokončena a zkolaudována na začátku 90. let. Již při dokončení budovy, byly instalovány datové rozvody. Tyto rozvody byly realizovány koaxiálním kabelem a byla využita sběrnicová topologie sítě. Přenosová rychlost dosahovala 10 Mbit/s. Pro každé podlaží byl instalován jeden samostatný segment. Segmenty jednotlivých podlaží byly mezi sebou propojeny přes zařízení multiconnect repeater, který byl později z důvodu propustnosti nahrazen Ethernet přepínačem, k němuž byly připojeny jednotlivé segmenty a vzniklá síť tak byla rozdělena do sedmi samostatných kolizních domén. Pro telefony byly instalovány samostatné telefonní rozvody, které byly zakončeny telefonní zásuvkou. V každé místnosti byla jedna EAD zásuvka se 2 přípojnými porty a koncová zařízení byla připojena tzv. EAD kabelem.

V roce 2000 došlo k instalaci strukturované kabeláže. Využita byla topologie hvězda, kdy byly všechny rozvody svedeny do společných datových rozvaděčů v prvním podzemním podlaží. Toto zapojení umožňovalo přenosové rychlosti maximálně 100 Mbit/s. Ke každé dvojzásuvce byl přiveden jeden UTP kabel, který byl rozdvojen pomocí speciálních ACO modulů na dva porty RJ-45 po čtyřech vodičích. Samostatné telefonní rozvody byly zrušeny a telefony byly připojeny po strukturované kabeláži, kdy byly v datových rozvaděčích propojeny příslušné porty s telefonní ústřednou budovy.

V roce 2013 došlo k nahrazení strukturované kabeláže novými UTP rozvody CAT 6A technologie SYSTIMAX, které podporují přenosové rychlosti 10 Gbit/s. Existují dvě datová centra. Hlavní je v prvním podzemním podlaží a podružné je v pátém nadzemním podlaží. Toto řešení bylo nutné z důvodu garance technologických délek jednotlivých segmentů do devadesáti metrů. Páté nadzemní podlaží je tedy svedeno na přepínač v pátém podlaží, který je propojen s hlavním datovým centrem. V pozdějších letech docházelo ke změnám a rozšiřování některých částí rozvodů v souvislosti s realizací různých projektů a rekonstrukcí. Aktuálně je v budově instalováno třicet kusů přepínačů v datových centrech a pět kusů lokálních přepínačů v učebnách.

3.1.2 Bezdrátová síť

Začátek bezdrátové sítě na budově U2 se datuje do roku 2005, kdy byly instalovány první přístupové body. Tyto přístupové body sloužili zpočátku především pro studenty fakulty a byly instalovány hlavně do větších společných prostor, kde se shromažďovalo velké množství studentů. Šlo především o foyer, chodby a vestibuly. Pro připojení těchto přístupových bodů byly ve stejném roce instalovány dodatečné rozvody metalické kabeláže z prvního podzemního podlaží. Jako první byly používány přístupové body Cisco Aironet AP1232, které podporovaly pouze 2,4 GHz frekvenci a podporovaly standardy 802.11b/g. V této době ještě neexistovali přepínače s PoE, proto se pro napájení přístupových bodů používaly tzv. Power Injectory, které byly instalovány mezi přepínačem a přístupovým bodem. Každý jednotlivý přístupový bod fungoval v autonomním módu. Všechny přístupové body tedy byly konfigurovány samostatně. V síti fungovaly dvě SSID, a to SSID UTB-STAFF, které bylo určeno pro zaměstnance a SSID UTB-STUDENT, které sloužilo studentům. Využívalo se zabezpečení WPA Enterprise/TKIP, ověřování uživatelů probíhalo proti RADIUS serveru. Přístupových bodů existovalo jedenáct.

V roce 2008 došlo k připojení bezdrátové sítě univerzity do federace eduroam, kdy byly všichni uživatelé převedeni pod SSID eduroam a byly zrušeny dříve používané SSID. Dle potřeb fakulty probíhalo postupné doplňování a výměna přístupových bodů za novější typ přístupových bodů Cisco Aironet AP1242AG, který podporoval frekvence 2,4 GHz a 5 GHz a standardy 802.11a/b/g/n.

V roce 2012 byl pro centrální řízení bezdrátové sítě pořízen Wireless Controller WiSM2, což je servisní modul do centrálního L3 přepínače Cisco Catalyst 6500 a současně byly

nahrazeny staré přístupové body modelem Cisco AIR-CAP 1602I, které podporují frekvence 2,4 GHz a 5 GHz a standardy 802.11a/b/g/n.

V posledních letech dochází k výměně vybraných přístupových bodů za přístupové body Cisco AIR CAP1702I a Cisco AIR CAP1832I, které podporují obě používané frekvence a podporují standardy 802.11a/b/g/n/ac. Současně se používá zabezpečení WPA2 Enterprise/AES, uživatelé jsou dále ověřování proti RADIUS serveru, který je propojen s databází na LDAP serveru. Z bezpečnostních důvodů je pro bezdrátovou síť vyžadováno jiné heslo, než které uživatelé využívají pro přístup k ostatním informačním systémům univerzity. Přístupové body jsou připojovány k distribučním přepínačům nebo k přístupovým přepínačům, zpravidla jde na budovách univerzity o kombinaci obojího.

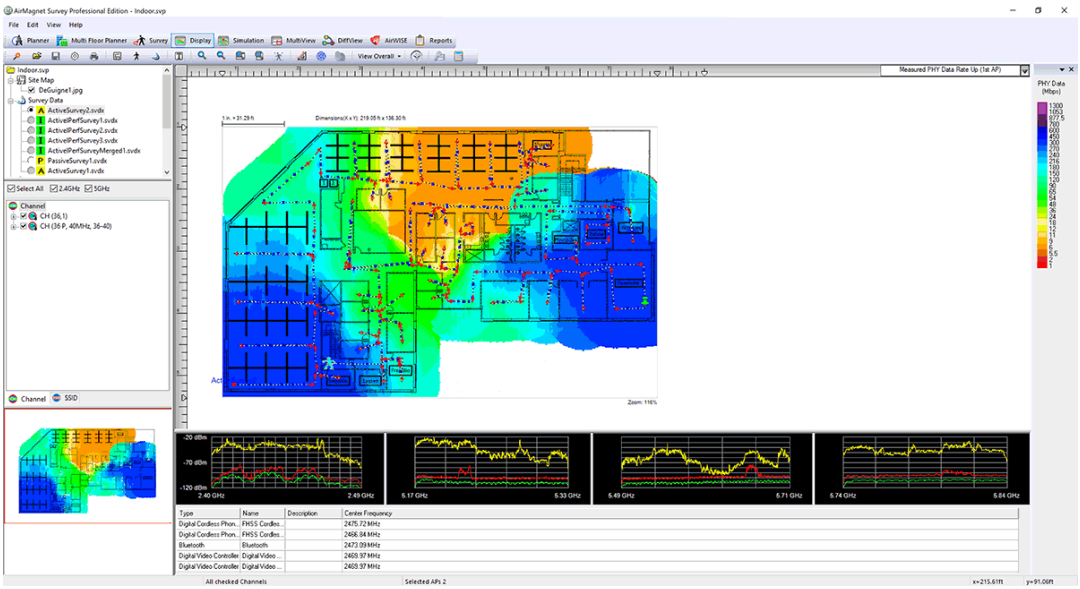
3.2 Použité prostředky

Před začátkem měření, analýzou a návrhem změn bylo nutné vybrat takové prostředky, které umožní měření a poskytnou přesná data o aktuálním stavu před samotnou optimalizací a také po optimalizaci, a umožní s daty dále pracovat a provádět různé druhy analýz. Jelikož se jedná o rozsáhlou podnikovou síť, která má vysoké nároky na výkon, dostupnost i bezpečnost nebylo možné použít zdarma dostupné nástroje, jelikož nedosahují takové míry přesnosti, která byla požadována a navíc nedokáží vytvářet modely, provádět simulace, pracovat s různými druhy přístupových bodů, a to vše v rámci jednoho softwaru. Těchto nástrojů na trhu není mnoho a můj výběr se zmenšil na software od firem Ekahau a NetAlly. Společnost Ekahau nabízí zdarma software Ekahau HeatMapper, pomocí kterého je možné vytvořit mapu pokrytí v určitém objektu, ovšem narazil jsem na četná omezení. Proto jsem oslovil obě společnosti sídlící v USA s žádostí o poskytnutí plné verze softwaru na zkušební dobu, během které bych realizoval všechny fáze práce. Nakonec jsem dokázal zajistit software od společnosti NetAlly. Jde o software AirMagnet Survey PRO a zajistil jsem jej přes české zastoupení společnosti NetAlly. Zároveň s tímto softwarem byl zapůjčen přístroj AirCheck G2, který slouží pro měření bezdrátových signálů. [29, 30]

3.2.1 Softwarové prostředky

Jak již bylo zmíněno výše, pro potřeby této práce jsem se rozhodl využít software AirMagnet Survey PRO, což je profesionální nástroj sloužící k plánování, měření bezdrátových sítí a následné analýze získaných dat. Tento software sdružuje různé druhy nástrojů, které jsou spjaty s bezdrátovými sítěmi. Samotný software nabízí nástroje pro různé fáze projektů

a užití. Jedna část softwaru slouží k návrhům bezdrátové infrastruktury v objektech a dokáže provádět simulaci šíření signálu. Další část softwaru se zaměřuje na měření bezdrátových signálů a následné zpracování získaných dat. V softwaru je také několik typů náhledů, kdy je možné pracovat s klasickým zobrazením plánu nebo pracovat s porovnávacím módem, kdy je možné srovnávat data získaná před změnami a po změnách. Další součástí tohoto softwaru je tzv. AirWISE, což je nástroj, který automaticky vyhodnotí data dle předem definovaných podmínek. Poslední funkcí softwaru je generování reportů, a to ze všech součástí softwaru. Tyto nástroje byly pro zpracování práce kritické a jelikož jsou součástí jednoho softwaru, byl tento software použit na zpracování všech částí práce. [30]



Obrázek 8 Software AirMagnet Survey PRO [30]

3.2.2 Hardwarové prostředky

Pro samotné měření byl využit ruční přístroj AirCheck G2, který slouží jako tester bezdrátových sítí, dokáže detekovat rušení, vyhledávat přístupové body a testovat připojení. Tento přístroj dokáže fungovat i samostatně, kdy jednou jeho funkcí je možné provést automatických test a zobrazit všechny relevantní informace, které mohou vést k rychlému řešení nejčastějších potíží s bezdrátovou sítí. Pro potřeby této práce jsem použil funkci AirMapper, která dokáže shromažďovat data v definovaných bodech na podkladu a shromážděná data exportovat pro hlubší analýzu do softwaru Airmagnet Survey PRO, která poskytuje mnohem větší možnosti analýzy a vizualizace dat. [31]

3.3 Analýza rozmístění přístupových bodů a identifikace míst se zvláštními požadavky

Před začátkem samotného měření pokrytí v budově U2 bylo nutné vytvořit pro každé patro plán s aktuálním umístěním všech přístupových bodů a identifikovat místa se zvláštními požadavky. Tyto plány již existovali jako podklady pro správce sítě, ovšem jejich poslední aktualizace proběhla v roce 2019. Od té doby proběhlo mnoho změn, které nebyly do plánů zavedeny, proto je nutné před započetím práce tyto podklady aktualizovat. Tyto plány budou sloužit správcům sítě a také poslouží pro potřeby této práce jako podklady pro model budovy, v němž se budou simulovat různé scénáře úprav a jejich dopad.

Jak je zmíněno výše, nejprve bylo nutné aktualizovat stávající plány všech pater a vyznačit v nich rozmístěné přístupové body a dále identifikovat prostory se zvláštními požadavky a určením. Proto je do plánů v každém patře přidán popis, o jaký typ místnosti se jedná, aby bylo možné identifikovat místnosti s vyššími požadavky na výkon a pokrytí a na tato místa se zaměřit. Popisy vychází z určení místnosti a názvosloví je odvozené od tohoto určení. Písmenem „U“ jsou označeny učebny, „K“ je označení kanceláří, „Z“ je označení zasedacích místností a „VK“ je označení významných kanceláří.

Rozdělení místností na kancelář a významnou kancelář je dáno především jinými požadavky na výkon a kvalitu bezdrátové sítě. Významná kancelář je označení takové kanceláře, ve které dochází k časté kumulaci osob. Jde především o kanceláře ředitelů ústavů, děkanů, tajemnic a proděkanů.

Ostatní kanceláře slouží akademickým pracovníkům a provozně-technickým zaměstnancům.

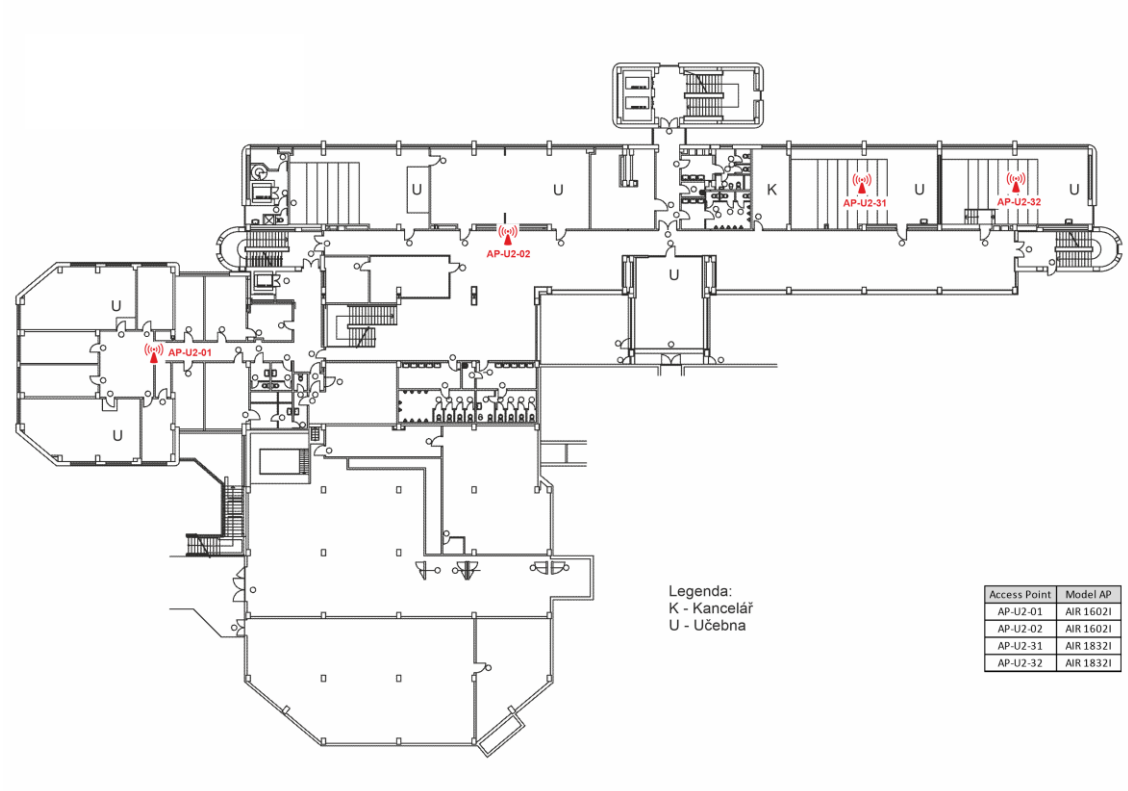
Zasedací místnosti slouží k zasedáním jednotlivých ústavů a dále různých pracovních skupin napříč ústavy a celou univerzitou, dochází zde také k častým jednáním s osobami mimo univerzitu a slouží také jako reprezentační prostory.

Učebny slouží k samotné výuce, a i zde jsou požadavky na výkon sítě a její zabezpečení vysoké. Jako kriticky důležité ovšem vnímám všechny významné kanceláře a zasedací místnosti, jelikož zde dochází ke schůzkám s osobami, které nejsou zaměstnanci univerzity a fungování bezdrátové sítě je možné již vnímat jako standard, a jejich funkčnost je možné vnímat i jako budování dobrého jména univerzity.

V těchto plánech je záměrně vynecháno druhé podzemní podlaží, jelikož toto podlaží již není součástí fakulty managementu a ekonomiky, ale patří pod fakultu technologickou. Není proto nutné toto podlaží zahrnovat do modelu ani zde provádět měření, jelikož tyto operace byly provedeny v roce 2019 při výstavbě nových prostor.

3.3.1 Plán prvního podzemního podlaží

V tomto patře jsou rozmístěné čtyři přístupové body a jsou zde především učebny. V pravé části budovy jsou umístěny dva přístupové body v podhledech v každé přednáškové místnosti, jelikož se jedná o nově zrekonstruované přednáškové místnosti a pokrytí zajišťují AP-U2-31 a AP-U2-32. Z kapacitních důvodů má každá místnost svůj vlastní přístupový bod. V levé části budovy jsou dvě počítačové učebny, kde je připojení realizováno pro mobilní zařízení uživatelů, především telefonů, jelikož jsou učebny vybaveny stolními počítači s pevným připojením. Tyto učebny jsou obklopeny kancelářemi, ovšem tyto kanceláře využívá Fakulta technologická. Celou tuto část pokrývá AP-U2-01. AP-U2-02 pokrývá zbývající dvě učebny, přičemž jedna z nich se nevyužívá, jelikož se jedná o rezervní místnost a patří rektorátu.

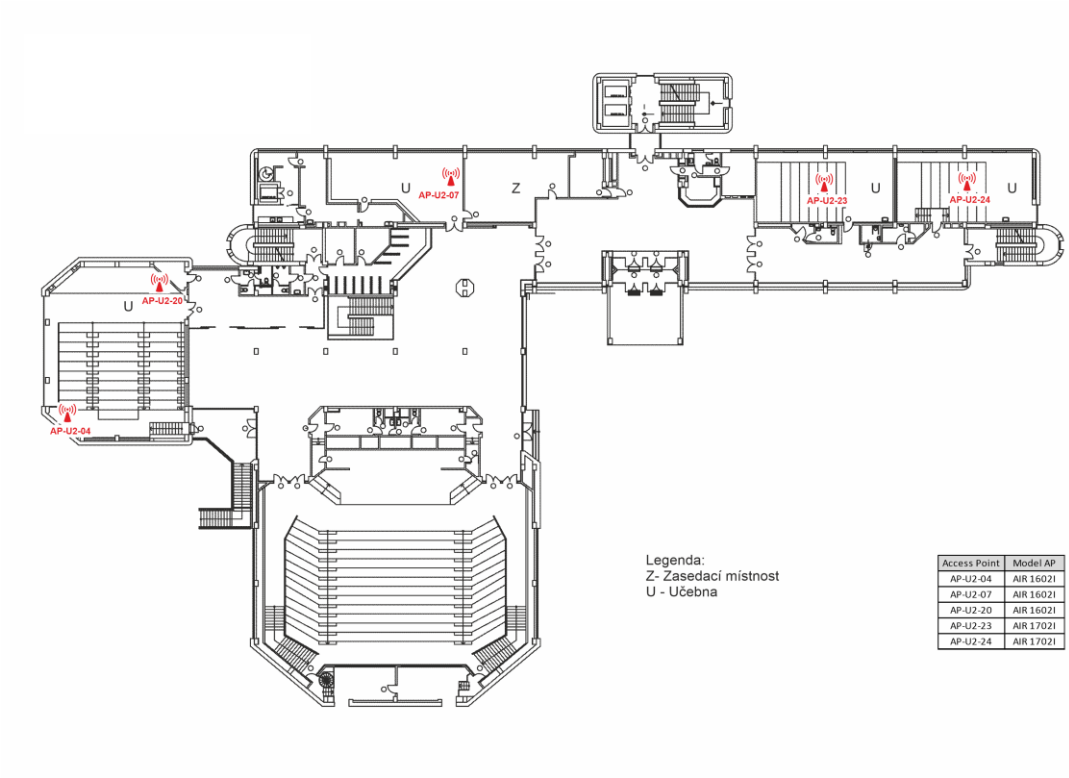


Obrázek 9 Plán prvního podzemního podlaží (Vlastní zpracování)

3.3.2 Plán prvního nadzemního podlaží

První nadzemní podlaží budovy pokrývá pět přístupových bodů a jsou zde především učebny. V levé části budovy se nachází velká přednášková místnost, proto ji pokrývá AP-U2-04 a později přidané AP-U2-20. Od hlavního vchodu směrem vlevo je také univerzitní aula. Tyto prostory jsou v době vypracování práce nepřístupné z důvodu generální rekonstrukce celé auly, jejího předsálí a šaten. Z tohoto důvodu také není možný přístup do přednáškové místnosti. V těchto místech tedy není možné provést zakreslení přístupových bodů, jelikož byly všechny odstraněny a budou nahrazeny v rámci rekonstrukce. V levé části podlaží je také nově rekonstruovaná zasedací místnost, vedle které je univerzitní bufet označený jako učebna, jelikož má stejnou prioritu pokrytí. Oba tyto prostory pokrývá AP-U2-07.

V pravé části budovy jsou dvě přednáškové místnosti, které prošly rekonstrukcí v roce 2018. V každé místnosti je přístupový bod umístěn v podhledu a pokrývá jednu přednáškovou místnost.

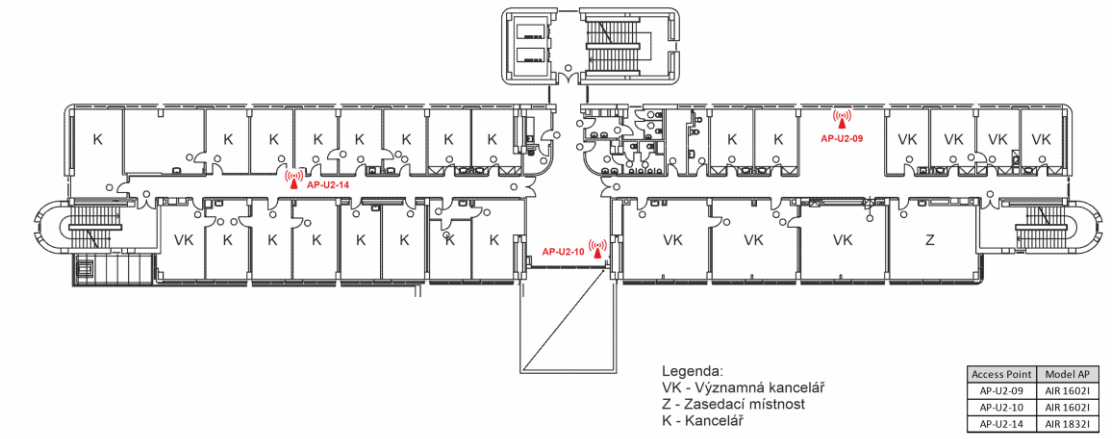


Obrázek 10 Plán prvního nadzemního podlaží (Vlastní zpracování)

3.3.3 Plán druhého nadzemního podlaží

Ve druhém podlaží budovy U2 jsou především kanceláře a také zasedací místnost. Toto patro slouží v levé části především provozně-technickým zaměstnancům a všechny kanceláře pokrývá AP-U2-14.

V pravé části budovy se nachází prostory děkanátu a jde o prostory s vysokými nároky na výkon a kvalitu. Nachází se zde také většina významných kanceláří. Všechny tyto prostory pokrývá AP-U2-09.

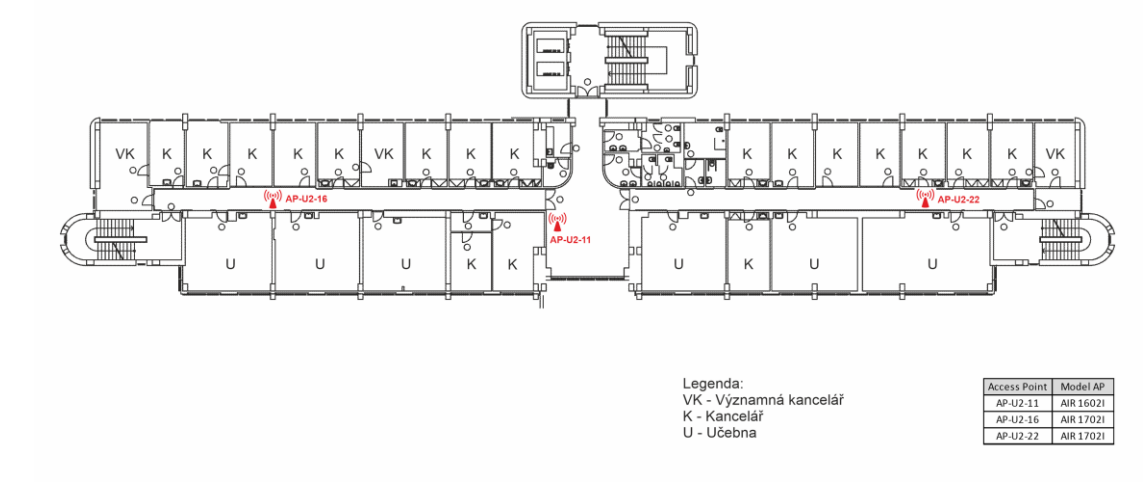


Obrázek 11 Plán druhého nadzemního podlaží (Vlastní zpracování)

3.3.4 Plán třetího nadzemního podlaží

Ve třetím podlaží se nachází menší přednáškové místnosti a kanceláře akademických pracovníků. Každá strana budovy slouží jinému ústavu. V levé části jsou dvě významné kanceláře a tři menší učebny. Tyto prostory pokrývá AP-U2-16.

V pravé části budovy se nachází dvě malé přednáškové učebny a také jedna počítačová učebna. Dále je zde jedna významná kancelář a kanceláře akademických pracovníků. Tyto prostory pokrývá AP-U2-22.

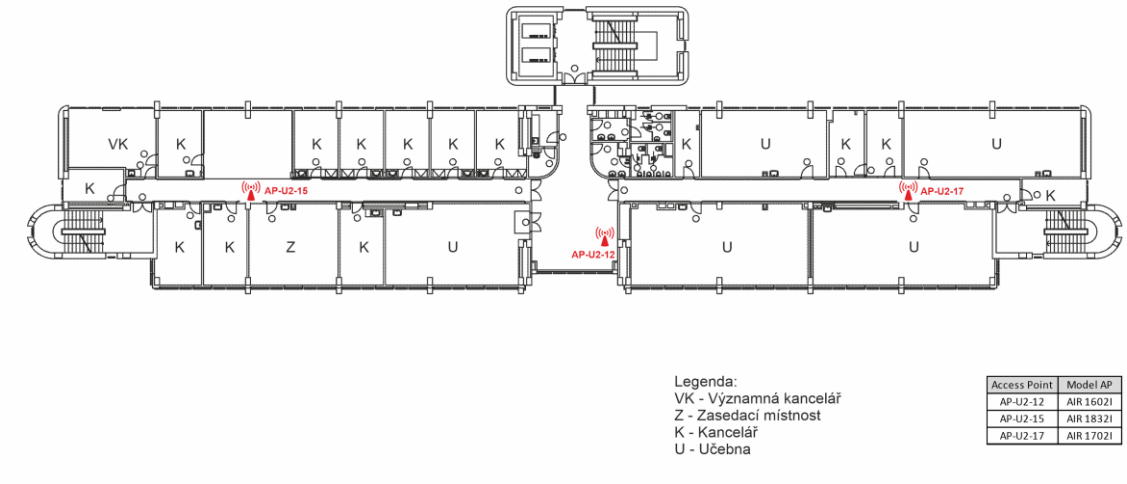


Obrázek 12 Plán třetího nadzemního podlaží (Vlastní zpracování)

3.3.5 Plán čtvrtého nadzemního podlaží

V tomto patře se v levé části nachází kanceláře akademických pracovníků a jedna významná kancelář. Nachází se zde také zasedací místnost. Dále se zde nachází počítačová učebna, kterou ovšem využívají pouze studenti U3V a nejedná se o klasickou učebnu. Tyto prostory pokrývá AP-U2-15.

V pravé části se nachází větší přednáškové učebny a jedna počítačová učebna. Tyto prostory pokrývá AP-U2-17.



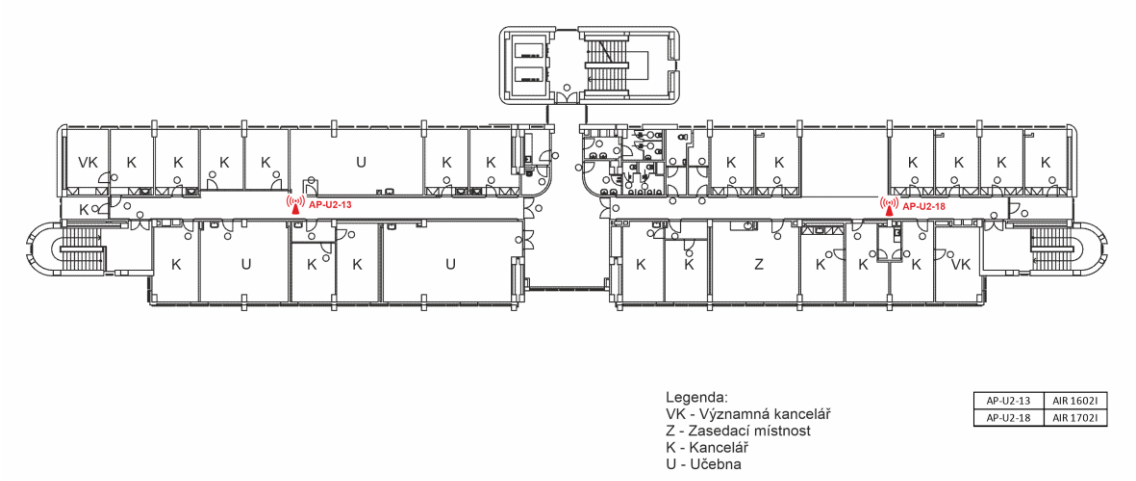
Obrázek 13 Plán čtvrtého nadzemního podlaží (Vlastní zpracování)

3.3.6 Plán pátého nadzemního podlaží

Poslední podlaží je také rozděleno na dvě části, přičemž každou část využívá jiný ústav. V levé části se nachází významná kancelář a kanceláře akademických pracovníků. Jsou zde

také dvě malé počítačové učebny a jedna větší přednášková učebna. Tyto prostory pokrývá AP-U2-13.

V pravé části podlaží se nachází významná kancelář, kanceláře akademických pracovníků a zasedací místnost. Tyto prostory pokrývá AP-U2-18.



Obrázek 14 Plán pátého nadzemního podlaží (Vlastní zpracování)

3.3.7 Analýza budovy a míst se zvláštním určením

V první řadě je nutné identifikovat všechny místa se zvláštními požadavky a určením. Toto rozdělení bylo provedeno v kapitole 3.3. Je také potřebné těmto místům přidělit určitou prioritu, aby bylo zřejmé, která místa musí splňovat ty nejvyšší požadavky na kvalitu, výkon a bezpečnost bezdrátové sítě. Rozdělení priorit není jednoduché, jelikož všechny prostory využívají sice jiné skupiny uživatelů, ovšem jsou si zcela rovny. Není možné ani jedné skupině z tohoto dělení dávat vyšší prioritu nad ostatními, jelikož pro studenty je důležité bezdrátové připojení pro potřeby studia, pro zaměstnance zase pro potřeby pracovních činností. Z hlediska pokrytí je tedy nutné, aby všechny prostory byly dostatečně pokryté bezdrátovým signálem. Z hlediska míst se zvláštními požadavky a určením je potřebné věnovat zvýšenou pozornost významným kancelářím a zasedacím místnostem, jelikož zde dochází k častým zasedáním, poradám a pracovním schůzkám. Proto se práce zaměřuje především na tato místa, ale pouze z pohledu na bezpečnost a výkon.

Z výše uvedených popisů jednotlivých pater je zřejmé, že budova je rozdělena do určitých logických bloků. První podzemní podlaží a první nadzemní podlaží slouží především pro potřeby výuky a jde i o reprezentační prostory. V těchto podlažích jsou především větší přednáškové učebny. Ve druhém nadzemním podlaží jsou prostory děkanátu a kanceláře

většiny provozně-technických zaměstnanců, proto se bude práce zaměřovat nejvíce na tyto prostory. Ve třetím, čtvrtém a pátém patře jsou všechny kanceláře akademických pracovníků, menší přednáškové a také počítačové učebny. Sídlí zde také všechny ústavy. Dále je pak zřejmé, že na těchto patrech na obou okrajích budovy jsou významné kanceláře, proto se práce zaměřuje i na tyto prostory, jelikož se stranami budovy bývají spojeny největší problémy.

3.4 Používané typy AP

Tato kapitola se zaměřuje na popis aktuálně používaných typů přístupových bodů na fakultě. Jsou zde uvedeny pouze nejdůležitější specifikace přístupových bodů, které jsou důležité z hlediska následného modelování a přiblížení rozdílů mezi jednotlivými typy.

3.4.1 Cisco AIR CAP1602I

Tento přístupový bod podporuje frekvence 2,4 GHz, 5 GHz a podporuje standardy 802.11a/b/g/n. Jde o přístupový bod pro malé a středně velké podnikové sítě. Jde o lehký přístupový bod, který musí být připojen a konfigurován přes bezdrátový řadič. Využívá technologii 3x3 MIMO, kdy využívá tři antény pro vysílání a tři pro příjem signálu. Maximální rychlost přístupového bodu je 300 Mbps. Poskytuje také pokročilé funkce jako CleanAir pro lepší pokrytí a Clientlink 2.0, která zlepšuje konektivitu klientů, kteří používají starší standardy. [32]

Obrázek 15 Přístupový bod Cisco Aironet 1602I [32]

3.4.2 Cisco AIR CAP1702I

Tento přístupový bod podporuje frekvence 2.4 GHz, 5 GHz a podporuje standardy 802.11a/g/n/ac. Jde o přístupový bod pro malé a středně velké podnikové sítě. Jde také o lehký přístupový bod, který musí být připojen k bezdrátovému řadiči, kde probíhá jeho konfigurace a správa. Oproti předchozímu přístupovému bodu podporuje standard 802.11ac, díky čemuž je schopný na 5 GHz frekvenci dosáhnout vyšší rychlosti přenosu. Využívá technologii 3x3 MIMO. Maximální teoretická rychlost přístupového bodu je 867 Mbit/s. Poskytuje pokročilé funkce jako CleanAir pro lepší pokrytí a lépe optimalizovaný roaming. [33]

Obrázek 16 Přístupový bod Cisco Aironet 1702I [33]

3.4.3 Cisco AIR CAP1832I

Tento přístupový bod patří mezi nejnovější používané. Podporuje frekvence 2,4 GHz a 5 GHz a podporuje standardy 802.11a/g/n/ac. Také se jedná o přístupový bod pro malé až středně velké podnikové sítě. Jde o lehký přístupový bod, který musí být připojen k bezdrátovému řadiči. Maximální teoretická rychlost přenosu je 867 Mbit/s. Využívá technologii 3x3 MU-MIMO. Jde o stejnou technologii vysílání a příjmu signálu, ovšem dokáže obsloužit více uživatelů současně. [34]

Obrázek 17 Přístupový bod Cisco Aironet 1832I [34]

3.5 Nastavení bezdrátového řadiče

Všechny přístupové body jsou připojeny k bezdrátovému řadiči, který je umístěn na hlavním přepínači. Nastavení jednotlivých přístupových bodů probíhá na řadiči. Řadič upravuje automaticky kanál, který má daný přístupový bod použít a výkon. Nastavení kanálů a výkonu v den prvního měření a vytváření modelu zobrazují následující tabulky pro 2,4 GHz a 5 GHz frekvence. Z těchto tabulek jsou záměrně vyřazeny přístupové body, které se nachází ve druhém podzemním podlaží.

3.5.1 Nastavení bezdrátového řadiče pro 2,4 GHz frekvenci

Tabulka 1 zobrazuje nastavení jednotlivých přístupových bodů na bezdrátovém řadiči pro 2,4 GHz frekvenční pásmo v době prvního měření. Řadič automaticky volí kanál a výkon. U některých přístupových bodů je výkon nastaven ručně. K těmto nastavením docházelo ve chvíli, kdy uživatelé měli problémy s výpadky sítě, a pokud to bylo možné, byl zvednut výkon na nejbližším přístupovém bodu pro odstranění problémů. Hodnoty s hvězdičkou jsou nastaveny automaticky řadičem.

Tabulka 1 Nastavení WLC pro 2,4 GHz

Název AP	Kanál	Výkon
AP-U2-01	1*	1*
AP-U2-02	1*	1*
AP-U2-03	1*	4*
AP-U2-04	1*	1*
AP-U2-05	6*	1*
AP-U2-06	6*	2*
AP-U2-07	11*	1*
AP-U2-08	11*	1*
AP-U2-09	1*	2*
AP-U2-10	11*	1*
AP-U2-11	11*	2*
AP-U2-12	1*	2*
AP-U2-13	11*	1
AP-U2-14	1*	2*
AP-U2-15	6*	2
AP-U2-16	11*	1*
AP-U2-17	11*	4*
AP-U2-18	1*	2*
AP-U2-19	1*	1*
AP-U2-20	6*	1*
AP-U2-22	1*	2*
AP-U2-23	11*	3*
AP-U2-24	6*	3*
AP-U2-31	6*	5*
AP-U2-32	1*	5*

3.5.2 Nastavení bezdrátového řadiče pro 5 GHz frekvenci

Tabulka 2 zobrazuje nastavení jednotlivých přístupových bodů na bezdrátovém řadiči pro 5 GHz frekvenční pásmo v době prvního měření. I zde je kanál a výkon řízen automaticky řadičem. Hodnoty s hvězdičkou jsou nastaveny automaticky řadičem.

Tabulka 2 Nastavení WLC pro 5 GHz

Název AP	Kanál	Výkon
AP-U2-01	48*	1*
AP-U2-02	40*	1*
AP-U2-03	36*	1*
AP-U2-04	40*	1*
AP-U2-05	44*	1*
AP-U2-06	60*	1*

AP-U2-07	48*	1*
AP-U2-08	64*	1*
AP-U2-09	36*	1*
AP-U2-10	36*	1*
AP-U2-11	44*	1*
AP-U2-12	36*	1*
AP-U2-13	36*	1*
AP-U2-14	40*	1*
AP-U2-15	40*	2
AP-U2-16	36*	1*
AP-U2-17	64*	1*
AP-U2-18	52*	1*
AP-U2-19	36*	1*
AP-U2-20	36*	1*
AP-U2-22	40*	1*
AP-U2-23	48*	1*
AP-U2-24	40*	1*
AP-U2-31	36*	2*
AP-U2-32	48*	2*

3.6 Model stávajícího stavu pokrytí

V první fázi bylo potřebné vytvořit co nejvěrnější model budovy. K tomuto účelu posloužil AirMagnet Planner, který je součástí výše zmíněného softwaru. Jelikož je budova víceposchoďová použil jsem Multi Floor Planner, který funguje podobně, ovšem zohledňuje více podlaží a působení signálu mezi jednotlivými podlažími.

Nejprve bylo nutné nastavit výšku jednotlivých podlaží, šířku podlah a útlum dle použitého materiálu mezi podlažími. Poté byly nahrány plány jednotlivých pater. V dalším kroku je nutné provést kalibraci jednotlivých plánů, kdy je nadefinována pro osu X i osu Y reálná vzdálenost dvou vybraných bodů na podkladu pro každé patro. Tento krok zajistí, že simulace šíření signálu bude věrnější, jelikož model bude pracovat s reálnými vzdálenostmi. Po kalibraci je potřebné pro správnou funkci provést vystředění pater v ose Z. Při tomto kroku jsou definovány dva stejné body mezi dvěma patry, přičemž jedno patro slouží jako podklad, nad který se budou ostatní podlaží středit a jednotlivá patra se postupně nad sebou vystředí. Tento postup je opakován pro každé patro, dokud nedojde k vyrovnání budovy v ose Z. Tento krok je velmi důležitý pro správné vykreslení simulace šíření signálu, jelikož signál se bude šířit i mezi patry korektně.

Dalším krokem při tvorbě modelu je definování různých stavebních materiálů s různým útlumem. V softwaru jsou předdefinovány nejvíce používané materiály, které se pouze zakreslí na podkladové plány. Tímto způsobem se na každém patře definuje materiál zdí, dveří, oken atp.

V posledním kroku se umístí všechny přístupové body, přičemž je možné pro každý přístupový bod definovat jaký mají název, kanál, výkon, název SSID, jaký používají standard, a především pak charakteristiku vyzařovaného signálu anténou. Toto nastavení je možné provést pro 2,4 GHz i 5 GHz pásmo.

Po umístění všech přístupových bodů do všech pater a jejich co nejpřesnějším nastavení je možné spustit simulaci, která ukazuje, jakým způsobem se bude šířit signál, jaké budou útlumy v jednotlivých místech budovy, kde dochází k překrývání kanálů, jaká je předpokládaná rychlost stahování i nahrávání atp.

Tento model slouží jako podklad aktuálního stavu a odkryl několik míst se slabším pokrytím, která již byla monitorována z důvodů občasných výpadků signálu a upozorněním na špatnou kvalitu signálu od uživatelů. Tento model bylo ovšem nejprve nutné validovat ještě před tím, než by byl model využit pro simulaci změn. Proto bylo nutné nejprve model porovnat s reálně získanými výsledky měření.

Výsledky simulací šíření signálu jsou součástí příloh. Příloha PI-PVI zobrazuje simulaci pokrytí pro první podzemní podlaží až páté nadzemní podlaží. Příloha PVII zobrazuje simulaci šíření mezi patry.

3.7 Měření pokrytí

Druhou fází této práce bylo po vytvoření modelu změření signálu ve všech patrech a všech prostorách budovy. Účelem tohoto měření je získání celkového obrazu o stavu bezdrátového pokrytí ve všech prostorách budovy a následné porovnání s modelem pomůže model validovat. V tomto kroku bylo nutné pozorovat, zda vytvořený model odpovídá skutečně naměřeným hodnotám a je možné jej využít pro modelování a simulaci změn. Měření má také posloužit k přesné analýze pokrytí v celé budově, odhalit nedostatky a získat celkový přehled o stavu pokrytí a kvalitě signálu. Jedná se o historicky první měření celkového pokrytí na této budově.

Samotné měření bylo prováděno ručním přístrojem AirCheck G2. Toto zařízení je připojené do cloudu společnosti NetAlly kam přenáší výsledky měření, které je poté možné exportovat

k hlubším analýzám do softwaru. Nejprve se tedy zařízení připojilo ke cloudu, kam byly nahrány plány jednotlivých pater a byla provedena kalibrace těchto plánů. Poté se z cloudu tyto podklady nahrály do zařízení. Zařízení má funkci AirMapper, která dokáže naměřené hodnoty přiřadit přesnému bodu v prostoru.

Měření tedy probíhalo tak, že se po spuštění funkce AirMapper vybral správný plán patra, provedla se jeho kalibrace a poté započalo měření. Měření bylo provedeno tak, že se měřila předem definována trasa a po definování bodu na plánu se provedlo měření. Tyto body jsem vybíral na plánu dle aktuální, co nejpřesnější polohy. Body jsou od sebe vzdáleny cca 3 metry, což se osvědčilo jako dostatečná vzdálenost pro dosažení přesných výsledků. V každé kanceláři bylo umístěno minimálně šest bodů, v každé učebně dle její rozlohy více. Po změření celého patra se výsledky měření přenesly zpět na cloud. Toto měření bylo provedeno v každém patře dle stejného klíče. Poté byly všechny výsledky z cloudu exportovány a vloženy do softwaru Airmagnet Survey Pro a analyzovány. V následující kapitole jsou zobrazeny a komentovány výsledky měření pouze na nedostatečně pokrytých místech.

Dalším parametrem, který je nutné definovat je přijatelná velikost útlumu. V místech se slabým signálem bylo vyzkoušeno několik různých používaných mobilních zařízení, které měli pomoci definovat, jak velký útlum je hraniční pro bezproblémové fungování těchto zařízení. S pomocí tohoto testu byly hodnoty útlumu nadefinovány následovně:

- Útlum menší než 50 je vynikající signál bez výpadků.
- Útlum mezi 50-60 je dostatečný signál.
- Útlum 60-70 je podprůměrný signál kdy dochází k výpadkům a kolísání připojení.
- Útlum větší než 70 je velmi podprůměrný a dochází k častému kolísání a výpadkům.

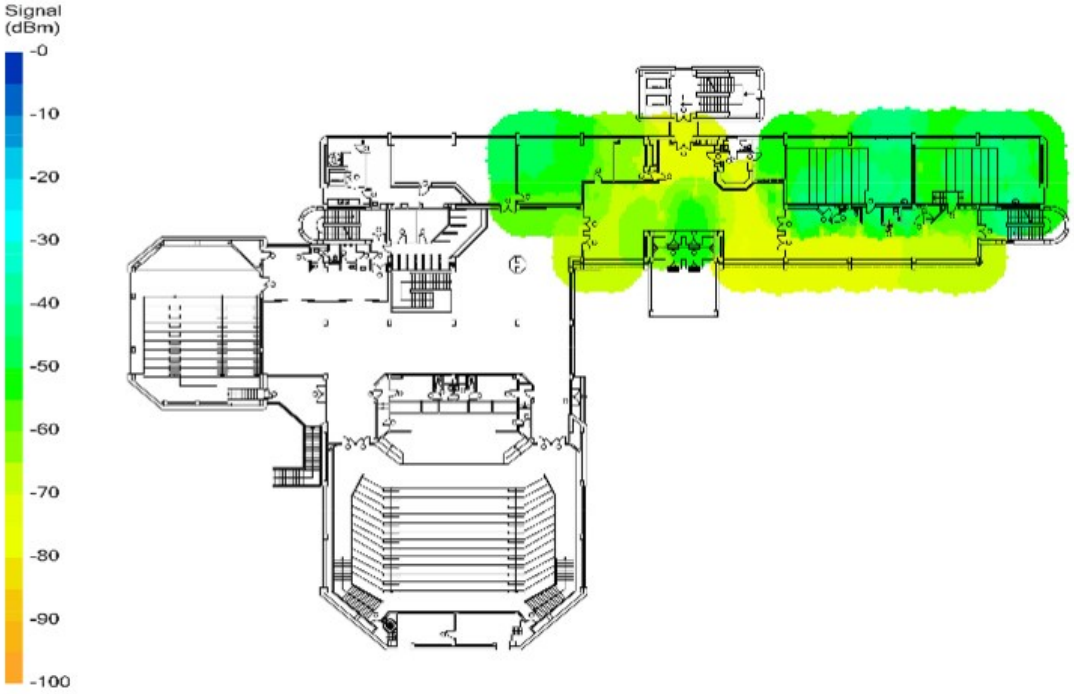
3.7.1 Výsledky měření signálu v prvním podzemním podlaží

Měření odhalilo vyšší útlum signálu v pravé části budovy na chodbě. V těchto prostorách má v budoucnosti vzniknout odpočinková zóna pro studenty, nyní je zde sezení pro studenty rozmístěné v celé délce chodby. Dalším slabým místem je posluchárna v levé části budovy, kde v zadní části je útlum vyšší a může docházet k výpadkům a nižšímu výkonu sítě. Toto nedostatečné pokrytí je dáno především probíhající rekonstrukcí v prvním nadzemním podlaží, jelikož z něj byly odstraněny přístupové body, které byly přímo nad touto místností a v minulosti zde nebyly hlášeny žádné problémy s připojením.

Obrázek 18 Výsledek měření v prvním podzemním podlaží (Vlastní zpracování)

3.7.2 Výsledky měření signálu v prvním nadzemním podlaží

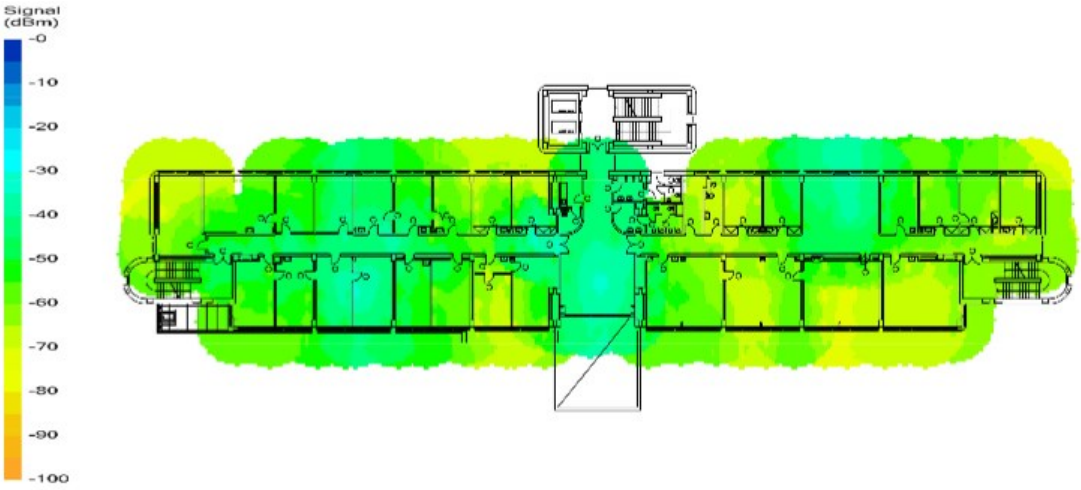
Z výsledků měření je zřejmé, že nedostatečné pokrytí je přímo u vstupu do budovy a dále v pravé části před přednáškovými učebnami. V těchto místech je také zřízeno sezení pro studenty. Jak již bylo zmíněno výše, bohužel nebylo možné provést měření v celé levé části budovy z důvodu probíhající rekonstrukce.



Obrázek 19 Výsledek měření v prvním nadzemním podlaží (Vlastní zpracování)

3.7.3 Výsledky měření signálu ve druhém nadzemním podlaží

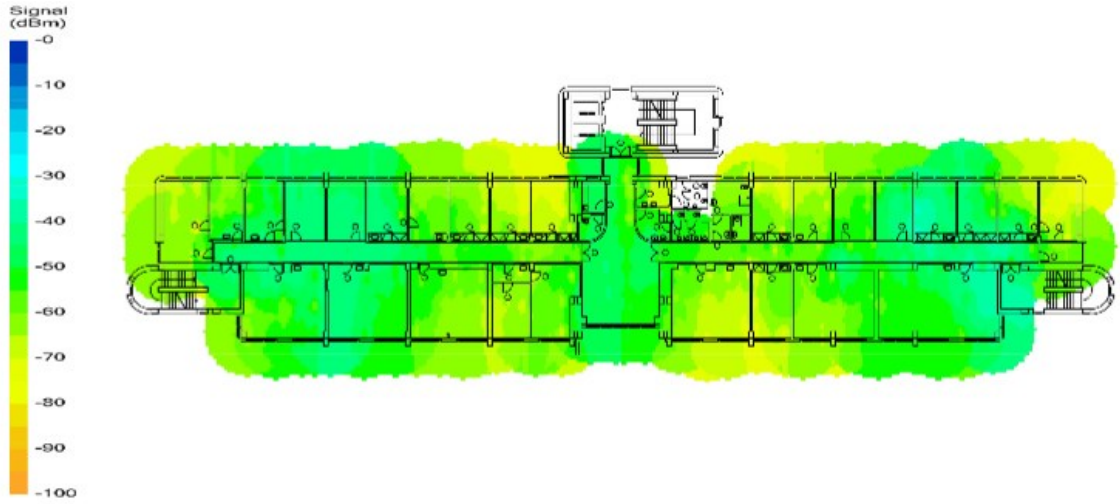
Výsledky odhalily v tomto důležitém patře nedostatečné pokrytí na obou stranách podlaží. V levé části je nedostatečně pokrytý roh budovy, kde se nachází kancelář a dále uprostřed budovy v dalších kancelářích. V pravé části budovy měření odhalilo nedostatečné pokrytí v zájmových prostorách, jako jsou významné kanceláře a v zasedací místnosti.



Obrázek 20 Výsledek měření ve druhém nadzemním podlaží (Vlastní zpracování)

3.7.4 Výsledky měření signálu ve třetím nadzemním podlaží

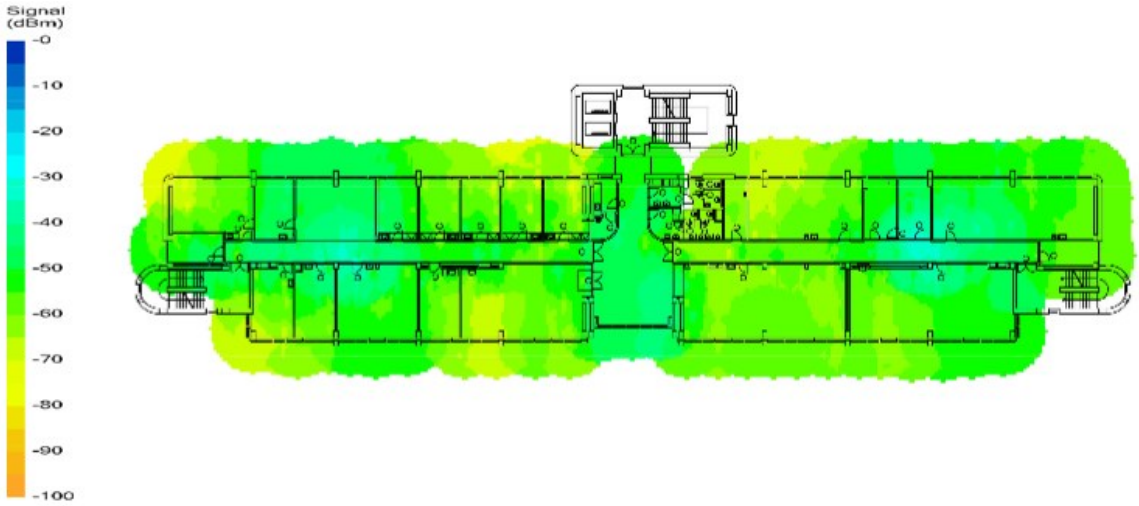
Měření odhalilo ve třetím podlaží nedostatečné pokrytí na obou krajích budovy, kde jsou významné kanceláře a také uprostřed budovy, kde se nacházejí kanceláře akademických pracovníků.



Obrázek 21 Výsledek měření ve třetím nadzemním podlaží (Vlastní zpracování)

3.7.5 Výsledky měření signálu ve čtvrtém nadzemním podlaží

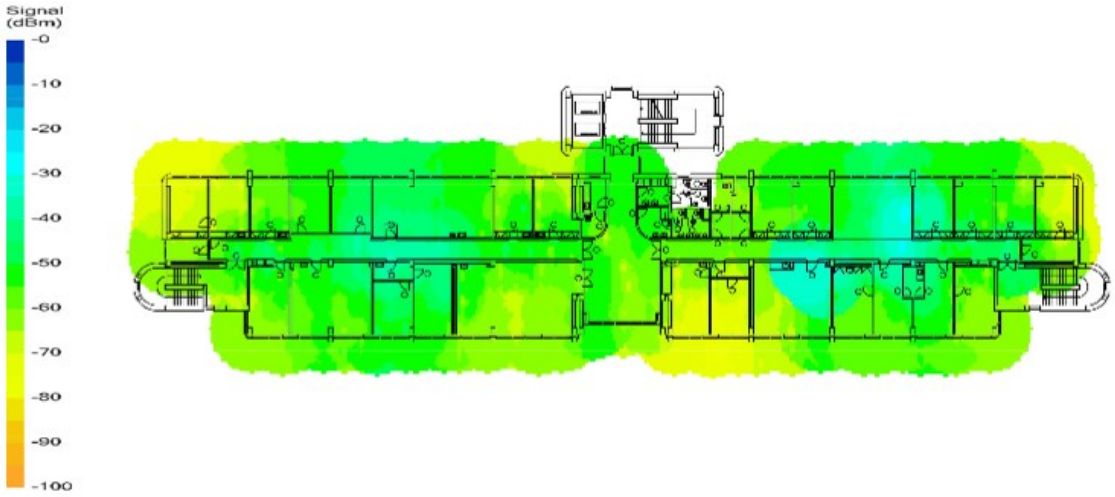
Měření odhalilo na tomto patře velmi málo špatně pokrytých míst. V levé části budovy jde o významnou kancelář v jedné její části, kde zrovna ovšem leží pracovní plocha zaměstnance.



Obrázek 22 Výsledek měření ve čtvrtém nadzemním podlaží (Vlastní zpracování)

3.7.6 Výsledky měření signálu v pátém nadzemním podlaží

V tomto patře měření odhalilo hned několik míst s nedostatečným pokrytím. Jedná se o oba okraje budovy a také o prostřední část budovy kde se nachází kanceláře akademických pracovníků.



Obrázek 23 Výsledek měření v pátém nadzemním podlaží (Vlastní zpracování)

3.7.7 Analýza aktuálního stavu

Měření celé budovy odhalilo hned několik slabých míst v pokrytí. V prvním podzemním podlaží a prvním nadzemním podlaží jde především o nedostatečně pokryté chodby, kde mají studenti odpočinkové a studijní zóny. Dále ve druhém nadzemním podlaží na levém kraji budovy a ve významných prostorách na pravé straně budovy. V podlaží třetím, čtvrtém a pátém měření odhalilo nedostatečné pokrytí na obou okrajích budovy, které jsou definovány jako významné kanceláře a několik slabších míst náhodně se vyskytující v jiných prostorách. Práce se zaměří na všechny odhalené nedostatky a vhodným způsobem se je pokusí odstranit.

Měření bylo nutné provést také z důvodu validace připraveného modelu. Porovnáním reálných hodnot získaných měřením s vytvořeným modelem bylo odhaleno jen několik nepřesností, jelikož model není schopen simulovat všechny možné vyskytující se odrazy a vyšší útlumy způsobené členitostí budovy nebo silnějšími zdmi v určitých místech. Ovšem až na několik nepřesností se model téměř rovnal získaným datům, z toho důvodu bylo možné model považovat za předlohu aktuálního stavu a využít ho k simulaci změn.

4 OPTIMALIZACE INTERNETOVÉ KONEKTIVITY

V této části se práce zabývá navrženými změnami, které mají pomoci zlepšit pokrytí na budově. Práce popisuje další úkony, kdy nejprve přiblíží, jakým způsobem byly změny navrhovány, dále přiblíží, jaké změny byly navrženy a následně realizovány. V poslední fázi práce popíše, jak se pokrytí budovy změnilo po realizaci všech navržených změn.

4.1 Optimalizační model

Pro vytvoření různých návrhů, které měli pomoci zlepšit pokrytí byl využit model, který je součástí přílohy PI-PVI. V tomto modelu jsou simulovány změny v pokrytí při posunu a přenastavení výkonu u různých přístupových bodů, dokud nedošlo k pokrytí celého patra signálem s útlumem v rozmezí 40-65 dB jakožto krajní hodnoty pro stabilní připojení. Dle tohoto modelu došlo k přemístění a přenastavení dotčených přístupových bodů. Model po optimalizace je dostupný v příloze PVII-PXIII.

Po validaci modelu, který odpovídá aktuálnímu rozmístění všech přístupových bodů na budově a odpovídá reálně naměřeným hodnotám byl tento model použit pro simulaci změn v pokrytí při různých nastaveních a přemístěních přístupových bodů. Tato fáze měla pomoci vyřešit problematická místa, která se nachází na téměř každém patře. Model má sloužit jako podklad pro provedení změn, jelikož na takto rozsáhlé síti není možné za provozu zkoušet způsobem pokus-omyl, zda se pokrytí zlepší. Jelikož je změny nutné provést mimo běžný provoz, který je od 6:00 do 22:00, musí být změny provedeny v co nejkratším čase. V době vypracování této práce je nařízená distanční výuka, z toho důvodu není možné provádět změny v takovém rozsahu v běžném provozu, jelikož většina zaměstnanců využívá své kanceláře k zajištění distanční výuky. Po samotné realizaci změn je také nutné prověřit její reálné dopady na stav pokrytí. Jelikož byly v referenčním modelu drobné nesrovnalosti s reálně naměřenými hodnotami v určitých místech budovy, každá provedená změna musela být ověřena z hlediska reálných dopadů na stav pokrytí.

V simulacích bylo provedeno několik desítek různých přesunů a nastavení, které měli za cíl zlepšit pokrytí ve dříve identifikovaných místech. Samotná optimalizace v modelu probíhala po jednotlivých patrech a jednotlivých identifikovaných místech. Cílem bylo zachovat stejný počet přístupových bodů bez nutnosti přidávat další a jen pomocí změn ve výkonu jednotlivých přístupových bodů a jejich umístění dosáhnout celkové optimalizace bezdrátové sítě. Všechny simulované změny byly několikrát analyzovány z hlediska dopadů

změn na pokrytí a blízko umístěné přístupové body. Analýza dopadů byla prováděna především v identifikovaných místech a byl zkoumán vliv změn proti referenčnímu modelu. V kapitole 4.3 budou popsány dislokační změny jednotlivých přístupových bodů. V kapitole 4.2. budou popsány provedené změny ve výkonu jednotlivých přístupových bodů. Kapitola 4.4 se zabývá měřením signálu v budově po realizaci změn a budou zde popsány reálné dopady jednotlivých změn v identifikovaných místech.

Po provedení a analýze několika možných scénářů byl vybrán a realizován pouze ten, který dle simulace splňoval všechny požadavky a dokázal odstranit problémy v zájmových prostorách. Tento model je součástí příloh PVI-PVIII.

Nejprve se změny týkaly nastavení výkonu jednotlivých přístupových bodů. Z reálných výsledků měření byl analyzován dle typu přístupového bodu jejich dosah při nastaveném výkonu. Jelikož jsou na budově tři typy přístupových bodů s různými nastaveními výkonu, provedl jsem analýzu jednotlivých typů a sledoval, jaký mají dosah dle jejich výkonu. Tato analýza pomohla porovnat mezi sebou typy přístupových bodů z hlediska dosahu, aby bylo možné předurčit reálnou změnu pokrytí při zvýšení výkonu. Pomocí tohoto nastavení se mělo dosáhnout pokrytí slabších míst bez nutnosti přidávat nebo přesunovat přístupové body. Toto nastavení se nejprve provedlo v modelu, kde se na dotčených přístupových bodech zvýšil výkon a následná simulace zobrazila dopad těchto změn.

V místech, kde ani zvýšení výkonu nepomohlo k pokrytí identifikovaných míst bylo nutné přistoupit k přemístění přístupových bodů tak, aby byla tato místa eliminována.

4.2 Návrhy na přenastavení bezdrátového řadiče

Při optimalizaci byl kladen důraz na zachování stejného počtu přístupových bodů. Během simulací byl tento požadavek brán v potaz, a proto docházelo i k nastavení různých úrovní výkonu na přístupových bodech. Následující tabulky zobrazují kanál a úroveň výkonu u jednotlivých přístupových bodů ve frekvenčním pásmu 2,4 GHz a 5 GHz po provedení přesunů identifikovaných přístupových bodů. U některých byl výkon navýšen manuálně, zbylé dále řídí bezdrátový řadič. Z tabulek jsou vynechány ty přístupové body, které se nachází na druhém podzemním podlaží.

4.2.1 Nastavení bezdrátového řadiče pro 2,4 GHz frekvenci

Tabulka 3 zobrazuje nastavení jednotlivých přístupových bodů na bezdrátovém řadiči pro 2.4 GHz frekvenční pásmo po aplikaci změn. Řadič automaticky volí kanál a výkon. U

některých přístupových bodů je výkon nastaven ručně. K těmto nastavením docházelo z důvodu lepšího pokrytí signálem v prostorách, kde byl identifikován nedostatečný signál. Změny ve výkonu a jejich důvod jsou popsány v následující kapitole. Hodnoty s hvězdičkou jsou nastaveny automaticky řadičem.

Tabulka 3 Nastavení WLC pro 2,4 GHz

Název AP	Kanál	Výkon
AP-U2-01	1*	1*
AP-U2-02	6*	1*
AP-U2-03	1*	1
AP-U2-04	1*	1*
AP-U2-05	11*	1*
AP-U2-06	1*	2*
AP-U2-07	11*	1*
AP-U2-08	11*	1*
AP-U2-09	1*	1
AP-U2-10	6*	1*
AP-U2-11	11*	2*
AP-U2-12	1*	2*
AP-U2-13	11*	1
AP-U2-14	1*	1
AP-U2-15	6*	2*
AP-U2-16	11*	1*
AP-U2-17	11*	2*
AP-U2-18	1*	2*
AP-U2-19	1*	1*
AP-U2-20	6*	1*
AP-U2-22	1*	2*
AP-U2-23	11*	1
AP-U2-24	6*	2*
AP-U2-31	6*	2
AP-U2-32	1*	5*

4.2.2 Nastavení bezdrátového řadiče pro 5 GHz frekvenci

Tabulka 4 zobrazuje nastavení jednotlivých přístupových bodů na bezdrátovém řadiči pro 5 GHz frekvenční pásmo po aplikaci změn. U identifikovaných přístupových bodů došlo k manuálnímu zvýšení výkonu a je shodný se změnami, které byly provedeny v 2.4 GHz frekvenčním pásmu. Důvody těchto změn je popsány v následující kapitole. Hodnoty s hvězdičkou jsou nastaveny automaticky řadičem.

Tabulka 4 Nastavení WLC pro 5 GHz

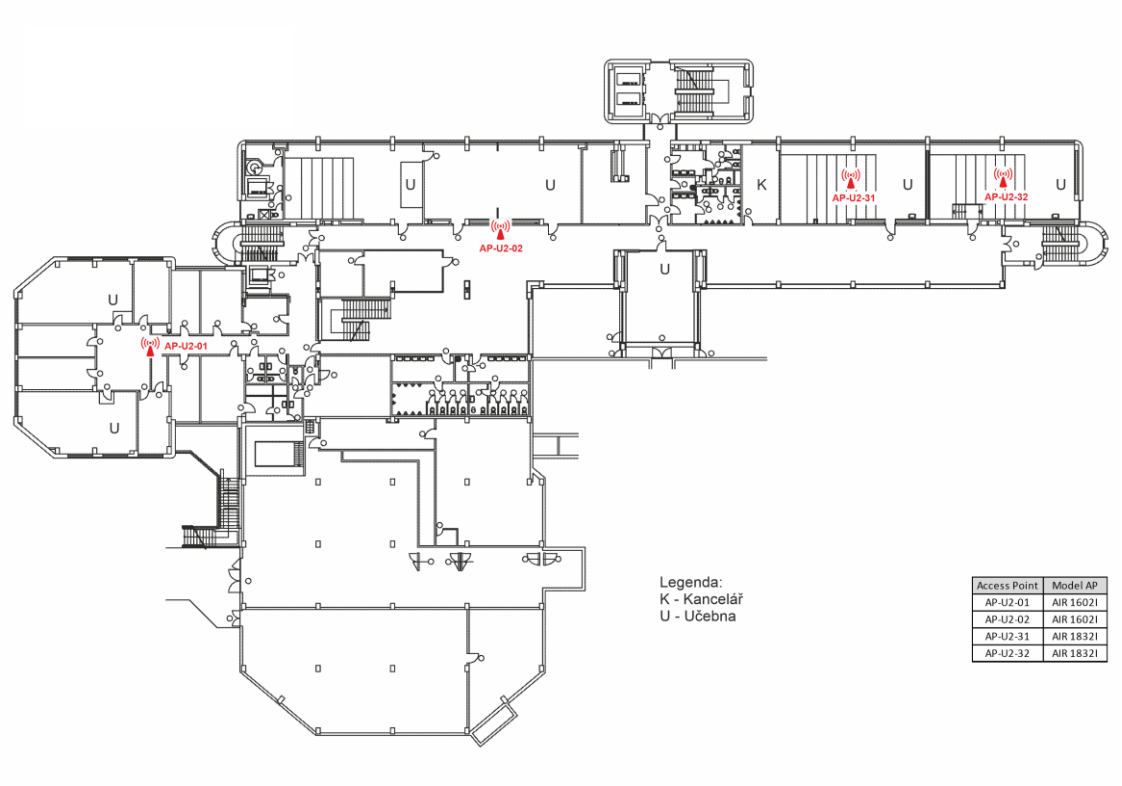
Název AP	Kanál	Výkon
AP-U2-01	48*	1*
AP-U2-02	40*	1*
AP-U2-03	36*	1
AP-U2-04	40*	1*
AP-U2-05	44*	1*
AP-U2-06	60*	1*
AP-U2-07	48*	1*
AP-U2-08	64*	1*
AP-U2-09	36*	1
AP-U2-10	36*	1*
AP-U2-11	44*	1*
AP-U2-12	36*	1*
AP-U2-13	36*	1*
AP-U2-14	40*	1
AP-U2-15	40*	2*
AP-U2-16	36*	1*
AP-U2-17	64*	2*
AP-U2-18	52*	1*
AP-U2-19	36*	1*
AP-U2-20	36*	1*
AP-U2-22	40*	1*
AP-U2-23	48*	1
AP-U2-24	40*	1*
AP-U2-31	36*	2
AP-U2-32	48*	2*

4.3 Dislokační návrhy

V této kapitole je popis změn v umístění jednotlivých přístupových bodů a jejich výkonu na každém patře. Tyto změny byly nejprve simulovány z hlediska jejich předpokládaného dopadu na stav bezdrátové pokrytí.

4.3.1 Plán prvního podzemního podlaží po provedení změn

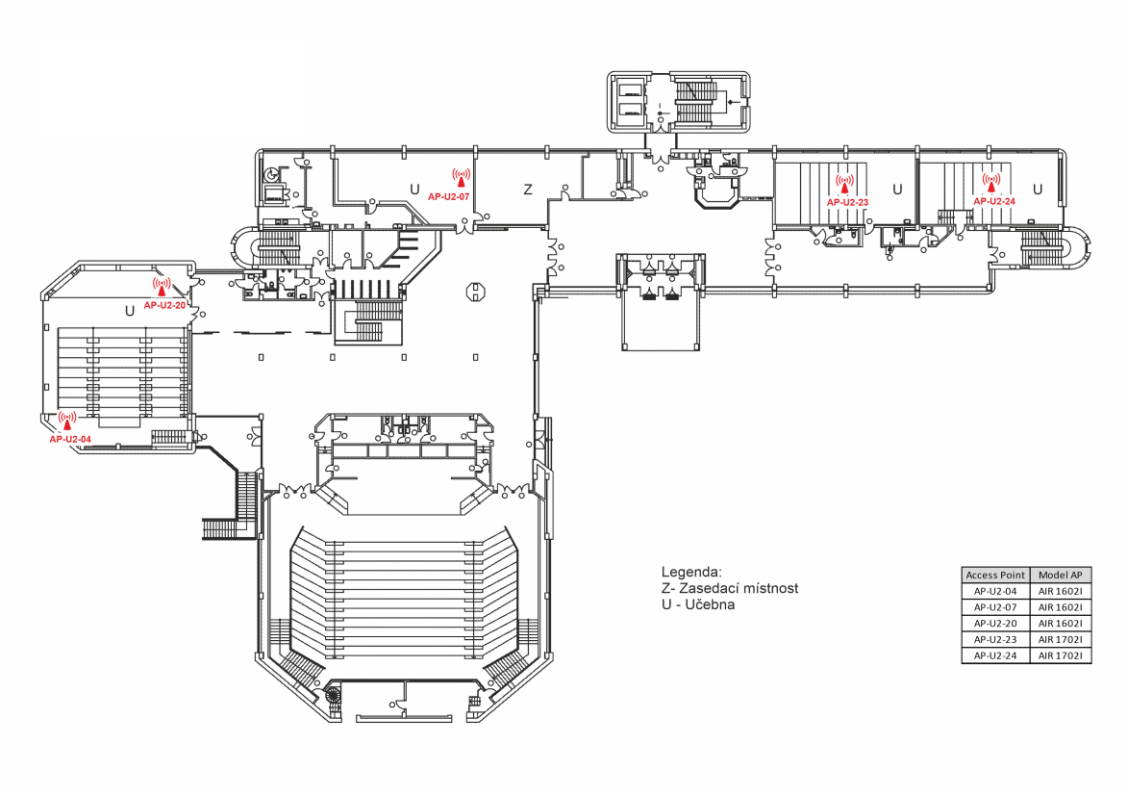
V prvním podzemním podlaží došlo pouze k manuálnímu zvýšení výkonu u AP-U2-31, jelikož tato změna dle simulace měla pomoci zvýšit kvalitu signálu v prostorách před učebnami, kde se nachází studentské odpočinkové a studijní zóny. Přesuny přístupových bodů na tomto podlaží nebyly potřebné.



Obrázek 24 Plán prvního podzemního podlaží po změnách (Vlastní zpracování)

4.3.2 Plán prvního nadzemního podlaží po provedení změn

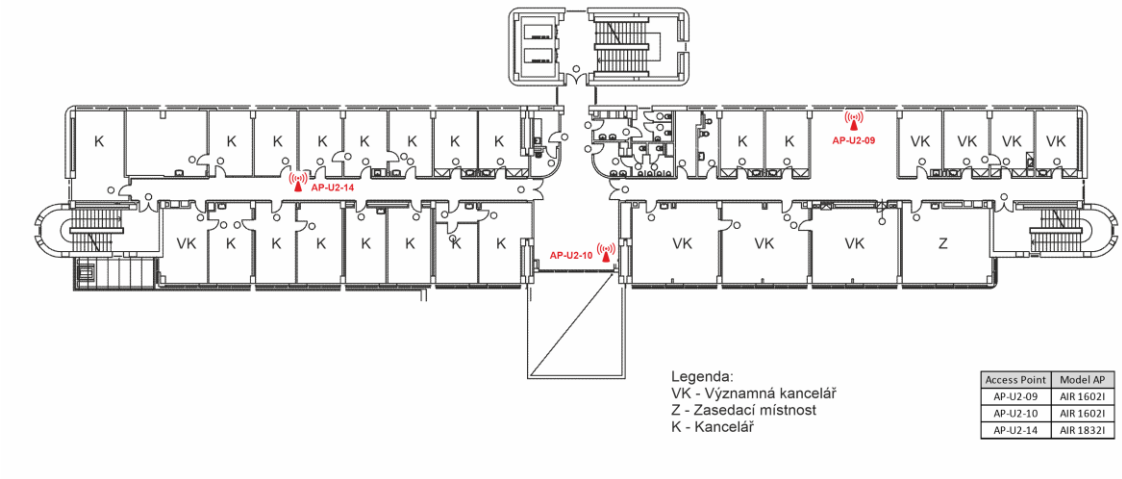
V prvním nadzemním podlaží došlo k manuálnímu zvýšení výkonu u AP-U2-23 a AP-U2-24, jelikož dle simulace měla tato změna zvýšit kvalitu signálu v prostorách před učebnami, kde se nachází odpočinkové a studijní zóny pro studenty. Dále mělo toto navýšení zlepšit kvalitu signálu i v druhém nadzemním podlaží v prostorách umístěných nad učebnami. Přesuny přístupových bodů na tomto podlaží nebyly dle simulací nutné.



Obrázek 25 Plán prvního nadzemního podlaží po změnách (Vlastní zpracování)

4.3.3 Plán druhého nadzemního podlaží po provedení změn

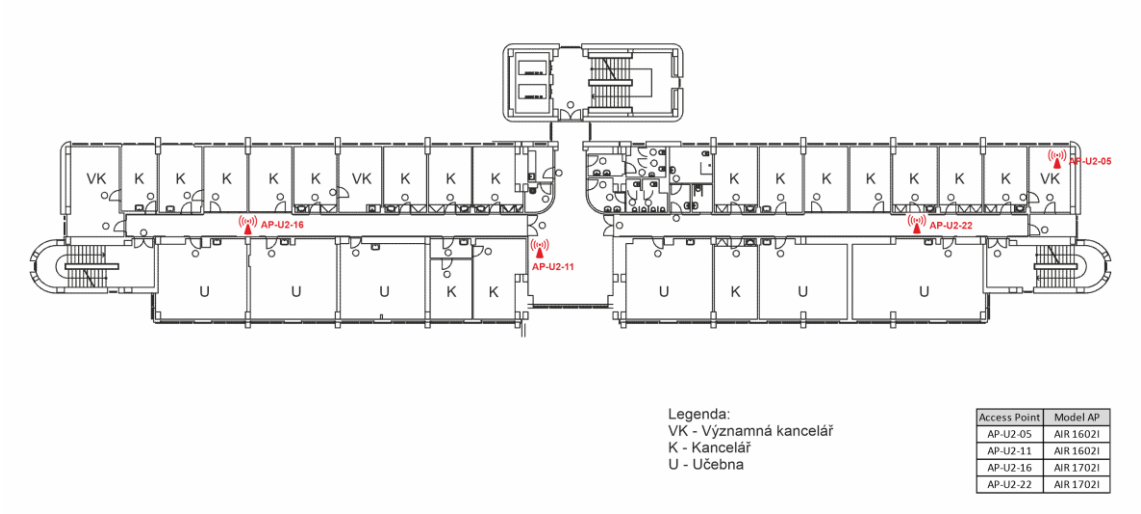
V druhém nadzemním podlaží došlo k manuální změně výkonu u AP-U2-14 a AP-U2-09. Obě tyto změny měly pomoci se zvýšením kvality signálu v zájmových prostorách, kde byl identifikován vyšší útlum, než je požadován. Přesuny přístupových bodů na tomto podlaží nebyly dle simulací nutné.



Obrázek 26 Plán druhého nadzemního podlaží po změnách (Vlastní zpracování)

4.3.4 Plán třetího nadzemního podlaží po provedení změn

Ve třetím nadzemním podlaží nedošlo ke změnám ve výkonu u žádných přístupových bodů. Byl sem přesunut přístupový bod AP-U2-05, který byl přesunut z auly a byl instalován do významné kanceláře. K tomuto kroku bylo nutné přistoupit, jelikož ani umístění přístupového bodu do rohu chodby k dotčené kanceláři nezajistilo zvýšení kvality signálu a tato změna tedy nepřinesla žádné výsledky. Po provedených simulacích se tento krok ukázal jako jediný možný, který by zajistil požadovanou kvalitu signálu ve významné kanceláři. Prvním záměrem bylo tento přístupový bod přesunout do čtvrtého nadzemního podlaží na okraj budovy, jelikož toto umístění se zdálo ideálním z hlediska zlepšení kvality signálu pro tři podlaží zároveň. Jelikož je ale ve čtvrtém nadzemním podlaží v těchto prostorách učebna, autor se z bezpečnostních důvodů rozhodl pro umístění přístupového bodu do třetího podlaží do kanceláře, které se jeví jako bezpečnější z hlediska možnosti odcizení z učebny. Dále došlo k přesunu AP-U2-22 více do středu chodby, jelikož při změnách na čtvrtém nadzemním podlaží bylo žádoucí, aby přístupové body nebyly přímo nad sebou mezi patry, ale zapadali do mezer mezi přístupovými body ve vyšším a nižším podlaží.



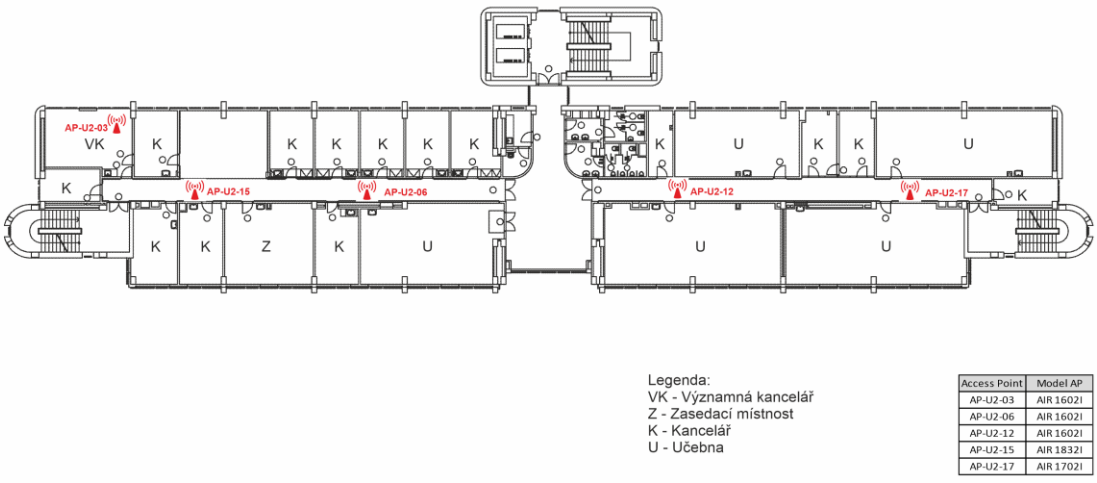
Obrázek 27 Plán třetího nadzemního podlaží po změnách (Vlastní zpracování)

4.3.5 Plán čtvrtého nadzemního podlaží po provedení změn

Nejvíce změn bylo provedeno na čtvrtém nadzemním podlaží. Dle výsledků získaných při měření přístupové body dostatečně pokrývají i podlaží nad i pod ním se nacházející. Jelikož ve třetím, čtvrtém a pátém nadzemním podlaží bylo nejméně přístupových bodů a byly nelogicky umístěné, touto změnou má dle simulací dojít ke zvýšení kvality signálu ve třech podlažích zároveň. Tyto změny také v několika simulacích potvrdily citelné

zlepšení kvality signálu ve všech zájmových prostorách. Na tomto patře tedy došlo k přesunu AP-U2-03, které dříve bylo v aule do významné kanceláře na levém rohu. Toto umístění také jako jediné bylo schopné vyřešit problém se slabým pokrytím na rohu budovy. Takto umístěný přístupový bod je schopný pokrýt ve třech patrech současně celý levý okraj budovy a tím zlepšit kvalitu signálu ve třech významných kancelářích. Toto řešení dle simulace bylo jediné smysluplné, aby nebylo nutné přidávat další přístupové body, jelikož by bylo nutné přidat tři přístupové body do každého patra budovy na samotný okraj chodby a ani toto umístění by nebylo schopné výrazně zlepšit pokrytí významných kanceláří. Toto umístění tedy ze simulací vycházelo jako nejideálnější. U tohoto přístupového bodu také došlo k manuálnímu zvýšení výkonu. Dále bylo na toto podlaží přesunuto AP-U2-06, které mělo pomoci pokrýt učebnu a slabě pokryté kanceláře na levé straně budovy a dále také učebnu a kanceláře na pátém nadzemním podlaží. Další změnou bylo přesunutí AP-U2-12 ze středu chodby do pravé části budovy na chodbu. Tato změna měla eliminovat umístění přístupového bodu přímo nad sebou a také pomoci pokrýt kanceláře a učebny na třetím a pátém nadzemním podlaží.

Změny ve výkonu jednotlivých přístupových bodů byly v tomto případě ponechány na automatickém nastavení řadiče, z důvodu hustšího osazení přístupovými body.

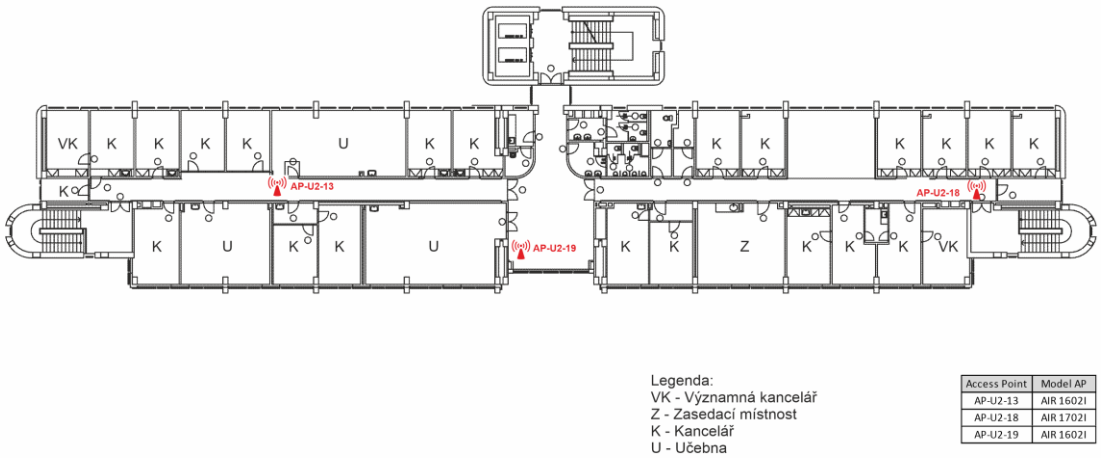


Obrázek 28 Plán čtvrtého nadzemního podlaží po změnách (Vlastní zpracování)

4.3.6 Plán pátého nadzemního podlaží po provedení změn

Na pátém nadzemním podlaží došlo k manuálnímu zvýšení výkonu u AP-U2-18 a jeho přesunutí na okraj chodby. Tato změna má dle simulací pomoci pokrýt pravý okraj budovy. Bohužel, jak bylo zmíněno, k této změně bylo nutné přistoupit individuálně, jelikož pokud

by byl umístěn přístupový bod ve čtvrtém podlaží v těchto místech, došlo by k pokrytí i této kanceláře a nebylo by tedy nutné ji pokrývat jiným způsobem. Dále bylo přesunuto AP-U2-19 a umístěno na střed chodby. Tato změna má dle simulací pomoci pokrýt místa se špatnou kvalitou signálu v kancelářích a učebně umístěných blízko středu budovy, kde byla kvalita signálu nejhorší z celé budovy.



Obrázek 29 Plán pátého nadzemního podlaží po změnách (Vlastní zpracování)

4.3.7 Souhrn změn a jejich účel

V prvním podzemním, prvním a druhém nadzemním podlaží nedošlo k žádným dislokačním změnám přístupových bodů. V těchto místech bylo totiž měřením zjištěno jen velmi málo míst se špatnou kvalitou signálu a tato místa bylo možné odstranit jen nastavením jiné úrovně výkonu u blízkých přístupových bodů. Došlo k tedy nejprve k simulaci pokrytí po změnách a poté byly tyto změny na jednotlivé přístupové body aplikovány.

Ve třetím, čtvrtém a pátém nadzemním podlaží bylo měřením zjištěno několik míst se slabým signálem, a to především na okrajích budovy ve všech patrech. Tato místa bylo nutné eliminovat. V těchto patrech také bylo provedeno největší množství simulací, které měly zjištěné nedostatky odstranit. K celkovému zlepšení kvality signálu mělo dojít změnami na čtvrtém nadzemním podlaží, které má být schopné zajistit pokrytí i třetího a pátého podlaží. Okraje budovy byly pokryty umístěním přístupových bodů do kanceláří, což se nejeví jako ideální řešení, ovšem toto řešení bylo z hlediska zvýšení kvality signálu jediné možné. Na čtvrtém patře tedy došlo k přesunu dvou přístupových bodů, které byly přesunuty z univerzitní auly a dále k přemístění již instalovaných přístupových bodů. Na třetím a pátém nadzemním podlaží došlo k přesunu instalovaných přístupových bodů

takovým způsobem, aby přístupové body nebyly umístěny přímo nad sebou, ale zapadaly do mezer mezi přístupovými body instalovanými na čtvrtém podlaží.

4.4 Měření signálu po realizaci změn

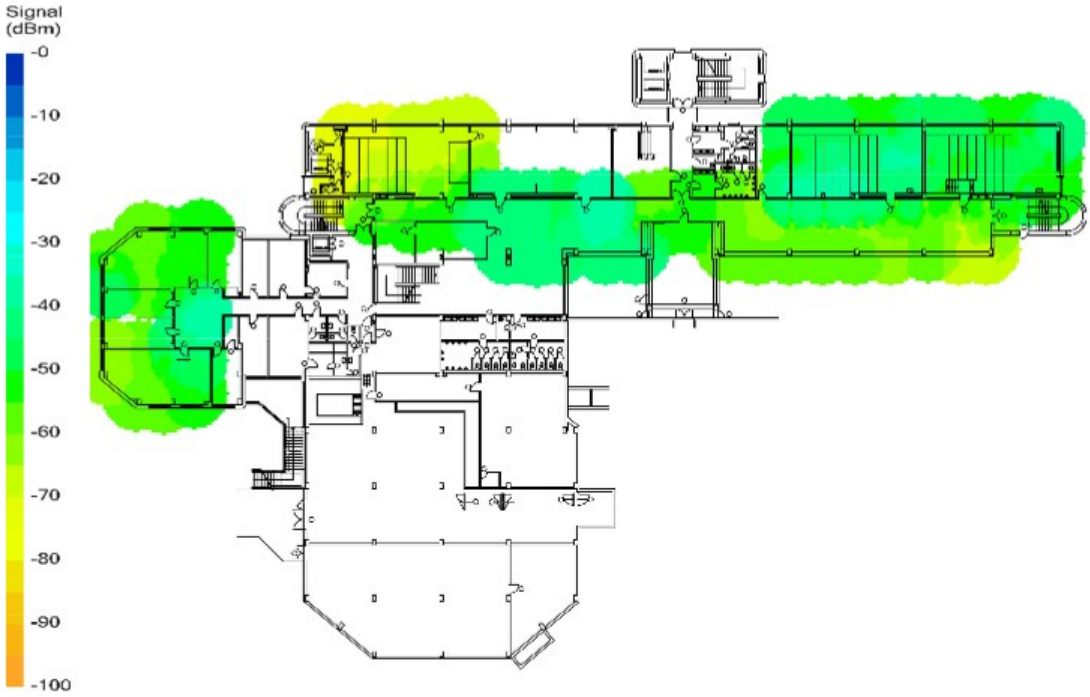
Poslední fází práce bylo konečné měření ve všech prostorách budovy po realizaci změn. Tato konečná fáze měla odhalit reálné dopady změn na kvalitu signálu v celé budově. Toto měření se poté porovnalo s optimalizačním modelem, kde byly zkoumány reálné odpady oproti dopadům simulovaným a v případě potřeby provést dodatečné simulace a úpravy navrženého řešení dle reálného stavu pokrytí.

Samotné měření bylo prováděno totožným způsobem jako měření před realizací změn. V každé kanceláři bylo provedeno měření v šesti bodech, v každé učebně a zasedací místnosti i více dle rozlohy místnosti. Jednotlivé body jsou od sebe vzdálené také cca 3 metry a zachycují co nejpřesnější pozici bodu při měření.

4.4.1 Výsledky měření prvního podzemního podlaží po realizaci

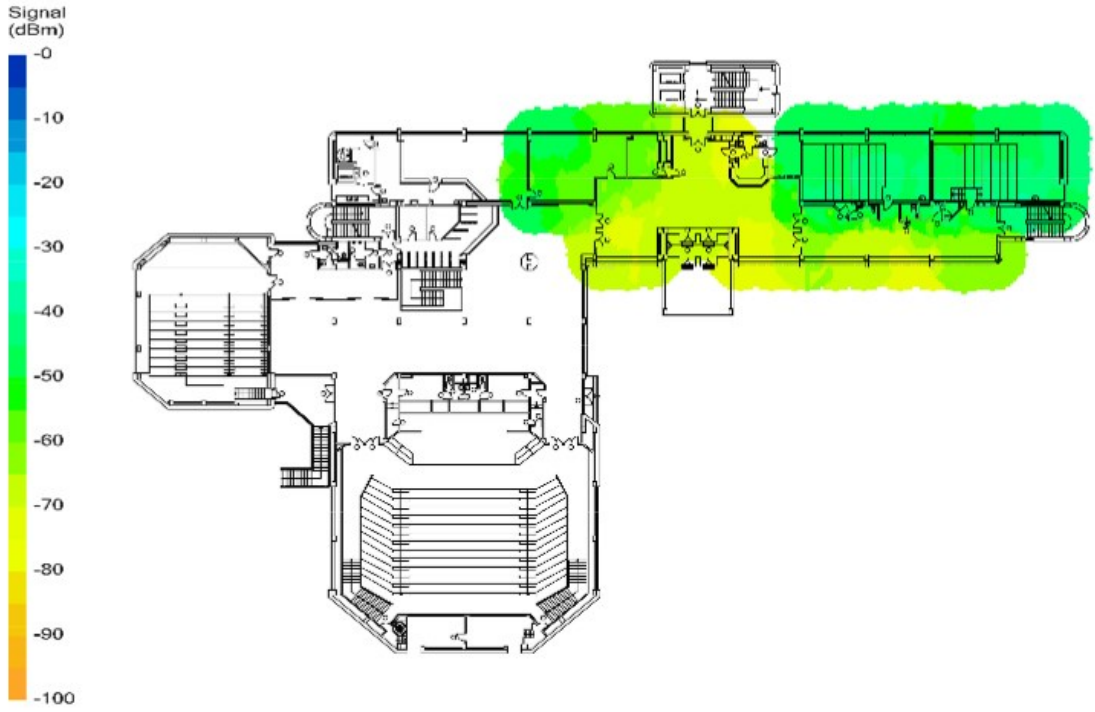
V prvním podzemním podlažím byla optimalizace zaměřena především na prostory v pravé části budovy před učebnami, kde se nachází odpočinkové a studijní zóny. V těchto místech mělo dojít ke zlepšení kvality signálu zvýšením výkonu přístupových bodů v učebnách. Dalším zájmovým místem byla učebna umístěna v levém okraji budovy, kde došlo oproti prvnímu měření ke zhoršení v určitých částech místnosti. K této změně došlo z důvodu odstranění přístupového bodu AP-U2-07 realizovaného před posledním měřením z důvodu rekonstrukce bufetu. Tento prostor ovšem není nutné dále optimalizovat, jelikož po dokončení stavby, která má být hotová v červenci roku 2021 dojde k instalaci nových přístupových bodů a tento prostor budou pokrývat přístupové body umístěné v prvním nadzemním podlaží v prostoru bufetu.

V prostoru před učebnami došlo ke zlepšení kvality signálu podobným způsobem, jaký předpokládaly simulace. V těchto místech ke snížení útlumu průměrně o 7 dB.



Obrázek 30 Výsledek měření v prvním podzemním podlaží po změnách (Vlastní zpracování)

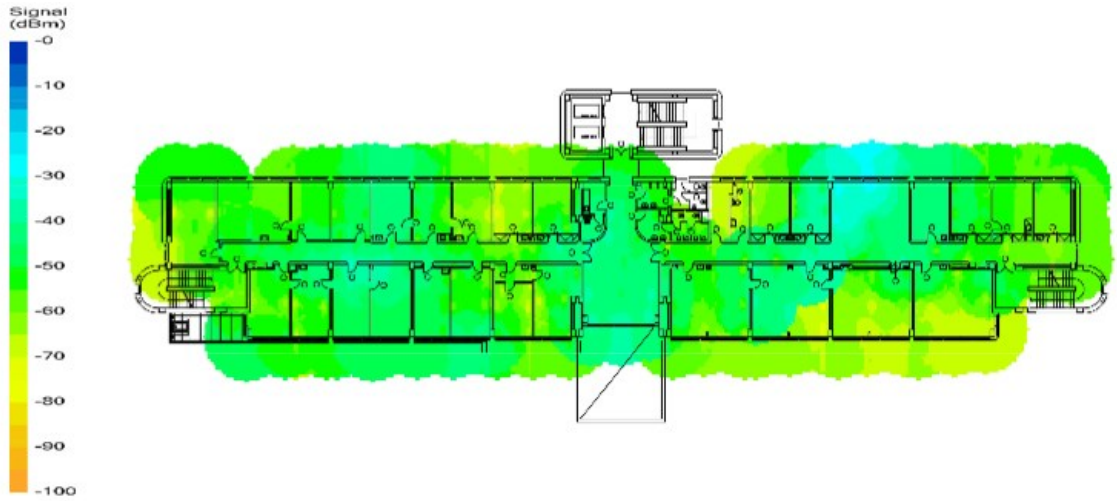
V prvním nadzemním podlaží byly identifikovány problémy pouze v pravé části budovy. Bohužel nebylo možné provést měření v celé levé části, jelikož celá levá část prochází rekonstrukcí. Po dokončení rekonstrukce má firma provést i nasazení nových přístupových bodů a celý tento prostor optimálně pokrýt. Z tohoto důvodu se optimalizace prováděla pouze na pravé straně budovy před učebnami, jelikož se zde nachází odpočinkové zóny pro studenty a byl zde identifikován větší útlum, než je požadován. Vestibul budovy nebylo nutné dále optimalizovat, jelikož tento prostor je průchozí a uživatelé se zde nezdržují, z toho důvodu nebylo nutné zde optimalizaci provádět. Na pravé straně budovy došlo ke snížení útlumu průměrně o 5 dB.



Obrázek 31 Výsledek měření v prvním nadzemním podlaží po změnách (Vlastní zpracování)

4.4.2 Výsledky měření druhého nadzemního podlaží po realizaci

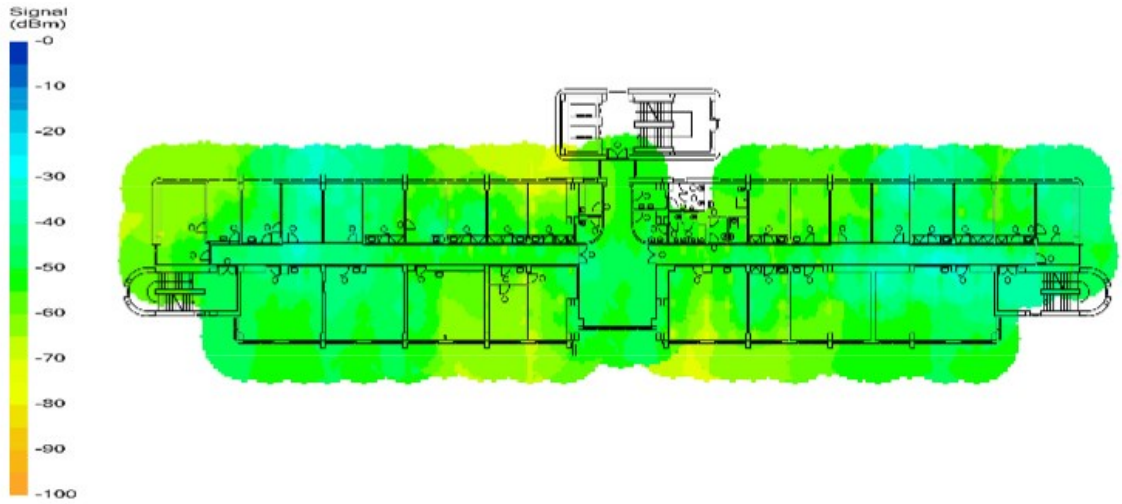
Druhé nadzemní podlaží, kde je nejvíce významných kanceláří a kanceláří provozně-technických zaměstnanců došlo k celkovému zlepšení bezdrátového pokrytí. Identifikovaná nedostatečně pokrytá místa na krajích budovy a také ve významných kancelářích byla eliminována zvýšením výkonu u dotčených přístupových bodů. Na levé straně budovy navíc po dokončení rekonstrukce bude situace ještě lepší, jelikož tuto část budou pokrývat i nově instalované přístupové body v prvním nadzemním podlaží. Zvýšením výkonu se také podařilo lépe pokrýt kanceláře na levé straně budovy. Na pravé straně došlo také ke zlepšení pokrytí, a to ve všech kancelářích a také v rohu budovy. Roh budovy nyní pokrývá přístupový bod umístěný ve třetím nadzemním podlaží a dále zvýšený výkon přístupového bodu umístěného uprostřed pravé části. V levé části budovy došlo ke snížení útlumu průměrně o 10 dB v rohu budovy a průměrně o 8 dB v kancelářích blíže středu podlaží. V pravé části budovy došlo ke snížení útlumu ve všech identifikovaných místech průměrně o 6 dB.



Obrázek 32 Výsledek měření ve druhém nadzemním podlaží po změnách (Vlastní zpracování)

4.4.3 Výsledky měření třetího nadzemního podlaží po realizaci

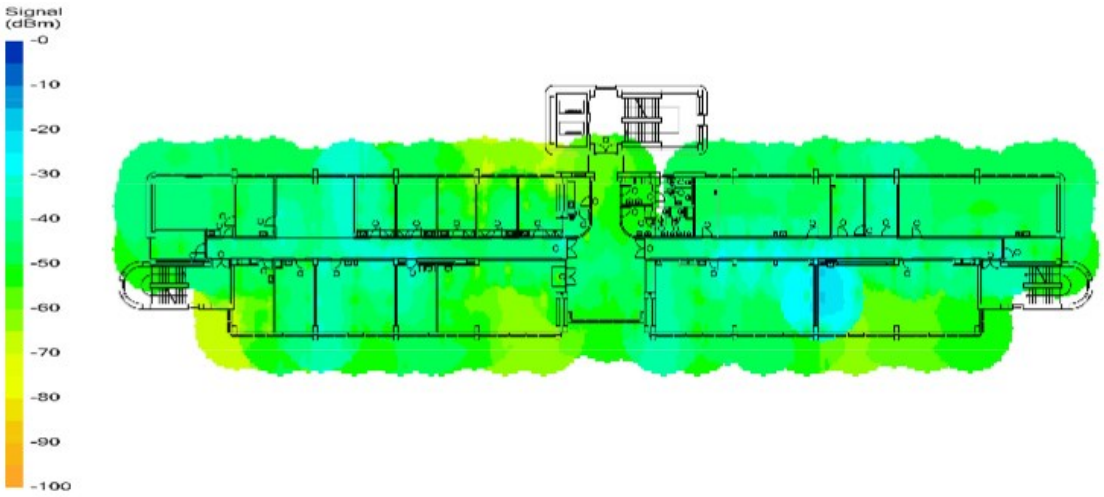
Ve třetím nadzemním podlaží bylo po prvním měření identifikováno několik míst s nedostatečným pokrytím. Šlo především o oba okraje budovy, kdy na pravé části budovy byl útlum opravdu vysoký. Bylo identifikováno také nedostatečné pokrytí ve dvou kancelářích na středu budovy a také v jedné učebně. Tyto problémy měly být odstraněny přesunutím několika přístupových bodů ve čtvrtém nadzemním podlaží a také přesunutím přístupového bodu do významné kanceláře v pravém rohu budovy. Tyto provedené změny měly velký vliv a útlum se snížil i o desítky decibelů. Konkrétně v pravém rohu budovy došlo ke snížení útlumu o 30 dB, což je pochopitelné, jelikož sem byl přesunut přístupový bod. Ovšem i na ostatních identifikovaných místech došlo ke snížení útlumu. V levém rohu budovy se útlum snížil průměrně o 8 dB a v kancelářích u středu podlaží průměrně o 12 dB. V učebně v pravé části podlaží se útlum snížil průměrně o 10 dB.



Obrázek 33 Výsledek měření ve třetím nadzemním podlaží po změnách (Vlastní zpracování)

4.4.4 Výsledky měření čtvrtého nadzemního podlaží po realizaci

Ve čtvrtém nadzemním podlaží bylo měřením odhaleno jen velmi málo slabě pokrytých míst, ale nejvíce změn bylo provedeno právě v tomto podlaží. Tyto změny měly zlepšit situaci ve třech podlažích současně a také pomoci eliminovat slabá místa na tomto podlaží. Po provedení změn došlo ke snížení útlumu v levém rohu budovy průměrně o 15 dB, jelikož sem byl přesunut přístupový bod přímo do významné kanceláře. Tento přesun měl především pokrýt roh významné kanceláře, kde se nachází pracovní zóna uživatele. V celém patře došlo ke snížení útlumu průměrně o 10 dB, což je dáno především novým umístěním všech přístupových bodů, které již nejsou umístěné v přilehlých patrech přímo nad sebou, ale zapadají do mezer mezi přístupovými body v jednotlivých patrech.



Obrázek 34 Výsledek měření ve čtvrtém nadzemním podlaží po změnách (Vlastní zpracování)

4.4.5 Výsledky měření pátého nadzemního podlaží po realizaci

V pátém nadzemním podlaží bylo identifikováno nejvíce slabých míst v celé budově. Jednalo se o oba kraje budovy a dále o kanceláře umístěné ve středu podlaží. Na tomto podlaží došlo k přesunu dvou přístupových bodů, kdy jeden byl přesunut do středu budovy a druhý byl posunut v pravé části podlaží co nejvíce do rohu chodby. Zbytek podlaží je pokryt přístupovými body, které byly přesunuty ve čtvrtém nadzemním podlaží. Po provedení všech změn konečné měření potvrdilo výstupy z optimalizačního modelu. V celém levém rohu podlaží se útlum snížil o průměrně 20 dB a dalších kancelářích na levé straně budovy průměrně o 5 dB. V pravé části budovy došlo také ke snížení útlumu. V pravém rohu budovy došlo ke snížení útlumu průměrně o 15 dB a v kancelářích umístěných u středu podlaží se útlum snížil průměrně o 15 dB. Ve všech ostatních místech pravé části budovy útlum klesl o průměrně 5 dB.

Obrázek 35 Výsledek měření v pátém nadzemním podlaží po změnách (Vlastní zpracování)

4.5 Analýza celkového stavu po optimalizaci

Optimalizace internetové konektivity na budově U2 byla provedena na základě vytvořeného modelu a po aplikaci změn a konečném měření bylo možné ze získaných dat potvrdit korektnost optimalizačního modelu. Po porovnání získaných dat z prvního měření před plánováním úprav s daty získanými konečným měřením je možné konstatovat, že optimalizace internetového připojení byla úspěšná ve všech prostorách budovy. Cílem práce bylo zlepšit konektivitu na celé budově při stávajícím počtu přístupových bodů. Oba tyto cíle se podařilo splnit, jelikož nebylo nutné přidávat žádné přístupové body a celkovou optimalizaci se podařilo provést se stejným počtem přístupových bodů, které byly k dispozici před začátkem optimalizace, což je ekonomicky výhodnější. Pouhou změnou umístění vybraných přístupových bodů a změnách ve výkonu přístupových bodů se podařilo zvýšit kvalitu připojení v celé budově. V prvním podzemním podlaží a prvním nadzemním podlaží došlo ke zlepšení pokrytí před učebnami, kde dochází ke shlukování studentů v odpočinkové zóně. Ve druhém nadzemním podlaží se optimalizací podařilo zlepšit internetové připojení na obou krajích budovy a také ve střední části budovy v kancelářích. Nejvíce změn proběhlo ve čtvrtém nadzemním podlaží, které měly mít přímý vliv na pokrytí ve třetím a pátém nadzemním podlaží. Tyto změny reálně pomohly s pokrytím třetího nadzemního podlaží na obou okrajích budovy, ale i ve střední části v kancelářích a učebnách. Čtvrté nadzemní podlaží, kde bylo identifikováno nejméně problematických míst je nyní nadstandardně pokryto a byly eliminovány i identifikovaná problematická místa. V pátém nadzemním podlaží, kde bylo identifikováno nejvíce míst se slabým pokrytím došlo

k citelným změnám v pokrytí. Oba okraje budovy, kde bylo pokrytí velmi slabé jsou nyní dostatečně pokryty stejně tak jako kanceláře ve střední části podlaží. V pátém nadzemním podlaží byla odstraněna všechna identifikovaná místa se slabým pokrytím.

V celé budově byly prvním měřením identifikovány velké rozdíly v pokrytí. V rámci podlaží byly rozdíly v útlumu i několik desítek decibelů. Optimalizace budovy tak dokázala nejen eliminovat místa se slabým pokrytím, ale zároveň dokázala eliminovat i rozdíly v útlumu v rámci jednotlivých podlaží i celé budovy. Nyní již uživatelé nepocítí rozdíly mezi různými kancelářemi ani učebnami, jelikož pokrytí je téměř shodné a tím je zajištěn stejný výkon bezdrátové sítě v rámci celé budovy.

4.6 Zabezpečení bezdrátové sítě

Před připojením zařízení k bezdrátové síti si musí student i zaměstnanec vytvořit unikátní heslo, které nesmí být stejné jako heslo, které uživatel používá k ověření v ostatních informačních systémech univerzity jako například do systému STAG, Moodle nebo office365. Tato politika byla zavedena v roce 2020 a vychází ze zkušeností z předchozích let. Dříve nebylo požadováno unikátní heslo a bylo možné použít heslo stejné jako do dalších systémů. Heslo se však i před rokem 2020 muselo vytvořit přímo uživatelem. Heslo a vlastně i celý uživatelský účet se vytváří pomocí formuláře, který je dostupný na webových stránkách Univerzity Tomáše Bati ve Zlíně. Na webových stránkách je nejen formulář, ale i všechny potřebné informace o tom, jak připojení zařízení provést, jaké je možné použít nastavení, a především také pravidla pro užívání bezdrátové sítě UTB a sítě eduroam. Registrací každý uživatel souhlasí s dodržováním těchto pravidel. Přihlášení do formuláře je ověřováno proti AD (active direktory). Tím je ověřena uživatelova identita a po přihlášení má uživatel právo vytvořit přístupové údaje k bezdrátové síti. Uživatelské jméno uživatele je přebráno z AD a rozšířeno o tzv. realm, který je v případě UTB „@utb.cz“. Realm slouží k rozlišení instituce a pomocí něj je prováděno směrování požadavku na ověření uživatele v síti eduroam. Uživatelské jméno je tímto krokem převedeno do tvaru, který požaduje federace eduroam. Poté je uživatel vyzván k vyplnění unikátního hesla a po odeslání formuláře jsou jeho údaje z registrace uloženy na LDAP server, který obsahuje databázi všech uživatelů bezdrátové sítě. Tímto způsobem se vytváří uživatelské účty pro připojení do bezdrátové sítě. Tvorba uživatelských účtů do bezdrátové sítě nikdy neprobíhala automaticky při zápisu studenta.

Po vytvoření uživatelského účtu je možné provést připojení k bezdrátové síti. Dříve musel každý uživatel na svém zařízení provádět konfiguraci připojení ručně dle dostupných návodů na webových stránkách. Tento přístup byl nahrazen uživatelsky přívětivější, a především bezpečnější metodou a k připojení se využívá aplikace eduroam CAT. Při ruční konfiguraci mohl uživatel vybrat možnost, při které nedocházelo k ověření certifikátu RADIUS serveru. Jelikož nebyl certifikát serveru ověřován, mohlo dojít k podvržení RADIUS serveru a tím k odcizení uživatelova účtu. Ruční konfigurace je sice stále možná, ovšem na webových stránkách jsou již odebrány návody, jak ji provést a místo toho je preferováno použití nástroje eduroam CAT. Tento nástroj musí být nakonfigurován správcem sítě dané organizace. Již nakonfigurovaný program po spuštění požaduje pouze uživatelské jméno a heslo. Po jejich vyplnění proběhne konfigurace připojení automaticky, a navíc je do uživatelova zařízení nainstalován kořenový certifikát certifikační autority, která vydala certifikát RADIUS serveru instituce. Tento způsob je pro uživatele mnohem jednodušší, kdy nemusí složitě provádět konfiguraci ručně, a navíc je oproti ruční konfiguraci nadstandardně chráněn před odcizením svého uživatelského účtu, jelikož nemůže dojít k podvržení radius serveru.

Při připojování uživatele k bezdrátové síti si nejprve zařízení uživatele vyžádá certifikát RADIUS serveru a po jeho předložení serverem je pomocí kořenového certifikátu ověřen podpis certifikátu certifikační autoritou. Pokud se podpisy shodují, je RADIUS server považován za důvěryhodný a dochází k autentizaci uživatele proti RADIUS serveru, který je připojen k LDAP serveru a po úspěšné autentizaci je uživatel připojen k bezdrátové síti.

Politika hesel pro připojení k bezdrátové síti, kdy je vyžadováno unikátní heslo a nelze použít heslo používané k přihlášení do dalších systémů vychází z požadavků na bezpečnost uživatelských účtů. Pokud by někdo získal přihlašovací údaje uživatele do bezdrátové sítě, což je dnes již poměrně jednoduchou záležitostí, došlo by i k získání přístupů do všech informačních systémů univerzity a útočník by mohl s totožným heslem a účtem přistupovat do systémů Moodle, STAG, Office365 a dalších, což je z hlediska bezpečnosti nežádoucí.

Aktuálně je využíváno zabezpečení WPA2 Enterprise a šifrování AES. Ověření probíhá přes protokol PEAP a uživatel se ověřuje pomocí protokolu EAP – MSCHAPv2. To znamená, že není požadován klientský certifikát, ale ověřuje se pouze certifikát serveru.

Pro zvýšení bezpečnosti bezdrátové sítě navrhuji používat zabezpečení WPA3 Enterprise se šifrováním AES a zachovat protokol PEAP. Bohužel jsem narazil na problém v podobě

staršího bezdrátového řadiče, který univerzita používá. Aktuálně využívaný řadič Wism2 podporuje verzi firmwaru do verze 8.5.X.X. Aktuálně je na řadiči firmware verze 8.5.160.0, který podporuje všechny typy přístupových bodů, které jsou aktuálně provozovány. Aby bylo možné zvýšit zabezpečení na WPA3 musí mít bezdrátový řadič minimálně verzi 8.10.X.X. Tato verze firmwaru již ale nepodporuje přístupové body Cisco řady 1600, kterých je aktuálně na univerzitě více než třetina. Zde se vyskytl další problém v podobě nasazování nových přístupových bodů, které by podporovaly nový standard 802.11ax. Při rozšiřování bezdrátové infrastruktury tedy univerzita nemůže přistoupit k pořízení nejnovějších přístupových bodů, jelikož tyto přístupové body nejsou podporovány aktuálně používaným bezdrátových řadičem.

Tyto odhalené problémy tedy znamenají, že nemůže být použito zabezpečení WPA3 na aktuálně používaném řadiči a také nemůžou být pořízeny přístupové body, které podporují standard 802.11ax, což značně omezuje budoucí rozvoj bezdrátové sítě univerzity. Tento problém je možné vyřešit nahrazením stávajícího řadiče za nový a zároveň s touto výměnou nahradit všechny přístupové body Cisco řady 1600. Druhou možností je pořízení nového řadiče a nově pořízené přístupové body se budou připojovat k tomuto novému řadiči, a navíc se k němu připojí i přístupové body Cisco řady 1700 a řady 1800. Přístupové body Cisco řady 1600 zůstanou připojené ke starému řadiči, ale musí se přemístit do jedné lokace. Tímto krokem by odpadla nutnost nahrazení třetiny nejstarších přístupových bodů. Zároveň s tím by bylo podporováno zabezpečení WPA3. Znamenalo by to ovšem, že správa přístupových bodů by se musela provádět na dvou řadičích.

ZÁVĚR

Cílem diplomové práce bylo navrhnout a realizovat optimalizaci internetové konektivity na budově Fakulty managementu a ekonomiky Univerzity Tomáše Bati ve Zlíně. Pro splnění cíle práce bylo definováno několik fází, které měli vést k optimalizaci konektivity. Práce také bude sloužit správcům jednotlivých součástí jako podklad a návod, jakým způsobem je možné provést optimalizaci internetové konektivity a jaké prostředky a metody mohou použít.

Teoretická část práce obsahuje literární rešerši problematiky bezdrátových sítí. Je rozdělena na dvě části, přičemž první část se zabývá fungováním bezdrátových sítí a druhá část se zabývá zabezpečením bezdrátových sítí. V první části práce přibližuje historický vývoj bezdrátových sítí, standardizační organizace a regulační orgány a dále existující standardy bezdrátových sítí. Jsou zde také zkoumány negativní vlivy, které se mohou v bezdrátových sítích objevit. Je zde také popsáno fungování a účel bezdrátových řadičů a síťový roaming. Druhá část teoretické části práce je zaměřena na problematiku bezpečnosti bezdrátových sítí. V této části se práce zabývá obecnými metodami autentizace a také jednotlivými EAP autentizačními metodami a přibližuje také standard 802.1X a ověřovací protokoly.

Praktická část práce byla rozdělena do tří jednotlivých fází. Před začátkem samotné práce bylo nutné vybrat takové prostředky, které umožňují vytvořit model budovy, dokáží provést měření bezdrátového signálu v budově a poté umožní provést analýzy získaných dat. K tomuto účelu byl vybrán software AirMagnet Survey PRO od společnosti NetAlly. Nejprve bylo nutné analyzovat, jaký je aktuální stav internetové konektivity na budově a na základě této analýzy identifikovat nedostatečně pokryté prostory. Proto nejprve došlo k zakreslení všech přístupových bodů, které se na budově nachází do podkladových materiálů. Na základě těchto podkladů byl vytvořen model budovy a byla provedena simulace šíření signálu v budově. Tento model poté slouží k tvorbě návrhů na dislokační a další změny, které povedou k optimalizaci. Také došlo k identifikaci míst se zvláštním určením. Pro získání přehledu o aktuálním stavu konektivity bylo provedeno měření bezdrátového signálu v celé budově a získané reálné výsledky byly porovnány s připraveným modelem. Tento krok měl validovat model a určit, zda se model přibližuje skutečnosti a zda simulované šíření signálu odpovídá reálnému šíření signálu. Po validaci modelu bylo možné model použít k modelování změn a simulacím dopadů těchto změn.

Ve druhé fázi byla provedena příprava několika možných scénářů, které měli vést ke zlepšení kvality signálu v dříve identifikovaných prostorách. Tyto scénáře byly připraveny ve vytvořeném modelu budovy a poté byly všechny změny realizovány. Jelikož se jedná o rozsáhlejší podnikovou síť, nebylo možné optimalizaci provádět za provozu a všechny změny musely být realizovány a ověřeny v co nejkratším čase. Z tohoto důvodu byly všechny změny již připravené dopředu a byly pouze realizovány a ověřeny a nebylo tak nutné během realizace provádět žádné korekce. Při optimalizaci byly prováděny pouze dislokační změny a změny v konfiguraci jednotlivých přístupových bodů.

V poslední fázi byly ověřeny všechny provedené změny opětovným měřením signálu v celé budově a následnou analýzou získaných dat byl zjišťován reálný dopad provedených změn. Po této analýze a srovnání stavu pokrytí před optimalizací a po optimalizaci vyšlo najevo, že při zachování stejného počtu přístupových bodů došlo k výraznému zlepšení pokrytí v celé budově, a to pouhým přesunem a přenastavením určitých přístupových bodů. Optimalizací bylo navíc nejen zlepšeno pokrytí identifikovaných míst, ale také došlo k celkové optimalizaci ve všech prostorách budovy, jelikož došlo ke srovnání hladiny útlumu v rámci celé budovy.

Po dokončení optimalizace bylo analyzováno celkové zabezpečení bezdrátové sítě univerzity a byly zkoumány možnosti pro zvýšení bezpečnosti. Výzkum se zabývá také bezpečností uživatelských účtů a politikou hesel. Při tomto výzkumu bylo odhaleno, že nyní není možné změnit zabezpečení sítě na WPA3, protože by bylo nutné vyměnit bezdrátový řadič, a proto byly zkoumány i způsoby řešení tohoto problému.

SEZNAM POUŽITÉ LITERATURY

[1] CARROLL, Brandon. *Bezdrátové sítě Cisco: autorizovaný výukový průvodce.* Brno: Computer Press, 2011, 478 s. Samostudium. ISBN 9788025128848.

[2] SURYNEK, Jiří. *Problematika bezdrátových sítí* [online]. Brno, 2010 [cit. 2021-5-19]. Dostupné z: https://dspace.vutbr.cz/xmlui/bitstream/handle/11012/351/final-thesis.pdf?sequence=6&isAllowed=y. Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce doc. Ing. Miloš Koch, CSc.

[3] BEČVÁŘ, Zdeněk, Pavel MACH a Ivan PRAVDA. *Mobilní sítě* [online]. V Praze: České vysoké učení technické, [2013] [cit. 2017-02-22]. ISBN 9788001053058.

[4] Bezdrátové mikrofony vs. televizní vysílání – tabulka. *FADER.cz* [online]. 2017 [cit. 2021-5-19]. Dostupné z: http://www.fader.cz/2017/11/06/bezdratove-mikrofony-vs-televizni-vysilani-tabulka/

[5] GONCHARUK, Sergii. *Měření šíření rádiového signálu v pásmu 5GHz* [online]. Ostrava, 2013 [cit. 2021-5-19]. Dostupné z: https://core.ac.uk/download/pdf/17305328.pdf. Bakalářská práce. Technická univerzita Ostrava. Vedoucí práce Ing. Artem Ganiyev.

[6] SLÍŽEK, David. ČTÚ uvolnil pásmo 60 GHz, které může změnit bezdrátový trh. *Lupa.cz* [online]. Internet Info, 2019 [cit. 2021-5-19]. Dostupné z: https://www.lupa.cz/aktuality/ctu-uvolnil-pasmo-60-ghz-ktere-muze-zmenit-bezdratovy-trh/

[7] CARROLL, Brandon. Chapter 1: Introduction to Wireless Networking Concepts. *NETWORKWORLD* [online]. IDG Communications, © 2021, 13. 1. 2009 [cit. 2021-5-19]. Dostupné z: https://www.networkworld.com/article/2272293/chapter-1--introduction-to-wireless-networking-concepts.html?page=2

[8] SHAW, Keith. What is MU-MIMO and why you need it in your wireless routers. *NETWORKWORLD* [online]. IDG Communications, © 2021, 26. 1. 2018 [cit. 2021-5-19]. Dostupné z: https://www.networkworld.com/article/3250268/what-is-mu-mimo-and-why-you-need-it-in-your-wireless-routers.html

[9] KENTON, Will. Federal Communications Commission (FCC). *Investopedia* [online]. Dotdash, 30. 3. 2021 [cit. 2021-5-19]. Dostupné z: https://www.investopedia.com/terms/f/fcc.asp

[10] IEEE. About IEEE. *IEEE Advancing Technology for Humanity* [online]. © Copyright 2021 [cit. 2021-5-24]. Dostupné z: https://www.ieee.org/about/index.html

[11] WI-FI ALLIANCE. Who We Are. *Wi-Fi Alliance* [online]. © Copyright 2021 [cit. 2021-5-24]. Dostupné z: https://www.wi-fi.org/who-we-are

[12] ORR, Ruby Ashby. *Sto a jedna věc co dělat, když wifi nefunguje*. Ilustroval Kenny PITTOCK, přeložil Kateřina NEJEDLÁ. Praha: Ikar, 2020. Esence. ISBN 978-80-249-4280-3.

[13] REJZEK, Jakub. Wi-Fi 6 přichází. Co je pod pokličkou nového standardu? *Lupa.cz* [online]. Internet Info, 11. 6. 2019 [cit. 2021-5-19]. Dostupné z: https://www.lupa.cz/clanky/wi-fi-6-prichazi-co-je-pod-poklickou-noveho-standardu/

[14] Jaký je rozdíl mezi Wi-Fi standardy? *Kvalitní internet* [online]. 2020, 8. 4. 2021 [cit. 2021-5-19]. Dostupné z: https://www.kvalitni-internet.cz/jaky-je-rozdil-mezi-wi-fi-standardy

[15] Wireless LAN Controller Explained and FAQs. *FS Community* [online]. Copyright © 2009-2021: FS.COM, Copyright © 2009-2021, 6. 11. 2020 [cit. 2021-5-24]. Dostupné z: https://community.fs.com/blog/wireless-lan-controller-explained.html

[16] The Layer 2 Roaming Process. *Cisco Certified Expert* [online]. 18. 12. 2020 [cit. 2021-5-19]. Dostupné z: https://www.ccexpert.us/wireless-networks/the-layer-2-roaming-process.html

[17] The Layer 3 Roaming Process. *Cisco Certified Expert* [online]. 18. 12. 2020 [cit. 2021-5-19]. Dostupné z: https://www.ccexpert.us/wireless-networks/the-layer-3-roaming-process.html

[18] *ManagementMania: profesionální dynamická znalostní síť* [online]. Wilmington USA: MANAGEMENTMANIA.COM, © 2011-2020 [cit. 2020-11-20]. ISSN 2327-3658. Dostupné z: https://managementmania.com

[19] Digitální certifikát. *ManagementMania* [online]. ManagementMania.com, © 2011-2021, 27.3.2018 [cit. 2021-5-19]. Dostupné z: https://managementmania.com/cs/digitalni-certifikat

[20] FRUHLINGER, Josh a Joel SNYDER. 802.1X: What you need to know about this LAN-authentication standard. *NETWORKWORLD* [online]. IDG Communications,

© 2021, 2021 [cit. 2021-5-19]. Dostupné z: https://www.networkworld.com/article/2216499/wireless-what-is-802-1x.html

[21] MILFAJT, Jiří. *Bezpečnostní protokoly v praxi* [online]. Brno, 2008 [cit. 2021-5-19]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=9194. Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce Ing. Tomáš Pelka.

[22] LUDIN, Jake. 802.1X EAP-TLS Authentication Flow Explained. *Security Boulevard* [online]. MediaOps, © 2021, 13. 4. 2021 [cit. 2021-5-19]. Dostupné z: https://securityboulevard.com/2021/04/802-1x-eap-tls-authentication-flow-explained/

[23] LUDIN, Jake. EAP-TLS vs. PEAP-MSCHAPv2: Which Authentication Protocol is Superior? *Security Boulevard* [online]. MediaOps, © 2021, 31. 1. 2020 [cit. 2021-5-19]. Dostupné z: https://securityboulevard.com/2020/01/eap-tls-vs-peap-mschapv2-which-authentication-protocol-is-superior/https://securityboulevard.com/2020/01/eap-tls-vs-peap-mschapv2-which-authentication-protocol-is-superior/

[24] POSPÍŠIL, Radek. Autentizace v počítačových sítích a návrh mechanismu jednorázového navýšení uživatelských práv. *Elektrorevue* [online]. ISES, 2013, 2013, **15**(2), 10 [cit. 2021-5-19]. ISSN 1213-1539. Dostupné z: http://www.elektrorevue.cz/cz/download/autentizace-v-pocitacovych-sitich-a-navrh-mechanismu-jednorazoveho-navyseni-uzivatelskych-prav/

[25] Uživatelská příručka k Nástroji pro připojení Intel® PROSet/Wireless WiFi. *Support elmark* [online]. © 2004–2010: Intel Corporation, 2010 [cit. 2021-5-24]. Dostupné z: http://support.elmark.com.pl/rgd/drivery/u12c/wlan/win7/Docs/CSY/overview.htm#authenticate

[26] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

[27] WEP vs. WPA vs. WPA2 vs. WPA3. *FS Community* [online]. Copyright © 2009-2021: FS.COM, Copyright © 2009-2021, 6. 11. 2020 [cit. 2021-5-24]. Dostupné z: https://community.fs.com/blog/wep-vs-wpa-vs-wpa2-vs-wpa3.html

[28] SIMANDL, Martin. K čemu je dobré WPA3? *ChanelWorld* [online]. Internet Info DG, 24. 9. 2018 [cit. 2021-5-19]. Dostupné z: https://channelworld.cz/software/k-cemu-je-dobre-wpa3-21474

[29] SOMMERVILLE, Ian. *Software engineering*. Tenth edition. Boston: Pearson, [2016]. ISBN isbn-978-0133943030.

[30] NETALLY. AirMagnet® Survey PRO. *NetAlly* [online]. NetAlly, © 2020 - 2021 [cit. 2021-5-24]. Dostupné z: https://www.netally.com/products/airmagnet-survey-pro/

[31] NETALLY. AirCheck™ G2 Wireless Tester. *NetAlly* [online]. NetAlly, 2020 - 2021 [cit. 2021-5-24]. Dostupné z: https://www.netally.com/aircheck-g2-request-demo/

[32] CISCO. Cisco Aironet 1600 Series Access Point Data Sheet: Products & Services. *Cisco* [online]. 2021, 8. 8. 2016 [cit. 2021-5-24]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1600-series/data_sheet_c78-715702.html

[33] CISCO. Cisco Aironet 1700 Series Access Point Data Sheet: Products & Services. *Cisco* [online]. 2021, 20. 7. 2018 [cit. 2021-5-24]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1700-series/datasheet-c78-732347.html

[34] CISCO. Cisco Aironet 1830 Series Access Points Data Sheet: Products & Services. *Cisco* [online]. 2021, 1. 6. 2020 [cit. 2021-5-24]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1830-series-access-points/datasheet-c78-735582.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAA	Authentication, Authorization, Accounting
ACS	Auto Configuration Server
AD	Active Directory
AES	Advanced Encryption Standard
AP	Access Point
BSS	Basic Service Set
CA	Certification Authority
CCMP	CCM mode Protocol
CUWN	Cisco Unified Wireless Network
DSSS	Direct-Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication via Secure Tunnel
EAP-TLS	EAP-Transport Layer Security
EAPoL	EAP over LAN
EHF	Extremely High Frequency
ELF	Extremely Low Frequency
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
Gbit/s	Gigabit za sekundu
GHz	Gigahertz
GMK	Group Master Key
GTC	Generic Token Card
GTK	Group Temporal Key
CHAP	Challenge Handshake Authentication Protocol
IEEE	Institute of Electrical and Electronics Engineers

IoT	Internet of Things
IP	Internet Protocol
kHz	Kilohertz
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Light Extensible Authentication Protocol
LWAPP	Lightweight Access Point Protocol
Mbit/s	Megabit za sekundu
MHz	Megahertz
MIC	Message Integrity Code
MIMO	Multiple-Input Multiple-Output
MU-MIMO	Multi User-Multiple-Input Multiple-Output
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
PAC	Protected Access Credential
PAP	Password Authentication Protocol
PEAP	Protected EAP
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PPP	Point to Point Protocol
PoE	Power over Ethernet
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
QAM	Quadrature Amplitude Modulation
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency

RSSI	Recieved Signal Strenght Indicator
SAE	Simultaneous Authentication of Equals
SNR	Signal to Noise Ratio
SSID	Service Set Identifier
SSL	Secure Socket Layer
TKIP	Temporal Key Integrity Protocol
TWT	Target Wake Time
UTP	Unshielded Twisted Pair
VLAN	Virtual LAN
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN
WLC	Wireless LAN Controller
WPA	Wi-Fi Protected Access

SEZNAM OBRÁZKŮ

Obrázek 1 Radiové spektrum [4] 13
Obrázek 2 Proces EAP [1] (Vlastní zpracování) 29
Obrázek 3 Proces EAP-TLS [22] (Vlastní zpracování) 30
Obrázek 4 Proces EAP-FAST [1] (Vlastní zpracování) 32
Obrázek 5 Proces PEAP [23] (Vlastní zpracování) 34
Obrázek 6 Autentizace WPA [1] (Vlastní zpracování) 38
Obrázek 7 Čtyřfázová komunikace WPA [1] (Vlastní zpracování) 39
Obrázek 8 Software AirMagnet Survey PRO [30] 45
Obrázek 9 Plán prvního podzemního podlaží (Vlastní zpracování) 47
Obrázek 10 Plán prvního nadzemního podlaží (Vlastní zpracování) 48
Obrázek 11 Plán druhého nadzemního podlaží (Vlastní zpracování) 49
Obrázek 12 Plán třetího nadzemního podlaží (Vlastní zpracování) 50
Obrázek 13 Plán čtvrtého nadzemního podlaží (Vlastní zpracování) 50
Obrázek 14 Plán pátého nadzemního podlaží (Vlastní zpracování) 51
Obrázek 15 Přístupový bod Cisco Aironet 1602I [32] 52
Obrázek 16 Přístupový bod Cisco Aironet 1702I [33] 53
Obrázek 17 Přístupový bod Cisco Aironet 1832I [34] 54
Obrázek 18 Výsledek měření v prvním podzemním podlaží (Vlastní zpracování) 59
Obrázek 19 Výsledek měření v prvním nadzemním podlaží (Vlastní zpracování) 60
Obrázek 20 Výsledek měření ve druhém nadzemním podlaží (Vlastní zpracování) 60
Obrázek 21 Výsledek měření ve třetím nadzemním podlaží (Vlastní zpracování) 61
Obrázek 22 Výsledek měření ve čtvrtém nadzemním podlaží (Vlastní zpracování) 61
Obrázek 23 Výsledek měření v pátém nadzemním podlaží (Vlastní zpracování) 62
Obrázek 24 Plán prvního podzemního podlaží po změnách (Vlastní zpracování) 67
Obrázek 25 Plán prvního nadzemního podlaží po změnách (Vlastní zpracování) 68
Obrázek 26 Plán druhého nadzemního podlaží po změnách (Vlastní zpracování) 68
Obrázek 27 Plán třetího nadzemního podlaží po změnách (Vlastní zpracování) 69
Obrázek 28 Plán čtvrtého nadzemního podlaží po změnách (Vlastní zpracování) 70
Obrázek 29 Plán pátého nadzemního podlaží po změnách (Vlastní zpracování) 71
Obrázek 30 Výsledek měření v prvním podzemním podlaží po změnách (Vlastní zpracování) 73

Obrázek 31 Výsledek měření v prvním nadzemním podlaží po změnách (Vlastní zpracování) 74
Obrázek 32 Výsledek měření ve druhém nadzemním podlaží po změnách (Vlastní zpracování) 75
Obrázek 33 Výsledek měření ve třetím nadzemním podlaží po změnách (Vlastní zpracování) 76
Obrázek 34 Výsledek měření ve čtvrtém nadzemním podlaží po změnách (Vlastní zpracování) 77
Obrázek 35 Výsledek měření v pátém nadzemním podlaží po změnách (Vlastní zpracování) 78

SEZNAM TABULEK

Tabulka 1 Nastavení WLC pro 2,4 GHz.....55
Tabulka 2 Nastavení WLC pro 5 GHz.....55
Tabulka 3 Nastavení WLC pro 2,4 GHz.....65
Tabulka 4 Nastavení WLC pro 5 GHz.....66

SEZNAM PŘÍLOH

Příloha P I: Model prvního podzemního podlaží

Příloha P II: Model prvního nadzemního podlaží

Příloha P III: Model druhého nadzemního podlaží

Příloha P IV: Model třetího nadzemního podlaží

Příloha P V: Model čtvrtého nadzemního podlaží

Příloha P VI: Model pátého nadzemního podlaží

Příloha P VII: Model šíření mezi podlažími

Příloha P VIII: Model prvního podzemního podlaží po změnách

Příloha P IX: Model prvního nadzemního podlaží po změnách

Příloha P X: Model druhého nadzemního podlaží po změnách

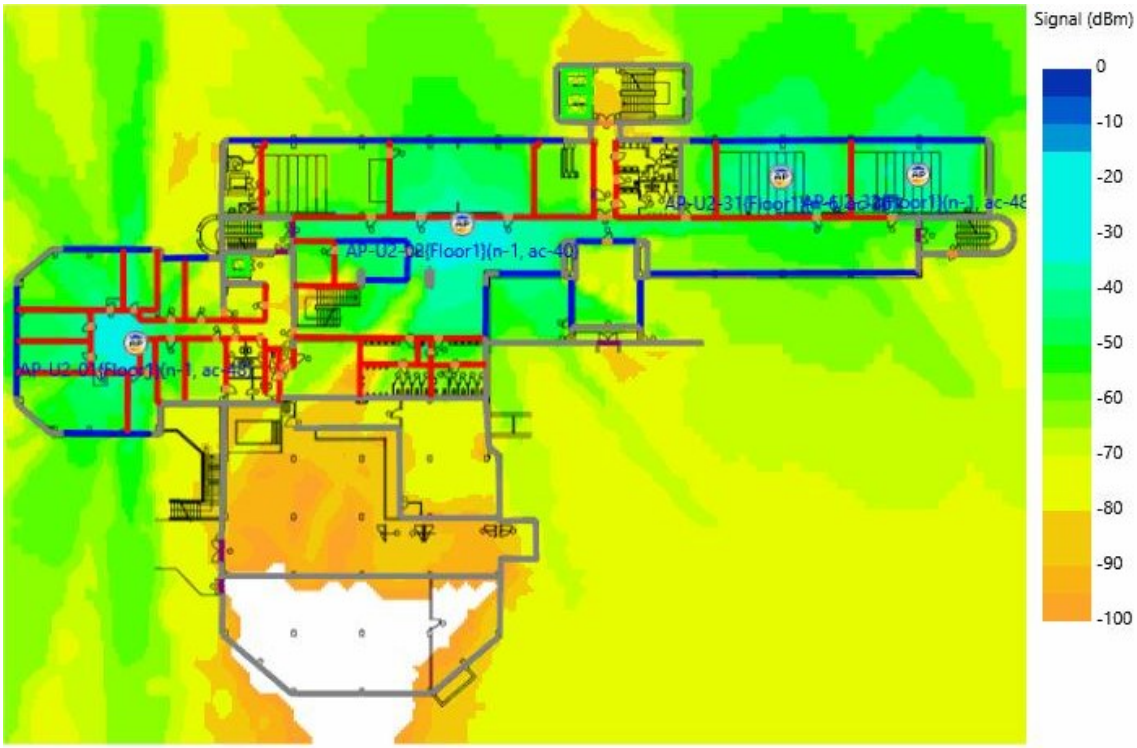
Příloha P XI: Model třetího nadzemního podlaží po změnách

Příloha P XII: Model čtvrtého nadzemního podlaží po změnách

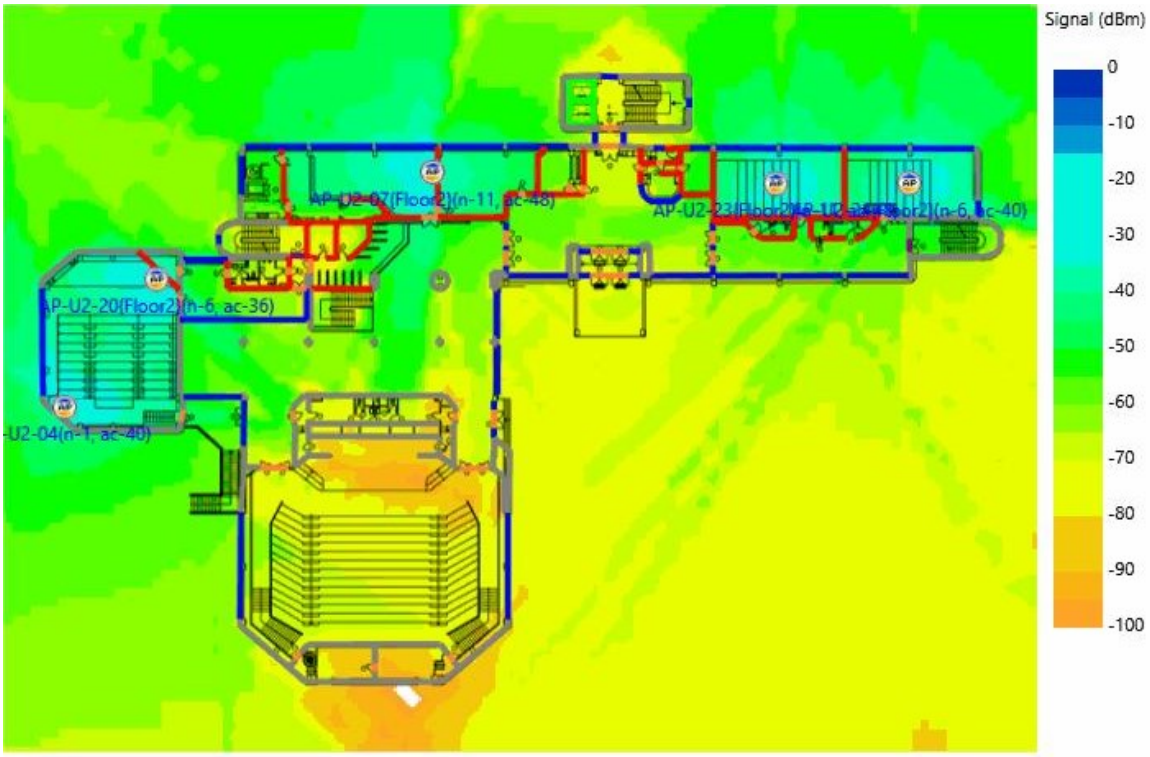
Příloha P XIII: Model pátého nadzemního podlaží po změnách

Příloha P XIV: Model šíření mezi podlažími po změnách

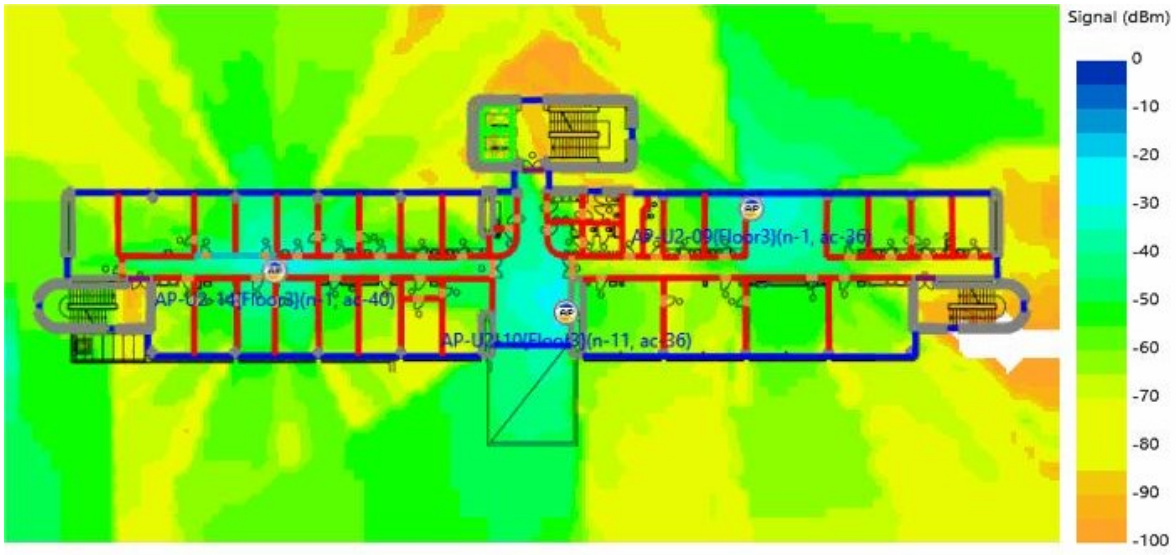
PŘÍLOHA P I: MODEL PRVNÍHO PODZEMNÍHO PODLAŽÍ



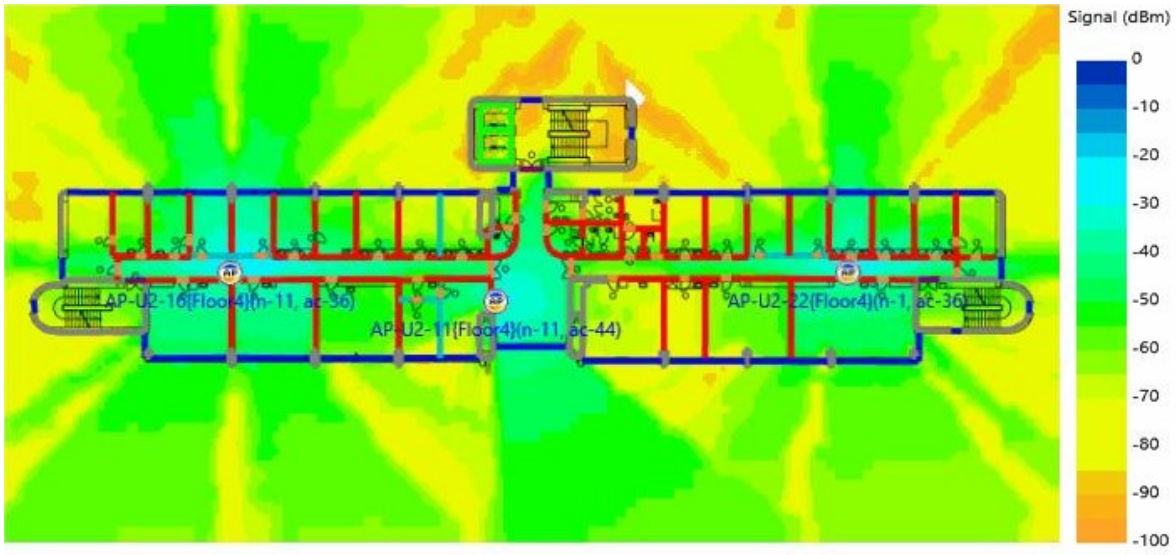
PŘÍLOHA P II: MODEL PRVNÍHO NADZEMNÍHO PODLAŽÍ



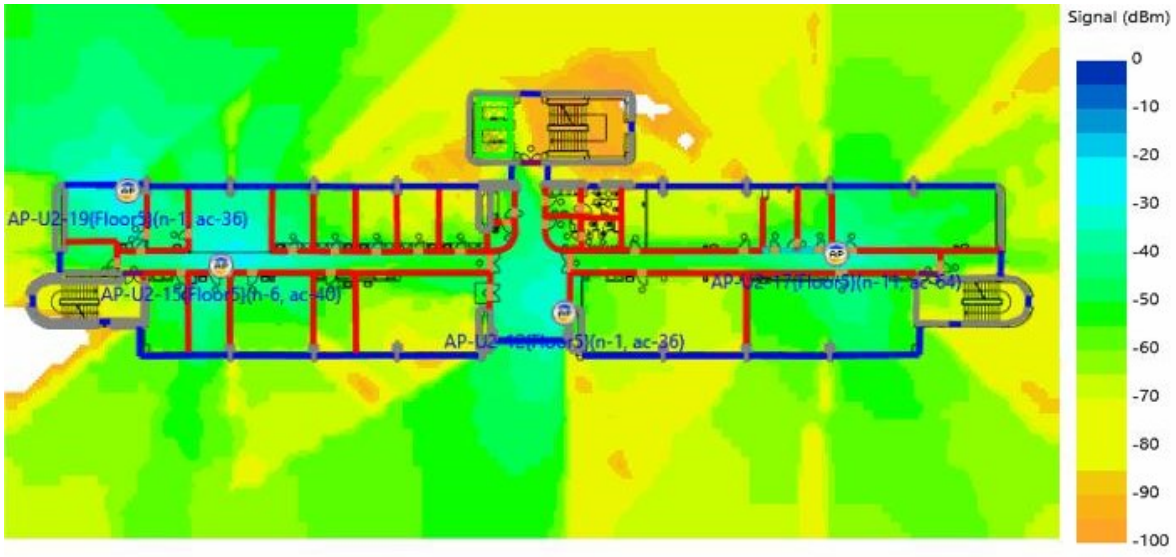
PŘÍLOHA P III: MODEL DRUHÉHO NADZEMNÍHO PODLAŽÍ



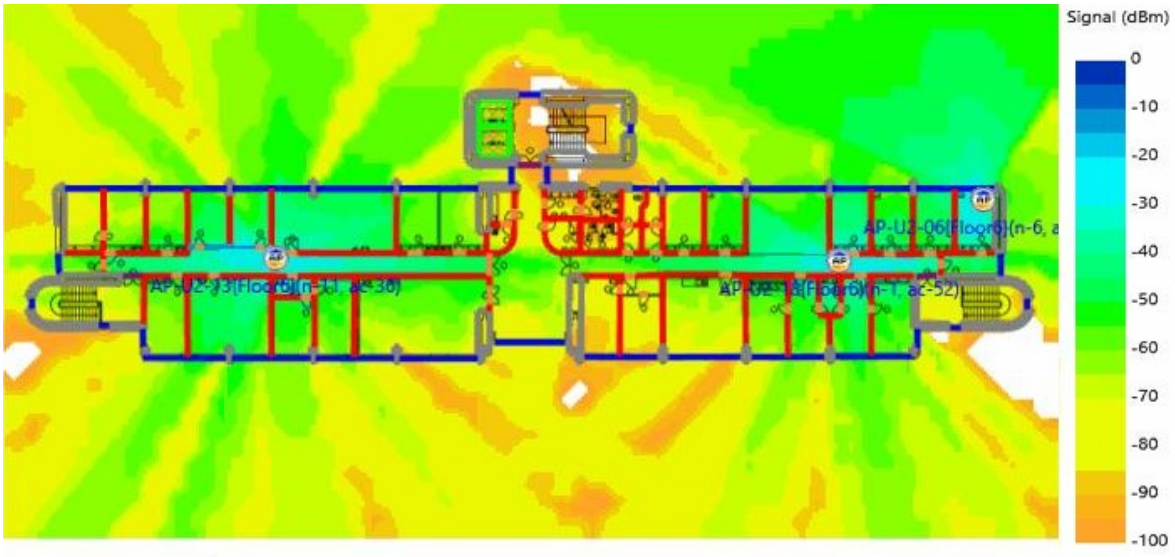
PŘÍLOHA P IV: MODEL TŘETÍHO NADZEMNÍHO PODLAŽÍ



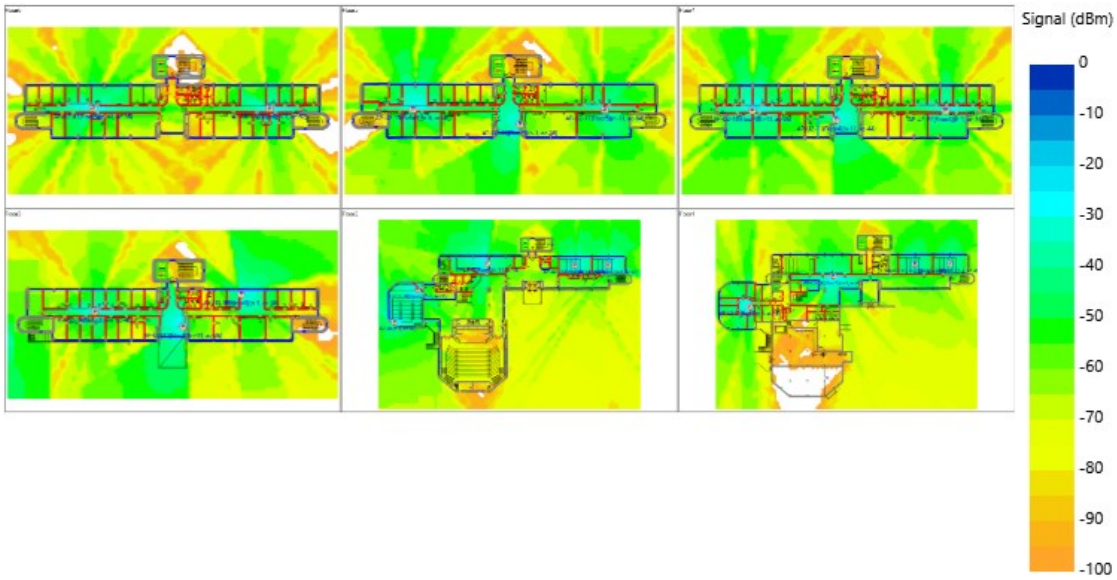
PŘÍLOHA P V: MODEL ČTVRTÉHO NADZEMNÍHO PODLAŽÍ



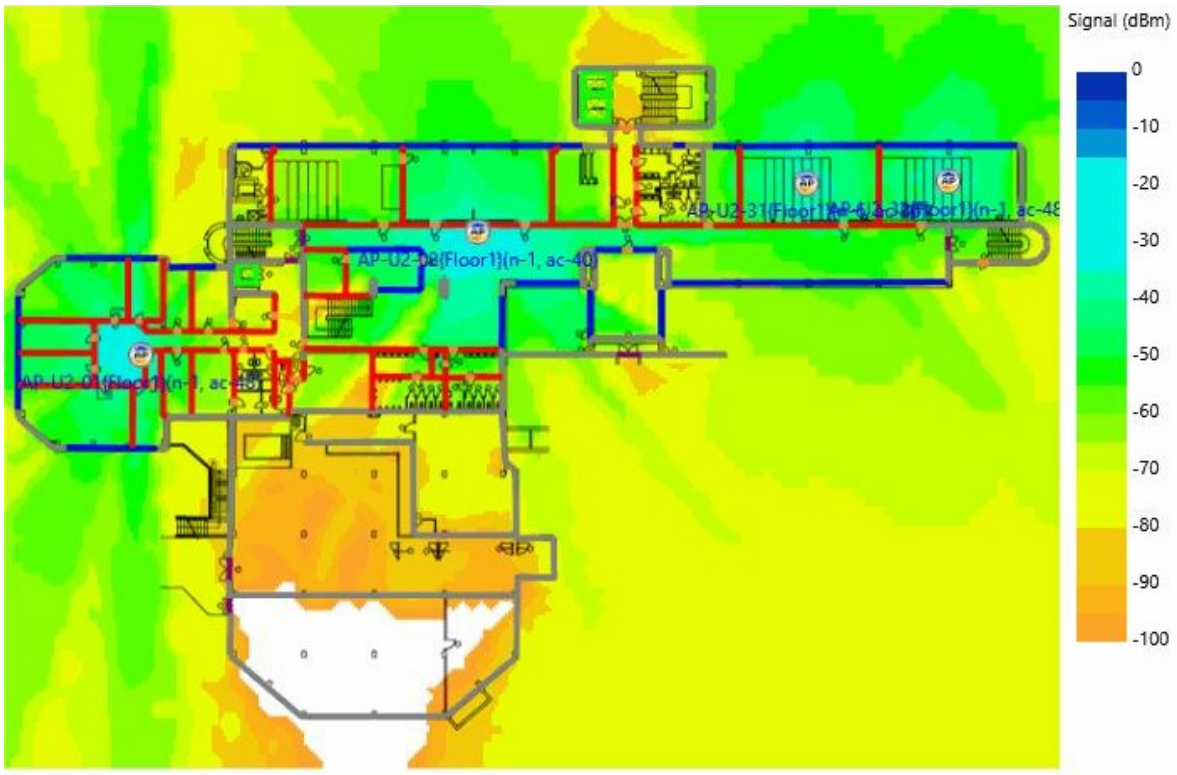
PŘÍLOHA P VI: MODEL PÁTÉHO NADZEMNÍHO PODLAŽÍ



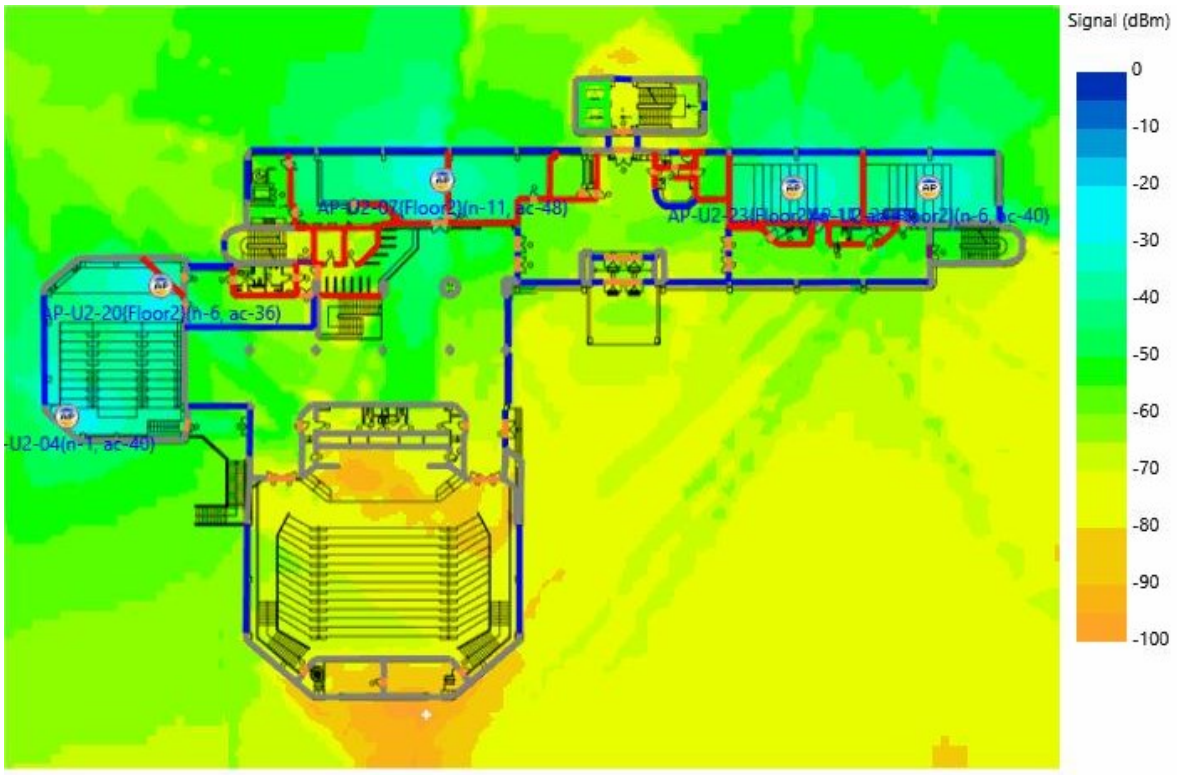
PŘÍLOHA P VII: MODEL ŠÍŘENÍ MEZI PODLAŽÍMI



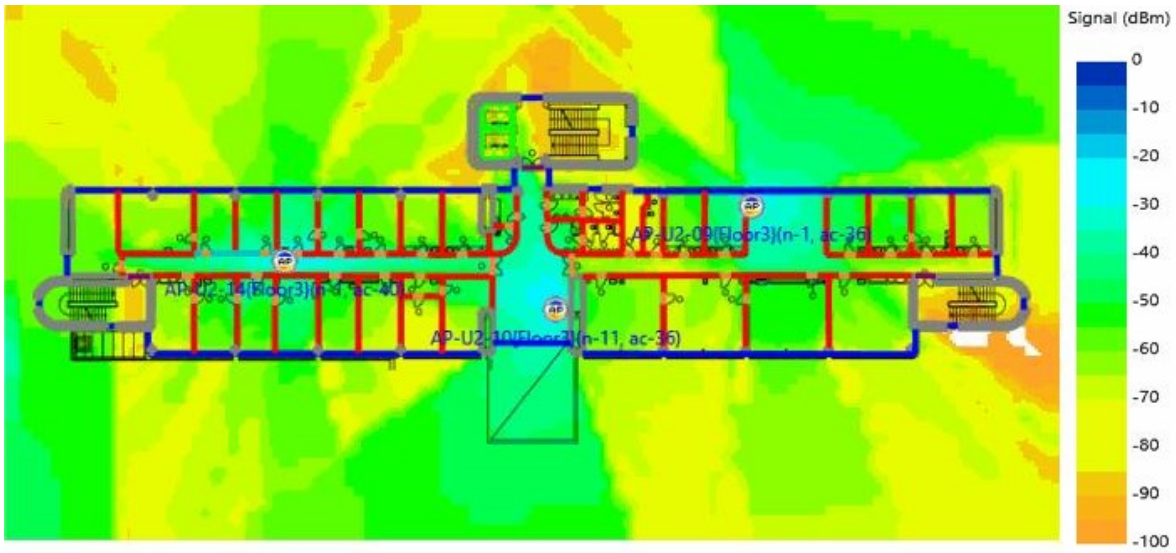
PŘÍLOHA P VIII: MODEL PRVNÍHO PODZEMNÍHO PODLAŽÍ PO ZMĚNÁCH



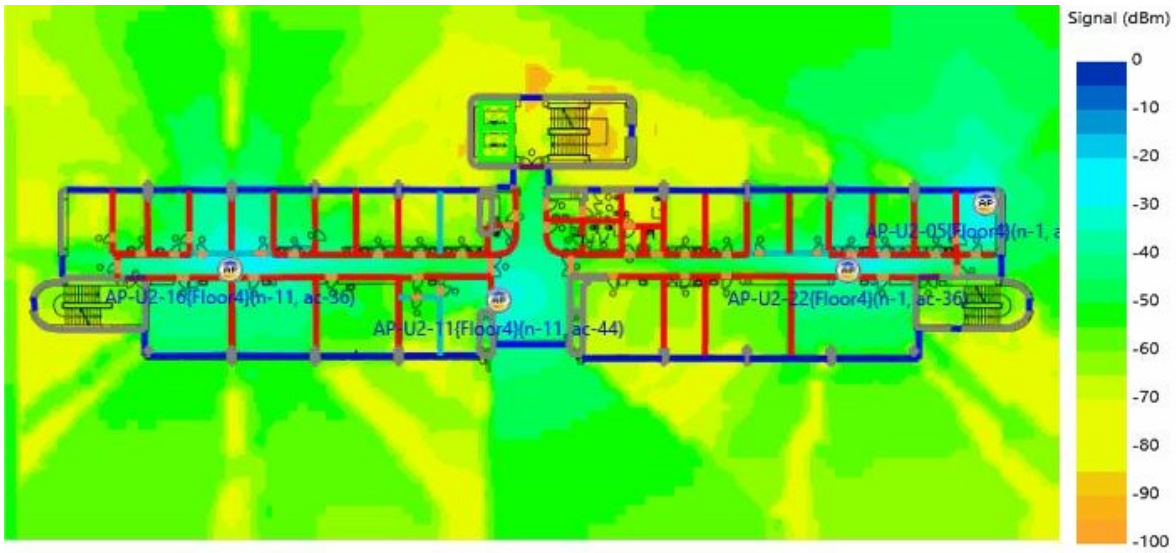
PŘÍLOHA P IX: MODEL PRVNÍHO NADZEMNÍHO PODLAŽÍ PO ZMĚNÁCH



PŘÍLOHA P X: MODEL DRUHÉHO NADZEMNÍHO PODLAŽÍ PO ZMĚNÁCH

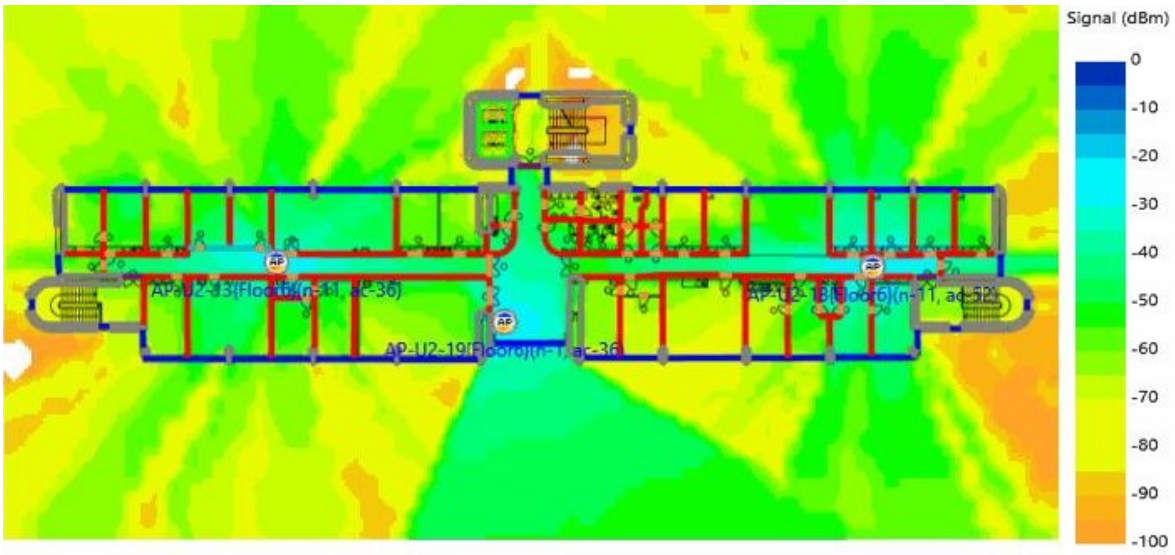


PŘÍLOHA P XI: MODEL TŘETÍHO NADZEMNÍHO PODLAŽÍ PO ZMĚNÁCH



PŘÍLOHA P XII: MODEL ČTVRTÉHO NADZEMNÍHO PODLAŽÍ PO ZMĚNÁCH

PŘÍLOHA P XIII: MODEL PÁTÉHO NADZEMNÍHO PODLAŽÍ PO ZMĚNÁCH



PŘÍLOHA P XIV: MODEL ŠÍŘENÍ MEZI PODLAŽÍMI PO ZMĚNÁCH