Připojení do Internetu pomocí bezdrátové sítě v areálu U5

Connecting to the Internet via a Wireless Network in the U5 Site

Pavel Machala

Bakalářská práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

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

Jméno a příjmení:	**Pavel Machala**
Osobní číslo:	**A13298**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Připojení do Internetu pomocí bezdrátové sítě v areálu U5**
Téma anglicky:	**Connecting to the Internet via a Wireless Network in the U5 Site**

Zásady pro vypracování:

1. **Zpracujte literární rešerši na dané téma.**
2. **Popiště stávající řešení bezdrátové sítě v areálu U5.**
3. **Zvolte způsob, metodu a zařízení, kterými budete provádět měření.**
4. **Proveďte měření intenzity signálu jednotlivých přístupových bodů v areálu U5.**
5. **Vytvořte schéma půdorysu areálu U5, na kterém bude graficky znázorněna intenzita signálu jednotlivých přístupových bodů.**
6. **Proveďte průzkum dostupných bezdrátových přístupových bodů na trhu a navrhněte případný přechod na nová zařízení.**
7. **Na základě měření intenzity signálu od jednotlivých přístupových bodů navrhněte změny v umístění bezdrátových přístupových bodů v areálu U5.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ZURAWSKI, Richard. Industrial communication technology handbook. Second edition. Boca Raton: CRC Press, 2014, 1756 p. ISBN 978-1-4822-0732-3.**
2. **DULÍK, Tomáš. Methods for interference mitigation in wireless networks: doctoral thesis summary. Zlín: Tomas Bata University, 2012, 78 p. ISBN 978-80-7454-233-6.**
3. **CARROLL, Brandon. Bezdrátové sítě Cisco: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2011, 478 s. ISBN 978-80-251-2884-8.**
4. **HOLT, Alan a Chi-Yu HUANG. 802.11 wireless networks: security and analysis. London: Springer, 2010, 212 p. ISBN 978-1-84996-275-9.**
5. **GARG, Vijay Kumar. Wireless communications and networking. San Francisco, Calif.: Morgan Kaufmann, 2007, 821 s. ISBN 978-0-12-373580-5.**

Vedoucí bakalářské práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **3. února 2017**

Termín odevzdání bakalářské práce: **30. května 2017**

Ve Zlíně dne 3. února 2017

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

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Miroslav Matýsek, Ph.D.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

- že jsem na diplomové/bakalářské 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 29.5.2017

.....
podpis diplomanta

ABSTRAKT

Tato práce se dělí do dvou částí. Nejprve se zabývá problematikou bezdrátových sítí. Shrnuje technologie používané při bezdrátovém připojení a jejich možnosti zabezpečení. Následně analyzuje existující řešení bezdrátové sítě v objektu U5 Univerzity Tomáše Bati ve Zlíně, zaměřuje se na vytvoření mapy pokrytí areálu a předkládá potencionální vylepšení stávající bezdrátové sítě společně s předpokládanými náklady.

Klíčová slova: Bezdrátové sítě, bezdrátové připojení, IEEE, 802.11, eduroam.

ABSTRACT

This thesis is divided into two parts. At first, It is looking into wireless networks in general and all the wireless technologies are being summarized together with all the security possibilities. The current existing wireless network at Tomas Bata University is being analyzed after. This thesis focuses on creating a map of wireless connectivity and suggesting how to improve the existing network. All the improvements costs are enumerated at the end.

Keywords: Wireless networks, wireless connection, IEEE, 802.11, eduroam.

Poděkování

Rád bych poděkoval Ing. Miroslavu Matýskovi, Ph.D. za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce.

OBSAH

ÚVOD

Bezdrátové sítě nás v dnešní době obklopují a stále se masivně rozšiřují. Děje se tomu tak hlavně díky jednoduchosti zapojení a vysoké přenosové rychlosti při dnešních standardech sítí. S rostoucím zájmem společnosti o bezdrátové sítě dále také rostou nároky na dostupnost těchto sítí, jejich reálnou přenosovou rychlost a bezpečnost. Tato práce se zabývá právě problematikou bezdrátových sítí, popisuje různé standardy těchto sítí, seznamuje s možnostmi zabezpečení a pojednává o jejich vývoji.

Tato práce analyzuje bezdrátovou síť v univerzitním areálu a v souladu s tím popisuje architekturu této sítě. Univerzita Tomáše Bati je členem celoevropského projektu s názvem eduroam, díky kterému mají uživatelé možnost se připojit do sítě v rámci celé univerzity bez jakýchkoliv omezení.

Hlavním cílem práce bylo vytvoření schématu zachycujícího jednotlivé přístupové body bezdrátové sítě společně s intenzitou signálu v celém areálu. Dalším cílem práce byla tvorba návrhu inovované bezdrátové sítě na základě získaných informací z provedených měření, vyhodnocení a vylepšení stávajícího zabezpečení sítě v areálu. Následně byla provedena kalkulace nákladů potřebných k realizaci navrhovaných inovací.

I. TEORETICKÁ ČÁST

1 HISTORIE BEZDRÁTOVÉ KOMUNIKACE

Elektronické komunikační systémy měly obrovský dopad na moderní společnost. Prvním počinem v oblasti elektrické telegrafie byl projekt Josepha Henryho a Samuela F.B. Morse v roce 1832 krátce po objevení elektromagnetismu Hansem Christianem Oerstedem a Andre-Marie Amperem v brzkých 20. letech 19. století. První telegrafní sítě byly vybudovány na Východním Pobřeží Spojených Států Amerických a v Kalifornii. Následoval rapidní nárůst využití telegrafních sítí a v roce 1858 byl položen první transatlantický kabel, který spojil Evropu a Severní Ameriku.

V roce 1864 bylo předpovězeno bezdrátové šíření elektromagnetických vln fyzikem Jamesem Maxwellem, které bylo následně potvrzeno experimentem německého fyzika Heinricha Hertze v roce 1887. Krátce poté, začal italský fyzik Guglielmo Marconi experimentovat s radio-telegrafií a stal se také prvním člověkem, kterému se povedlo úspěšně přenést informaci bezdrátově a to v roce 1895 za použití bezdrátového telegrafu na vzdálenost dvou kilometrů, načež si použitý přístroj následující rok patentoval. Při dalším experimentu, v roce 1897, již uskutečnil bezdrátový přenos informace na vzdálenost 15 km. Koncem roku 1901 bylo poprvé navázáno bezdrátové spojení přes Atlantský oceán. Dalším milníkem v bezdrátové komunikaci byl rok 1906, kdy se historicky poprvé podařilo rádiově přenést hlas.

Bezdrátová komunikace prošla značným vývojem i v době První světové války, kdy byla tato technologie hojně využívána.

V roce 1921 detroitská policie zprovoznila první automobil, který měl na své palubě radiopřijímač, který byl schopný zachycovat morseovku. O sedm let později, v roce 1928 již byli schopni přenášet také hlas, což významně usnadnilo strážníkům práci.

Mezitím, v roce 1924 sestrojili v Amerických „Bell Laboratories“ první mobilní rádio, které bylo schopné přenést hlas v obou směrech.

Ve Druhé světové válce bezdrátová komunikace sehrála taktéž důležitou roli, když se na bojišti využívala ke komunikaci radio vysílačka.

První návrhy mobilních radiových stanic se začaly objevovat v 50. letech minulého století a fungovaly na podobném principu jako je tomu u dnešních GSM sítí. Zhruba o deset let později byl uskutečněn první analogový telefonní přenos.

Na konci 80. let 20. století se začaly objevovat první digitální telefonní systémy. Nejznámějším z nich je GSM (Globální Systém pro Mobilní komunikaci), který se používá dodnes.

Posledním velkým mezníkem pro bezdrátovou komunikaci byl rok 1997, kdy byl IEEE 802.11 přijat jako standard pro bezdrátovou komunikaci mezi počítači [8], [9].

2 STANDARD IEEE 802.11

802.11 je standardem, který byl zveřejněn v roce 1997 americkým institutem IEEE (Institute of Electrical and Electronics Engineers). IEEE je nezisková organizace, která usiluje o zdokonalování elektrotechnických technologií. Jde o specifikaci bezdrátové lokální sítě zvané také WLAN (Wireless Local Area Network).

Používá se nejčastěji v místech, kde by bylo technicky nemožné nebo ekonomicky nevýhodné provozovat počítačovou síť s použitím optických kabelů. Jednou z největších výhod, pomineme-li finanční výhodnost, bezdrátových sítí LAN (Local Area Network) je bezesporu uživatelská mobilita, kterou bezdrátové sítě nabízí. Původní standard 802.11 z roku 1997 pracoval s maximální přenosovou rychlostí pouze 1–2 Mbits/s [2], [13].

Obr. 1 – Logo - Institute of Electrical and Electronic Engineers [12].

S postupem času se zvyšovaly nároky na bezdrátovou síť, zejména na schopnost přenášet větší množství dat za stejnou jednotku času. S ohledem na nároky uživatelů začaly postupně vznikat v rámci standardu 802.11 další pracovní podskupiny, které se věnovaly změnám a vylepšením tohoto standardu [11].

Bezdrátová síť je obecně specifikována protokolem 802.11. Tento standard se dále dělí na různé verze standardu 802.11. Příkladem: 802.11.a, 802.11b, 802.11 apod. Tyto verze standardu k šíření radiového signálu používají spektrum vysokých frekvencí. V dnešní době však bývají nejčastěji používány zařízení s frekvencemi 2,4 GHz a 5 GHz [16], [17].

Standard 802.11 je zaměřen na dvě nejnižší vrstvy OSI (Open Systems Interconnection)modelu, kterými jsou vrstva fyzická a vrstva spojová. Všechny síťové

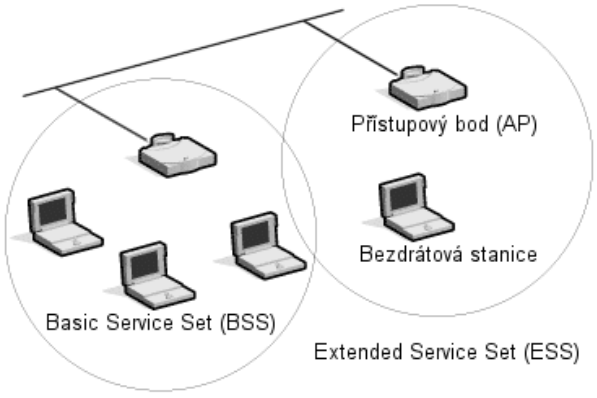
aplikace, síťové operační systémy a protokoly (TCP/IP apod.) pracují na síti, která je kompatibilní se standardem 802.11 stejně tak, jako je tomu u Ethernetu.

Standard 802.11 definuje dvě různá zařízení. Prvním z nich bývá nejčastěji osobní počítač, popřípadě jiné zařízení vybavené síťovou kartou vhodnou pro připojení do bezdrátové sítě, druhým zařízením je vždy přístupový bod. Tento přístupový bod slouží jako most mezi bezdrátovou částí a částí lokální počítačové sítě. Stanice, které vyžadují přístup k prostředkům umístěným mimo bezdrátovou síť (např. Internet) komunikují s přístupovými body, které jim to umožní [11].

Bezdrátové sítě výše zmíněného standardu mohou pracovat ve dvou různých režimech podle použité architektury:

Infrastruktura

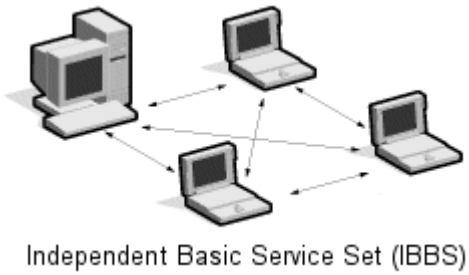
Bezdrátová síť se v tomto režimu skládá z alespoň jednoho přístupového bodu, který je připojený na lokální počítačovou síť. Mimo tohoto přístupového bodu se také bezdrátová síť skládá z několika bezdrátových stanic připojených právě k přístupovému bodu. Veškerý přenos dat je uskutečněn přes přístupový bod. Tato architektura sítě bývá také nazývána BSS, což je zkratka pro anglické slovní spojení Basic Service Set. Sítě typu BSS je možné kombinovat a spojením více BSS sítí dohromady vznikne lokální síť s označením ESS (zkratka pro Extended Service Set). V současné době jde o nejčastěji používanou architekturu bezdrátové sítě a to z mnoha důvodů. Jedním a zároveň nejzásadnějším důvodem je, že bezdrátové stanice vyžadují přístup k tiskárnám, internetu nebo třeba k souborovému serveru. Níže uvedený obrázek uvádí klasický příklad použití bezdrátové sítě, kdy je několik bezdrátových stanic připojeno k různým přístupovým bodům uvnitř budovy, které umožňují připojení k internetu, nebo ke sdíleným prostředkům [2], [13].



Obr. 2 – Infrastruktura [13].

Ad hoc

Bezdrátová síť se v tomto režimu skládá pouze z bezdrátových stanic. Tento režim sítě tedy neobsahuje žádný přístupový bod sloužící k přístupu do fixní počítačové sítě. Tuto síť lze vytvořit kdekoliv bez potřeby jakékoliv fixní složky. Jednotlivá bezdrátová zařízení, která tvoří tuto síť mezi sebou navzájem komunikují. Této architektuře bezdrátové sítě se také říká peer to peer nebo IBSS (Independent Basic Service Set) [2], [13].



Obr. 3 – Ad hoc [13].

2.1 802.11b

V minulosti nejrozšířenější standard 802.11b byl následně nahrazen standardem 802.11g. 802.11b vysílá radiový signál ve stejném spektru 2,4 GHz s fyzickou vrstvou DSSS (Direct Sequence Spread Spectrum). Díky tomuto faktu jsou oba standardy navzájem kompatibilní. Jinými slovy, starší zařízení, která využívají standard 802.11b, mohou být kombinována s modernějšími zařízeními pracujícími se standardem 802.11g a také naopak. Drtivá většina dnes dostupných nových WiFi zařízení podporuje všechny dostupné standardy IEEE 802.11/b/g/n/ac atd. Hlavní nevýhodou staršího standardu 802.11b je zejména jeho nízká maximální přenosová rychlost (11 Mb/s). Díky tomuto faktu lze standard 802.11b označit jako zastaralý, jelikož tato přenosová rychlost nevyhovuje dnešním požadavkům pro rychlost přenosu dat [2].

2.2 802.11g

802.11g je WiFi standard rozšiřující IEEE802.11b. Je zpětně kompatibilní, jelikož vysílá ve stejném frekvenčním spektru 2,4 – 2,485 GHz, ovšem výše zmíněný standard figuruje maximální přenosovou rychlostí bezmála pětinásobně vyšší, než tomu bylo u jeho předchůdce a to 54 Mbit/s.

802.11g používá modulační schéma OFDM pro rychlosti 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s, přičemž pro rychlosti 1, 2, 5.5 a 11 Mbit/s je použito stejné schéma jako ve standardu IEEE 802.11b [2].

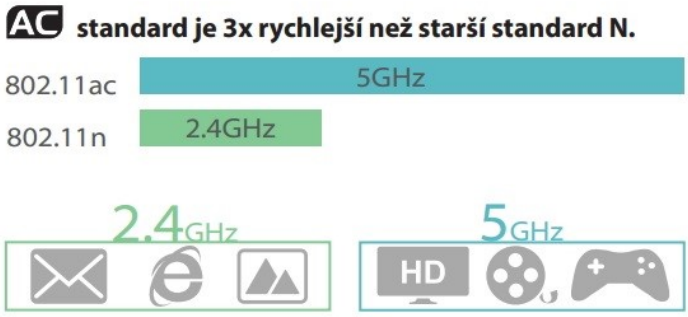
2.3 802.11n

Dalším standardem z řady 802.11 je standard 802.11n. Tento standard modifikuje fyzickou vrstvu zároveň s částí linkové vrstvy, která se nazývá MAC (Media Access Control). Maximální přenosová rychlost u tohoto standardu činí 100 Mbit/s a to zejména díky modifikacím uvedeným výše [2].

2.4 802.11ac

Bezdrátová síť pracující na frekvenci 2,4 GHz je k dispozici od roku 1999, kdy nebyly nároky na bezdrátovou síť tak vysoké jako je tomu dnes. Postupem času se však začalo objevovat stále více zařízení využívajících bezdrátového připojení (chytré telefony, tablety, chytré televize, herní konzole apod.) a tím se maximální přenosové rychlosti pásma 2,4 GHz začaly stávat nedostačujícími.

Z tohoto důvodu byl vyvinut standard 802.11ac pracující na frekvenci 5 GHz, který disponuje až třikrát vyšší přenosovou rychlostí a zároveň je stabilnější, než 2,4 GHz.



Obr. 4 – Standard 802.11ac [14].

802.11ac standard umožňuje díky vysoké přenosové rychlosti hraní her po síti nebo například plynulé streamování kvalitního obrazu (Full HD, Ultra HD) a to vše souběžně i na více zařízeních. Požadavkem pro provoz 5 GHz bezdrátové sítě je router podporující toto pásmo. V dnešní době je však pořizovací cena takového zařízení relativně nízká a přechod na rychlejší pásmo se zcela určitě uživatelům vyplatí.

Tento standard nabízí minimální teoretickou propustnost jedné linky 500 Mbit/s a 1 Gbit/s v případě propojení dvou zařízení.

Těchto výsledků je dosaženo pomocí modifikovaných konceptů standardu 802.11n. Nabízí širší RF pásmo, více MIMO kanálů, víceuživatelské MIMO a modulaci s vysokou hustotou [14], [16].

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

Obr. 5 – 802.11 standardy [1].

3 KOMPONENTY SÍTĚ

Všechny bezdrátové sítě standardu 802.11 se skládají z následujících síťových komponent:

- Distribuční systém.
- Přístupový bod.
- Bezdrátové médium.
- Stanice.

3.1 Distribuční systém

Jedná se o logický komponent standardu 802.11 sloužící ke směrování datového toku. Tento komponent je potřebný v případě, že se jedná o rozsáhlou síť tvořenou z více přístupových bodů. Je nutné, aby byla zajištěna komunikace mezi všemi přístupovými body a informace o pohybu mobilních stanic byly předávány [6].

3.2 Přístupový bod

Přístupový bod je zařízení, které přemosťuje bezdrátové sítě a sítě kabelové. Všechny stanice v bezdrátové síti komunikují přes tyto přístupové body [6].

3.3 Bezdrátové médium

Bezdrátové médium, jinými slovy také rádiová frekvence (2,4 a 5 GHz). Toto médium slouží k přenosu dat mezi stanicemi, nebo stanicemi a přístupovými body [6].

3.4 Stanice

Jedná se o místa, mezi kterými se přenášejí data. Stanicí se může stát takřka jakékoliv zařízení disponující možností bezdrátového připojení (PC s bezdrátovou síťovou kartou, notebook, chytré telefony, chytré televize apod.), nemusí se tedy vždy jednat o mobilní zařízení [6].

4 ZABEZPEČENÍ BEZDRÁTOVÝCH SÍTÍ

Existuje několik způsobů jak zabezpečit bezdrátovou síť, jak na straně klienta, tak na straně přístupového bodu.

4.1 Filtrování MAC adres

Jednou z možností zabezpečení bezdrátových sítí je takzvané filtrování MAC adres. MAC adresa je unikátní číslo, které nese síťová karta. Administrátor WLAN má možnost vytvořit seznam MAC adres, které mohou se sítí komunikovat. Jakmile se poté bude chtít na WiFi síť připojit stanice neuvedená v seznamu, router mu přístup nepovolí, jelikož MAC adresa jeho zařízení není uvedena v seznamu povolených adres. Filtr MAC adres je možné nastavit dvěma různými způsoby. Je možné zadat MAC adresy povolených zařízení, kdy bude všem ostatním zařízením přístup zamítnut. Druhou možností je zakázat určité MAC adresy. K síti se tak budou moci připojit všechny ostatní zařízení nesoucí rozdílnou adresu oproti zařízením uvedeným v seznamu routeru.

Největší nevýhodou tohoto zabezpečení je fakt, že je nutné každé nové zařízení přidat na seznam povolených zařízení. Toto řešení zabezpečení se nedoporučuje v případě, že má jít o jediné zabezpečení sítě. Toto zabezpečení je doporučeno kombinovat s některým druhem šifrování, jakým je například WPA nebo WPA2 [10], [11].

4.2 Skrytí SSID sítě

Zkratka SSID (Service Set Identifier) představuje název sítě, kterou musí zařízení znát pro přístup k síti. SSID je velmi slabý způsob zabezpečení bezdrátové sítě. Přístupový bod pravidelně vysílá rámec zvaný beacon, který obsahuje toto SSID pojmenování. Z tohoto důvodu není těžké toto zabezpečení prolomit a různými nástroji tento název potřebný k přístupu do sítě zjistit. Po zvolení SSID jména sítě je možné tuto síť skrýt. Síť následně nebude viditelná v seznamu dostupných WiFi sítí. Pokud se do této sítě někdo bude chtít připojit, musí znát přesné SSID jméno. U tohoto způsobu zabezpečení se taktéž důrazně doporučuje kombinovat jej s některým z dostupných šifrování, jakými jsou například WPA nebo WPA2 [10], [11].

4.3 802.1x a Radius Server

802.1x je používán pro autentizaci uživatelů, zajišťování integrity zpráv a distribuci klíčů. Jedná se o bezpečnostní rámec používaný ve veškerých LAN sítích. Cílem tohoto zabezpečení je bránit přístupu neoprávněným uživatelům do lokální sítě

Za pomoci funkce Network Login 802.11x lze ověřit uživatele pomocí uživatelského jména a hesla. Následně, po ověření uživatelských údajů, je uživateli povolen přístup do lokální sítě. Uživatelé mohou být prověřování takzvanými aktivními prvky (bezdrátový přístupový bod, nebo například přístupový server). Aktivní prvek komunikuje s centrální databází uživatelů jako její klient. Na základě informací převzatých z centrální databáze uživatelů následně povoluje nebo zamítá přístup do sítě. Tato centrální databáze držící informace o všech povolených uživatelích se nazývá RADIUS neboli Remote Authentification Dial In User. Radius lze provozovat jako službu integrovanou v Microsoft Active Directory.

Obr. 6 – Ověření pomocí funkce NetworkLogin 802.1x [15].

Proces ověřování uživatele probíhá následovně, zařízení se připojí k portu zabezpečenému pomocí 802.1x a dá mu najevo svoji existenci. To provede tak, že portu odešle libovolný paket. Přístupový bod obratem žádá připojující se zařízení o identifikaci, místo toho aby poslal přijatý DHCP požadavek dál. Zařízení se musí prokázat odesláním uživatelského jména a hesla zpět na přístupový bod. Přístupový bod obdržené informace zašifruje do paketu a paket odesílá na Radius server. Radius vyhodnotí přijaté informace a přepínači pošle zpět zamítnutí nebo potvrzení uživatele. Přepínač podle přijaté informace povolí, nebo zakáže uživateli přístup [15].

4.3.1 RADA

Radius Authenticated Device Access je rozšířením Network Login technologie. Toto rozšíření umožňuje přihlásit do sítě veškerá zařízení, jako jsou IP telefony, bezdrátové přístupové body, síťové tiskárny a terminály bez ohledu na klienta. Další funkcionalitou rozšíření RADA je možnost definovat dočasný přístup uživatelům do sítě. Toto připojení je řízené. Uživatelům může být přístup omezen například pouze pro internet. K ověření je používána fyzická adresa zařízení, která může být kombinována s ověřením pomocí uživatelského jména a hesla [15].

4.4 WEP

WEP, neboli Wired Equivalent Privacy, je nyní již zastaralým šifrovacím standardem pro bezdrátové sítě, který pochází z roku 1999. Tento bezpečnostní standard se podařilo relativně brzo prolomit (rok 2001) a z toho důvodu byl v roce 2003 nahrazen novějším a odolnějším standardem WPA. WEP používá pro šifrování přenášených dat sdílený klíč o délce 40b nebo 104b. Tento standard je stále podporován i na nových zařízeních. Při používání tohoto standardu často dochází k opakovanému použití stejného vektoru IV z důvodu krátké délky tohoto generovaného vektoru. Z tohoto důvodu se také výrazně doporučuje používat některý z novějších dostupných šifrovacích standardů (WPA, WPA2) [11].

4.5 WPA

WPA zabezpečení bylo vydáno v roce 2002 společností Wi-Fi Alliance. Jako základ k tvorbě tohoto zabezpečení posloužil základ 802.11i. Hlavní devizou této technologie je oproti WEP zabezpečení značně lepší šifrování dat. Další výhodou WPA technologie je možnost autentizace uživatelů. O to se starají různé autentizační služby (např. Radius). Ověřování probíhá vždy ještě před připojením uživatele do sítě. Na základě této autentizace může být uživateli přístup do sítě odepřen nebo povolen. Další výhodou této formy zabezpečení je možnost využít již používaných zařízení podporujících WEP. Na těchto zařízeních bylo pouze nutné aktualizovat software, aby podporoval WPA v plném rozsahu.

WPA k šifrování používá 128 bitový klíč a 48 bitový inicializační vektor. WPA používá stejnou šifru jako WEP, ale je schopný odolávat útokům, které by prolomily WEP. WPA nabízí také vylepšenou kontrolu integrity dat. Předchůdce WEP používal algoritmus

zvaný CRC-32, který je relativně jednoduchý a zašifrovaná data neobsahují kontrolní součet. Z tohoto důvodu jde poměrně jednoduše pozměnit zprávu a kontrolní součet bez znalosti WEP klíče. V případě WPA je používán algoritmus MIC (Message Integrity Code), který je součástí MAC. MIC obsahuje počítadlo rámců, které se využívá k ochraně před útoky, které se snaží zopakovat odposlouchanou komunikaci [7].

4.6 WPA2

WPA2 obsahuje všechny povinné prvky standardu 802.11i. Jmenovitě jsou to prvky TKIP, MIC a nově také algoritmus CCMP neboli Counter mode with Cipher block chaining Message authentication Code protokol. Tento standard zabezpečení je od roku 2006 povinný pro všechna nová zařízení označována jako Wi-Fi.

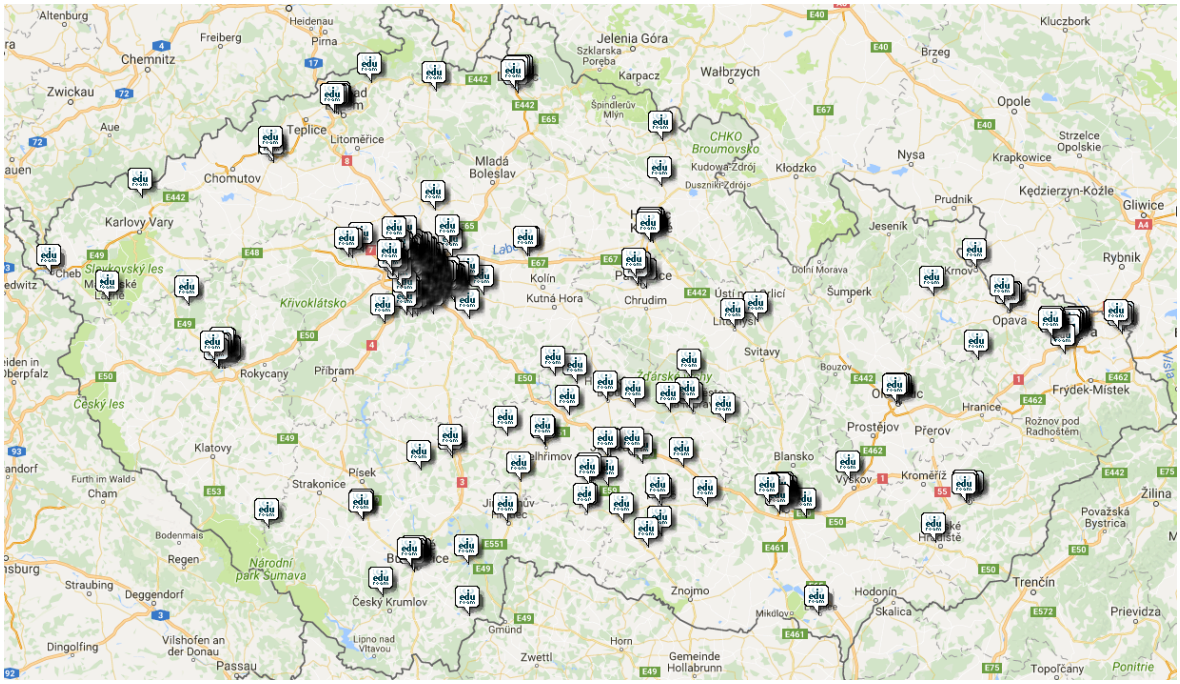
Mnoho zařízení podporuje kombinovaný mód, kdy přístupový bod WLAN sítě podporuje jak WPA tak i WPA na jediném WLAN rozhraní. Toto řešení dovoluje vytvořit více SSID, kdy je pro každé SSID použito jiné šifrování [7].

5 EDUROAM

Eduroam je mezinárodním projektem, který se snaží zajistit lepší podporu mobility a roamingu v sítích využívaných národními výzkumnými a vzdělávacími ústavy. O tento projekt se v České republice stará sdružení CESNET, které zajišťuje provoz těchto sítí. CESNET byl založen sdružením vysokých škol a Akademií věd České republiky.

Obr. 7 – Logo Eduroam [5].

Síť Eduroam se skládá z bezdrátových přístupových bodů, které komunikují s RADIUS serverem, čímž se zajišťuje autentizace uživatelů této sítě. Hlavní devizou využívání této sítě je snadné používání všech služeb dostupných v síti podobně, jako je tomu u roamingu mobilních sítí. Každý uživatel, který je zaregistrovaným členem sítě eduroam se může připojit k jakékoliv bezdrátové síti, která je součástí sítě eduroam. Všechny informace o uživatelích jsou udržovány v centrální RADIUS databázi [5].



Obr. 8 – Mapa pokrytí ČR Eduroam sítěmi [5].

Na obrázku (Obr. 8) výše je zobrazeno pokrytí ČR eduroam sítěmi. Česká republika ovšem není jediným působištěm sítí eduroam. Tento projekt má zastoupení napříč celou Evropou.

5.1 Roamingová politika

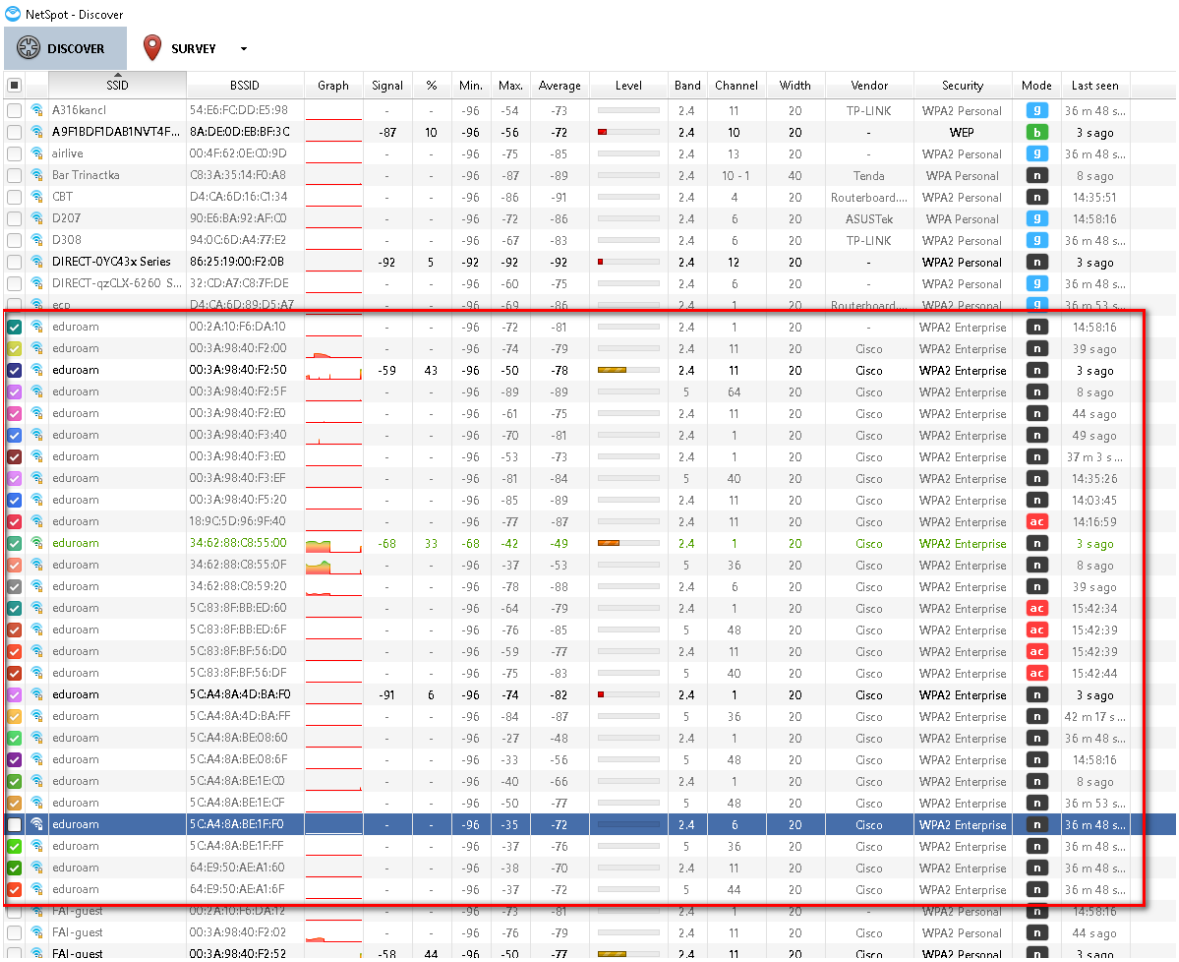
Největší devizou využívání roamingu je možnost přístupu k síti z více míst. Tento fakt dovoluje studentům a zaměstnancům univerzity přistupovat k bezdrátové síti eduroam v rámci celého komplexu eduroam pod stejným uživatelským jménem a heslem. Pokud se uživatel kdekoliv připojí do sítě eduroam, síť odešle žádost o autentizaci do jeho domovské sítě, kde je mu pomocí RADIUS serveru přístup povolen, nebo zakázán a toto rozhodnutí je posláno zpět do sítě, která se dotazuje.

Tento princip je postaven na dvou pilířích. Prvním z nich je uživatelské jméno, které má pevně danou podobu jmenouzivatele@realm.xx. Jméno uživatele je běžné uživatelské jméno, nejčastěji vytvořené spojením jména a příjmení uživatele v určitém formátu a realm představuje jméno organizace, do které uživatel patří. Poslední část uživatelského jména tvoří přípona, která je určena oblastí působení organizace, v případě České republiky je přípona .cz. Druhým pilířem je autentizační struktura, která zajišťuje přenášení informací o uživatelích.

6 POUŽITÝ SOFTWARE

6.1 NetSpot

NetSpot je program sloužící k mapování, posuzování a analyzování pokrytí a výkonu Wi-Fi sítí. Tento program je dostupný pro Mac OS a pro Windows. Plná verze programu nabízí možnost Wireless site survey, kterou lze využít pro zmapování a zakreslení síly signálu jednotlivých přístupových bodů v bezdrátové síti. Bezplatná verze nabízí pouze možnost zobrazení všech přístupových bodů v okolí. Tato funkce se jmenuje NetSpot Discover a kromě SSID přístupových bodů nám také zobrazuje BSSID, aktuální intenzitu signálu, pásmo, které přístupový bod využívá, typ zabezpečení a mnoho dalších užitečných informací.

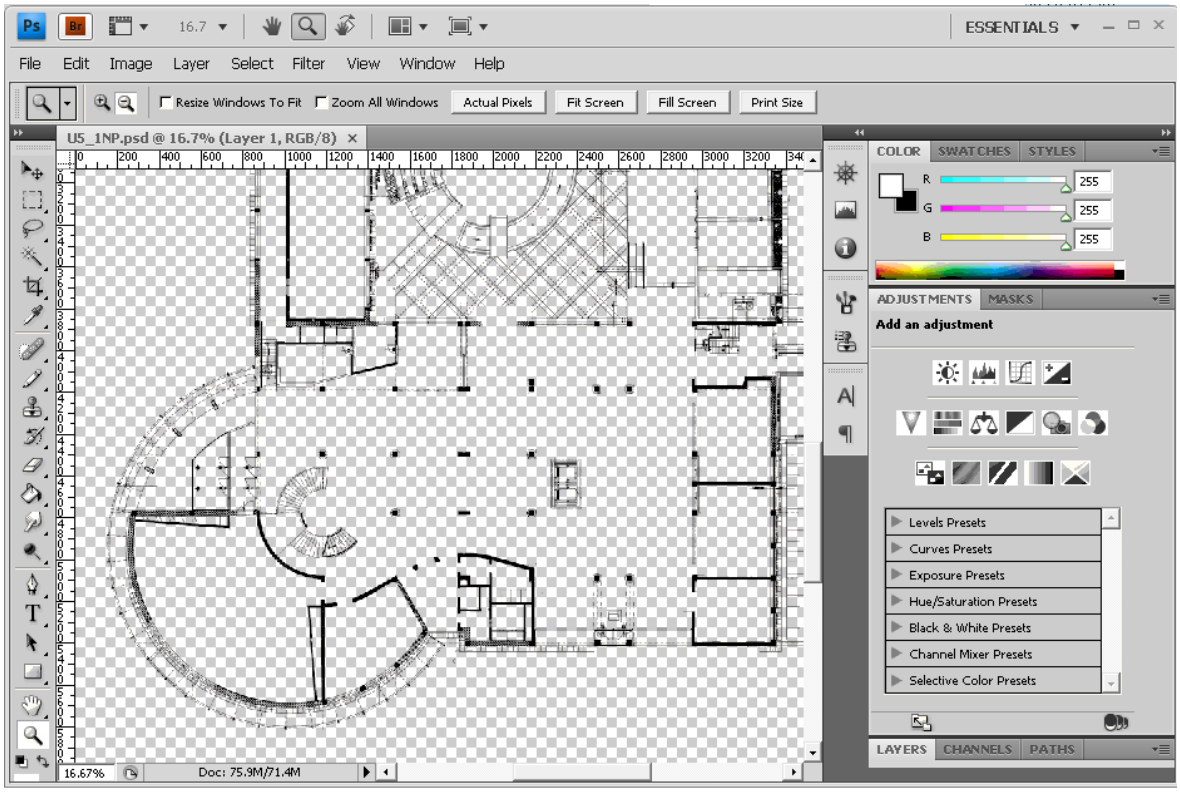


Obr. 9 – Rozhraní programu NetSpot.

6.2 Adobe Photoshop CS4

Adobe Photoshop je velmi oblíbeným bitmapovým editorem sloužícím pro úpravu fotografií. Tento nástroj podporuje širokou škálu formátů, mezi nimi také formát RAW. Photoshop uživateli nabízí bohatý výběr dostupných nástrojů sloužících pro úpravu obrazu.

Tento grafický nástroj podporuje také práci ve více vrstvách, což bylo hlavním faktorem při výběru vhodného grafického programu pro tuto práci.



Obr. 10 – Rozhraní programu Adobe Photoshop CS4.

6.3 Wifi Analyzer

Tato aplikace promění chytrý telefon v zařízení schopné analyzovat bezdrátové sítě. Kromě aktuálně využívaného přístupového bodu také aplikace zobrazuje všechny dostupné přístupové body. Aplikace zobrazuje veškeré informace o dostupných přístupových bodech (BSSID, SSID, pásmo, intenzita signálu, zabezpečení a mnohé další užitečné informace). Tato aplikace je dostupná zdarma na portálu Google play.

Obr. 11 – Rozhraní programu Wifi Analyzer.

II. PRAKTICKÁ ČÁST

7 ANALÝZA SOUČASNÉHO STAVU BEZDRÁTOVÉ SÍTĚ V AREÁLU U5

Pro snadnější orientaci byly univerzitou poskytnuté mapové podklady areálu zjednodušeny použitím grafického editoru programu Adobe photoshop. Z nákresu byly odstraněny veškeré prvky, které měly neblahý vliv na přehlednost nákresu.

Areál se skládá z 8 podlaží. První tři podlaží byla z důvodu rozlehlosti rozdělena na dvě části. Všechna podlaží (a jejich části) byla zvlášť zmapována a naměřená data byla pečlivě zaznamenána do nákresu. Analýza bezdrátové sítě byla provedena aplikací Wifi Analyzer pro android a programem NetSpot pro Windows 10. Na ilustracích je uvedena intenzita signálu v jednotkách dBm spolu s aktuálně využívaným přístupovým bodem v daném místě.

7.1 Zabezpečení bezdrátové sítě

Bezdrátová síť v areálu je součástí komplexu sítí eduroam. Každý uživatel této sítě musí být před povolením přístupu do sítě eduroam ověřen. K tomuto účelu síť eduroam využívá centrální databázi uživatelů zvanou RADIUS. Autentizace probíhá tak, že uživatelská stanice vyšle přístupovému bodu požadavek na připojení do sítě. Přístupový bod komunikuje s centrální databází RADIUS jako její klient. Na základě informací převzatých z centrální databáze uživatelů následně přístupový bod povoluje nebo zamítá přístup do sítě.

7.2 Výčet přístupových bodů

K měření signálu a mapování bezdrátové struktury sítě byl použit program NetSpot, za pomoci kterého bylo možné zobrazit všechny dostupné přístupové body v síti.

Tab. 1 – Seznam Eduroam přístupových bodů v budově U5.

BSSID	SSID	Pásmo	Standard	Výrobce
00:2A:10:F6:DA:10	Eduroam	2.4 GHz	n	Cisco
00:3A:98:40:F2:00	Eduroam	2.4 GHz	n	Cisco
00:3A:98:40:F2:50	Eduroam	2.4 GHz	n	Cisco

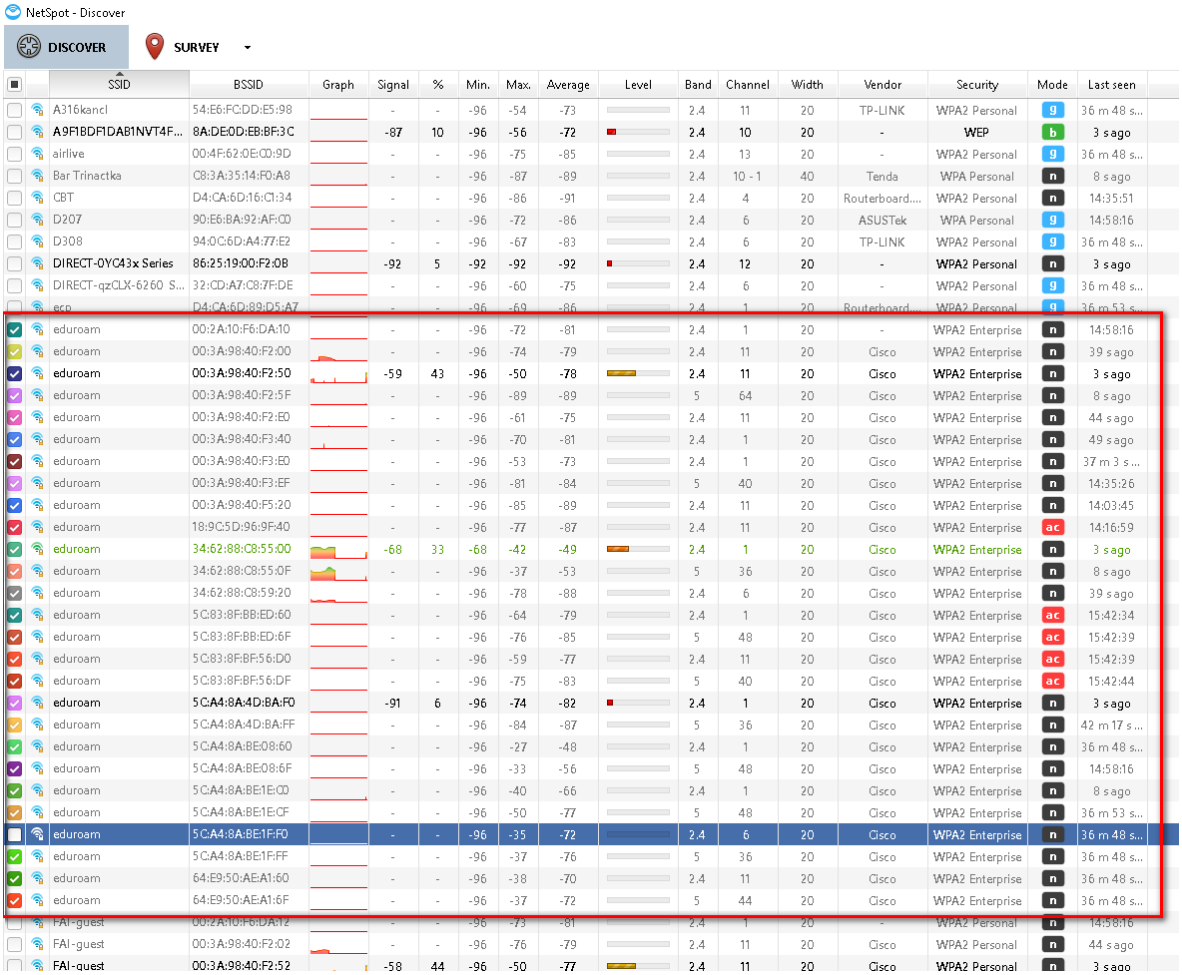
00:3A:98:40:F2:5F	Eduroam	5 GHz	n	Cisco
00:3A:98:40:F2:E0	Eduroam	2.4 GHz	n	Cisco
00:3A:98:40:F3:40	Eduroam	2.4 GHz	n	Cisco
00:3A:98:40:F3:E0	Eduroam	2.4 GHz	n	Cisco
00:3A:98:40:F3:EF	Eduroam	5 GHz	n	Cisco
00:3A:98:40:F5:20	Eduroam	2.4 GHz	n	Cisco
18:9C:5D:96:9F:40	Eduroam	2.4 GHz	ac	Cisco
34:62:88:C8:55:00	Eduroam	2.4 GHz	n	Cisco
34:62:88:C8:55:0F	Eduroam	5 GHz	n	Cisco
34:62:88:C8:59:20	Eduroam	2.4 GHz	n	Cisco
5C:83:8F:BB:ED:60	Eduroam	2.4 GHz	ac	Cisco
5C:83:8F:BB:ED:6F	Eduroam	5 GHz	ac	Cisco
5C:83:8F:BF:56:D0	Eduroam	2.4 GHz	ac	Cisco
5C:83:8F:BF:56:DF	Eduroam	5 GHz	ac	Cisco
5C:A4:8A:4D:BA:F0	Eduroam	2.4 GHz	n	Cisco
5C:A4:8A:4D:BA:FF	Eduroam	5 GHz	n	Cisco
5C:A4:8A:BE:08:60	Eduroam	2.4 GHz	n	Cisco
5C:A4:8A:BE:08:6F	Eduroam	5 GHz	n	Cisco
5C:A4:8A:BE:1E:C0	Eduroam	2.4 GHz	n	Cisco
5C:A4:8A:BE:1E:CF	Eduroam	5 GHz	n	Cisco
5C:A4:8A:BE:1F:F0	Eduroam	2.4 GHz	n	Cisco
5C:A4:8A:BE:1F:FF	Eduroam	5 GHz	n	Cisco
64:E9:50:AE:A1:60	Eduroam	2.4 GHz	n	Cisco
64:E9:50:AE:A1:6F	Eduroam	5 GHz	n	Cisco

7.3 Analýza a grafické vyhodnocení síly signálu v areálu

Nejpřesnějších naměřených hodnot bylo dosaženo při kombinování naměřených hodnot z programu Wifi Analyzer a programu NetSpot, kdy byl program Wifi analyzer použit ke zjištění aktuálně využívaného přístupového bodu v daném místě a program NetSpot ke zjištění dalších informací jako například MAC adresa přístupového bodu, SSID, pásmo, standard, výrobce a aktuální hodnotu signálu v dBm. Intenzita signálu je v grafickém vyhodnocení mimo číselných hodnot také znázorněna barvou a to z důvodu lepší orientace v nákresu.

Tab. 2 – Barevná škála intenzity signálu.

- 40 dBm	- 50 dBm	- 60 dBm	- 70 dBm	- 80 dBm	- 90 dBm

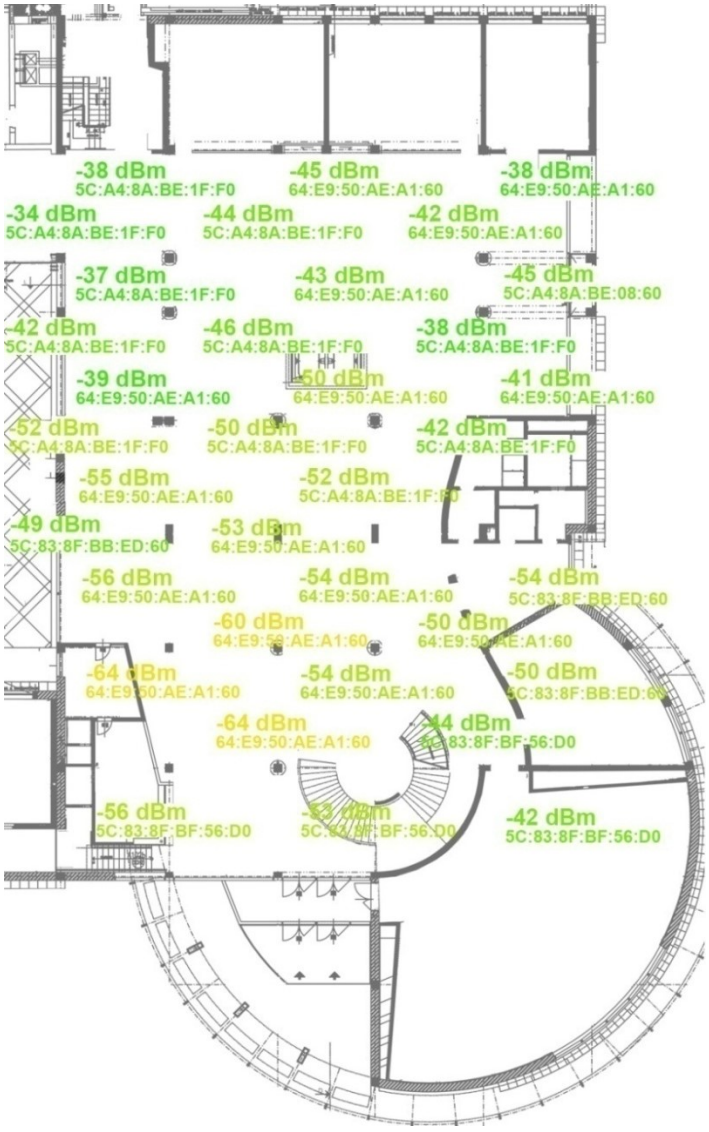


Obr. 12 – Seznam dostupných eduroam přístupových bodů v budově U5.

7.3.1 První podlaží

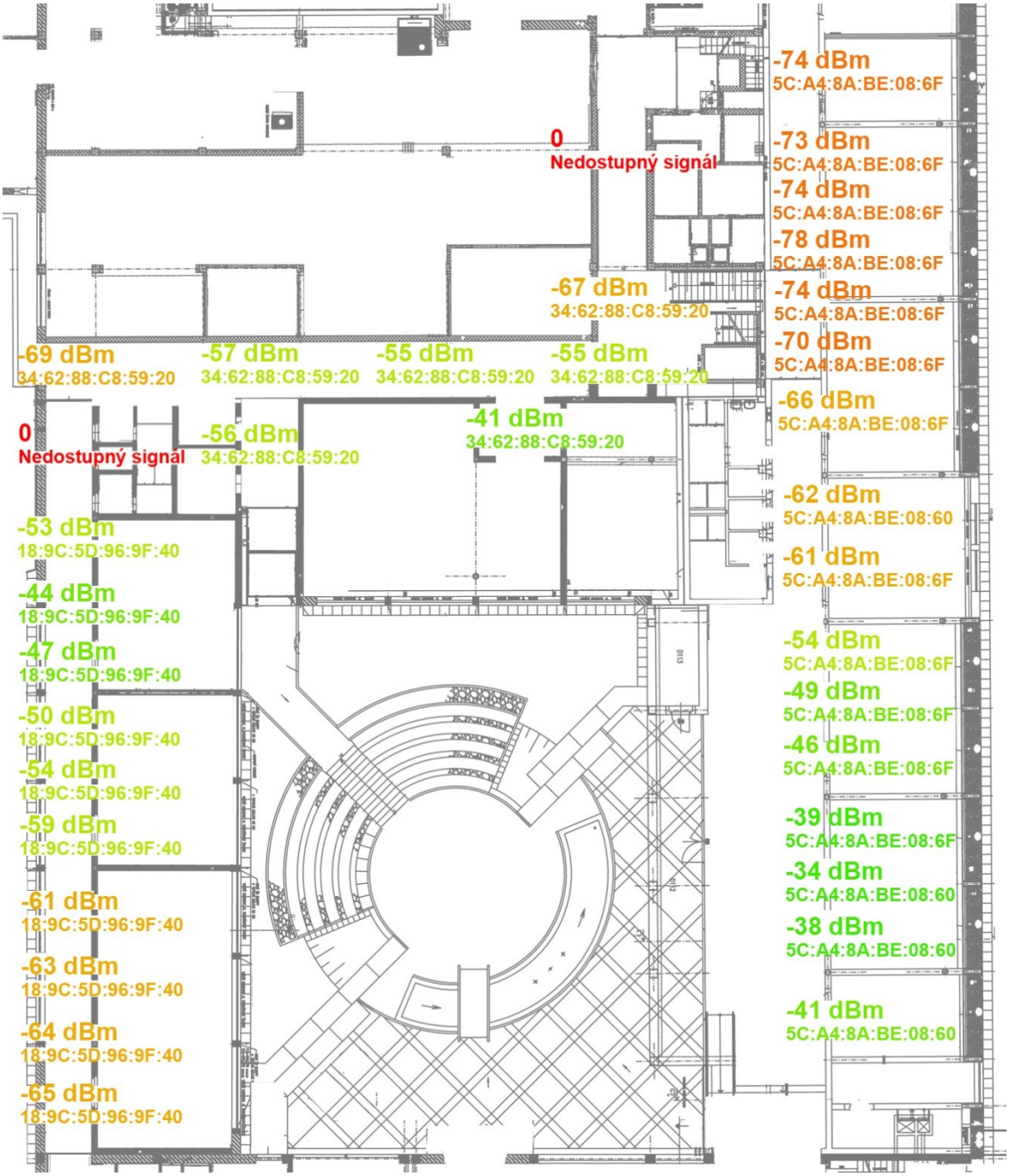
V případě budovy U5 se dá první podlaží považovat za nejdůležitější oblast z pohledu pokrytí bezdrátovou sítí. Jedná se o studenty nevyužívanější část budovy a z toho důvodu je zde kladen důraz na dostupnost kvalitního připojení k síti. V prvním podlaží se nachází vstup do budovy, posluchárna, mnoho učeben a rozlehlé společné prostory, které jsou studenty využívány ke studiu. Z důvodu rozlehlosti bylo první podlaží při grafickém znázornění síly signálu rozděleno do dvou částí. První část zachycuje stav sítě ve společných prostorách, v oblasti poslucháren, vchodu a čtyř přilehlých učeben. Druhá část následně zobrazuje zbylé prostory prvního podlaží, kde se nachází zejména učebny, respektive laboratoře.

První část



Obr. 13 – První podlaží budovy U5 – část první.

Druhá část

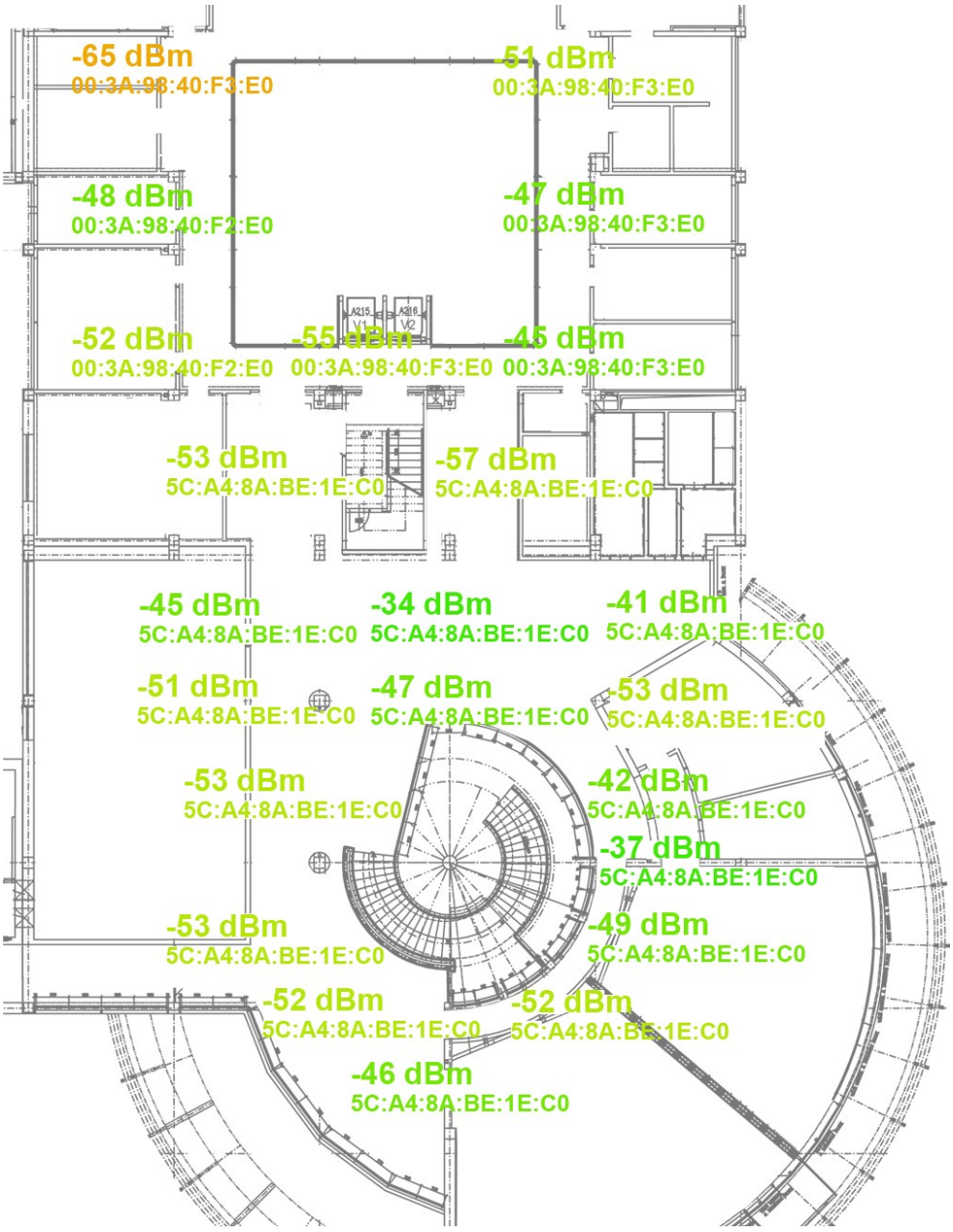


Obr. 14 – První podlaží budovy U5 – část druhá.

7.3.2 Druhé podlaží

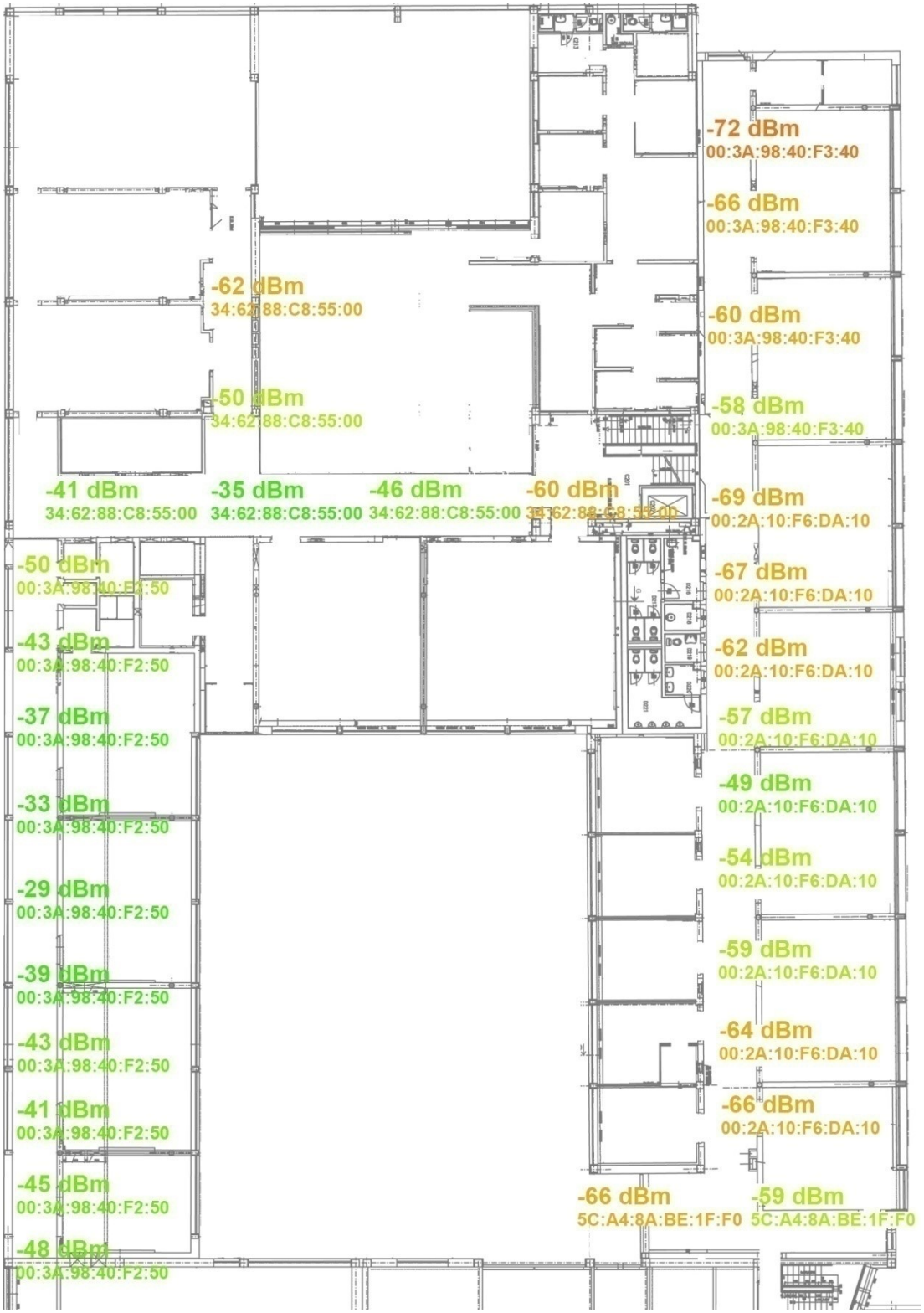
Druhé podlaží již není využíváno studenty v takové míře, jako tomu bylo u podlaží prvního, stále se však v tomto podlaží nachází mnoho tříd společně se dvěmi posluchárnami. Důležitým prvkem druhého podlaží je také studovna, což je místo velmi frekventovaně využívané studenty. Druhé podlaží je při grafickém znázornění taktéž rozděleno do dvou částí. První část zachycuje studovnu, společné prostory, studovny a kanceláře. V druhé části se nachází učebny, laboratoře a školní menza.

První část



Obr. 15 – Druhé podlaží budovy U5 – část první.

Druhá část

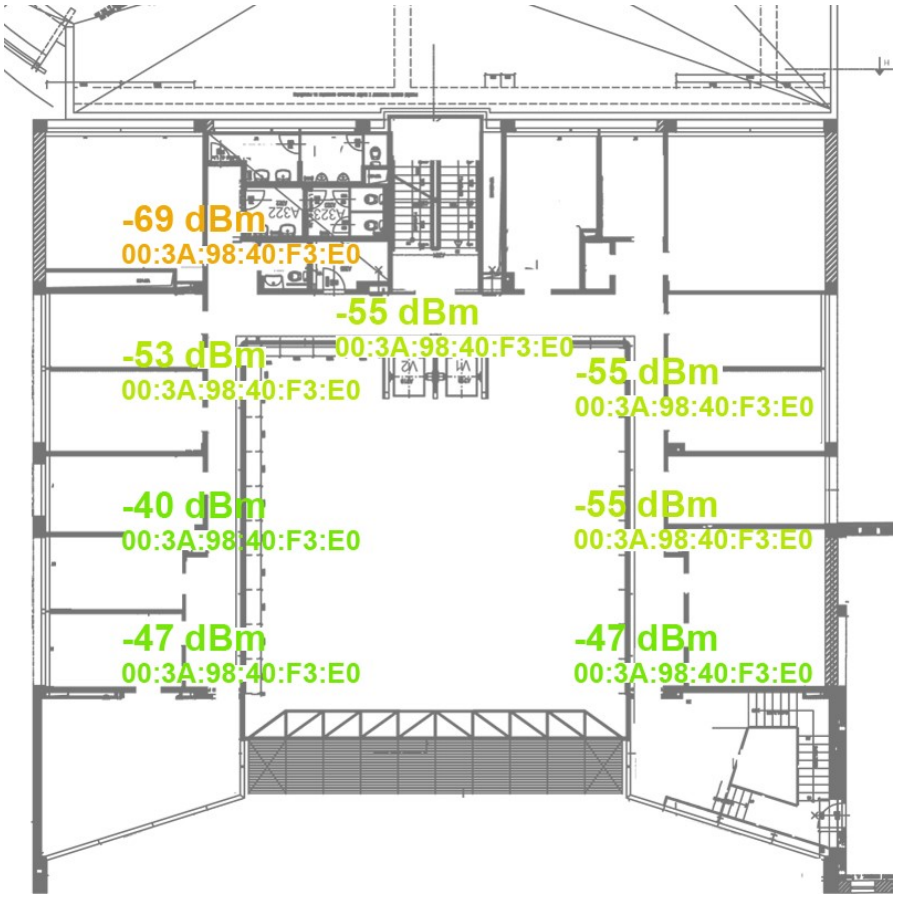


Obr. 16 – Druhé podlaží budovy U5 – část druhá.

7.3.3 Třetí podlaží

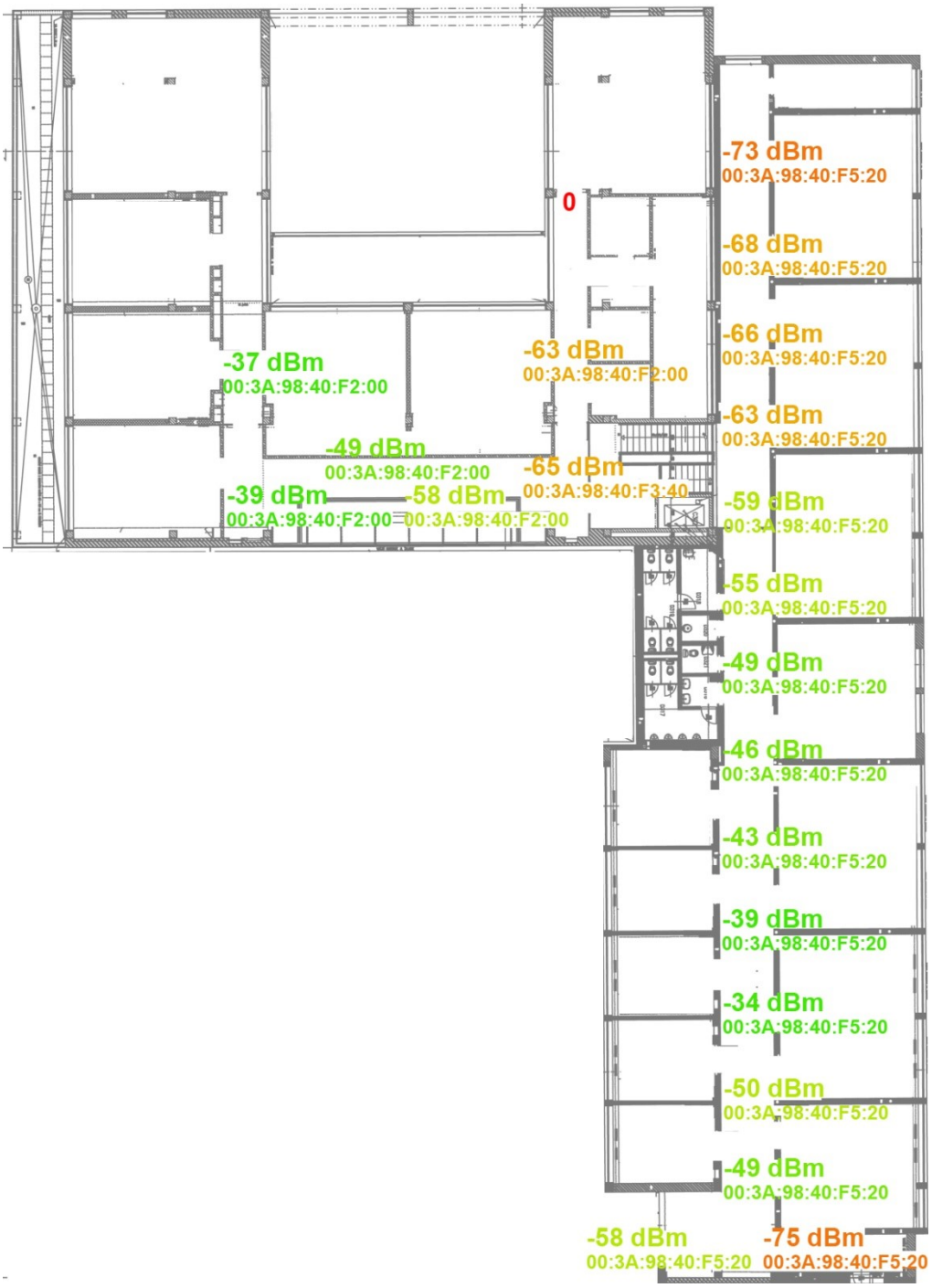
Na třetím podlaží se již nachází o poznání méně učeben a laboratoří. První část třetího podlaží zobrazuje stav bezdrátové sítě v oblasti kanceláří. Druhá část dále zobrazuje stav bezdrátové sítě v prostorách učeben a laboratoří. Na tomto podlaží je výskyt studentů minimální.

První část



Obr. 17 – Třetí podlaží budovy U5 – část první.

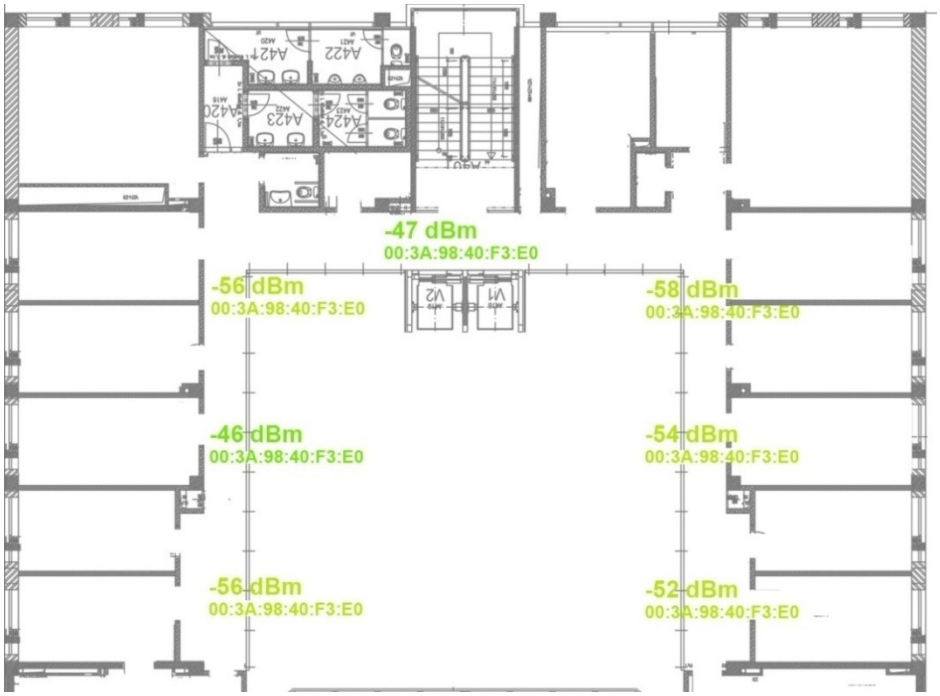
Druhá část



Obr. 18 – Třetí podlaží budovy U5 – část druhá.

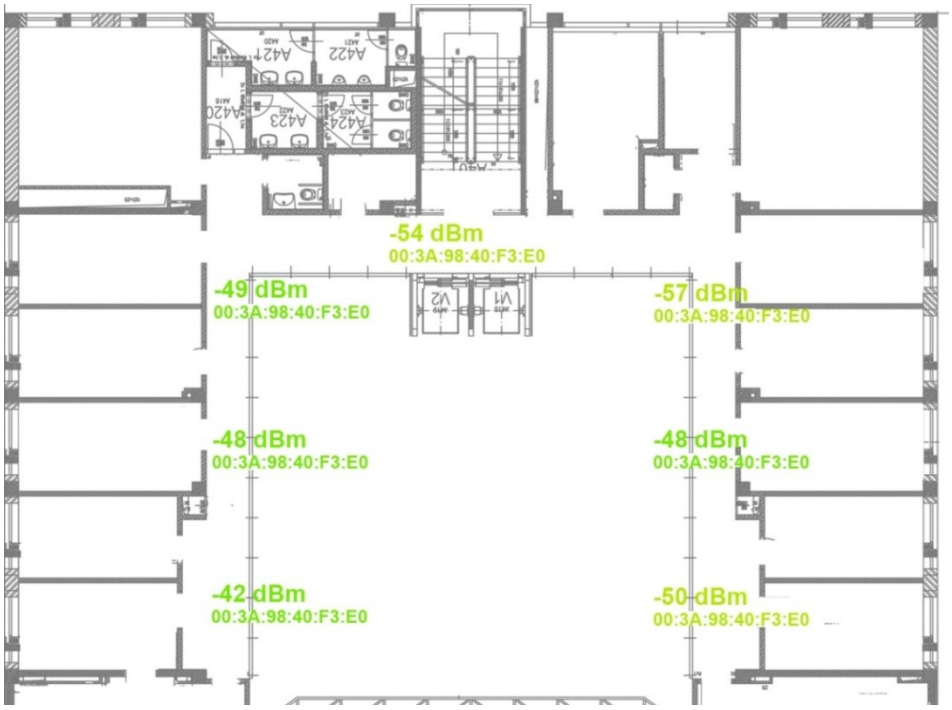
7.3.4 Čtvrté podlaží

Na čtvrtém až osmém podlaží se nachází pouze kanceláře a pokrytí je zde zcela dostačující.



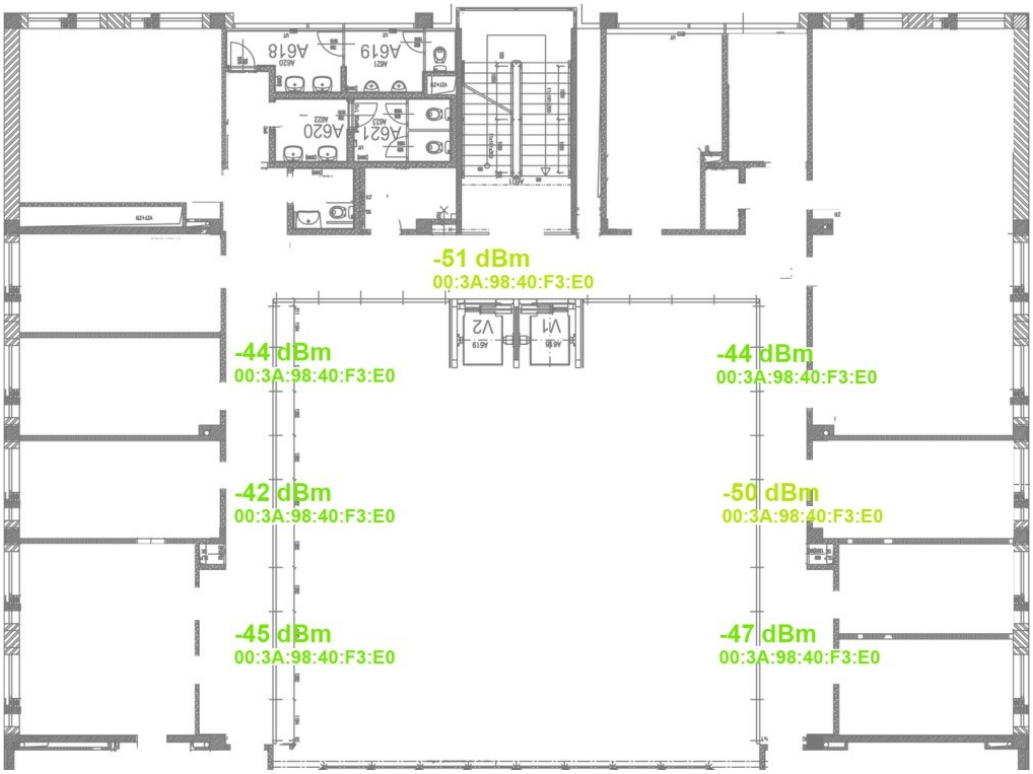
Obr. 19 – Čtvrté podlaží budovy U5.

7.3.5 Páté podlaží



Obr. 20 – Páté podlaží budovy U5.

7.3.6 Šesté podlaží

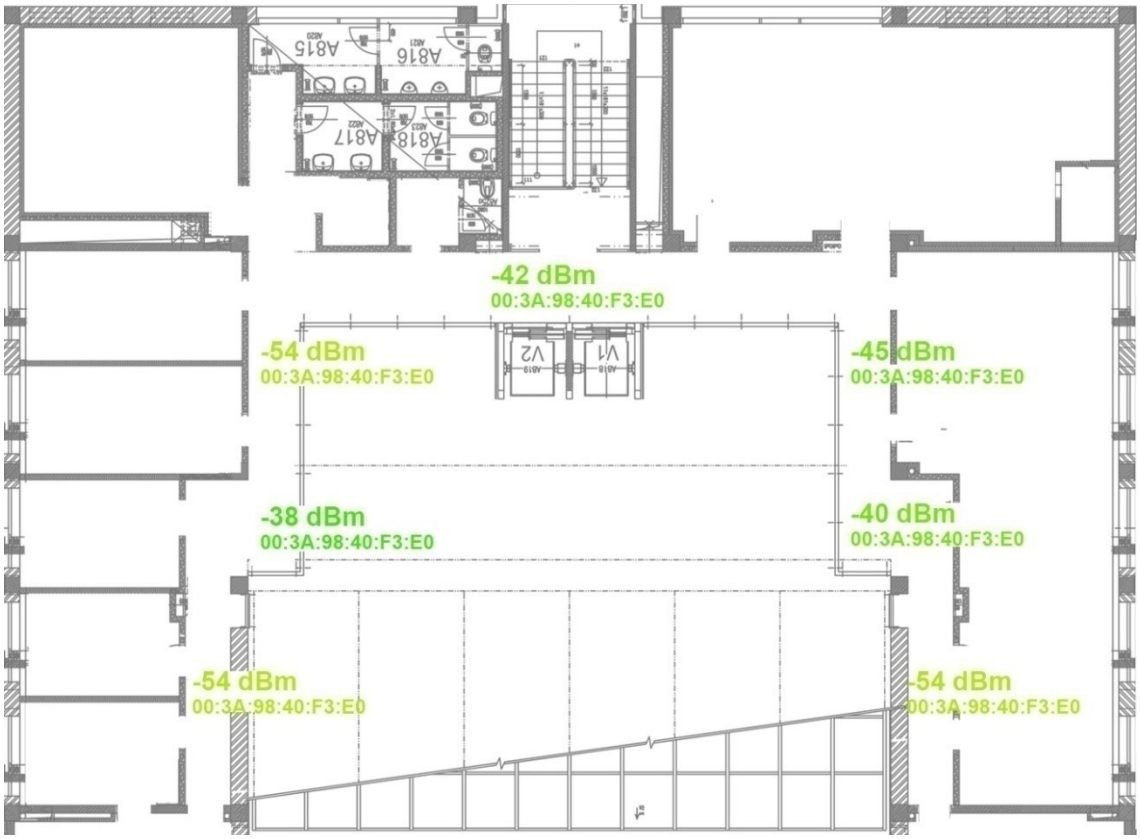


Obr. 21 – Šesté podlaží budovy U5.

7.3.7 Sedmé podlaží

Obr. 22 – Sedmé podlaží budovy U5.

7.3.8 Osmé podlaží



Obr. 23 – Osmé podlaží budovy U5.

8 NÁVRH ŘEŠENÍ INOVACE BEZDRÁTOVÉ SÍTĚ V AREÁLU

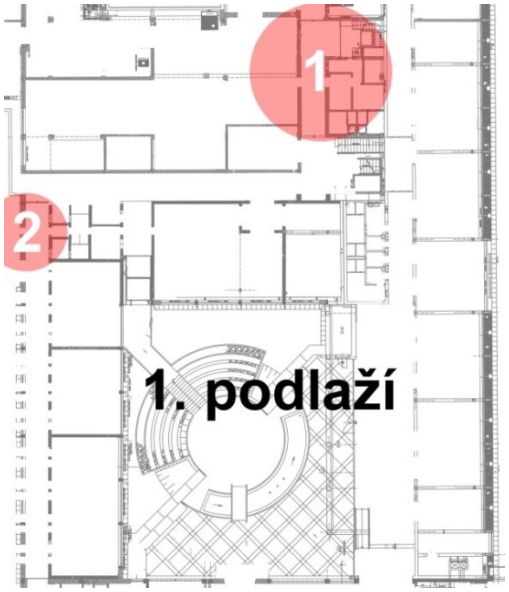
Na základě předchozí analýzy bezdrátové sítě v budově U5 vyšlo najevo několik slepých míst, ve kterých není bezdrátová síť dostupná, nebo síť trpí nestabilitou z důvodu nízkého dosahu signálu.

V prvním a ve třetím podlaží se ve společných prostorách nachází tři oblasti, kde je připojení k síti zcela nedostupné. Na základě měření bylo také zjištěno, že v prostorách poslucháren (první a druhé podlaží) a sousedních učeben je pokrytí nedostačující. Tyto prostory trpí častými výpadky sítě, slabým signálem a na některých místech je připojení do bezdrátové sítě zcela nedostupné.

Z důvodů frekventovaného využívání zmíněných prostor studenty by bylo vhodné bezdrátovou síť rozšířit o dva přístupové body. Tím by bylo zajištěno kvalitní pokrytí bezdrátové sítě v posluchárnách a přilehlých učebnách.

8.1 Oblasti bez připojení

V celém areálu se nachází pouze několik oblastí (volně dostupných míst) bez přístupu k bezdrátové síti eduroam. Při analýze sítě byla objevena tato tzv. hluchá místa na prvním a třetím podlaží. Tyto oblasti jsou vyobrazeny na obrázcích (Obr. 24, Obr. 25). Tyto oblasti byly z návrhu na vylepšení stávající bezdrátové sítě vynechány, jelikož se nejedná o nijak studenty využívané oblasti, ani o místa kde by bylo bezdrátové připojení nutně vyžadováno.



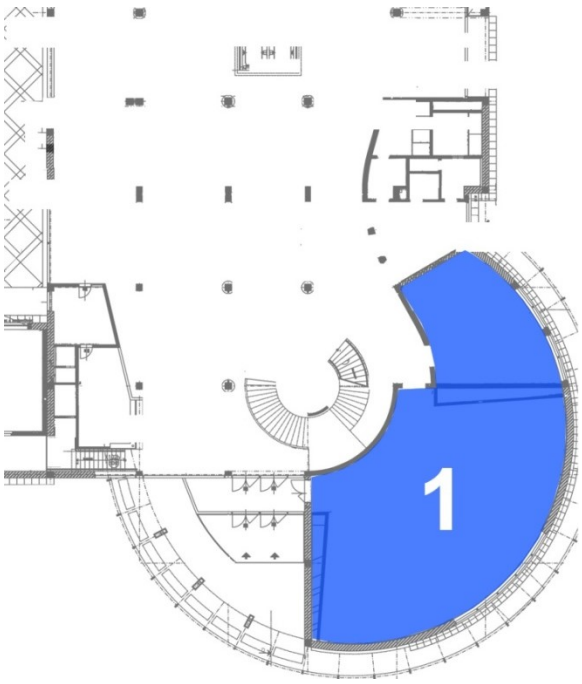
Obr. 24 – První podlaží – nedostupná bezdrátová síť.

Obr. 25 – Třetí podlaží – nedostupná bezdrátová síť.

8.2 Rozmístění přístupových bodů

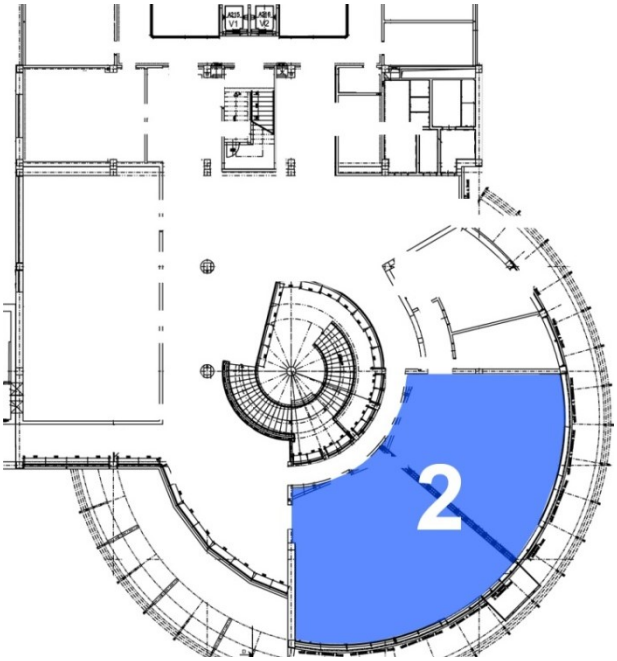
Návrh rozšíření stávající bezdrátové sítě přidáním dalších přístupových bodů pro posluchárny je zobrazen na následujících obrázcích (obr. 26 a obr. 27).

8.2.1 První podlaží



Obr. 26 – První podlaží – umístění AP.

8.2.2 Druhé podlaží



Obr. 27 – Druhé podlaží – umístění AP.

8.3 Návrh zabezpečení sítě

Autentizace uživatelů pomocí centrální databáze RADIUS je takřka ideálním řešením zabezpečení sítě tohoto formátu. Tento systém autentizace nabízí řadu výhod oproti běžným zabezpečovacím protokolům, jakými jsou například WPA, nebo WPA2.

Eduroam ve spojení s autentizací uživatelů pomocí centrální databáze nabízí uživatelům značnější volnost pohybu a možnost připojit se kdekoliv do této bezdrátové sítě přes dostupné přístupové body eduroam při zadání svého uživatelského jména a hesla, které si každý uživatel volí sám. Každý uživatel by si měl svědomitě zvolit přístupové heslo podle daných bezpečnostních standardů.

8.3.1 Odolné heslo

Volba odolného hesla je základním prvkem bezpečnosti sítě. Každý uživatel by měl své heslo udržovat v tajnosti a nikomu jej nesdělovat. Hesla obsahující pouze text nebo naopak pouze čísla se považují za velmi slabá a snadno prolomitelná slovníkovým útokem. Při výběru svého hesla je třeba dbát na následující pravidlo.

Heslo uživatele by se mělo skládat z velkých a malých znaků, číslic a podporovaných speciálních znaků.

8.3.2 Pravidelná změna hesla

Uživatel by si měl své heslo pravidelně měnit. Toto pravidlo by mohlo být zavedeno v rámci zabezpečení sítě jako povinnost, kdy by si studenti museli každý měsíc, nebo čtvrtletí změnit heslo. Nabízí se také možnost hesla uživatelům generovat automaticky v pravidelných intervalech a zasílat je zašifrovaná na univerzitní emaily.

8.4 Kalkulace finančních nákladů na inovaci sítě

Stávající bezdrátová síť v areálu U5 sestává z přístupových bodů od výrobce Cisco. Z tohoto důvodu byl výběr dvou nových vhodných přístupových bodů pro inovaci bezdrátové sítě zúžen pouze na Cisco zařízení.

Pro inovaci sítě bylo vybráno zařízení z řady Cisco Aironet 2800, které je určeno pro použití ve středních až velkých sítích. Jedná se o dvoupásmový (2,4 GHz a 5 GHz) přístupový bod s rychlostí přenosu dat až 2,6 Gb/s a podporou standardů 802.11a, 802.11g,

802.11n včetně nejnovějšího standardu 802.11ac. Zařízení také poskytuje 4x4 MU-MIMO a sílu anténního signálu 5 dBi. Pořizovací cena jednoho zařízení činí 16 000 Kč. [3]

Kalkulace nákladů na inovaci sítě je sestavena z pouze orientačních cen zvolených zařízení, materiálu a montáže.

Obr. 28 – Cisco Aironet 2802 [3].

K inovaci bezdrátové sítě budou potřeba dvě, tato výše zmíněná zařízení, což dohromady činí odhadovaných 32 000 Kč za pořízení nových přístupových bodů. Přibližná cena za další potřebný materiál a montáž byla stanovena na 9 000 Kč. Celkové náklady na inovaci činí 41 000 Kč.

Tab. 3 – Kalkulace finančních nákladů na inovaci sítě.

Položka	Odhadovaná cena (Kč)
Cisco Aironet 2802	16 000
Cisco Aironet 2802	16 000
Materiál	5 000
Montáž	4 000
Celkové náklady	**41 000**

ZÁVĚR

Tato práce analyzovala bezdrátovou síť v areálu U5 Univerzity Tomáše Bati. Část práce stručně nastínila historii bezdrátové komunikace a následně popsala vznik a další vývoj bezdrátových sítí společně s detailním představením aktuálně dostupných standardů.

Dále byly představeny různé technologie zabezpečení bezdrátových sítí spolu s podrobným vysvětlením eduroam sítě, která je využívána Univerzitou Tomáše Bati. V další části práce byl uveden výčet programů použitých ke zpracování této práce.

Hlavním cílem práce bylo důkladné zmapování bezdrátové sítě v areálu U5. Pro tento účel byly upraveny mapové podklady areálu. Za účelem získání co nejpřesnějších hodnot bylo provedeno důkladné měření intenzity signálu bezdrátové sítě ve všech podlažích areálu Fakulty aplikované informatiky. Následně byly všechny naměřené hodnoty pečlivě zakresleny na mapy jednotlivých podlaží budov.

Na základě získaných informací byl následně vypracován přehled oblastí s omezeným přístupem, nebo žádným přístupem k bezdrátové síti. V následující kapitole byl vypracován návrh inovace stávající bezdrátové sítě. Dále byla provedena analýza stávajícího zabezpečení sítě spolu s představením drobných inovací tohoto zabezpečení.

Posledním bodem práce byla přibližná kalkulace finančních nákladů na navrhovanou inovaci bezdrátové sítě v areálu U5.

SEZNAM POUŽITÉ LITERATURY

[1] An A to Z review of the 802.11 standards. L-com.com [online]. Florida: l-com, 2016 [cit. 2017-05-21]. Dostupné z: http://www.l-com.com/content/Article.aspx?Type=N&ID=10638.

[2] CARROLL, Brandon. Bezdrátové sítě Cisco: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2011, 478 s. ISBN 978-80-251-2884-8.

[3] Cisco Aironet 2800 Series Access Points: Access Points. Eduroam.cz [online]. Praha: Cisco Systems, 2017 [cit. 2017-05-21]. Dostupné z: http://www.cisco.com/c/en/us/products/wireless/aironet-2800-series-access-points/index.html.

[4] DULÍK, Tomáš. Methods for interference mitigation in wireless networks. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-233-6.

[5] Eduroam.cz: Pokrytí. *Eduroam.cz* [online]. CESNET z. s. p. o., 2017 [cit. 2017-05-21]. Dostupné z: https://www.eduroam.cz/.

[6] GARG, Vijay Kumar. Wireless communications and networking. San Francisco, Calif.: Morgan Kaufmann, 2007, 821 s. ISBN 978-0-12-373580-5.

[7] HOLT, Alan a Chi-Yu HUANG. 802.11 wireless networks: security and analysis. London: Springer, 2010, 212 p. ISBN 978-1-84996-275-9.

[8] History of wireless. Wirelesscommunication.nl [online]. Jean-Paul M.G. Linnartz, 2000 [cit. 2017-05-21]. Dostupné z: http://www.wirelesscommunication.nl/reference/chaptr07/history.htm.

[9] History of Wireless Communications. Microwavejournal.com [online]. Norwood: Microwave Journal, 2015 [cit. 2017-05-21]. Dostupné z: http://www.microwavejournal.com/articles/24759.

[10] Jak zabezpečit WiFi síť. *Dsl.cz* [online]. Beroun: ADSL, 2016 [cit. 2017-05-21]. Dostupné z: http://www.dsl.cz/jak-na-to/jak-zabezpecit-wifi.

[11] KLEMENT, Milan. *Bezdrátové sítě ve vzdělávání*. Olomouc: Univerzita Palackého v Olomouci, 2011. ISBN 978-80-244-2789-8.

[12] San Diego State IEEE Chapter. Ieee.sdsu.edu [online]. San Diego: San Diego State University, 2017 [cit. 2017-05-21]. Dostupné z: http://ieee.sdsu.edu/about/.

[13] Technologie pro mobilní komunikaci: IEEE 802.11. Tomas.richtr.cz [online]. Praha: ČVUT, 2002 [cit. 2017-05-21]. Dostupné z: http://tomas.richtr.cz/mobil/wlan.htm.

[14] Wifi router – Co je standard 802.11ac?: IEEE 802.11. Unet.cz [online]. Polička: COMA, 2016 [cit. 2017-05-21]. Dostupné z: https://www.unet.cz/blog/2016/02/28/wifi-router-co-je-standard-802-11ac/.

[15] Zabezpečení sítě proti neoprávněnému přístupu pomocí funkce NetworkLogin 802.1x: NetworkLogin 802.1x. Svetsiti.cz [online]. Luboš Klaška, 2007 [cit. 2017-05-21]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Zabezpeceni-site-proti-neopravnenemu-pristupu-pomoci-funkce-NetworkLogin-8021x-14112007.

[16] Základní přehled standardů IEEE 802.11. Eprin.cz [online]. Brno: EPRIN spol. s r.o., 2012 [cit. 2017-05-21]. Dostupné z: https://www.eprin.cz/zakladni-prehled.html.

[17] ZURAWSKI, Richard. Industrial communication technology handbook. Second edition. Boca Raton: CRC Press, 2014, 1756 p. ISBN 978-1-4822-0732-3.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BSS	Basic Service Set
CESNET	Czech Education and Scientific NETwork
CCMP	Counter mode with Cipher block chaining Message authentication Code protokol
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
ESS	Extended Service Set
IEEE	Institute of Electrical and Electronics Engineers.
IBSS	International Bibliography of the Social Sciences
GSM	Globální Systém pro Mobilní komunikaci.
LAN	Local-Area Network.
MAC	Medium Access Control.
MIC	Message Integrity Code.
MIMO	Multiple-input multiple-output.
OFDM	Orthogonal Frequency Division Multiplexing.
OSI	Open Systems Interconnection.
RF	Frekvenční pásmo.
RADA	Radius Authenticated Device Access.
RADIUS	Remote Authentication Dial In User Service.
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
WLAN	Wireless Local-Area Network.
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha č. 1 – Půdorys areálu – přiložené CD, \Půdorys areálu\UP5_PODLAŽÍ.NP.pdf.
Příloha č. 2 – Použité programy – přiložené CD, adresář \Programy.