

# Návrh bezdrátové sítě v budově základní školy Kunovice

Vojtěch Vagunda

---

Bakalářská práce  
2018



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2017/2018

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Vojtěch Vagunda**  
Osobní číslo: **A15078**  
Studijní program: **B3902 Inženýrská informatika**  
Studijní obor: **Informační a řídicí technologie**  
Forma studia: **prezenční**

Téma práce: **Návrh bezdrátové sítě v budově základní školy Kunovice**  
Téma anglicky: **Designing a Wireless Network in the Kunovice Primary School Building**

Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma.
2. Popište technologie, standardy a bezpečnost bezdrátových sítí.
3. Proměřte šíření signálu v budově základní školy.
4. Na základě měření a simulace vytvořte signálovou mapu.
5. Navrhněte do plánu budovy základní školy rozmístění AP a pokrytí jejich signálem.
6. Zvolte vhodný typ centrálního ověřování uživatelů bezdrátové sítě.
7. Navrhněte přístupová práva pro různé skupiny uživatelů.
8. Popište nastavení jednotlivých prvků bezdrátové sítě.
9. Realizujte bezdrátový systém v závislosti na rozpočtu školy v roce 2018.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SOSINSKY, Barrie A.** Mistrovství – počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.
2. **KUROSE, James F. a Keith W. ROSS.** Počítačové sítě. Vyd. 1. Brno: Computer Press, 2014, 622 s. ISBN 978-80-251-3825-0
3. **CARROLL, Brandon.** Bezdrátové sítě Cisco: autorizovaný výukový průvodce. Brno: Computer Press, 2011, 478 s. Samostudium. ISBN 978-80-251-2884-8
4. **MATOUŠEK, Petr.** Síťové aplikace a jejich architektura. Vyd. 1. Brno: VUTIUM, 2014, 396 s. ISBN 978-80-214-3766-1
5. **TANENBAUM, Andrew S. a D. WETHERALL.** Computer networks. Fifth edition. New Delhi: Dorling Kindersley, 2014, 804 s. ISBN 978-93-325-1874-2

Vedoucí bakalářské práce:

**Ing. Miroslav Matýsek, Ph.D.**

Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce:

**15. prosince 2017**

Termín odevzdání bakalářské práce:

**25. května 2018**

Ve Zlíně dne 15. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.  
*děkan*



prof. Ing. Vladimír Vašek, CSc.  
*ředitel ústavu*

## **ABSTRAKT**

Tato práce se zabývá vybudováním centrálně řízené bezdrátové sítě s použitím síťových prvků od firmy ZyXEL. Teoretická část je věnována obecnému začlenění wi-fi vysílání do celkového elektromagnetického spektra, různým způsobům propojení zařízení v bezdrátové síti, popsání bezdrátových standardů, přehledu základních typů antén a jejich vyzařovacích charakteristik, standardům PoE, teorií pro pochopení fungování virtuálních počítačových sítí. V závěru je věnována přehledu některých rozsáhlejších vlastností nastavovaných na síťových prvcích v praktické části.

Praktická část popisuje konkrétní kroky spojené s výstavbou nové centrálně řízené bezdrátové sítě. Nejprve analýzou současného stavu bezdrátové sítě, poté definováním požadavků zákazníka na nový systém. Následně se zabývá sestavením podkladů pro vytvoření matematického modelu signálových map. Dále pak řeší proměření matematického modelu a volbou vhodných síťových prvků. Poslední část je věnována podrobnému popisu konfigurace jednotlivých síťových zařízení spolu s četným množstvím doplňujících obrázků.

Klíčová slova: wi-fi, LAN, IEEE 802.11, WLAN, ZyXEL

## **ABSTRACT**

This work deals with building of centrally controlled wireless networks using network devices from ZyXEL company. The theoretical part is dedicated to general integration of wi-fi broadcasts into the overall electromagnetic spectrum, different ways of wireless devices connections, description of wireless standards, overview of basic types of antennas and their radiation patterns, standards of PoE, theories for understanding the functioning of virtual computer networks. The end is dedicated to an overview of some of the more extensive features set up on network elements in the practical part.

The practical part describes the specific actions connected with the construction of a new centrally managed wireless network. First by analyzing the current state of wireless network, then by specifying customers requests for the new system. Subsequently the work deals with compilation of data for the creation of a mathematical model of signal maps. Next solve measuring the mathematical model and choosing suitable network elements.

The last part is devoted to a detailed description of the configuration of each network device along with a numerous amount of additional images.

Keywords: wi-fi, LAN, IEEE 802.11, WLAN, ZyXEL

Chtěl bych poděkovat vedoucímu mé bakalářské práce Ing. Miroslavu Matýskovy, Ph.D., za odborné vedení, poskytnuté rady, trpělivost, ochotu a čas, který mi v průběhu zpracování bakalářské práce věnoval.

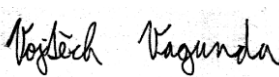
### **Prohlašuji, že**

- beru na vědomí, že odevzdáním 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 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 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

### **Prohlašuji,**

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

Ve Zlíně, dne 3. 5. 2018

  
.....  
podpis diplomanta

# OBSAH

<b>ÚVOD</b> .....	<b>10</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>11</b>
<b>1 SPECIFIKACE 802.11</b> .....	<b>12</b>
1.1 REŽIM AD HOC .....	13
1.2 REŽIM INFRASTRUKTURY .....	13
1.2.1 Distribuční systém.....	13
1.2.2 Roaming .....	14
<b>2 BEZLICENČNÍ FREKVENČNÍ PÁSMA 2,4 GHZ A 5 GHZ</b> .....	<b>15</b>
2.1 PÁSMO 2,4 GHZ .....	15
2.2 PÁSMO 5 GHZ .....	16
2.3 STANDARDY 802.11 .....	16
2.3.1 802.11b.....	16
2.3.2 802.11 a.....	16
2.3.3 802.11g.....	16
2.3.4 802.11n.....	17
2.3.5 802.11ac .....	17
2.4 FYZICKÉ VERSUS REÁLNÉ RYCHLOSTI .....	18
<b>3 ANTÉNY</b> .....	<b>20</b>
3.1 ZISK .....	20
3.2 TYPY ANTÉN A VYZAŘOVACÍ CHARAKTERISTIKY .....	20
3.2.1 Všesměrové antény .....	20
3.2.2 Směrové antény .....	21
<b>4 POE</b> .....	<b>25</b>
4.1 STANDARDY POE.....	25
4.1.1 IEEE 802.3af.....	25
4.1.2 IEEE 802.3at .....	25
4.2 KOMPATIBILITA A APLIKACE .....	26
<b>5 VLAN</b> .....	<b>27</b>
5.1 ZPŮSOBY DEFINICE ČLENSTVÍ VE VLAN.....	28
5.1.1 Statická metoda .....	28
5.1.2 Dynamická metoda.....	29
5.2 TYPY VLAN PŘIPOJENÍ NA PŘEPÍNAČI .....	29
5.2.1 Access link .....	29
5.2.2 Trunk link.....	29
5.3 TAGOVÁNÍ RÁMCŮ .....	29
<b>6 POUŽITÉ TECHNOLOGIE PŘI REALIZACI BEZDRÁTOVÉ SÍTĚ SE ZAŘÍZENÍMI OD FIRMY ZYXEL</b> .....	<b>31</b>
6.1 MOŽNOSTI QoS.....	31
6.2 SMART CLIENT STEERING .....	31
6.2.1 Band Select.....	32
6.2.2 Band Select - Stop Treshold.....	32
6.2.3 Band Select - Balance Ratio.....	32



6.2.4	RSSI (Received Signal Strength Indicator) Threshold .....	32
6.3	TECHNOLOGIE DFS (DYNAMIC FREQUENCY SELECTION) .....	33
6.4	OPERATING MODE .....	33
6.5	LOAD BALANCING SETTING .....	33
<b>II</b>	<b>PRAKTICKÁ ČÁST .....</b>	<b>35</b>
<b>7</b>	<b>PŘÍPRAVA PODKLADŮ .....</b>	<b>36</b>
7.1	STAV BEZDRÁTOVÉ SÍTĚ PŘED REALIZACÍ .....	36
7.2	DEFINICE POŽADAVKŮ VEDENÍ ŠKOLY .....	36
7.3	PROMĚŘENÍ ŠÍŘENÍ SIGNÁLU V BUDOVĚ ZÁKLADNÍ ŠKOLY .....	36
7.4	NÁVRH ROZMÍSTĚNÍ PŘÍSTUPOVÝCH BODŮ S POMOCÍ SIGNÁLOVÉ MAPY .....	36
7.5	VÝBĚR A NÁVRH SÍŤOVÝCH PRVKŮ .....	37
7.6	NÁVRH BEZDRÁTOVÉ SÍTĚ A PŘIDĚLENÍ ADRES .....	38
<b>8</b>	<b>KONFIGURACE SYSTÉMU .....</b>	<b>40</b>
8.1	SMĚROVAČ USG 110 .....	40
8.1.1	Registrace směrovače .....	40
8.1.2	Konfigurace směrovače .....	41
8.1.3	Konfigurace kontroleru bezdrátové sítě LAN na směrovači .....	46
8.1.4	Nastavení filtrace obsahu pro žáky .....	52
8.1.5	Další možnosti centrálního ověřování uživatelů .....	54
8.1.6	Oživení přístupových bodů v systému .....	55
8.1.7	Nastavení DHCP .....	56
8.2	PŘEPÍNAČE GS1900-24E A GS1900-10HP .....	58
8.2.1	Základní nastavení .....	58
8.2.2	Vytvoření VLAN .....	59
	<b>ZÁVĚR .....</b>	<b>61</b>
	<b>SEZNAM POUŽITÉ LITERATURY .....</b>	<b>63</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK .....</b>	<b>65</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>66</b>
	<b>SEZNAM TABULEK .....</b>	<b>68</b>
	<b>SEZNAM PŘÍLOH .....</b>	<b>69</b>

## ÚVOD

V dnešním moderním světě informačních technologií se dá považovat za téměř samozřejmé, že většina lidí má přístup k Internetu. Bez ohledu na to, jestli se jedná o činnost trávení volného času, rozšiřováním vědomostí, neformální komunikace v rámci mezilidských vztahů či pracovních jednání, případně skoro nutností nepřetržitého přístupu k internetu v rámci většiny zaměstnání. V současnosti existuje velké množství zařízení v různých odvětvích, které zaznamenávají, komunikují a následně odesílají informace přes Internet. Jedná se například o notebooky, různé měřicí zařízení, chytré telefony, tablety, kamery nebo datové úložiště. Je také velké množství profesí, ve kterých jsou pro plnění pracovních úkolů zaměstnavatelé nuceni poskytnout svým zaměstnancům používajícím přenositelné zařízení bezdrátové připojení k internetu.

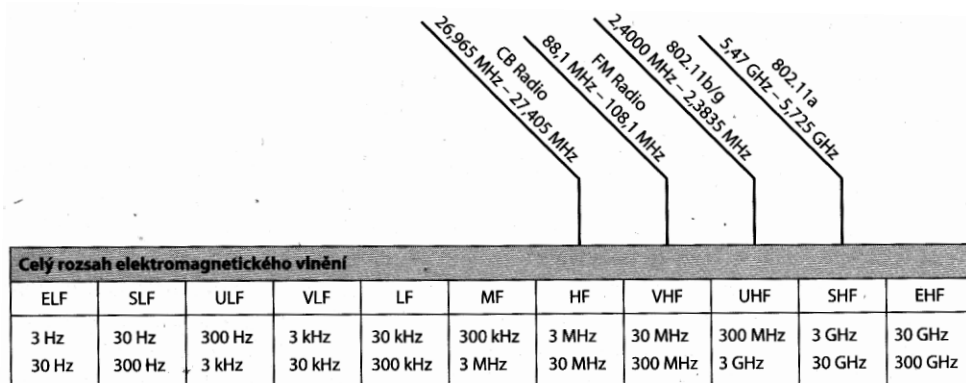
Firmy nucené okolnostmi používat bezdrátová zařízení, mají dvě volby. Buď si nechají v budově vybudovat kvalitní bezdrátový systém, který spolehlivě pokryje všechny potřebné místnosti, nebo sáhnou po rychlejší variantě připojení přes mobilní internet. Firmám, které často mění pracovní prostory, bude zcela jistě vyhovovat lépe mobilní připojení. Na druhou stranu pro firmy vykonávající svou práci na jednom místě, bude určitě výhodnější nechat si vybudovat kvalitní bezdrátovou síť po budově. Toto řešení má oproti mobilnímu připojení řadu výhod. Není příliš závislé na technických omezeních dané stavby, například tlusté obvodové betonové případně staré vlhké obvodové zdi, budou mobilní signál velmi tlumit a tím bude značně snížena rychlost připojení. Dále bezdrátové sítě nabízejí možnosti oddělení případně omezení síťového provozu, pro různé skupiny zaměstnanců. Podobně je tomu také v případě základní školy. S rozvojem používání moderních technologií vyvstává i v těchto organizacích větší potřeba přístupu k internetu. S tím se objevují také požadavky na oddělení provozu a oddělení přístupových práv pro zaměstnance a žáky. Na trhu existuje nemalé množství firem, které nabízejí vlastní řešení pro centrální zprávu větších a velkých firemních bezdrátových sítí. V této práci je popsána implementace a nasazení právě jednoho z nich.

## **I. TEORETICKÁ ČÁST**

## 1 SPECIFIKACE 802.11

Za účelem posílání dat vyvinula organizace IEEE (Institute of Electrical and Electronics Engineers) specifikaci 802.11, tato specifikace definuje half-duplexové operace s využitím stejné frekvence pro odesílání a přijímání dat po síti WLAN (wireless local area network). Standardy 802.11 se musí řídit jednak normami obsaženými v Generálních licencích pro „bezlicenční pásma“ a dále musí se respektovat pravidla stanovená příslušnou organizací spravující určitou oblast. Pro USA je to FCC (Federal Communication Commission), pro Evropu ETSI (European Telecommunications Standards Institute). Aby mohla být data vložena do podoby radiofrekvenční signálu, musí být použita modulační technika. Modulace znamená, přidání dat k přenosovému signálu.

Na obrázku (Obr. 1) je zobrazena část elektromagnetického spektra. Standardy 802.11x používají frekvenční pásma (2,400–2,483 GHz, 5.725-5.825GHz). Svým rozsahem se tyto pásma zařazují do kategorie ultrazvukových frekvencí UHF (Ultra High Frequency) nebo supervysokých frekvencí SHF (Super High Frequency). Ačkoliv všechny zařízení používající tyto pásma musí splňovat všeobecné podmínky generální licence, je možno tato pásma využívat zcela zdarma. Bohužel tento fakt je také známý všem výrobcům používajícím u svých výrobků bezdrátovou komunikaci např. u garážových vrat na dálkové ovládání, bezdrátových telefonů nebo dětských chůviček. Pásmo 2.4 GHz je právě díky častému využití jinými zařízeními více rušené než 5 GHz pásmo, takže 5 GHz pásmo se může jevit lepší pro používání, na druhou stranu má v budovách menší prostupnost díky používané vyšší frekvenci [1], [2], [3].

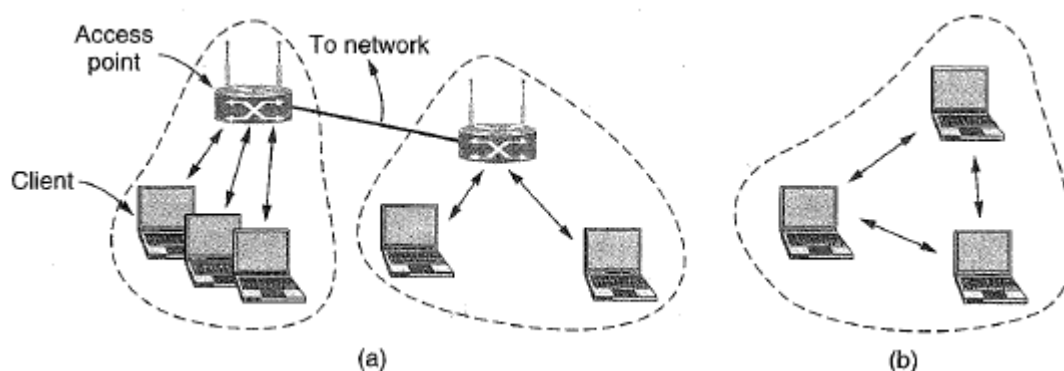


Obr. 1. Elektromagnetické spektrum [1].

Bezdrátové sítě 802.11 můžou být použity ve dvou módech:

## 1.1 Režim ad hoc

Pokud potřebují mezi sebou přímo komunikovat dva nebo více počítačů, vytvoří ad hoc síť (Obr. 2 b), je to síť, která nepotřebuje pro zprostředkování komunikace žádné centrální zařízení. Místo toho je jednomu zařízení nastaven název skupiny a parametry rádiového vysílání a druhé zařízení se k němu připojí [1].



Obr. 2. 802.11 architektura (a) mód infrastruktury (b) ad-hoc mód [12].

## 1.2 Režim infrastruktury

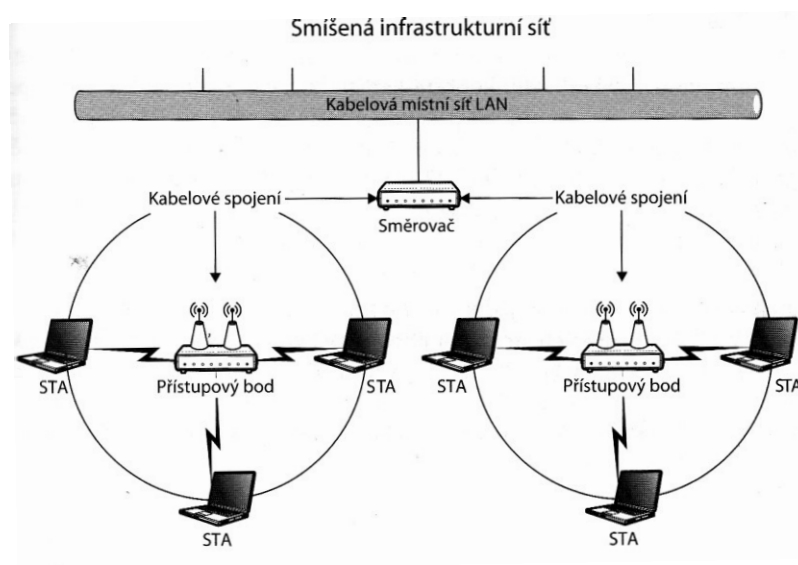
V režimu infrastruktury (Obr. 2 a) je každý klient (např. notebooky, chytré telefony) připojen k přístupovému bodu, který je přímo připojen k pevné síti. Klient posílá a přijímá pakety přes přístupový bod. Spojením více přístupových bodů vzniká distribuční systém [3].

### 1.2.1 Distribuční systém

Je skupina přístupových bodů nakonfigurovaných se stejným síťovým jménem SSID (Service Set Identifier) vytvářejících jednu distribuovanou bezdrátovou LAN. Přestože tyto přístupové body tvoří jednu logickou síť, musí existovat v jedné broadcast doméně. Když nějaká stanice pošle broadcast, ten musí přijít ke všem ostatním stanicím. V důsledku toho musí být všechny přístupové body tvořící jednu síť WLAN nějakým způsobem vzájemně propojeny. Jsou-li propojeny pomocí switche, je používané označení pro distribuční systém jako wired distribution system. Pokud jsou jednotlivé AP propojeny bezdrátově pomocí opakovačů, používá se označení WDS (wireless distribution system) [4], [5].

Bezdrátový distribuční systém má výhodu, že umožňuje rozšiřovat síť pomocí přístupových bodů v režimu most bez nutnosti rozvodů kabeláže. WDS nejčastěji propojuje přístupové body na odlišné frekvenci než klienty, protože většina přístupových

bodů má v dnešní době dvě radiové části. Nevýhodou při použití mostů je snižování výsledné rychlosti, kdy na každém skoku bezdrátového opakovače dojde zhruba k polovičnímu poklesu rychlosti oproti předchozímu skoku. Signál totiž musí vzduchem projít dvakrát – jednou od externího přístupového bodu k repeateru, podruhé od repeateru ke klientovi. Obecně WDS není žádný standard, přestože IEEE začíná na jeho standardizaci pracovat, zatím jde o nestandardizovaný koncept. Není tedy zaručeno, že jednotlivé výrobky různých výrobců označené WDS mezi sebou budou kooperovat, je vždy výhodnější nakoupit zařízení u jednoho výrobce [4],[6].



Obr. 3. Wired distribution systém [4].

### 1.2.2 Roaming

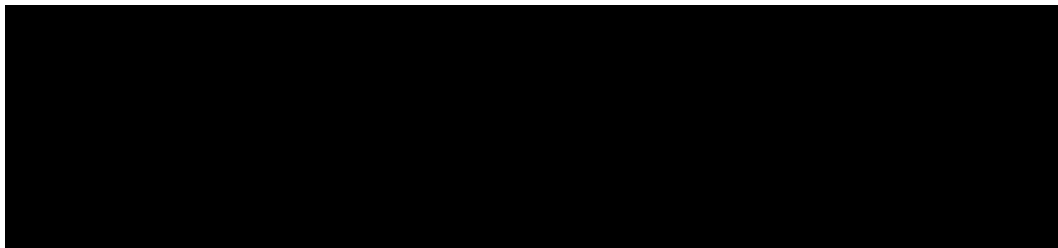
Pohyb klienta od jednoho přístupového bodu ke druhému se nazývá roaming. Má-li roaming správně fungovat, musí se dosahy přístupových bodů překrývat. Důvodem je, že klient musí vidět na oba přístupové body a připojí se k tomu, který mu dává silnější signál. V případě, že úroveň signálu od přípojného přístupového bodu poklesne pod prahovou hodnotu, klient začne vyhledávat jiný přístupový bod s lepším signálem [1], [2].

## 2 BEZLICENČNÍ FREKVENČNÍ PÁSMO 2,4 GHZ A 5 GHZ

Bezlicenční frekvenční pásma 2,4 a 5 GHz jsou výhodné tím, že vysílání v jejich rozsahu je zcela zdarma. V současnosti je mnohem používanější pásmo 2,4 GHz, nicméně začíná být v určitých oblastech, hlavně v husté městské zástavbě problém s vysokým zarušením. Z toho plyne, že v příliš zarušené oblasti může být spojení nestabilní a rychlost může značně kolísat. Proto je lepší používat nepříliš zarušené pásmo 5 GHz. V současnosti se ale stále naráží na problém, že je používané velké množství starších notebooků a chytrých telefonů, které nejsou vybaveny 5 Ghz přijmači.

### 2.1 Pásmo 2,4 GHz

Frekvenční rozsah 2,4 GHz je rozdělen od 2,412 do 2,848 po krocích 5 MHz, výjimkou je čtrnáctý kanál s krokem 12MHz od třináctého. Pásmo 2,4 GHz je tedy rozděleno do 14 kanálů. Počet povolených používaných kanálů se liší podle konkrétní krajiny. V Evropě je povoleno používat rozsah kanálů 1-13 dále například v USA je povoleno používat 1-11, a v Japonsku 1-14. Jeden používaný kanál obsadí šířku pásma o velikosti 20-22 MHz kolem své udávané frekvence. V Evropských státech díky tomu můžou současně v jednom místě běžet jen tři kanály 1, 6, 11 [7].



*Obr. 4. Grafická reprezentace wi-fi kanálů v pásmu 2,4 GHz [8].*

Pro dosažení vyšší rychlosti je možno obsadit i pásmo o šíři 40 MHz, tím zabereme polovinu možných kanálů. Teoreticky se tím sice dostáváme na vyšší přenosovou rychlost, nicméně prakticky roste pravděpodobnost, že širší pásmo bude kolidovat s jiným kanálem používaným jiným přístupovým bodem v dané oblasti, nebo bude rušeno jiným zařízením vysílajícím na 2,4 GHz tudíž bude častěji docházet ke kolizím signálu a provoz se naopak může zpomalit. Povolovaný maximální vyzářený výkon u 2,4 GHz vysílačů je v České republice omezen Českým telekomunikačním úřadem do 100 mW [7].

## 2.2 Pásmo 5 GHz

Pásmo 5 GHz je v Evropě rozprostřeno ve frekvenčním rozsahu 5,180 (36. Kanál) až 5,700 (140. Kanál). Ačkoliv číslování kanálů je odstupňované po 5 MHz, jsou používané kanály vzdálené od sebe 20MHz. Proto při nastavování kanálů, jsou dostupné kanály s číslem o 4 větší než předchozí kanál. Díky většímu rozsahu, než u pásma 2,4 GHz je v Evropě dostupných 19 kanálů. Prakticky je tedy možné provozovat celkem devatenáct 5 GHz wi-fi zařízení na jednom místě, aniž by se zařízení navzájem rušila. Prvních osm kanálů (36-64, 5,180-5,240 GHz) je určeno pro používání uvnitř budov. Maximální povolený vysílací výkon je 200mW. Ostatních jedenáct kanálů (100-140) je možnou použít mimo budovy a jejich vysílací výkon je omezen do 1 W. Zařízení vysílající mimo budovy na těchto kanálech musejí být dále vybaveny dynamickým výběrem frekvencí a regulací výstupního výkonu [7].

## 2.3 Standardy 802.11

### 2.3.1 802.11b

Tento standard byl schválen v roce 1999, představoval doplněk k normě IEEE 802.11. Pracoval v přenosovém pásmu 2,4 GHz. Používané přenosové rychlosti byly 1, 2, 5,5 a 11 Mb/s. Používal modulační technologii DSSS (Direct Sequence Spread Spectrum) [1].

### 2.3.2 802.11 a

Standard schválen v roce 1999. Pracoval v přenosovém pásmu 5 GHz, díky tomu není zpětně kompatibilní se standardy 802.11b a 802.11g. Používá modulační technologii OFDM (orthogonal frequency division multiplexing). Podporované přenosové rychlosti 6, 9, 12, 18, 24, 36, 48, 54 Mb/s [1].

### 2.3.3 802.11g

Standard schválen organizací IEEE v roce 2003. Pracuje v přenosovém pásmu 2,4 GHz. Používá modulační metodu OFDM. Pro tuto metodu poskytuje rychlosti 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s. Je zpětně kompatibilní se standardem 802.11b, pro tento standard používána modulační metoda DSSS [1].



### 2.3.4 802.11n

Vydán v roce 2009. Pracuje v přenosovém pásmu 2,4 nebo 5 GHz, maximální teoretická rychlost 600 Mb/s. Standard je zpětně kompatibilní se standardy 802.11b/g a a. Používá modulační metodu OFDM. Má implementovanou podporu šifrování WPA2. U předchozích standardů se pro komunikaci používala 1 anténa na vysílači i přijímači SISO (Single Input Single Output), standard 802.11n začal používat technologii SU-MIMO (Single User Multiple-Input, Multiple-Output) používající více antén na vysílači i přijímači. Dříve tato technologie byla označována pouze jako MIMO.

U SU-MIMO (neboli MIMO) technologie je díky více anténám vysíláno více signálů nezávislými streamy, každá anténa má svůj přijímač a vysílač, taktéž na straně příjemce jsou tyto signály přijímány více anténami. Antény musí být natočeny různými směry, aby signály šly k příjemci různými cestami a nedocházelo k jejich vzájemnému rušení. Při použití MIMO technologie jsme omezeni na stejný počet datových streamů, kolik je nejmenší počet antén u jednoho ze zařízení. Pokud má například vysílač 3 antény a klient pouze jednu anténu, degraduje se vysílač jako by vysílal pouze s 1 anténou [1].

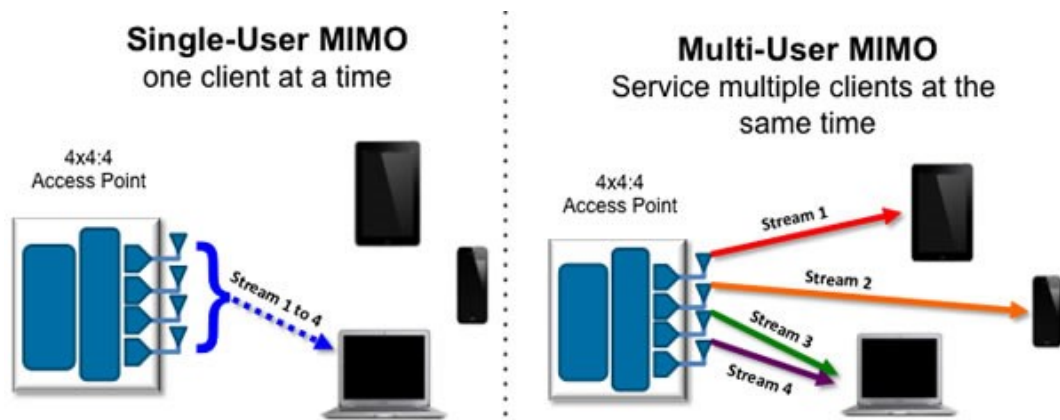
### 2.3.5 802.11ac

Standard schválen v roce 2014. Používá primárně 5 GHz pásmo, se šířkami kanálů od 20 do 160 MHz. Používaná modulační technologie OFDM. Všechny zařízení používající standard 802.11ac jsou zpětně kompatibilní se standardy 802.11g/n/b/a a tyto zařízení umí tedy komunikovat i na 2,4 GHz. Standard 802.11ac fungoval ve své první verzi s technologií SU-MIMO (Single-User Multiple Input – Multiple Output).

V současnosti jsou prvky ze standardem 802.11ac osazované vylepšenou technologií SU-MIMO takzvanou MU-MIMO (Multi-User Multiple Input – Multiple Output). Tato technologie umožňuje multistreamovému vysílači v jeden čas komunikovat s několika zařízeními současně. Pokud by se například k vysílači se třemi streamy připojili tři jednostreamové smartphony, takový vysílač obslouží všechny tři, aniž by jeden ovlivňoval rychlost druhého. Bez MU-MIMO by se v komunikaci musely telefony mezi sebou střídát [9], [10].

Nutnou podmínkou, která se musí brát na zřetel je, že aby MU-MIMO technologie opravdu fungovala, musí ji podporovat přístupový bod i klient. Aktuálně je stále malé množství zařízení, které tuto technologii podporují, proto investice do dražších směrovačů

a přístupových bodů využívajících tuto technologii je celkem zbytečná a tedy stačí investovat do prvků podporujících technologii SU-MIMO.



Obr. 5. Srovnání SU-MIMO a MU-MIMO [13].

## 2.4 Fyzické versus reálné rychlosti

Výše byly popsány teoretické maximální rychlosti jednotlivých standardů. Nicméně v reálném prostředí, díky rušení a útlum signálu, není těchto rychlostí prakticky nikdy dosaženo. V tabulce (Tab. 1) můžeme vidět srovnání teoretických a reálných rychlostí. Obecně se lze řídit jednoduchým pravidlem, že reálné rychlosti jsou 40 % hodnoty z teoretických rychlostí. Dále je vidět jaké výrazné zvýšení rychlosti přinesla technologie MIMO, kde je vysíláno více signálů více anténami a na straně příjemce také více anténami přijímáno. V cíli jsou signály sloučeny a data jsou přenášena s výslednou u 2T2R (2 transmit 2 receive antény), u 3T3R s 3× a u 4T4R s 4× vyšší rychlostí oproti rychlostem dosaženým při použití pouze jedné antény. Aby bylo dosaženo těchto rychlostí, musíme brát na zřetel, že máme-li k dispozici 2T přístupový bod a chceme využít komunikaci dvěma streamy, musí také klient mít 2R tzn. dvě antény, není-li tomu tak, bude výsledná rychlost patřičně nižší. Tabulkově je vidět, že při použití např. 1T1R přístupového bodu na 2,4GHz a šířce kanálu 40 MHz se dostaneme na stejnou rychlost, jako při použití 2T2R AP s šířkou kanálu 20 MHz. Nicméně prakticky má větší smysl u 2,4 GHz snažit se vysílat více anténami a menší šířkou pásma, důvodem je časté rušení, které se právě na větší šířce pásma více projevuje.

Rychlost může být také snížena kvůli zpětné kompatibilitě se staršími zařízeními. Pokud se v síti například ocitne staré zařízení ze standardem 802.11g, přístupový bod musí s tímto zařízením komunikovat nižší rychlostí. Proto takové zařízení bude omezovat všechny ostatní rychlejší zařízení a celkový provoz bude pomalejší [12].

Tab. 1. Rychlosti na aplikační vrstvě versus rychlosti na fyzické vrstvě [12].

Standard	MIMO	Rychlost na aplikační vrstvě (20 MHz)	Rychlost na aplikační vrstvě (40 MHz)	Rychlost na fyzické vrstvě (20 MHz)	Rychlost na fyzické vrstvě (40 MHz)
802.11	ne	2 Mb/s	nepodporuje	0,8 Mb/s	nepodporuje
802.11b	ne	11 Mb/s	nepodporuje	4,4 Mb/s	nepodporuje
802.11g	ne	54 Mb/s	nepodporuje	21,6 Mb/s	nepodporuje
802.11a	ne	54 Mb/s	nepodporuje	21,6 Mb/s	nepodporuje
802.11n	1T1R	75 Mb/s	150 Mb/s	30 Mb/s	60 Mb/s
802.11n	2T2R	150 Mb/s	300 Mb/s	60 Mb/s	120 Mb/s
802.11n	3T3R	225 Mb/s	450 Mb/s	90 Mb/s	180 Mb/s
802.11n	4T4R	300 Mb/s	600 Mb/s	120 Mb/s	240 Mb/s
Standard	MIMO	Rychlost na aplikační vrstvě (80 MHz)	Rychlost na aplikační vrstvě (160 MHz)	Rychlost na fyzické vrstvě (80 MHz)	Rychlost na fyzické vrstvě (160 MHz)
802.11ac	1T1R	433 Mb/s	866 Mb/s	173 Mb/s	346 Mb/s
802.11ac	2T2R	866 Mb/s	1 732 Mb/s	346 Mb/s	693 Mb/s
802.11ac	4T4R	1 732 Mb/s	3 464 Mb/s	693 Mb/s	1 385 Mb/s
802.11ac	8T8R	3 464 Mb/s	6 928 Mb/s	1 385 Mb/s	2 771 Mb/s

### 3 ANTÉNY

Nedílnou součástí každého přístupového bodu, jsou antény. Rozlišuje se několik druhů antén podle účelu použití. Charakteristickými vlastnostmi jsou zisk a směrovost.

#### 3.1 Zisk

Všechny antény jsou více či méně směrové, míru směrovosti udává zisk, který je největší právě ve směru kam anténa nejvíce vyzařuje. Anténa s vysokým ziskem musí být více směrová, ve srovnání s anténou s nízkým ziskem. Zisk antény je definován jako poměr intenzity vyzařování dané antény v určitém směru k intenzitě vyzařování referenční antény ve stejném směru. Jako referenční anténa se volí buď izotropní anténa, nebo ideální půlvlnný dipól.

Izotropní anténa je teoretická anténa, která vyzařuje energii rovnoměrně ve všech směrech. Zisk izotropní antény je 1. Vyjádřený v dBi se rovná 0.

$$G_{dBi} = 10 * \text{Log} \left( \frac{G_{Numeric}}{G_{Isotropic}} \right) = 10 * \text{Log}(G_{Numeric}) \quad (1)$$

$G_{dBi}$  zisk v dBi

$G_{Numeric}$  intenzita vyzařování v určitém směru v jednotkách dB

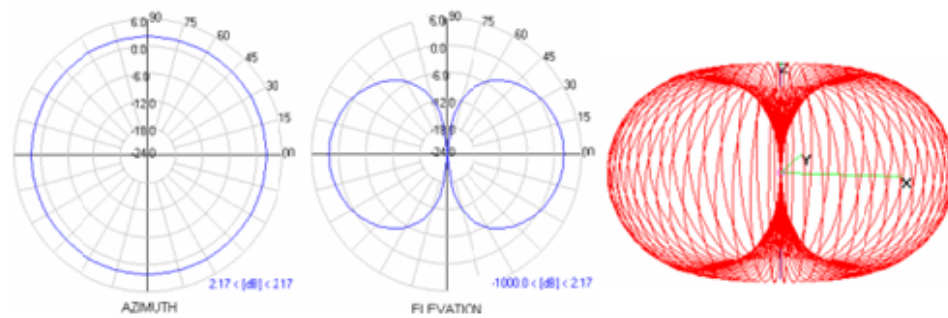
$G_{Isotropic}$  zisk izotropní antény

Druhým typem referenční antény je ideálním půlvlnný dipól, zisk vyjádřený s jeho poměrem se značí jednotkou dBd a je o 2,16 nižší než zisk udávaný v dBi [14], [15].

#### 3.2 Typy antén a vyzařovací charakteristiky

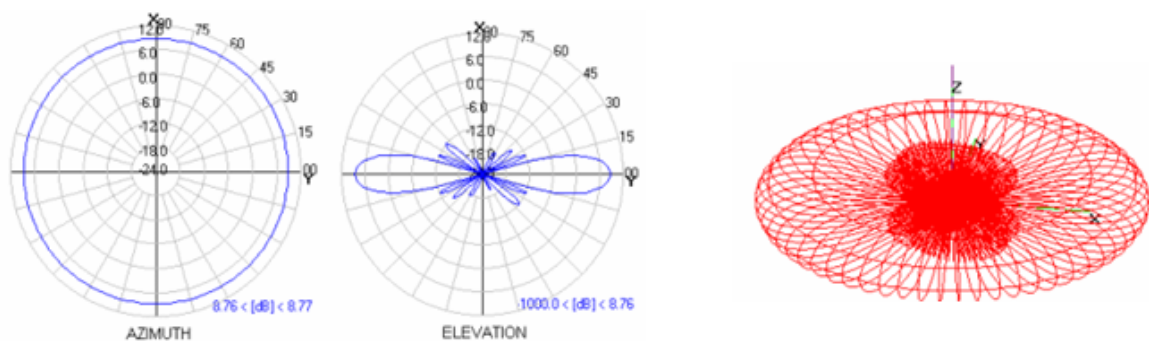
##### 3.2.1 Všesměrové antény

Typickým zástupcem je anténní dipól se ziskem přibližně 2,16 dBi je používán jako antény na většině přístupových bodů vyráběných pro použití uvnitř budov. Jeho ideální vyzařovací charakteristika proto připomíná tvarem koblíhu. Nejvíce energie vyzařují v horizontálním směru rovnoměrně 360° do všech stran. Zařízení pod a nad všesměrovými anténami, mohou mít velmi slabý, případně nulový signál [14], [15].



Obr. 6. Vyzařovací charakteristiky dipólu se ziskem 2,16 dBi [14].

V případech, kdy je vyžadován větší dosah ve vertikální rovině, jsou používány všesměrové antény s větším ziskem. Díky většímu zisku jsou však paprsky ve vertikální rovině vysílány v malém úhlu. Zisky těchto antén se pohybují nejčastěji mezi hodnotami 7-12 dBi. Dále vznikají ve vrchní a spodní části osy z postranní laloky [15], [16].



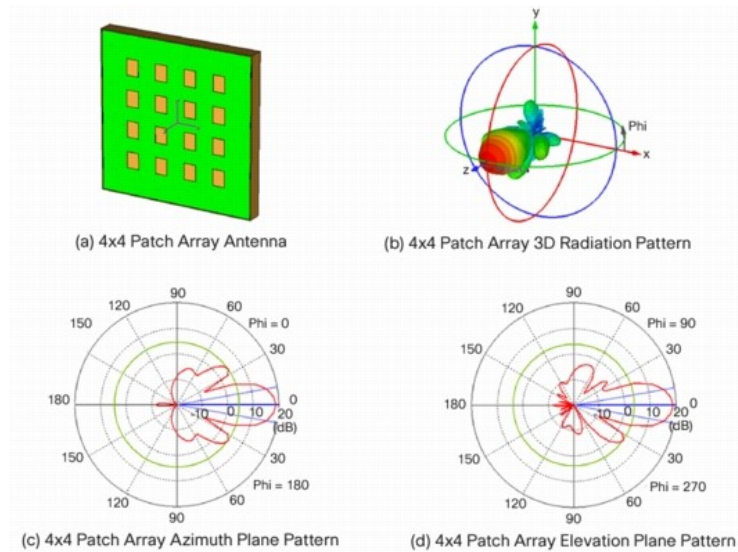
Obr. 7. Vyzařovací charakteristika dipólu s větším ziskem [14].

### 3.2.2 Směrové antény

Cílem směrových antén je vyzařovat energii určitým směrem. Tím dosahují do daného směru mnohem většího zisku. V interiéru jsou používány pro pokrytí například dlouhých chodeb, nebo skladů, většinou jsou používány v exteriéru pro bezdrátové připojení koncových klientů k poskytovateli internetu. Jsou používány panelové, směrové a parabolické antény.

#### a) Panelové

Jsou složeny z vodivých destiček naskládaných po řádcích pod sebe. Důvodem tohoto uspořádání je vyšší zisk antény. Vyšší zisk vede k zúžení šířky paprsku.

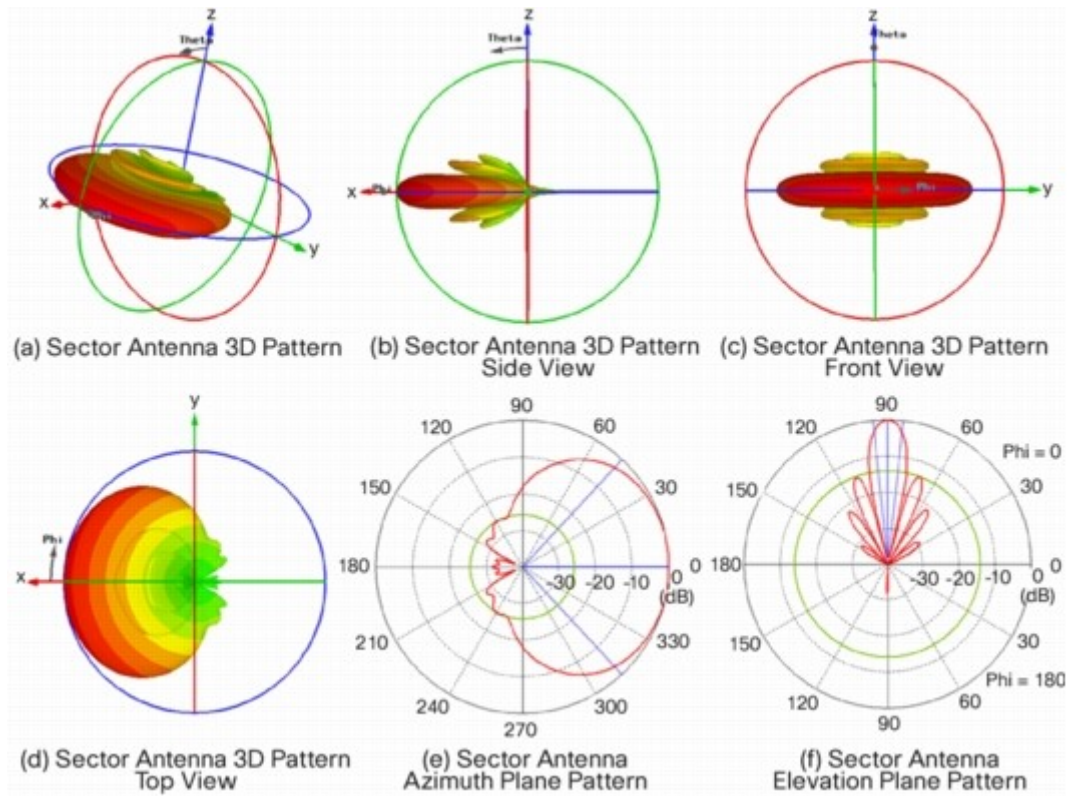


Obr. 8. Vyzářovací charakteristiky panelové směrové antény [15].

#### b) Sektorové

Jsou používány tam, kde je třeba pokrýt větší souvislý prostor, ale je zbytečné instalovat nízko ziskovou všesměrovou anténu. Jsou tvořeny polem dipólů, umístěným před tvarovaný reflektor. Velikost a tvar reflektoru určuje do značné míry výkon těchto antén. Nejlevnější sektorové antény mají vyzářovací úhel ve vertikální rovině cca.  $30^\circ$  kvalitnější a dražší, které jsou složeny z více sfázovaných zářičů, mají úhel až  $180^\circ$ .

Na obrázku máme příklad vyzářovací charakteristiky sektorové antény se ziskem 18 dBi a  $90^\circ$  sektorem [15], [16].

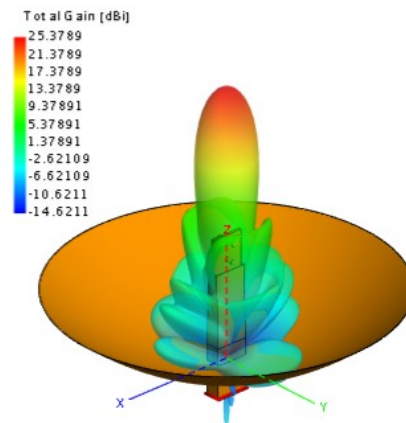


Obr. 9. Vyzařovací charakteristika  $90^\circ$  sektorové antény [15].

Zisky panelových a sektorových se pohybují mezi 9 až 20 dBi, záleží na kvalitě a ceně.

### c) Parabolické reflektory

Jsou tvořeny zářičem (dipól, malá YAGI anténa) a parabolickým reflektorem tvořeným plnou parabolou, nebo sítím. Zářič ozařuje plochu paraboly, která soustředí signál do úzkého paprsku. Tyto antény dosahují zisku i 30 dBi, ale vyzařovací úhly mají menší než  $10^\circ$  [16].



Obr. 10. Vyzařovací charakteristika parabolické antény [17].





## 4 POE

PoE (Power over Ethernet) je technologie, která umožňuje přenášet po ethernetovém kabelu zároveň data a napájení. Napájení PoE usnadňuje instalaci nových zařízení v místech, kde chybí elektrické rozvody, nebo elektrické zásuvky jsou umístěny příliš daleko od místa, kam je vyžadováno zařízení umístit. Nejčastěji napájenými zařízeními jsou webové kamery, IP telefony, bezdrátové přístupové body.

Při práci s PoE jsou často používány dvě následující zkratky. PSE (Power sourcing Equipment) jsou zařízení zodpovědné za napájení připojených zařízení. PD (Powered Devices) jsou označovány připojené napájené zařízení. Technologie PoE používá dva následující standardy.

### 4.1 Standardy PoE

#### 4.1.1 IEEE 802.3af

Tento standard byl představen v roce 2003. Zařízení s tímto standardem mohou dodávat maximálně 15,4 W na port, ale zařízení PD spolehlivě přijme pouze 12,95 W kvůli odporu vodičů.

#### 4.1.2 IEEE 802.3at

Standard uveden v roce 2009. Zařízení s tímto standardem jsou schopné dodávat výkon 30 W na jeden výstupní port. Stejně jako u staršího standardu je k připojeným zařízením přiveden efektivně nižší výkon, podle specifikace se jedná o maximálně 25,5 W

Aby se zabránilo přílišnému napájení napájeného zařízení, které by mohlo vést ke zkrácení jeho životnosti, je využíváno 5 následujících tříd:

- nultá třída Classification unimplemented - 0,44-12,94 W,
- první třída Very Low power 0,44-3,84 W,
- druhá třída Low power 3,84-6,49 W,
- třetí třída Mid power 6,49-12,95 W,
- čtvrtá třída High power 12,95-25,5 W.

Každá třída určuje množství energie, kterou připojené zařízení vyžaduje. Při připojení poskytne napájené zařízení PD napájecímu zařízení PSE svou třídu a tím se docílí dodávání správného množství energie [18], [19].

## 4.2 Kompatibilita a aplikace

Napájecí zařízení typu PoE+ je schopno poskytnout napájení připojeným zařízením typu PoE i PoE+, ale napájecí zařízení typu PoE jsou schopné poskytovat napájení připojeným zařízením typu PoE.

Napájecí zařízení můžeme mít dvojího druhu. Zařízení se zabudovanou technologií PoE kterými jsou nejčastěji síťové přepínače. Při jejich výběru je třeba se pozorně zaměřit, na celkový výkon, který jsou přepínače schopné dodat napájeným zařízením. Většina přepínačů, totiž neposkytuje dostatečnou energetickou kapacitu, aby mohly ze všech svých portů napájení dodávat. Při pořizování napájecího zařízení s funkcí PoE, je nutné si spočítat celkovou energetickou kapacitu pro všechna plánované připojené zařízení. Například, máme-li osmi portový přepínač, který má garantovaný výkon pro PoE 130 W z obrázku (Obr. 11) je zřejmé, že při normě 802.3af dokážeme dodávat potřebný výkon ze všech 8 portů, ale při normě 802.af je možné dodávat potřebný výkon pouze z 5 portů.

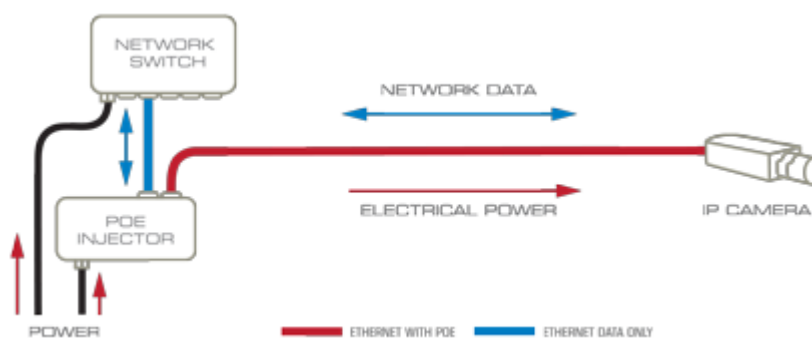
	Devices	Max. PoE Output
802.3af Standard	8 Devices	15.4 Watts
802.3at Standard	4 Devices*	30 Watts

Max. Watts per port at full capacity:	
$\frac{\text{Total PoE Budget}}{\# \text{ of Ports}}$	equation
$\frac{130 \text{ Watts}}{8 \text{ Ports}} = \text{Up to } 16.25 \text{ Watts per Port}$	

Obr. 11. Počet použitelných portů pro PoE na 130 W přepínači [18].

V případech, kdy je vyžadováno napájení PoE pouze pro jedno zařízení, jsou používány tzv. **injektory**. Jedná se o malé zařízení, které je umístěné mezi přepínačem nepodporujícím PoE a připojeným zařízením PD, které naopak PoE potřebuje.



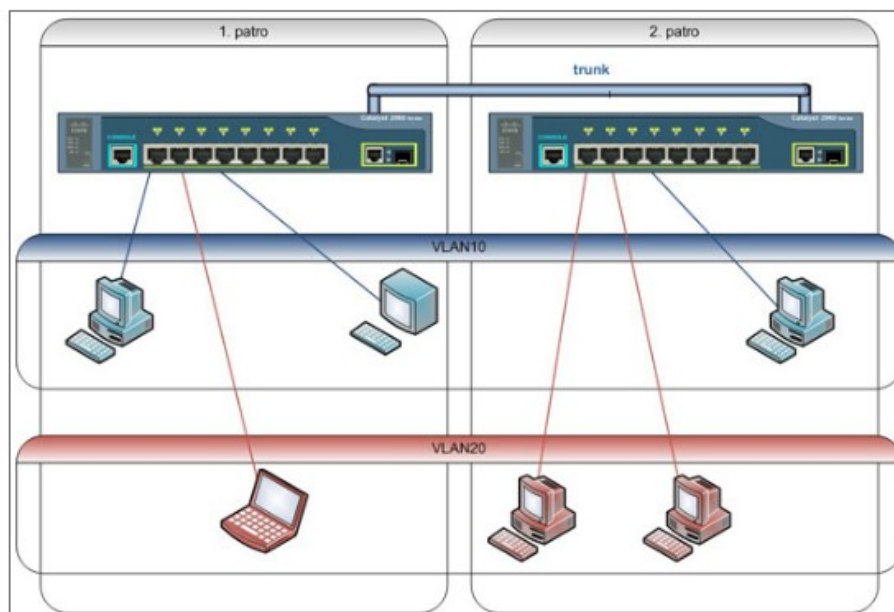
Obr. 12. PoE Injektor [20].

V případech, kdy je dostupný přepínač s funkcí PoE a na konci ethernetového kabelu je vyžadováno připojit zařízení, které PoE nepodporuje, je možné použít **splitter**. Jedná se o malý rozbočovač, do kterého se přivede ethernetový kabel s PoE a následně rozbočovač rozdělí napájení od dat a vyvede každé ve vlastním portu [18], [19].

## 5 VLAN

Virtuální LAN jsou používány k logickému rozdělení sítě, nezávisle na jejím fyzickém uspořádání. Prakticky lze díky VLAN (virtual local area network) dosáhnout stejného efektu, jako kdyby bylo vytvořeno více fyzických sítí, které spolu bez použití směrovače nemohou komunikovat. Bez použití VLAN by jedna skupina zařízení musela být zapojena do jednoho přepínače a druhá skupina zařízení do jiného přepínače. S využitím VLAN můžeme takovéto dvě sítě vytvořit na jednom (nebo více propojených) přepínačích.

Praktická ukázka je na obrázku (Obr. 13). Obrázek symbolizuje klienty na dvou patrech budovy. Na každém patře se nachází přepínač, vzájemně jsou přepínače propojeny trunkem, taktéž se na každém patře nachází klienti patřící do dvou různých sítí. Je-li požadováno, aby po připojení obdrželi klienti od DHCP serveru (není vyobrazen) IP adresu ze své subsítě, díky VLAN je možné síť rozdělit na (např. VLAN10 a VLAN20) a přidělit je patřičným portům, tím je možné k jednomu přepínači připojit zařízení patřící do různých sítí. Bez použití VLAN by musel být na každém patře oddělený přepínač pro připojení zařízení z jedné sítě [21].



Obr. 13. Ukázka VLAN [21].

Aby bylo možno mezi VLAN směrovat, nebo použít některé speciální funkce na přepínači, je nutno, aby byly pro určitou VLAN používány IP adresy z jedné sítě.

Jako praktické výhody VLAN jsou uváděny:

- Snížení broadcastů – Díky VLAN je vytvořeno více ale menších broadcastových domén. To vede ke zlepšení výkonu sítě.
- Zjednodušená správa - při přesunu zařízení do jiné sítě je potřeba překonfigurovat software (změnou zařazení do VLAN) a ne hardware (změna fyzické připojení).
- Zvýšení zabezpečení – oddělením zařízení do zvláštních VLAN se zvýší možnosti zabezpečení. Díky aplikaci VLAN lze jednodušeji aplikovat omezení, aby skupina s nižšími právy nemohla mít přístup k důležitým datům.
- Oddělení speciálního provozu – VLANy lze použít spolu s QoS pro zaručení kvality komunikace, například při použití IP telefonů.
- Snížení počtu HW prvků - tím, že mohou být různé podsítě na jednom přepínači, jej lze lépe využít a to vede k redukci nadbytečného počtu přepínačů.

Nejčastěji rámce taguje přepínač na konkrétních portech pomocí nastavení čísla PVID (port vlan id) pro konkrétní porty switchu. Při implementaci řízeného wi-fi systému byly využívány vlastnosti přístupových bodů, které také dokážou tagovat rámce.

Stanice (uživatel) se připojí k přístupovému bodu. Přístupový bod vysílá 3 různé SSID. Podle toho, ke které se klient připojí, jsou rámce tagovány příslušným tagem. Klient požádá DHCP server o přidělení IP adresy. DHCP server přečte číslo tagu. Podle tagu přidělí stanici, IP adresu.

## 5.1 Způsoby definice členství ve VLAN

Přiřazení do VLANy se typicky nastavuje na přepínači. Na přepínačích, které podporují VLAN, existuje vždy jedna defaultní VLAN s číslem 1, kterou není možné odstranit. Dále je možné vytvořit mnoho dalších VLAN. Pro přiřazení členství určitého zařízení do VLAN je možné použít jednu ze dvou základních metod:

### 5.1.1 Statická metoda

Při použití této metody nastavuje administrátor ručně určitým portům přepínače členství v požadované VLAN. Veškerá komunikace přicházející přes daný port spadá do zadané VLAN. Pokud je k portu připojen další přepínač, tak všechny zařízení do něj připojená budou v jedné VLAN. Jedná se o nejrychlejší metodu při vytváření virtuálních sítí, ale její

základní omezení spočívá v nutnosti předefinování členství při případných přesunech uživatelské stanice mezi porty přepínače.

### 5.1.2 Dynamická metoda

Dynamická metoda přiřazuje VLAN k portům přepínače automaticky po připojení zařízení. V případě použití této metody je nutno nejprve nakonfigurovat jeden přepínač ze sítě jako server. Na server jsou nahrány specifické informace o zařízeních připojovaných do počítačové sítě. Nejčastěji se jedná o MAC adresy připojovaných zařízení. Tyto adresy jsou následně mapovány do určitých VLAN. Pro speciální přepínače podporující funkci serveru je používána zkratka VMPS (VLAN Membership Policy Server). Dynamické VLAN podporují mobilitu plug and play. Pokud se například uživatel s počítačem John přepojí na přepínači z portu 2 na port 8. Portu 8 bude automaticky změněno členství ve VLAN ke které je adresa počítače John mapována.

## 5.2 Typy VLAN připojení na přepínači

### 5.2.1 Access link

Access link je nejběžnější konfigurace portů na přepínači podporujícím VLAN sítě. Porty nakonfigurované v tomto režimu, mají členství pouze v jedné VLAN, obvykle jsou používány pro koncové zařízení. Samotné zařízení připojené do access link portů na přepínači nevědí už nic o členství ve VLAN, protože přepínač vyjme z rámců veškeré informace o VLAN, před tím než je odešle z portu.

### 5.2.2 Trunk link

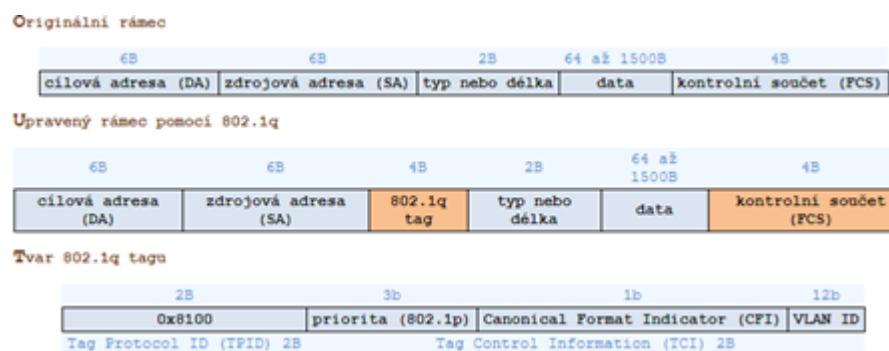
Trunk spoje umožňují přenášet rámce s členstvím v různých VLAN, obvykle jsou tyto spoje používány pro propojení více přepínačů, nebo pro propojení přepínače a směrovače. Pro správnou funkčnost trunk spoje, musí být na obou stranách spoje nastaveny porty v režimu trunk. Aby bylo možné využívat trunk spojů, musí být původní rámce rozšířeny o informace, které jasně řeknou do které VLAN rámec patří.

## 5.3 Tagování rámců

Standartní hlavička ethernetového rámce neobsahuje informace o jeho členství ve VLAN. V případě, že se začne v počítačové síti pracovat s VLAN a tím i s trunk spoji, je nutno začít do rámců informaci o VLAN přidávat, v angličtině se pro tento proces používá slovo

tagging. Aby byl systém značkování nějakým způsobem regulován, byl vytvořen standard IEEE 802.1q.

Protokol IEEE 802.1q se nazývá tagging někdy též trunking protokol. Tento protokol podporují zpravidla všechny říditelné přepínače. Funguje na principu rozšíření hlavičky rámce o přídatné informace. Když přepínač obdrží rámec na port konfigurovaný v access módu se členstvím v nějaké VLAN, vloží do hlavičky rámce celkem 4 byte nových informací, přepočítá kontrolní součet FCS (Frame Check Sequence) a odešle označovaný rámec na odchozí trunk port. Podrobnější popis informací přidaných do hlavičky je na obrázku (Obr. 14).



Obr. 14. Struktura tagu [21].

První dva byte ve VLAN tagu značí, že se jedná o protokol 802.1q (hodnota 0x8100). V dalších dvou bytech je uživatelská priorita, dále identifikátor zda je MAC adresa v kanonickém tvaru a poslední je číslo VLAN takzvané VLAN ID [22] [23].

## 6 POUŽITÉ TECHNOLOGIE PŘI REALIZACI BEZDRÁTOVÉ SÍTĚ SE ZAŘÍZENÍMI OD FIRMY ZYXEL

### 6.1 Možnosti QoS

Umožňuje přiřadit přístupové kategorie QoS (Quality of Service) pro daný SSID profil. Nastavení je umístěné v Object > AP Profile > SSID > SSID List. Je možné aplikovat jednu z následujících kategorií:

- a) Disable  
Vypne QoS pro daný SSID profil. Se všemi pakety bude zacházeno stejným způsobem.
- b) WMM (wi-fi multi media) – Povolí automatické tagování datových paketů. Kontroler přiřazuje automaticky přístupové kategorie paketům po jejich přijetí a dává prioritu na základě vlastního odhadu. Pokud například vyhodnotí daný paket, že je součástí video přenosu, otaguje ho jako video. Při tomto nastavení mají prioritu pakety označené jako hlasová data.
- c) WMM\_VIDEO – Veškerý bezdrátový provoz pro danou SSID je tagován jako video data. Doporučeno pro aktivity jako video konference.
- d) WMM\_VOICE – Veškerý bezdrátový provoz pro danou SSID je tagován jako hlasová data. Doporučeno tam, kde je SSID používána pro VoIP volání.
- e) WMM\_Best\_EFFORT - Veškerý bezdrátový provoz pro danou SSID je tagován jako „best effort“. Data jsou propouštěna bez vytváření priorit. Doporučeno tam, kde není vyžadována nejlepší propustnost šířky pásma, například pro běžné surfování na internetu.
- f) WMM\_BACKGROUND - Veškerý bezdrátový provoz pro danou SSID je tagován jako „background traffic“. Jako provoz s nízkou prioritou. Tam kde provoz v dané SSID nevyžaduje přísné nároky na propustnost, například u SSID které připojují pouze síťové tiskárny [24].

### 6.2 Smart Client Steering

Funkce pro inteligentní řízení klientů je rozdělena v ZyXEL kontroleru ve dvou oblastech. Část vlastností se umístěná v Object > AP Profile > SSID > SSID List a část je umístěná v Object > AP Profile > Radio [24].

### 6.2.1 Band Select

Je umístěné v menu SSID List pod popiskem Band Select, umožňuje zařízením se schopností fungovat ve dvojitým pásmu (2,4GHz a 5 GHz) první použít 5GHz. Funkce má 3 možnosti:

- a) standard – Rozhodnutí klientů schopných komunikovat v pásmu 2,4GHz a 5 GHz v jakém pásmu budou fungovat, je ponecháno na klientech samotných.
- b) force – Klienti schopní komunikovat na dvojitým pásmu jsou v tomto případě přinuceni přístupovým bodem připojit se pouze přes 5GHz pásmo.
- c) zakázána [25]

### 6.2.2 Band Select - Stop Threshold

Taktéž je umístěné v menu SSID List pod popiskem Band Select. Nastavuje prahové číslo, kolika bezdrátovým klientům bude dovoleno se připojit k přístupovému bodu na základě jejich vlastní volby. Tzn. funkce Band Select bude do překročení udaného počtu klientů ve stavu zakázána, po dosažení uvedeného počtu připojených klientů se funkce Band Select zapne a bude aplikována na každého nového připojeného klienta [24].

### 6.2.3 Band Select - Balance Ratio

Je opět umístěné v menu SSID List pod popiskem Band Select. Řídí v jakém poměru přístupový bod připojí bezdrátové klienty schopné komunikovat ve dvojitým pásmu. Doporučený poměr od výrobce je 4:1, první číslo vyjadřuje 5GHz klienty, druhé číslo vyjadřuje 2,4 GHz klienty [24].

### 6.2.4 RSSI (Received Signal Strength Indicator) Threshold

Je indikátor síly signálu přijaté přístupovým bodem od připojeného klienta. Umožňuje specifikovat sílu signálu připojených zařízení, aby se předešlo tomu, že připojení klienti se slabým signálem budou brzdít provoz na bezdrátové síti. V menu se skládá ze dvou podnastavení. Je možno je najít v Object > AP Profile > Radio > Advance

- a) Station Signal Threshold

Nastavuje minimální sílu signálu připojeného bezdrátového klienta, kdy je mu ještě povoleno připojit se k přístupovému bodu. Pokud je síla signálu klienta vůči přístupovému bodu slabší než specifikovaný práh, klientovi je žádost o připojení zamítnuta.



b) Disassociate Station Threshold

Nastaví minimální síly signálu pro odpojení klienta. Pokud je síla signálu připojeného klienta nižší než specifikovaný práh, kontroler odpojí takového klienta z daného přístupového bodu.

c) Station Retry Count

Výběrem této volby bude povoleno bezdrátovému klientu odpojenému od určitého přístupového bodu kvůli slabé síle signálu se znovu připojit k přístupovému bodu.

Je nutno specifikovat číslo, které určí počet neúspěšných pokusů o přihlášení klienta k přístupovému bodu, po překročení tohoto počtu mu bude možnost připojení k přístupovému bodu na určitou dobu uzamčena [26].

### 6.3 technologie DFS (Dynamic Frequency Selection)

Technologie dynamického výběru frekvencí je používána u přístupových bodů vysílajících na 5GHz, protože frekvence používané některými kanály mohou být používány také radary. Aby se zabránilo ochraně radarového vysílání, přístupový bod skenuje, jestli v jeho okolí není na určité 5GHz frekvenci vysíláno, pokud přístupový bod detekuje aktivity radaru na určité frekvenci, automaticky vyřadí kanál s danou frekvencí ze svého používání a nechá ho volný [26].

### 6.4 Operating Mode

Umístěn v sekci Wireless > AP Management > AP Group > edit. Přístupový bod je možno nastavit do dvou základních režimů.

- a) AP Mode – Znamená, že přístupový bod je v režimu kdy normálně přijímá data od připojených klientů a předává data dále na bránu.
- b) MON Mode – Znamená, že přístupový bod je v monitorovacím režimu a žádný klient se nemůže připojit. Přístupový bod monitoruje vysílání ve svém okolí a předává informace nadřazenému kontroleru [24].

### 6.5 Load Balancing Setting

Tato funkce nastavuje vyvažování zařízení. Má následující možnosti

- a) By Station Number - Vyvažování provozu na síti je založené na počtu připojených stanic k přístupovému bodu. Pokud je překročeno číslo, přístupový bod zpožduje

požadavky o přidružení z nových stanic, které se snaží připojit. Toto opatření umožňuje klientům pokusit se automaticky připojit k jinému dostupnému méně přetíženému přístupovému bodu.

- b) By Traffic Level – Vyvažování provozu na základě objemu průchozích dat. Pokud je překročen průchozí objem dat, přístupový bod zpožďuje požadavky o přidružení z nových stanic, které se snaží připojit. Toto opatření umožňuje klientům pokusit se automaticky připojit k jinému dostupnému méně přetíženému přístupovému bodu.
- c) By Smart Classroom – Vyvažování síťového provozu založené na počtu připojených klientů k přístupovému bodu. Přístupový bod bude ignorovat žádosti nových klientů o přidružení, pokud je dosaženo maximálního definovaného počtu připojených klientů [27].

## **II. PRAKTICKÁ ČÁST**

## **7 PŘÍPRAVA PODKLADŮ**

### **7.1 Stav bezdrátové sítě před realizací**

Před realizací byly v budově pouze dva dosluhující přístupové body SMC WGBR14-N2, ty pokrývaly pouze ředitelnu a sborovnu s dvěma kabinety. Tyto přístupové body byly nespolehlivé a bylo je nutno několikrát týdně restartovat.

### **7.2 Definice požadavků vedení školy**

Vybudovat nový kvalitní wi-fi systém, který by pokryl veškeré třídy a kabinety wi-fi signálem a umožnil řízení provozu. Nový systém by měl respektovat odlišná přístupová práva pro skupiny uživatelů učitele, žáky a návštěvy. Propojení přístupových bodů by mělo být realizováno tak, aby se zaměstnanci nemuseli při příchodu do jiné třídy znovu ručně připojovat k novému přístupovému bodu. Při realizaci vybudování nového wi-fi systému minimálně zasahovat do aktuální infrastruktury počítačové sítě v budově základní školy z důvodu úspory financí. Možnost zakázat žákům přístup na některé webové stránky.

### **7.3 Proměření šíření signálu v budově základní školy**

Pro vytvoření signálové mapy, bylo nejprve nutno změřit, jak jednotlivé zdi tlumí signál. Toto měření bylo provedeno pomocí mnou vlastněného přístupového bodu ZyXEL NWA1123-ACv2 a programu inSSIDer běžícím na notebooku. Postup byl následující. První byl změřen referenční útlum, ve vzdálenosti 1 metr mezi notebookem a přístupovým bodem bez překážky. Tento referenční útlum se pohyboval pro 2,4 GHz okolo -32 dBm. Poté byl přístupový bod umístěn ke zdi v místnosti a v sousední vedlejší místnosti byl ke zdi umístěn notebook s běžícím programem inSSIDer. Program ukázal aktuální útlum signálu procházejícího přes zeď, od tohoto útlumu byl odečten referenční, čímž zůstal výsledný útlum zdi. Půdorysy jednotlivých pater se změřenými útlumy zdí jsou v příloze PI a PII.

### **7.4 Návrh rozmístění přístupových bodů s pomocí signálové mapy**

Změřené útlumy zdí zakreslených do plánu budovy byly poslány na zákaznickou podporu firmy ZyXEL, kde zákazníkům poskytují na vyžádání návrh s rozmístěním přístupových bodů v dané budově včetně simulované signálové mapy. Tyto matematické modely ukázaly navrhované umístění přístupových bodů, modely signálových map jsou

v přílohách P III až P VI. Následně bylo provedeno reálné proměření matematických modelů opět pomocí NWA1123-ACv2. Po proměření bylo zjištěno, že simulovaný počet přístupových bodů lze snížit o dva v horním patře, a o jeden v prvním patře. Důvod snížení v druhém patře je díky faktu, že některé místnosti ve druhém patře získali pokrytí od přístupových bodů nacházejících se v prvním patře přímo pod nimi. Důvod snížení v prvním patře je, že přístupový bod v prvním patře (viz. plán v příloze P I velká místnost v nejvýchodnějším křídle budovy), získal výborné pokrytí od přístupového bodu umístěného přímo nad sebou ve druhém patře. Pro využití maximální rychlosti sítě je výrobcem definován hraniční parametr útlumu -65 dBm, tento útlum byl ve všech místnostech, které bylo požadováno pokrýt signálem, brán při závěrečném proměřování na zřetel. Konečný návrh rozmístění přístupových bodů je v příloze P VII a P VIII.

## 7.5 Výběr a návrh síťových prvků

Protože proměřování matematického návrhu bylo prováděno pomocí mnou vlastněného přístupového bodu NWA1123-ACv2 od firmy ZyXEL a po zjištění, že tato firma vyrábí vyšší řadu přístupových bodů, které je možno centrálně řídit navíc s podobným vysílacím diagramem jako NWA1123-ACv2, bylo rozhodnuto zaměřit realizaci systému na řešení od firmy ZyXEL.

Vlastnost přístupového bodu nechat se centrálně řídit je u firmy ZyXEL obchodně nazývána controller. Pro centrální řízení přístupových bodů je dále potřeba centrálního řídicího prvku. U ZyXELu byly následující dvě možnosti. První bylo pořízení některého z inteligentních kontrolerů bezdrátové sítě LAN s označením NXC. Druhou bylo pořízení některého z inteligentních směrovačů řady USG, zaměřené na účinnou a vysoce výkonnou integrovanou bezpečnostní architekturu společně s možností účinného filtru webového obsahu. Mimo mnoha dalších funkcí zaměřených právě na bezpečnost mají prvky USG také zabudovaný kontroler bezdrátové sítě stejně jako prvky z řady NXC.

Nakonec bylo pro řízení bezdrátové sítě vybráno zařízení z řady USG díky svým univerzálním možnostem použití. Prvky USG se vyrábějí v několika řadách, podle předpokládaných nároků na výkon. Pro potřeby základní školy a předpokládaný počet připojených zařízení byl firmou ZyXEL doporučen směrovač USG 110.

Po zdokumentování současného stavu strukturované kabeláže v budově bylo nutno pořídit 3 přepínače s podporou PoE pro připojení přístupových bodů a dva 24 portové 1 Gbps

přepínače, které nahradili stávající pomalé 100 Mbps přepínače. Veškeré zařízení, které bylo nutno zakoupit, jsou uvedeny v tabulce (Tab. 2).

Tab. 2. Seznam potřebných síťových prvků a materiálu.

zařízení	množství	obecné zařízení
ZyXEL ZyWALL USG110 UTM BUN, Security UTM solution: F	1 ks	směrovač+wi-fi kontoler
dodatečná licence pro připojení 8mi WI-FI přístupových bodů	8 ks	
ZyXEL NWA5123-AC, AP 802.11 ac	10 ks	přístupový bod
ZyXEL GS1900-24e, 24-port Gigabit Web Smart, 802.3az	2 ks	přepínač
ZyXEL GS1900-10HP, 10-port Desktop Gigabit Web Smart switch	3 ks	přepínač
Lan kabeláž (kabel UTP cat. 6)	600 m	
Lišty	110 m	

## 7.6 Návrh bezdrátové sítě a přidělení adres

Pro oddělení přihlašování pro učitele, žáky a hosty bylo rozhodnuto využít inteligentní vlastnost vybraných přístupových bodů, které dokážou vysílat více různých SSID sítí na jednom kanálu s jedinečným heslem. Dále přidělení konkrétní SSID sítě k patřičné VLAN, díky čemuž bude možné řídit případně omezovat jednotlivé přihlášené skupiny. V tabulce (Tab. 3) je rozvržení a přidělení statických IP adres nově použitým zařízením. Všechny přístupové body IP adresy obdrží ze stávajícího školního DHCP serveru.

Tab. 3. Rozvržení IP adres v defaultní síti.

zařízení	IP	maska	umístění
adresa defaultní sítě	172.16.152.0	255.255.255.0	
<b>již přidělené statické IP adresy</b>			
	172.16.152.1	255.255.255.0	
	172.16.152.2	255.255.255.0	
	172.16.152.3	255.255.255.0	
	172.16.152.7	255.255.255.0	
	172.16.152.8	255.255.255.0	
	172.16.152.9	255.255.255.0	
	172.16.152.13	255.255.255.0	
	172.16.152.4	255.255.255.0	
<b>nově přidělené statické IP adresy</b>			
ZyXEL GS1900-24	172.16.152.4	255.255.255.0	poc. ucebna 2. switch
ZyXEL GS1900-10 PoE	172.16.152.5	255.255.255.0	poc. ucebna 1. switch
ZyXEL GS1900-24	172.16.152.10	255.255.255.0	zástupce řed. přízemi
ZyXEL GS1900-10 PoE	172.16.152.11	255.255.255.0	zástupce řed. přízemi
ZyXEL GS1900-10 PoE	172.16.152.12	255.255.255.0	družina
USG110 směrovač	172.16.152.254	255.255.255.0	poc. ucebna

Dále budou v síti použity dvě virtuální sítě VLAN100 pro žáky a VLAN200 pro návštěvy. V tabulce (Tab. 4) je rozvržení adres pro tyto sítě.

Tab. 4. Rozvržení IP adres sítím VLAN.

virtuální síť	síť	maska	address pool	Interface směrovače
VLAN 100 - žáci				
	192.168.200.0	255.255.255.0	192.168.200.20	192.168.200.1
			192.168.200.220	
VLAN 200 - návštěvy				
	192.168.100.0	255.255.255.0	192.168.100.20	192.168.100.1
			192.168.100.240	

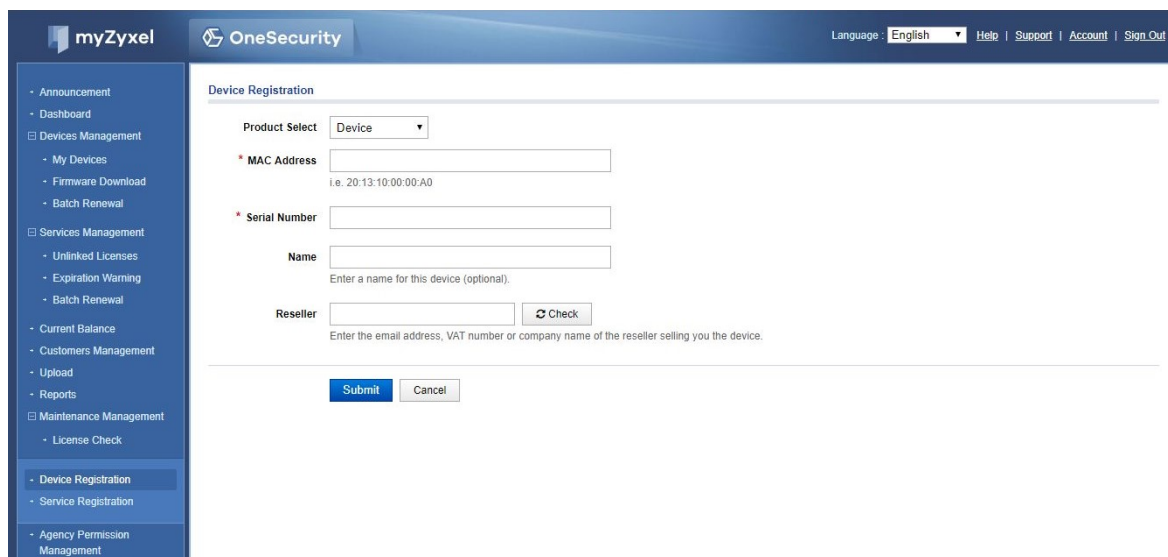
## 8 KONFIGURACE SYSTÉMU

Konfiguraci systému byla započata zprovozněním a nastavením směrovače USG110.

### 8.1 Směrovač USG 110

#### 8.1.1 Registrace směrovače

Pro správný průběh registrace bylo nejprve nutné připojit směrovač přes WAN port do internetu. Dále byla provedena samotná registrace směrovače u výrobce na stránce portal.myZyXEL.com. v menu Device Registration. Bylo požadováno vyplnit MAC adresu směrovače, sériové číslo a vytvořit jméno zařízení.



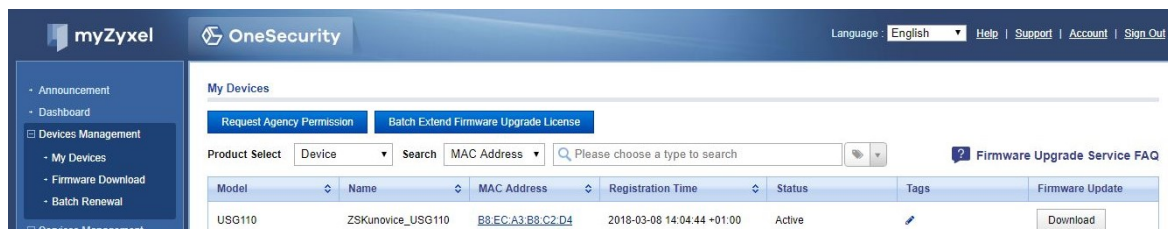
The screenshot shows the 'Device Registration' page on the myZyXel OneSecurity portal. The page has a blue header with the myZyXel logo, OneSecurity branding, and a language dropdown set to English. A navigation menu on the left lists various management options. The main content area contains a registration form with the following fields:

- Product Select:** A dropdown menu currently set to 'Device'.
- \* MAC Address:** A text input field with a placeholder example 'i.e. 20:13:10:00:00:A0'.
- \* Serial Number:** A text input field.
- Name:** A text input field with a note: 'Enter a name for this device (optional)'.
- Reseller:** A text input field with a 'Check' button and a note: 'Enter the email address, VAT number or company name of the reseller selling you the device.'

At the bottom of the form are 'Submit' and 'Cancel' buttons.

Obr. 15. Registrace směrovače.

Po potvrzení je v položce Device Management > My Devices možné zobrazit zaregistrovaná zařízení. V pravém sloupci pod ikonou Download je možnost stáhnout aktuální firmware, bylo provedeno stažení aktuálního V4.30.



The screenshot shows the 'My Devices' page on the myZyXel OneSecurity portal. The page has a blue header and a navigation menu on the left. The main content area shows a table of registered devices. The table has the following columns: Model, Name, MAC Address, Registration Time, Status, Tags, and Firmware Update. There are also buttons for 'Request Agency Permission' and 'Batch Extend Firmware Upgrade License' at the top of the table.

Model	Name	MAC Address	Registration Time	Status	Tags	Firmware Update
USG110	ZSKunovice_USG110	B8:EC:A3:B8:C2:D4	2018-03-08 14:04:44 +01:00	Active		Download

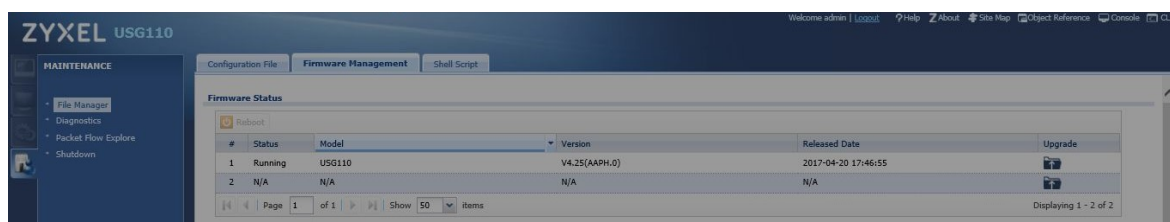
Obr. 16. Náhled registrovaných zařízení.



### 8.1.2 Konfigurace směrovače

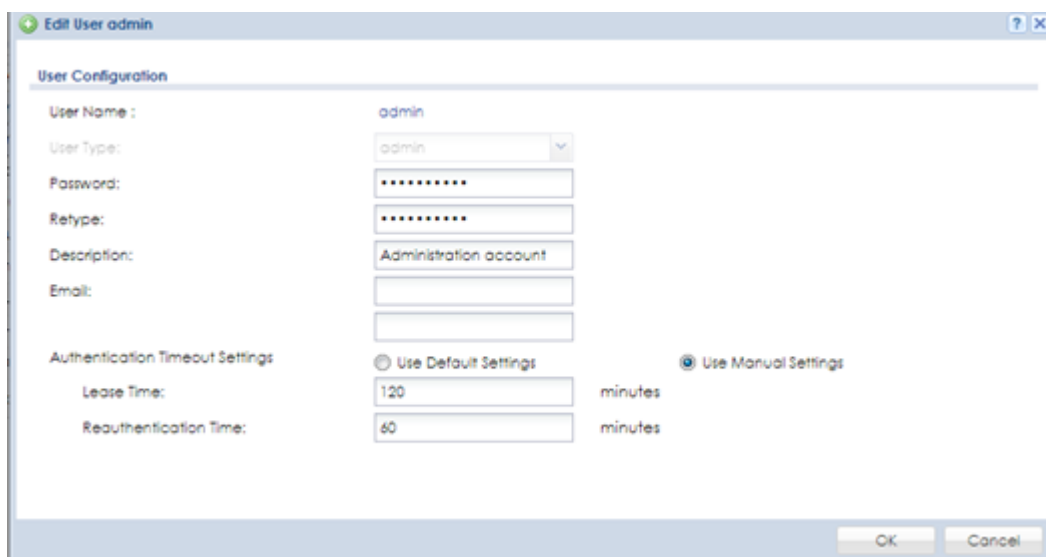
Směrovač byl úspěšně zaregistrován a nyní bylo možno přejít k samotné konfiguraci. K LAN portu směrovače byl připojen přepínač, do tohoto přepínače byl připojen počítač. Směrovač mněl ve výchozím režimu nastavenou IP adresu 192.168.1.1. Proto připojenému počítači bylo nutno nastavit statickou adresu ze sítě 192.168.1.0. Pomocí připojeného počítače bylo možno se přihlásit do webového rozhraní směrovače. Po přihlášení bylo nejprve nutno projít inicializační wizard, po jeho dokončení bylo zpřístupněno webové rozhraní s menu.

Nejprve byla nahrána nová verze firmware. V menu Maintenance > File Manager > Firmware Management > Local Firmware.



Obr. 17. Aktualizace firmware.

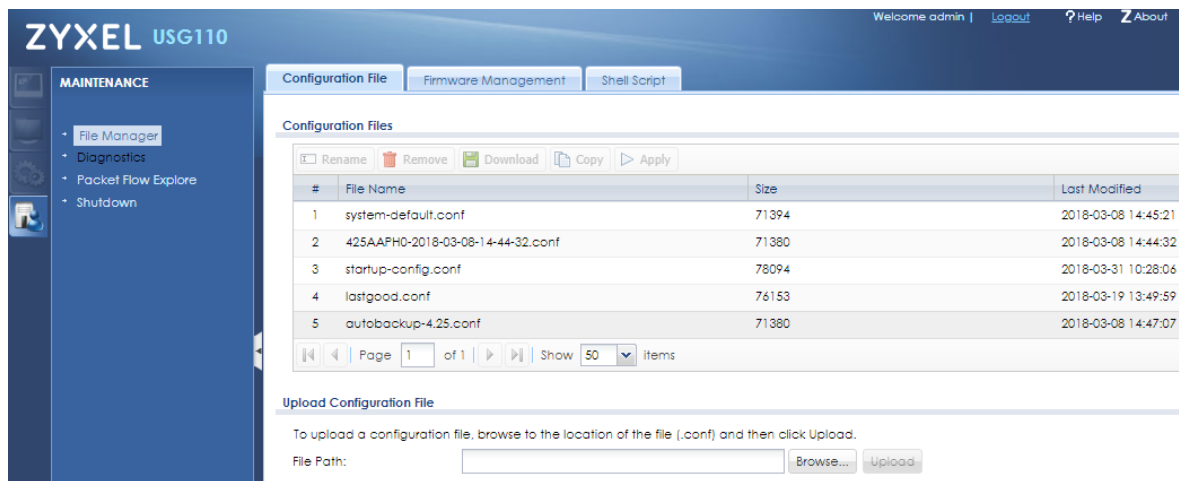
Poté bylo změněno heslo pro přihlášení administrátora. V menu se přešlo do Configuration > Object > User/Group > User bylo vybráno k editaci administrátorské jméno admin.



Obr. 18. Změna hesla u administrátora.

Místní správce spravuje již několik přepínačů ZyXEL USG 110. Aby mu byla ušetřena práce s konfigurací provozu pro drátovou počítačovou síť, byl nahrán jeho soubor startup-

config.conf. Nahrání startup souboru bylo provedeno v menu Maintenance > File Manager > Configuration File.



Obr. 19. Nahrání nového startup konfiguračního souboru.

Na směrovači je k dispozici 5 fyzických LAN portů, je možno k jednomu interface přiřadit více portů. Nastavení bylo provedeno v menu Configuration > UTM Profile > Port Role. Pro naše potřeby byly nastaveny dva porty k interface lan1.

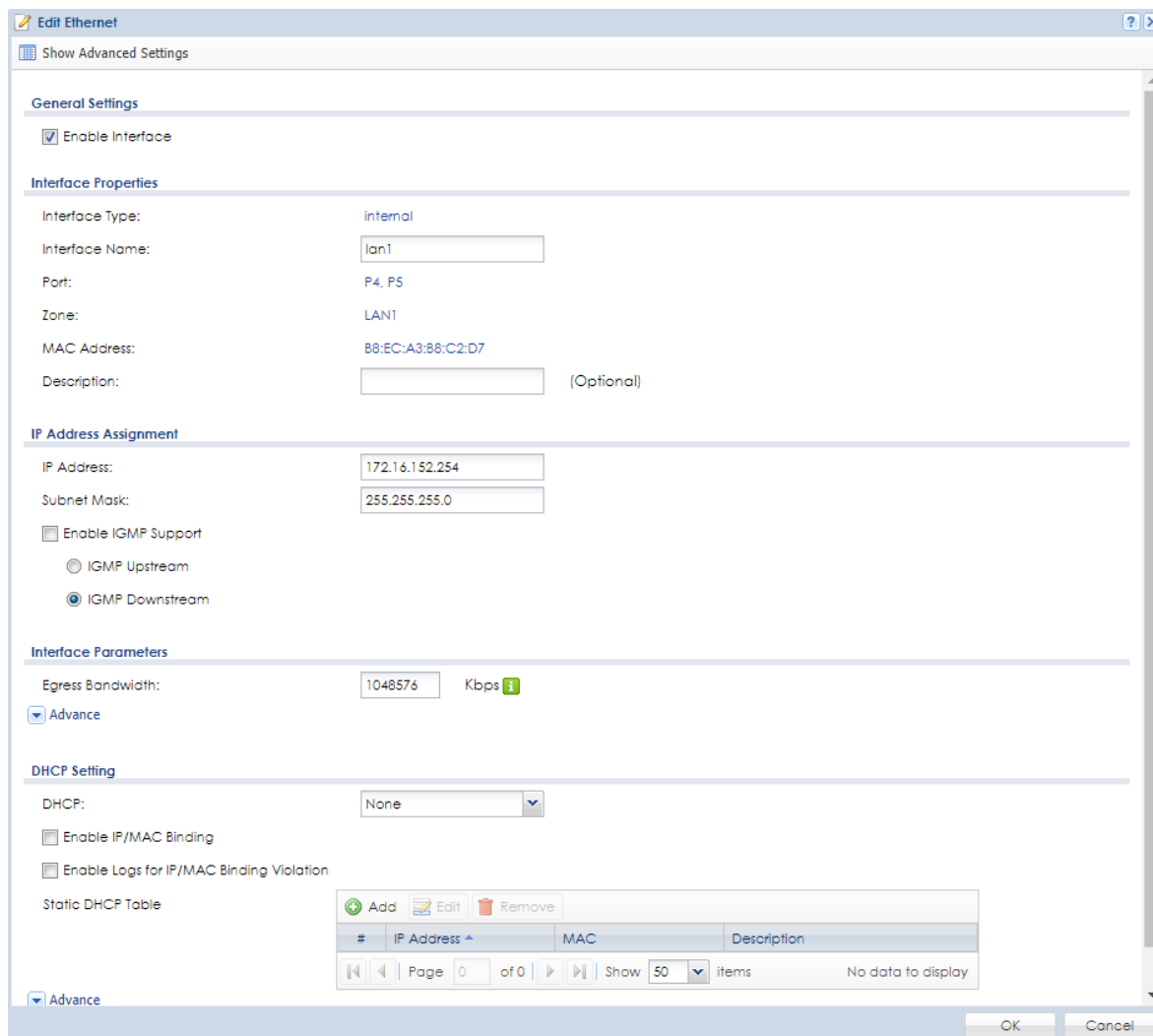


Obr. 20. Přiřazení portů k interface.

Dále byla nastavena v IP adresa interface lan1. Pro nastavení bylo nutno přejít do záložky Ethernet > Edit lan1. Dle výše vytvořeného návrhu tabulka (Tab. 3), byla přidělena statická IP adresa 172.16.152.254.

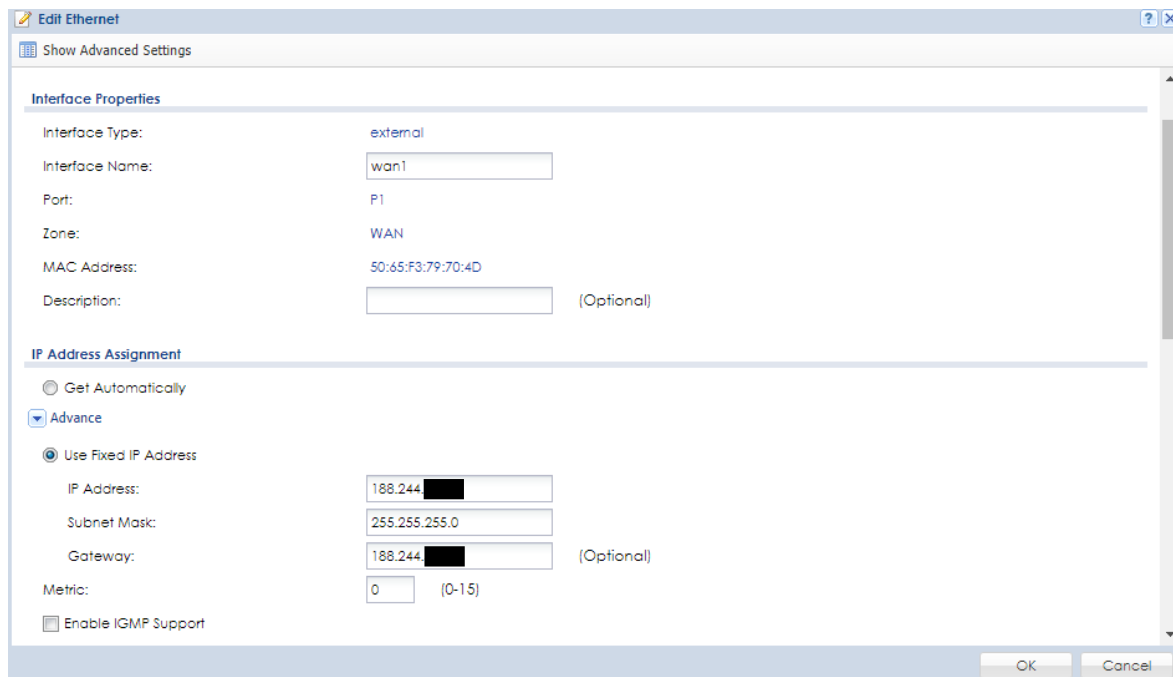
DHCP na interface lan1 bylo nutno zakázat, protože místní správce vyžaduje, aby připojeným přístupovým bodům byly přidělovány IP adresy ze sítě, kterou si dříve zvolil (z rozsahu neveřejných adres třídy B 172. 16. 152. 0), jsou tyto adresy přidělovány lokálním

DHCP serverem. Nastavení bylo potvrzeno tlačítkem ok a stiskem Apply uloženo do startup-config. Tento krok je zobrazen na obrázku (Obr. 21).



Obr. 21. Přidělení IP adresy k interface lan 1.

Dále bylo provedeno nastavení interface WAN. Pro toto nastavení se, zůstalo v položce menu Ethernet a zvolila se editace WAN1. IP adresa byla nastavena 188.244.x.x adresa brány, byla udaná poskytovatelem internetu 188.244.x.x



The screenshot shows the 'Edit Ethernet' configuration window. It is divided into two main sections: 'Interface Properties' and 'IP Address Assignment'. In the 'Interface Properties' section, the following fields are visible: 'Interface Type' is set to 'external'; 'Interface Name' is 'wan1'; 'Port' is 'P1'; 'Zone' is 'WAN'; 'MAC Address' is '50:65:F3:79:70:4D'; and 'Description' is an empty field with '(Optional)' next to it. The 'IP Address Assignment' section has two radio buttons: 'Get Automatically' (unselected) and 'Use Fixed IP Address' (selected). Under 'Use Fixed IP Address', there is a dropdown menu set to 'Advance'. Below this, the following fields are visible: 'IP Address' is '188.244.███'; 'Subnet Mask' is '255.255.255.0'; 'Gateway' is '188.244.███' with '(Optional)' next to it; and 'Metric' is '0' with '(0-15)' next to it. At the bottom of the window, there is a checkbox for 'Enable IGMP Support' which is unchecked, and 'OK' and 'Cancel' buttons.

Obr. 22. Konfigurace WAN interface.

Pro filtrování provozu na bezdrátové síti, bylo zvoleno využití chytré vlastnosti přístupových bodů, které dokáží tagovat komunikaci na základě přihlášení klientů do SSID sítě. SSID sítě jsou vysílány na každém přístupovém bodě tři: **ZS** pro zaměstnance, **zaci** pro žáky a **navstevy**. Celkem tedy bylo potřeba tří VLAN. První byla využita defaultní a další dvě bylo nutno vytvořit. Pro přidání nových VLAN bylo nutno se přesunout v menu Interface > VLAN. Volbou Add se otevře dialogové okno pro vytvoření nové VLAN.

**Add VLAN**

Hide Advanced Settings

**Interface Properties**

Interface Type: general

Interface Name: vlan200

Zone: VLAN

Base Port: lan1

VLAN ID: 200 (1-4094)

**Advance**

Priority Code: 0 (0-7)

Description: VLANverejnost (Optional)

**IP Address Assignment**

Get Automatically

**Advance**

DHCP Option 60: (Optional)

Use Fixed IP Address

IP Address: 192.168.201.1

Subnet Mask: 255.255.255.0

OK Cancel

Obr. 23. Vytvoření VLAN200.

Byla definována nová VLAN s ID 200, tato VLAN slouží pro tagování připojených návštěv. Base port byl vybrán lan1. Dále bylo nutno vstoupit do rozšířeného nastavení pomocí kliku na Advance.

**Advance**

DHCP Option 60: (Optional)

Use Fixed IP Address

IP Address: 192.168.200.1

Subnet Mask: 255.255.255.0

Gateway: (Optional)

Metric: 0 (0-15)

Enable IGMP Support

IGMP Upstream

IGMP Downstream

**Interface Parameters**

Egress Bandwidth: 1048576 Kbps

**Advance**

Ingress Bandwidth: 1048576 Kbps

MTU: 1500 Bytes

Obr. 24. Přiřazení IP adresy interface.

Na základě návrhu v tabulce (Tab. 4) byla nastavena IP adresa interface 192.168.200.1 a níže definován rozsah 200 IP adres od adresy 192.168.200.20, které bude DHCP server přidělovat zařízením v rámci VLAN200.

The screenshot shows the 'DHCP Setting' configuration page. The 'DHCP' checkbox is checked. The 'IP Pool Start Address' is set to 192.168.200.20, and the 'Pool Size' is 200. The 'First DNS Server (Optional)' is set to ZyWALL, and the other DNS servers are set to None. The 'First WINS Server (Optional)' and 'Second WINS Server (Optional)' are empty. The 'Default Router' is set to vian IP. The 'Lease Time' is set to 14 days.

DHCP:	<input checked="" type="checkbox"/>	DHCP Server	
IP Pool Start Address:		192.168.200.20	Pool Size: 200
First DNS Server (Optional):		ZyWALL	
Second DNS Server (Optional):		None	
Third DNS Server (Optional):		None	
First WINS Server (Optional):			
Second WINS Server (Optional):			
Default Router:		vian IP	
Lease Time:	<input type="radio"/> infinite	<input checked="" type="radio"/> 14 days	<input type="text"/> hours (Optional) <input type="text"/> minutes (Optional)

Obr. 25. Nastavení DHCP pro VLAN200.

Stejným způsobem byla přidána a nastavena VLAN100, jenom byly použity jiné IP adresy. IP adresy byly vybrány opět na základě návrhu v tabulce (Tab. 4) IP adresa interface 192.168.100.1 a rozsah pro DHCP server 200 adres počínaje adresou 192.168.100.20.

### 8.1.3 Konfigurace kontroleru bezdrátové sítě LAN na směrovači

Jak bylo uvedeno v kapitole 7. 6 každý přístupový bod bude vysílat 3 SSID sítě. Aby bylo možné vytvořit a nastavit jejich parametry, bylo nejdříve nutné vytvořit 3 bezpečnostní profily. Nastavení je v menu pod Configuration > Object > AP Profile. Nejdříve byly vytvořeny 3 bezpečnostní profily v záložce menu SSID > Security List klikem na ikonu Add se otevřelo dialogové okno pro vytvoření nového profilu.

První byl nastaven profil pro žáky. Jméno bezpečnostního profilu nastaveno ZACI\_sl, bezpečnostní mód wpa2, klíč pro přihlášení xxx, u zbylých vlastností byly ponechány výchozí hodnoty.

**Edit Security Profile ZACI\_sl**

**General Settings**

Profile Name: ZACI\_sl

Security Mode: wpa2

**Fast Roaming Settings**

802.11r

**Radius Settings**

Radius Server Type: Internal

Proxy by controller directly

**MAC Authentication Setting**

MAC Authentication

Auth. Method: default

Delimiter (Account): dash (-)

Case (Account): upper

Delimiter (Calling Station ID): dash (-)

Case (Calling Station ID): upper

**Authentication Settings**

802.1X

Auth. Method: default

ReAuthentication Timer: 0 (30~30000 seconds, 0 is unlimited)

PSK

Pre-Shared Key: [REDACTED]

Cipher Type: auto

Idle timeout: 300 (30-30000 seconds)

Group Key Update Timer: 3600 (30-30000 seconds)

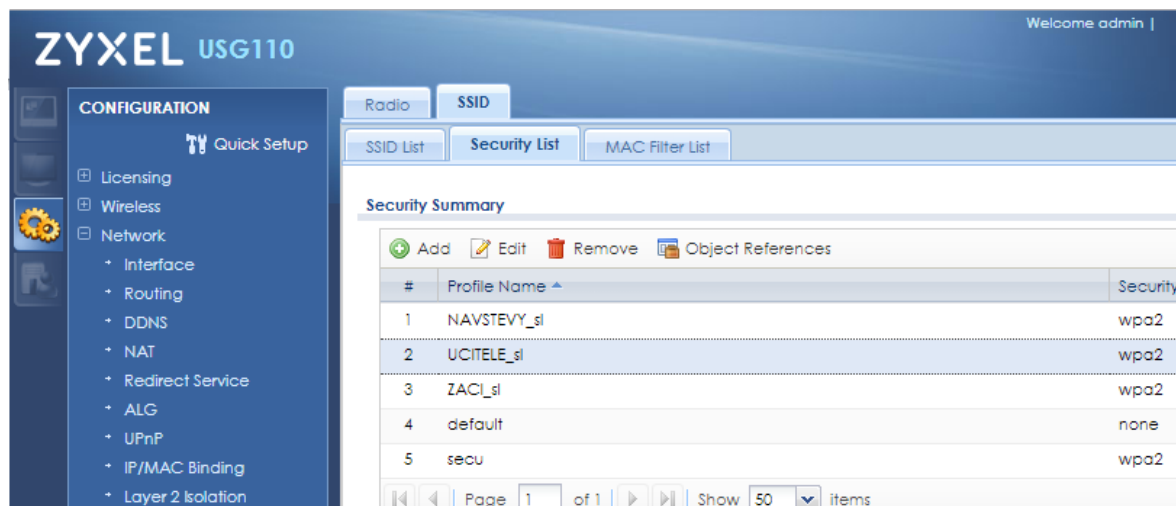
Management Frame Protection

Optional  Required

OK Cancel

Obr. 26. Vytvoření bezpečnostního profilu.

Stejným způsobem byly nastaveny bezpečnostní profily pro učitele s názvem UCITELE\_sl pro návštěvy s názvem NAVSTEVY\_sl. Přehled profilu je na obrázku (Obr. 27).



Obr. 27. Vytvořené bezpečnostní profily.

Po vytvoření bezpečnostních profilů bylo možno přejít do záložky SSID list pro vytvoření SSID profilů. První byl vytvořen SSID profil pro žáky se jménem ZACI\_ssaid. SSID, bylo nastaveno zaci, tomuto profilu byl přiřazen bezpečnostní profil ZACI\_sl, protože na bezdrátové síti není plánována žádná VoIP komunikace či video konference, bylo QoS ponecháno ve výchozím stavu WMM (Wi-fi Multi Media). V tomto stavu je řízení priority ponecháno na inteligentím vyhodnocování provozu směrovačem.

Aby byla připojovaným klientům ponechána větší volnost, byla vybrána volba Band Select: standard. Maximální počet klientů, kteří se mohou připojit přes pásmo dle vlastní preference, byl nastaven dle doporučení výrobce 15. Poměr připojených zařízení schopných komunikovat ve dvojnásobném pásmu byl nastaven dle doporučení výrobce 4:1.

Pro umožnění snadného filtrování provozu, bylo nastaveno tagování komunikace přihlášených uživatelů pod profilem ZACI\_ssaid identifikačním číslem VLAN 100. Nastavené popisované vlastnosti je možno vidět na obrázku (Obr. 28).

Dále byly vytvořeny SSID profily pro učitele UCITELE\_ssaid a pro návštěvy NAVSTEVEY\_ssaid. SSID profil pro učitele byl vytvořen prakticky stejně jako žákovský s tím rozdílem, že bezpečnostní profil byl přiřazen UCITELE\_sl a SSID bylo změněno na ZS. Taktéž vytvoření SSID profilu pro návštěvy bylo totožné, pouze SSID bylo změněno na navstevy a bezpečnostní profil byl přiřazen NAVSTEVEY\_sl.



Edít SSID Profile ZACI\_ssid

Create new Object ▾

Profile Name: ZACI\_ssid

SSID: zaci

Security Profile: ZACI\_sl ▾

MAC Filtering Profile: disable ▾

QoS: WMM ▾

Rate Limiting (Per Station Traffic Rate) ⓘ

Downlink: 0 mbps (0~160, 0 is unlimited) ▾

Uplink: 0 mbps (0~160, 0 is unlimited) ▾

Band Select: standard ▾

Stop Threshold 15 Station (10~20)

Balance Ratio 4:1 (5GHz : 2.4GHz) ▾

Forwarding Mode: Local bridge ▾

VLAN ID: 100 (1~4094)

Hidden SSID

Enable Intra-BSS Traffic blocking

Schedule SSID ⓘ

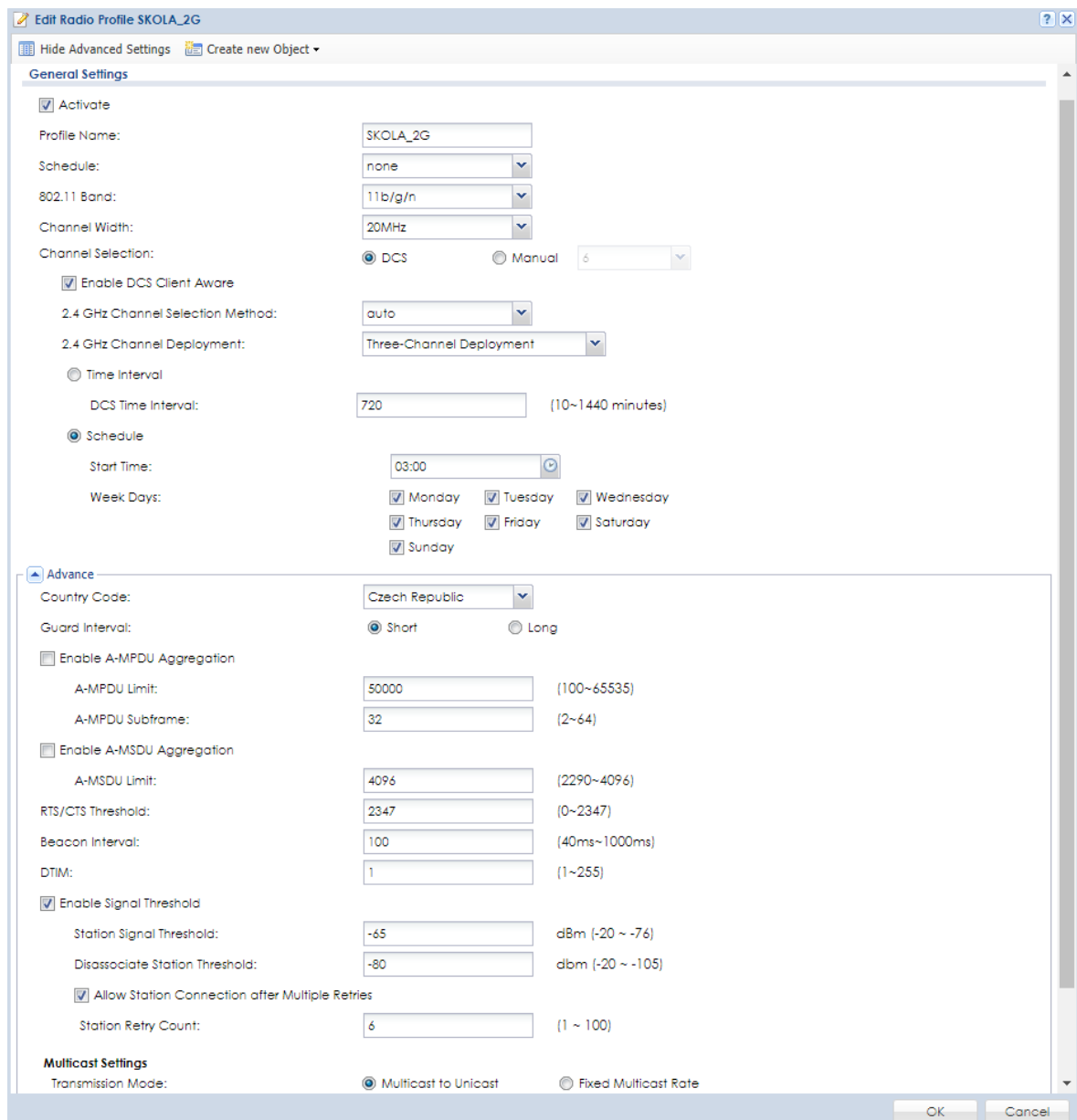
OK Cancel

Obr. 28. Vytvoření bezpečnostního profilu pro žáky.

Dále byly v záložce menu Radio vytvořeny dva rádiové profily.

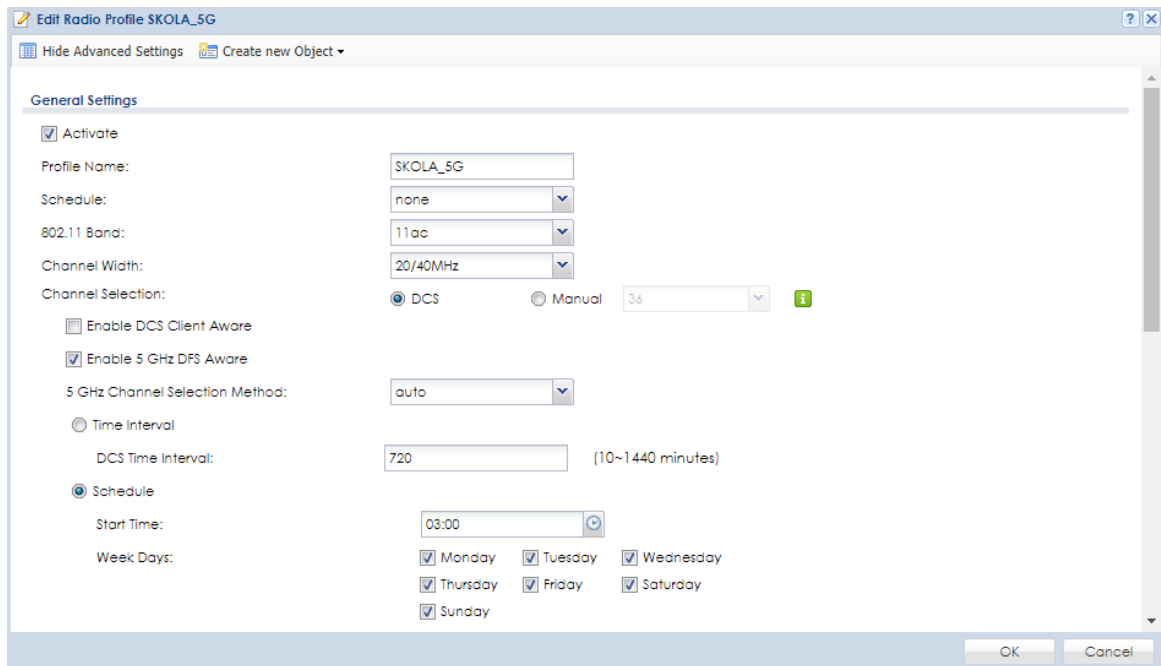
První byl vytvořen rádio profil SKOLA\_2G na obrázku (Obr. 29), tento profil slouží pro specifikaci vysílání na pásmu 2,4 GHz. Standardy byly nastaveny 11b/g/n, šířka kanálu byla nastavena na 20MHz, výběr kanálů byl nastaven dynamicky povolením volby DCS. Zakliknutím volby Enable DCS Client Aware je brán ohled na připojené klienty v době skenování. Před zahájením skenování musí být všichni klienti odpojeni, bude-li nějaký klient připojen, skenování nebude provedeno. Volbou Schedule byl nastaven čas skenování na 03.00 ráno každý den v týdnu. V záložce Advance byly nastaveny parametry pro práh síly signálu, síla signálu stanice potřebná pro připojení k přístupovému bodu byla nastavena -65 dBm a minimální síla signálu po jejímž překročení bude stanice odpojena byla nastavena na -80 dBm, dále bylo povoleno Allow Station Connection after Multiple Retries, definující po jakém počtu neúspěšných pokusů se může klient ke stanici znovu

pokusit připojit. Multicast Setting byl nastaven na Multicast to Unicast, zbylé hodnoty byly ponechány ve výchozím nastavení [24].



Obr. 29. Vytvoření Radio profilu SKOLA\_2G.

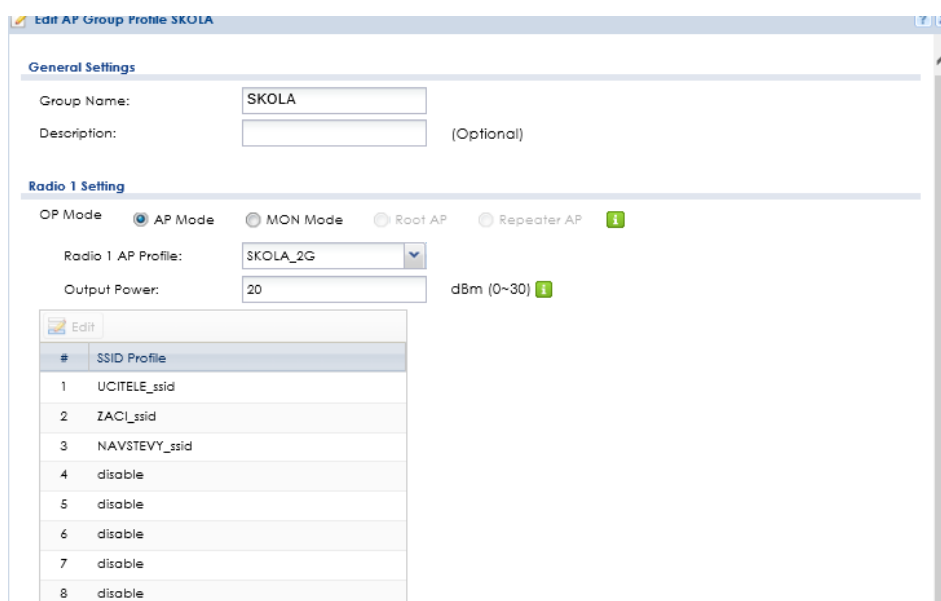
Následně byl vytvořen rádiový profil SKOLA\_5G na obrázku (Obr. 30), tento profil slouží pro specifikaci vysílání na pásmu 5 GHz. Byl povolen standard 802.11ac, díky velkému počtu kanálů, které se nepřekrývají a málo zarušenému okolí na 5GHz byla pro rychlejší přenos nastavena šířka kanálu 20/40MHz. Dále byla aktivována funkce DFS Aware. Zbylé vlastnosti byly nastaveny stejně jako u rádio profilu ŠKOLA\_2G.



Obr. 30. Vytvoření Radio profilu SKOLA\_5G.

Poté bylo nutné přejít v menu do záložky Wireless > AP Management > AP Group a vytvořit novou skupinu s názvem ŠKOLA. Tato skupina sdružuje nastavené parametry z rádio profilů a SSID profilů. Jeden přístupový bod může patřit do jedné skupiny.

OP Mode je požadováno, aby přístupové body fungovaly v běžném režimu, kdy přijímají data od bezdrátových klientů a předávají je dále na bránu, proto byl zvolen AP Mode. Dále byl rádiu 1 přeřazen AP profil SKOLA\_2G a maximální výkon 20dBm. Rádio 2 bylo nastaveno stejně, jen byl přiřazen AP profil SKOLA\_5G.



Obr. 31. Nastavení AP Group SKOLA, část 1.

**Radio 2 Setting**

OP Mode  AP Mode  MON Mode  Root AP  Repeater AP

Radio 2 AP Profile: SKOLA\_5G

Output Power: 20 d8m (0~30)

#	SSID Profile
1	UCITELE_ssid
2	ZAC_ssid
3	NAVSTEVY_ssid
4	disable
5	disable
6	disable
7	disable
8	disable

**VLAN Settings**

Force Overwrite VLAN Config

Management VLAN ID: 1 (1~4094)

As Native VLAN

**Port Settings**

Model Specific Setting: nwa5301-nj

**Port Setting**

#	Status	Port	PVID
1		uplink	n/a
2		lan1	1
3		lan2	1
4		lan3	1

Page 1 of 1 | Show 50 items | Displaying 1 - 4 of 4

**VLAN Configuration**

#	Status	Name	VID	Member
1		vlan0	1	lan1,lan2,lan3

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

**Load Balancing Setting**

Enable Load Balancing

Mode: By Station Number

Max Station Number: 25 (1~127)

Dissociate station when overloaded

Obr. 32. Nastavení AP Group ŠKOLA, část 2.

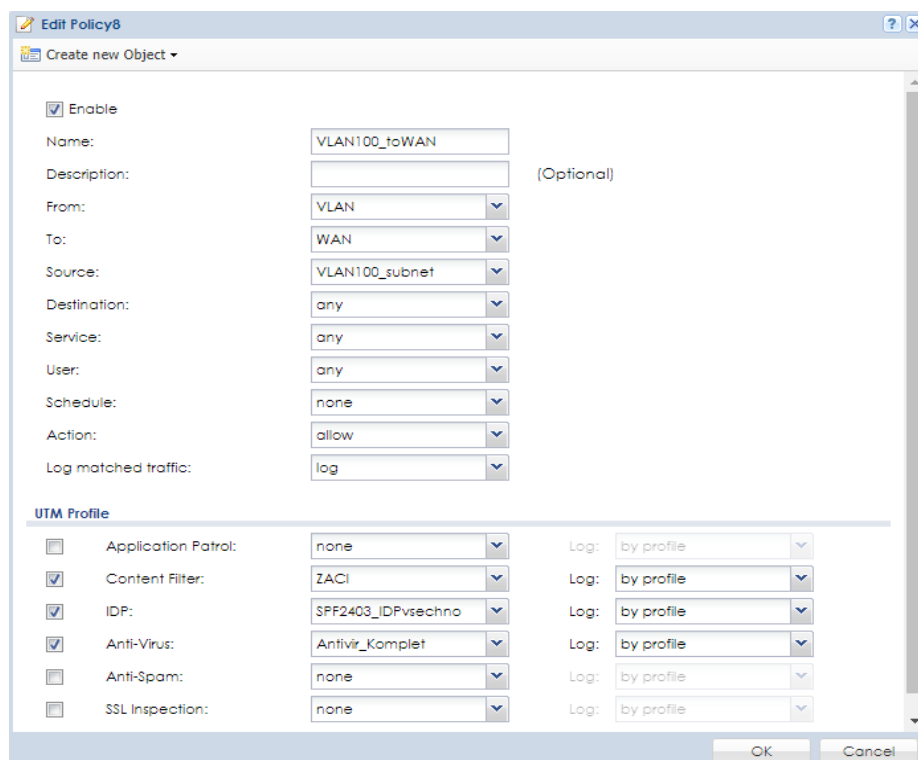
Pro vyvažování byl použit mód vyvažování podle počtu připojených stanic. Mód začne být aplikován po překročení 25 připojených klientů na všechny další klienty usilující o připojení.

#### 8.1.4 Nastavení filtrace obsahu pro žáky

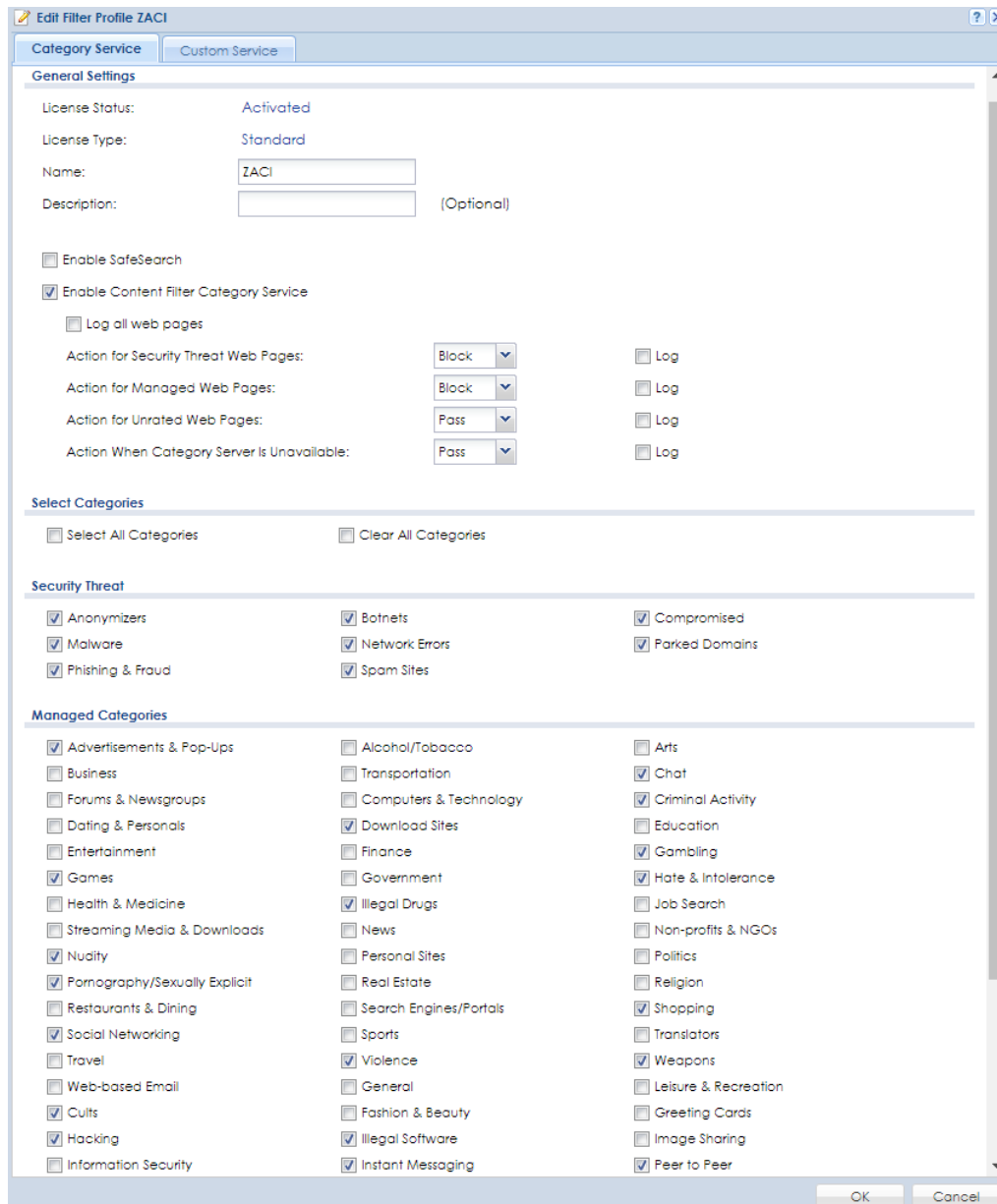
V požadavcích definovaných vedením základní školy byla požadována filtrace obsahu webových stránek pro žáky. Filtrace byla nastavena, na všechny přihlášené uživatele do

SSID zaci. Postup byl následující. Nejprve bylo nutno vytvořit profil. V menu Configuration > UTM Profile > Content Filter > Profile v části Profile Management byl vytvořen nový profil ZACI. Pro zapnutí filtru bylo nutno zvolit Enable Content Filter Category Service. Filtr obsahu je rozdělen na dvě části, bezpečnostní hrozby a spravované kategorie. Položky v sekci bezpečnostní hrozby byly vybrány všechny, protože do těchto sekcí jsou řazeny vyloženě nebezpečné webové stránky ohrožující operační systém na počítači. V sekci spravované kategorie byl vybráním určitých kategorií zakázán přístup k určitým webovým stránkám, které do těchto kategorií spadají. Například vybráním kategorie games bude odepřen přístup všem požadavkům o připojení na webové stránky s online hrami.

Jakmile bylo nastavení profilu ZACI dokončeno, bylo nutno tento profil aplikovat pro příslušný síťový provoz. To se provedlo v sekci Security Policy > Policy Control, zde se spravují a vytváří politiky. Byla vytvořena nová s názvem VLAN100\_toWAN. Položky From a To definují směr, ve kterém má být provoz filtrován, položka Source definuje VLAN v rámci které bude provoz filtrován, v položce Content Filter byl vybrán profil ZACI s nastaveným filtrem obsahu, dále bylo možno zapnout službu antivirus, ten je na směrovači nabízen, nicméně je pro dlouhodobější používání zpoplatněný, zdarma je pouze na 365 dní od zaregistrování směrovače.



Obr. 33. Vytvoření nové politiky pro filtrování obsahu.



Obr. 34. Nastavení filtru webového obsahu pro žáky.

### 8.1.5 Další možnosti centrálního ověřování uživatelů

V případě, že by bylo požadováno zvýšené opatření při ověřování uživatelů, jsou například možné následující dvě možnosti.

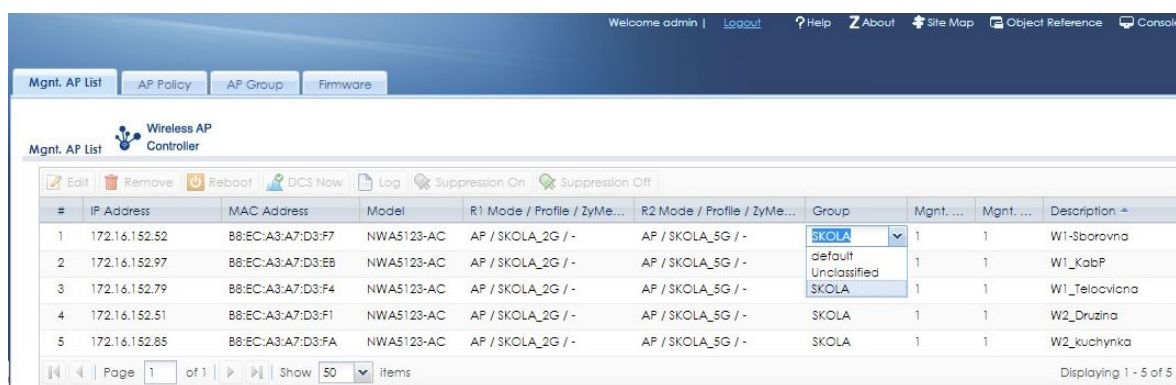
- a) Kontrola připojených zařízení na základě předem známé MAC adresy. Systém by fungoval tak, že odepře přístup všem zařízením, jejichž MAC adresa není zaznamenána v databázi. Toto nastavení lze najít v Configuration > Object > AP profile > SSID > MAC Filter List

- b) Ověřování uživatelů pomocí předem vytvořeného uživatelského jména a hesla. Postup by byl obecně následovný. Nejprve by bylo nutno vytvořit novou webovou autentizační politiku v menu Configuration > Web Authentication > General, dále vybrat Enable Web Authentication pro web authentication. Poté v Object > User/Group > User nechat přidat jednotlivé uživatele spolu s jejich hesly.

### 8.1.6 Oživení přístupových bodů v systému

Nejprve byl připojen k přepínači první přístupový bod NWA5123-AC. Nejdříve přístupový bod problikával zeleno oranžově, to značilo, že vyhledává nadřazený řídicí kontroler, po chvíli začal problikávat přerušovaně červeně, což informovalo o automatické aktualizaci firmware. Jakmile začala kontrolka svítit trvale zeleně, znamená to, že aktualizace firmware byla dokončena a přístupový bod započal vysílat. Poté bylo nutno opět se přihlásit na směrovač USG110.

Pro zajištění přehlednosti po přidání všech přístupových bodů ke kontroleru byl každému nově zjištěnému přístupovému bodu nastaven popisec popisující umístění přístupového bodu v budově. Ke konfiguraci se skrz menu dostalo následující cestou Configuration > Wireless > AP Management > Mgnt. AP list> pro editaci dvojklikem na nově zobrazený přístupový bod. Bylo změněno description a přiřazena nová skupina SKOLA. V této skupině jsou zahrnuté všechny výše předdefinované funkce pro rádiové vysílání 5GHz i 2,4GHz.

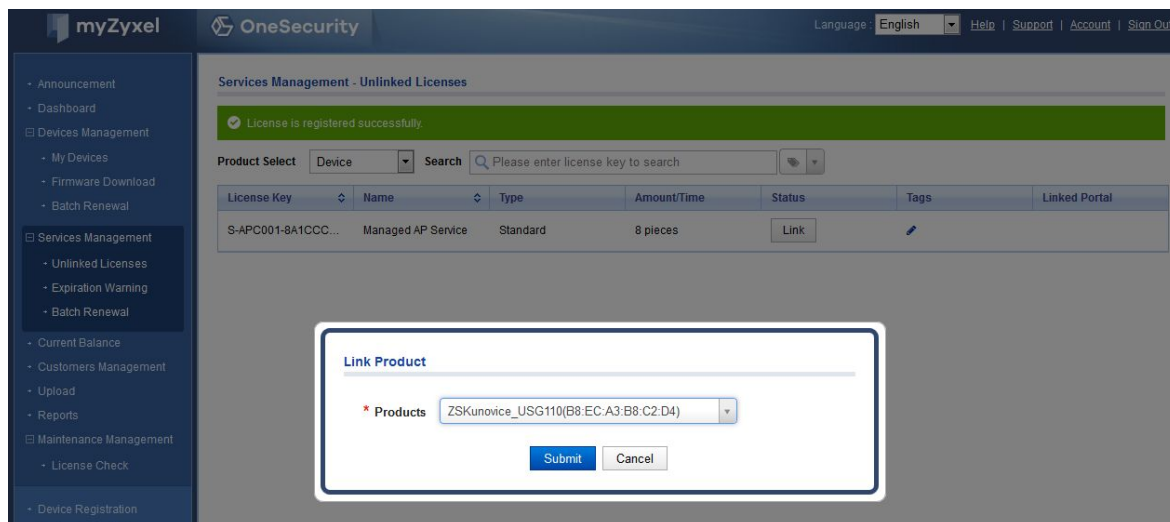


#	IP Address	MAC Address	Model	R1 Mode / Profile / ZyMe...	R2 Mode / Profile / ZyMe...	Group	Mgnt. ...	Mgnt. ...	Description
1	172.16.152.52	B8:EC:A3:A7:D3:F7	NWA5123-AC	AP / SKOLA_2G / -	AP / SKOLA_5G / -	SKOLA	1	1	W1-Sborovna
2	172.16.152.97	B8:EC:A3:A7:D3:E8	NWA5123-AC	AP / SKOLA_2G / -	AP / SKOLA_5G / -	default	1	1	W1_KabP
3	172.16.152.79	B8:EC:A3:A7:D3:F4	NWA5123-AC	AP / SKOLA_2G / -	AP / SKOLA_5G / -	Unclassified	1	1	W1_Telocvicna
4	172.16.152.51	B8:EC:A3:A7:D3:F1	NWA5123-AC	AP / SKOLA_2G / -	AP / SKOLA_5G / -	SKOLA	1	1	W2_Druzina
5	172.16.152.85	B8:EC:A3:A7:D3:FA	NWA5123-AC	AP / SKOLA_2G / -	AP / SKOLA_5G / -	SKOLA	1	1	W2_kuchynka

Obr. 35. Přiřazení nově připojeného přístupového bodu do skupiny.

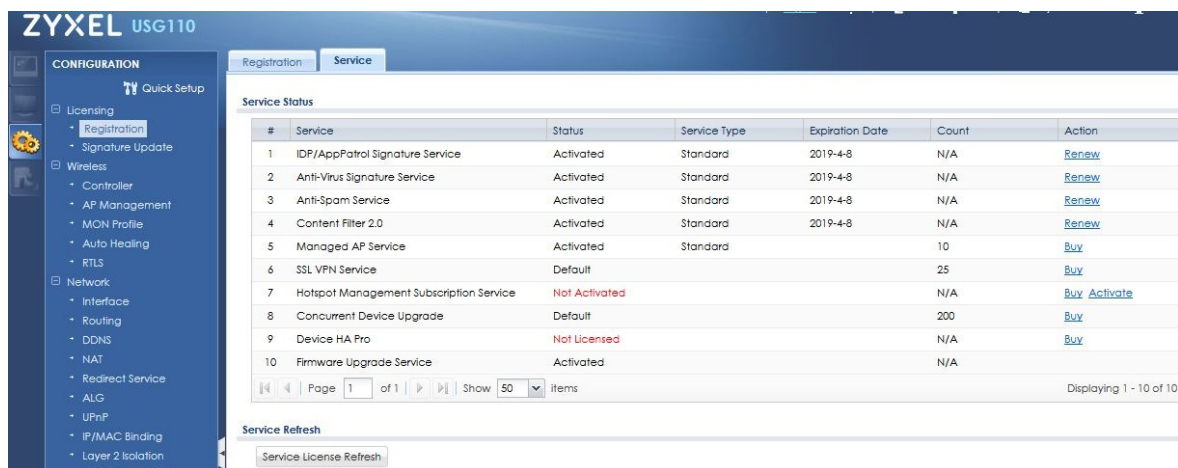
Aby bylo možno vidět a spravovat v systému všechny připojené přístupové body, bylo nutno si dokoupit licence. V základním stavu totiž systém umožňuje spravovat pouze první dva připojené přístupové body.

Pro zaregistrování licence bylo nutno se přihlásit do portálu myZyXEL.com, přejít v menu do Services Management > Unlinked Licenses. Byla zobrazena rozšiřující licence na 8 přístupových bodů. Tato licence byla přiřazena k zařízení ZS\_KunoviceUSG110.



Obr. 36. Rozšíření licence pro více přístupových bodů na myZyXEL.com.

Aby přepínač USG\_110 identifikoval nově přidanou licenci, bylo nutno aktualizovat informace o licencích. Jak je vidět na obrázku (Obr. 35), toto se provedlo v menu Configuration > Licencing > Registration > Service dvojklikem na ikonu Service License Refresh.



Obr. 37. Refresh licencí na směrovači USG 110.

### 8.1.7 Nastavení DHCP

Aby jednotlivé přístupové body zjistili adresu jejich řídicího kontroleru běžícím na směrovači USG 110 s OS 4.30, bylo nutno na školním serveru přidat do DHCP serveru záznam Capwap 138, ten má v sobě uloženou ip adresu interface směrovače na kterém běží



kontroler přístupových bodů. Capwap záznam je možno přidat, jednak přes grafické menu nebo pomocí příkazového řádku. Přes menu je postup následující: otevřít okno pro správu DHCP serveru, pravým klikem na IPv4 > Nastavit předdefinované možnosti, zde se přidá Capwap záznam.

Pomocí příkazového řádku je nutno použít následující posloupnost příkazů:

```
system32>netsh
```

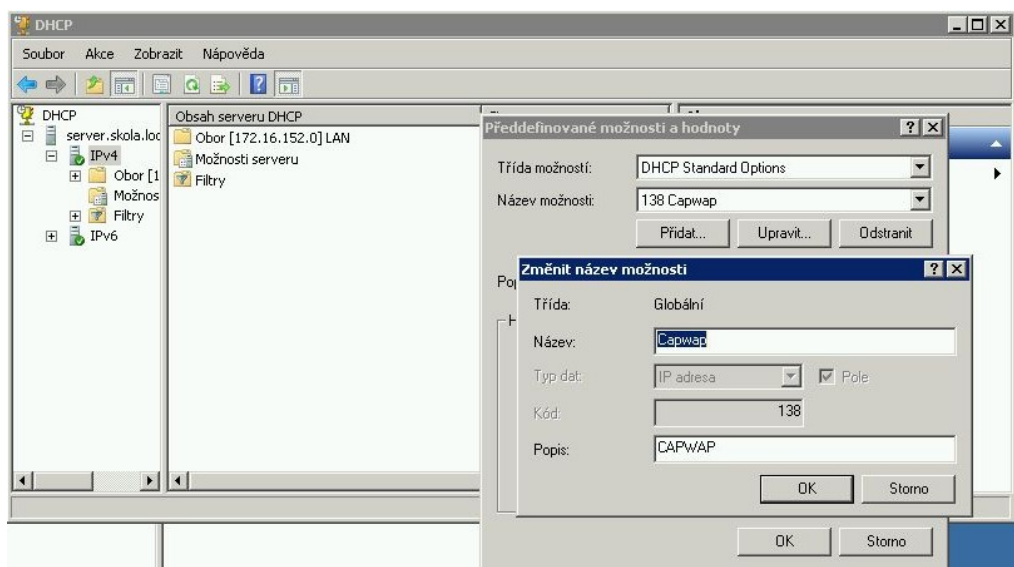
```
netsh>dhcp
```

```
netsh dhcp>server WW<server_machine_name>
```

```
netsh dhcp>add optiondef 138 Capwap IPADDRESS 1 comment=CAPWAP
```

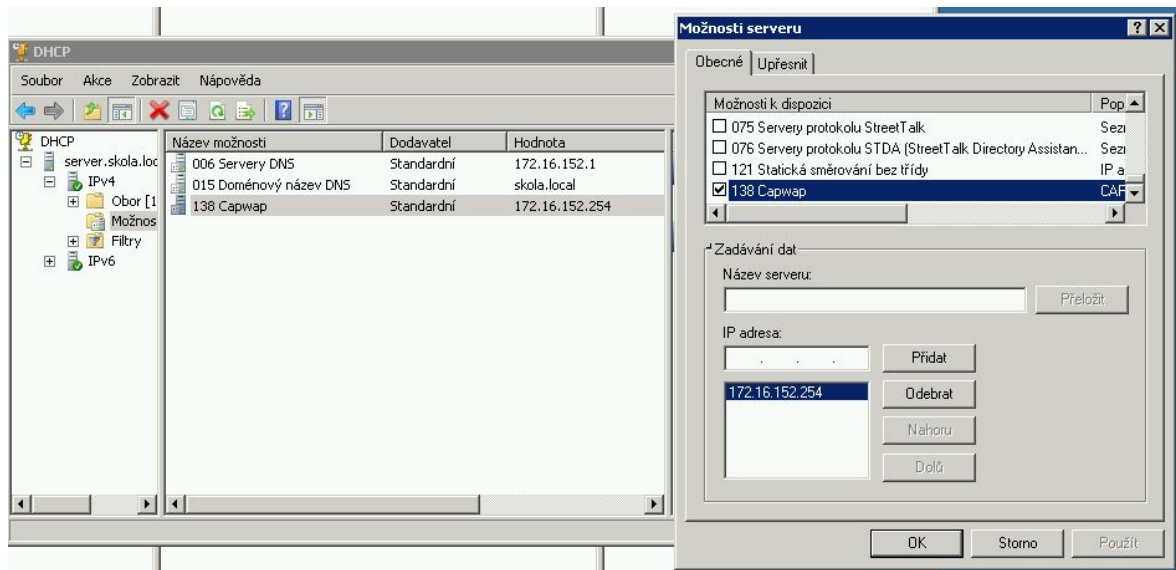
```
netsh dhcp>set optionvalue 138 IPADDRESS <A.B.C.D> <E.F.G.H>
```

```
netsh dhcp>show optiondef
```



Obr. 38. Vytvoření Capwap záznamu na DNS serveru.

Poté bylo nutno Capwap záznamu definovat ip adresu interface přepínače USG 110 172.16.152.254. Přiřazení je zobrazeno na obrázku (Obr. 38), provedlo se pravým klikem na Možnosti Oboru > konfigurovat zde se vybere vytvořený Capwap záznam a přidá se ip adresa 172.16.152.254.



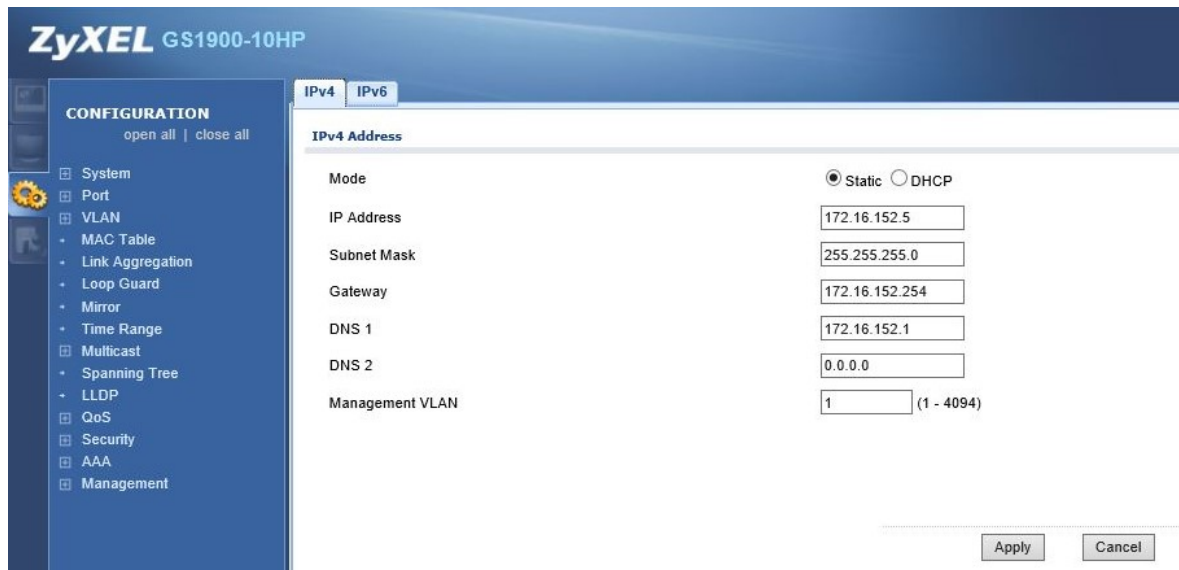
Obr. 39. Přřazení IPv4 Capwap záznamu.

## 8.2 Přepínače GS1900-24e a GS1900-10HP

### 8.2.1 Základní nastavení

Nejprve byl nastaven přepínač GS1900-10HP, přepínač s více porty má mírně odlišné grafické rozhraní, ale byl nastaven zcela shodně.

Aby bylo možno se na přepínač prvotně připojit, nejprve bylo nutno přenastavit IP adresu PC, tak aby patřila do stejné sítě, jako defaultní adresa přepínače, která byla 192.168.1.1. Na základě tabulky (Tab. 3) s rozvržením statických IP adres, byla nastavena IP adresa přepínače na 172.16.152.5, dále byla nastavena adresa brány. Klikem na ikonu Apply, byla uložena aktuální konfigurace do running configuration, pro uložení do startup-configuration, bylo nutno kliknout na malou nenápadnou ikonu **Save** v pravém horním rohu. Po změně IP adresy bylo nutno se odhlásit, přidělit PC, přes který je prováděna konfigurace, novou statickou IP adresu z nově použité sítě.



Obr. 40. Nastavení IP adresy, brány a DNS.

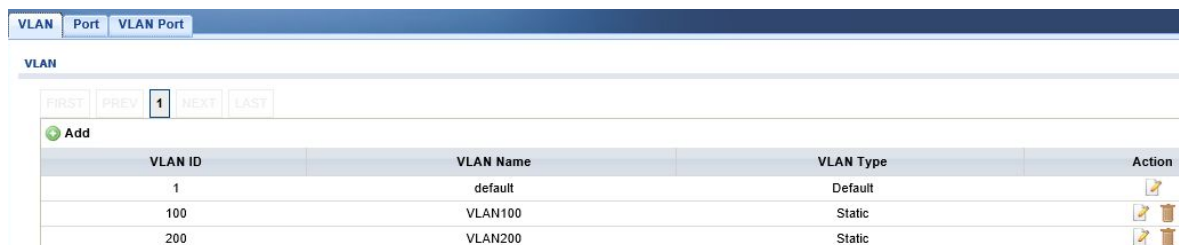
Dále bylo změněno heslo u defaultního uživatele admin. K editaci uživatelů je možno přistoupit z Configuration > Management > Users. Poté byl ještě vytvořen záložní účet správce. Opět bylo nutno uložit running configuration soubor do startup configuration pomocí ikony **Save**.



Obr. 41. Editace uživatelů.

## 8.2.2 Vytvoření VLAN

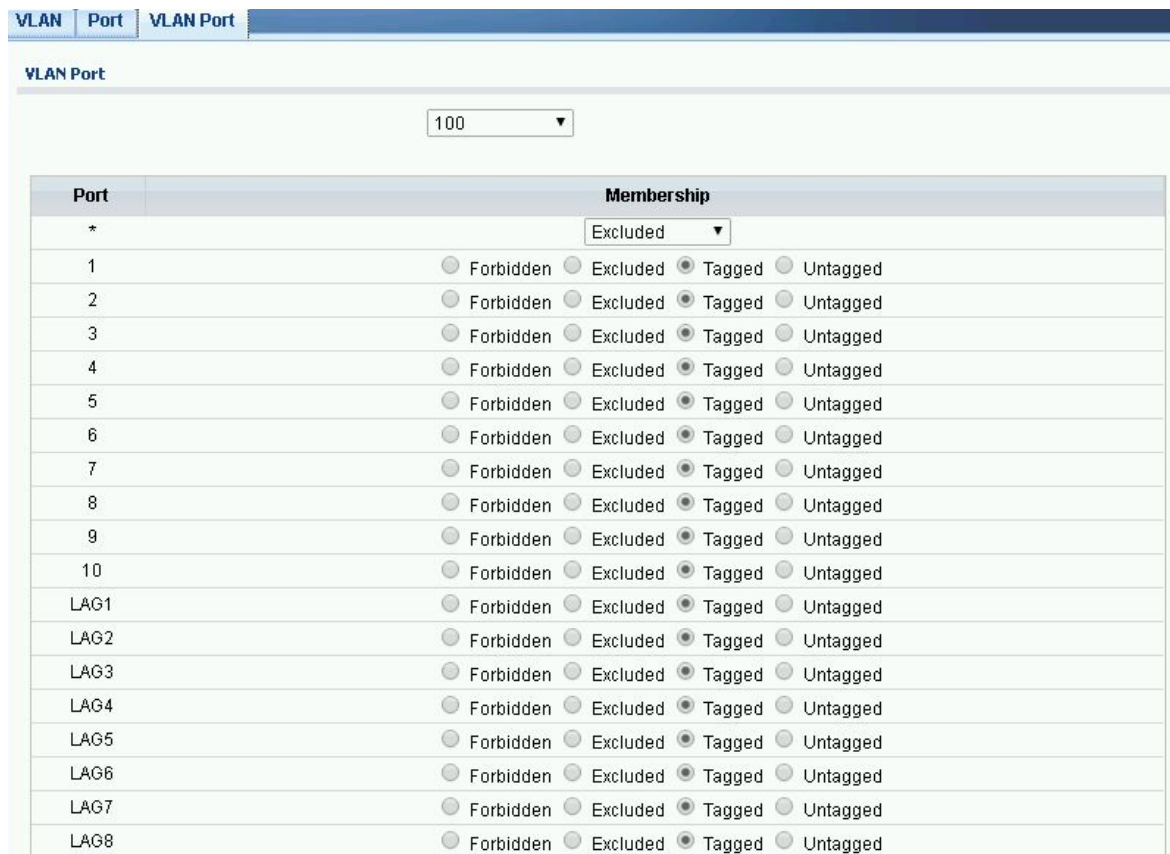
V záložce Configuration > VLAN > VLAN pomocí ikony Add byly definovány nové VLAN100 a VLAN200.



Obr. 42. Definice nových VLAN.

Nakonec bylo nutno nastavit všechny porty přepínače tak, aby propouštěly tagované rámce patřící ze všech sítí tzn. VLAN100, VLAN200 i z výchozí sítě. Pro toto nastavení bylo

nutno přejít do záložky VLAN port. Z rolovacího menu vždy vybrat patřičnou VLAN a všechny porty nastavit do režimu Tagged. Na obrázku (Obr. 42) je zobrazeno toto nastavení pro VLAN100. Úplně stejně bylo provedeno pro VLAN200 i defaultní síť.



The screenshot shows the 'VLAN Port' configuration page. At the top, there are tabs for 'VLAN', 'Port', and 'VLAN Port', with 'VLAN Port' being the active tab. Below the tabs, there is a dropdown menu showing '100'. The main content is a table with two columns: 'Port' and 'Membership'. The 'Membership' column has a dropdown menu set to 'Excluded'. The table lists ports 1 through 10, LAG1 through LAG8, and a '\*' row. For each port, there are four radio button options: 'Forbidden', 'Excluded', 'Tagged', and 'Untagged'. The 'Tagged' option is selected for all ports.

Port	Membership
*	Excluded
1	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
2	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
3	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
4	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
5	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
6	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
7	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
8	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
9	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
10	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
LAG1	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
LAG2	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
LAG3	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
LAG4	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
LAG5	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
LAG6	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
LAG7	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
LAG8	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged

Obr. 43. Nastavení přenosu tagovaných rámců na všech portech v síti VLAN100.

## ZÁVĚR

Hlavními cíli práce bylo proměření útlumů zdí budovy, vytvoření podkladů pro vygenerování matematického modelu s rozmístěním přístupových bodů a zobrazením jejich celkového pokrytí signálu po budově, ověření matematického modelu, na základě tohoto ověření nalezení potenciálně vhodnějších míst umístění, dále pak návrh vhodných síťových prvků a jejich následná konfigurace. Během proměrování matematického modelu se ukázalo, že nejvhodnější bude zaměřit se na řešení centrálního řízení bezdrátové sítě od firmy ZyXEL, jelikož byl používán k proměrování vhodného umístění přístupových bodů přístupový bod této firmy, který má velmi podobné vyzařovací vlastnosti, jako přístupové body vyšší řady s možností centrálního řízení. Po reálném proměření matematického modelu, bylo zjištěno, že lze ubrat 3 přístupové body navrhované matematickým modelem. Důvod byl ten, že firma ZyXEL ze zásady nepokrývá místnosti ve vícepatrových budovách vysíláním procházejícím přes stropy. V budově školy byl ale naměřen útlum stropu pouze -20 dBm, to umožnilo bez problému pokrýt přístupovými body z přízemí i místnosti nacházející se v druhém patře přímo nad nimi. Výsledný útlum se v těchto místnostech pohyboval mezi -50 až -60 dBm, což bylo pod mezní hranicí -65 dBm, při které je na 2,4 GHz garantována maximální přenosová rychlost. Při celkovém řešení projektu byl více kladen důraz na co nejlepší pokrytí s využitím co nejméně přístupových bodů, ze zpětného pohledu, pokud by se škola rozhodla zařadit v budoucnu do výuky notebooky, bylo by nutné vybavit každou třídu přístupovým bodem.

Co se týče konfigurace jednotlivých síťových prvků, firma ZyXEL má velké množství materiálů k jednotlivým prodávaným síťovým prvkům volně na svém ftp serveru, toto velmi usnadňovalo práci a tudíž při samotné konfiguraci nebylo nutno řešit žádné větší komplikace. Při popisu konfigurační části byla práce pojata jako návod pro možného potencionálního zájemce o toto řešení, proto jsou popisované kroky konfigurace doloženy mnoha obrázky.

Funkčnost celého bezdrátového systému, byla ověřena postupným procházením budovy nejprve zařízením připojeným na 2.4 GHz poté zařízením připojeným na 5 GHz. Ověření a připojení postupně do tří SSID sítí proběhlo v obou případech bez problému. Dále byla ověřena funkčnost nastaveného identifikátoru RSSI, kdy při jeho aktivaci se zařízení na 2,4 GHz automaticky přepojovala při pohybu klienta k přístupovým bodům s aktuálně nejsilnějším signálem. Pro přenos na 5 GHz nemělo aktivování nebo deaktivování RSSI žádný vliv, z provedených pokusů vyplynulo, že klienti komunikující na 5 GHz si přepojování řídí sami. Ověření filtru webového obsahu aplikovaného na skupinu žáci proběhlo pozitivně, byly ověřeny 3 nejpožadovanější oblasti pornografie, hry, sociální sítě. Testovacími stránkami byly

www.redtube.com, www.superhry.cz, www.facebook.com ve všech třech případech bylo připojení k těmto stránkám odepřeno.

Při proměňování matematického modelu pro následné rozhodnutí a umístění přístupových bodů bylo opomenuto proměření na frekvenci 5 GHz. Ve většině tříd je našťastí výsledný 5 GHz signál dostačující, ale jsou 3 třídy, ve kterých nebude možno normu AC používat s maximální rychlostí díky vysokému útlumu.

Další vývoj tohoto tématu by mohl být zaměřen přímo na zlepšení samotného bezdrátového systému, ať již směrem větších bezpečnostních opatření při centrálním ověřování uživatelů nastíněném v podkapitole 8. 1. 5, nebo směrem řízení rozdělení šířky pásma pro určité skupiny. Dále by se téma mohlo také rozvinout k ostatním částem inteligentního ZyXEL směrovače USG 110, jako je vestavěná antivirová ochrana, široké možnosti nastavení firewallu, antimalwaru, antispamu, hlídání aplikací proti zneužití šířky pásma, případně nastavením detekcí a prevencí průniků (IDP).

## SEZNAM POUŽITÉ LITERATURY

- [1] CARROLL, Brandon. *Bezdrátové sítě Cisco: autorizovaný výukový průvodce*. Brno: Computer Press, 2011. Samostudium. ISBN 978-80-251-2884-8.
- [2] KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.
- [3] TANENBAUM, Andrew a D WETHERALL. *Computer networks*. Fifth edition. New Delhi: Dorling Kindersley, 2014. ISBN 978-93-325-1874-2.
- [4] SOSINSKY, Barrie A. a D WETHERALL. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.
- [5] *Connect802 Corporation: Understanding Wireless Bridging and the Wireless Distribution System (WDS)*[online]. [cit. 2018-02-08]. Dostupné z: [http://www.connect802.com/wireless\\_bridging.htm](http://www.connect802.com/wireless_bridging.htm)
- [6] *Marigold.cz* [online]. [cit. 2018-02-08]. Dostupné z: [https://www.marigold.cz/wi-fi/doku.php/wds?do=export\\_xhtml](https://www.marigold.cz/wi-fi/doku.php/wds?do=export_xhtml)
- [7] TRČÁLEK, Antonín. Všechno, co byste měli vědět o Wi-fi. In: *Zive.cz* [online]. 14.3.2012 [cit. 2018-02-13]. Dostupné z: <https://www.zive.cz/clanky/vsechno-co-byste-meli-vedet-o-wi-fi/sc-3-a-162796/default.aspx>
- [8] [online]. 2018 [cit. 2018-02-13]. Dostupné z: [https://cs.wikipedia.org/wiki/IEEE\\_802.11](https://cs.wikipedia.org/wiki/IEEE_802.11)
- [9] TRČÁLEK, Antonín. Nový standard Wi-fi: Gigabit vzduchem. *Zive.cz* [online]. 2012 [cit. 2018-02-13]. Dostupné z: <https://www.zive.cz/clanky/novy-standard-wi-fi-gigabit-vzduchem/sc-3-a-165687/default.aspx>
- [10] LEITNER, Miroslav. *Svetsiti.cz* [online]. 2015 [cit. 2018-02-13]. Dostupné z: <http://svetsiti.cz/clanek.asp?cid=Co-prinasi-druha-generace-bezdratovych-siti-80211ac-Wave-2-1-cast-922015>
- [11] HOFMAN, Chriss. What Are Dual-Band and Tri-Band Routers? *Howtogeek.com* [online]. 2016 [cit. 2018-02-16]. Dostupné z: <https://www.howtogeek.com/242793/what-is-mu-mimo-and-do-i-need-it-on-my-router/>
- [12] PROKOP, Mirek. Jak zajistit velké pokrytí. *Zive.cz* [online]. 2014 [cit. 2018-02-22]. Dostupné z: <https://www.zive.cz/clanky/wi-fi-jak-si-zajistit-velke-pokryti-rychlost-a-silny-signal/sc-3-a-172347/>
- [13] HIDDENWIRES. Technology: Gigabit Wi-fi - Do Your Clients Need It?. *Hiddenwires.co.uk* [online]. 2014 [cit. 2018-02-22]. Dostupné z: <http://www.hiddenwires.co.uk/products/article/technology-gigabit-wi-fi-do-your-clients-need-it>
- [14] KASSNER, Michael. Time to clear up some antenna misconceptions. In: *TechRepublic* [online]. 2010 [cit. 2018-02-27]. Dostupné z: <https://www.techrepublic.com/blog/data-center/80211-time-to-clear-up-some-antenna-misconceptions/>

- [15] Antenna Patterns and Their Meaning. In: *Cisco.com* [online]. 2007 [cit. 2018-02-27]. Dostupné z: [https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod\\_white\\_paper0900aecd806a1a3e.html](https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/prod_white_paper0900aecd806a1a3e.html)
- [16] *Bezdratovepripojeni.cz* [online]. [cit. 2018-02-27]. Dostupné z: <http://www.bezdratovepripojeni.cz/cs/cz/clanky/anteny>
- [17] *AntennaMagus* [online]. 2017 [cit. 2018-02-27]. Dostupné z: [http://www.antennamagus.com/database/antennas/antenna\\_page.php?id=241](http://www.antennamagus.com/database/antennas/antenna_page.php?id=241)
- [18] *NETGAR* [online]. 2017 [cit. 2018-03-06]. Dostupné z: <https://kb.netgear.com/cs/209/Co-je-to-PoE-Power-over-Ethernet>
- [19] *Versatek: WHAT is PoE?* [online]. [cit. 2018-03-06]. Dostupné z: <https://www.versatek.com/what-is-poe/>
- [20] *Veracityglobal: Power over Ethernet (POE) Explained* [online]. [cit. 2018-03-06]. Dostupné z: <http://www.veracityglobal.com/resources/articles-and-white-papers/poe-explained-part-1.aspx>
- [21] BOUŠKA, Petr. VLAN - Virtual Local Area Network. *Samuraj-cz* [online]. 2007 [cit. 2018-03-30]. Dostupné z: <https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/>
- [22] *ComputerNetworkingNotes* [online]. 2018 [cit. 2018-03-30]. Dostupné z: <https://www.computernetworkingnotes.com/ccna-study-guide/vlan-basic-concepts-explained-with-examples.html>
- [23] *Firewall.cz* [online]. 2012 [cit. 2018-03-30]. Dostupné z: <http://www.firewall.cx/networking-topics/vlan-networks/218-vlan-access-trunk-links.html>
- [24] ZyXEL Communications Corporation. *USG110\_V4.30\_Ed1: ZyWall VPN/USG Series Users's Guide*. 2017. Dostupné také z: [ftp://ftp.zyxel.com/USG110/user\\_guide/USG110\\_V4.30\\_Ed1.pdf](ftp://ftp.zyxel.com/USG110/user_guide/USG110_V4.30_Ed1.pdf)
- [25] ZyXEL Communications Corporation. *Band\_Select\_4.20*. 2015. Dostupné také z: [https://www.zyxel.com/uploads/Band\\_Select\\_4.20.pdf](https://www.zyxel.com/uploads/Band_Select_4.20.pdf)
- [26] Glossary: DFS (wireless). *Zyxel* [online]. [cit. 2018-05-12]. Dostupné z: [https://www.zyxel.com/dk/da/support/glossary\\_20101214\\_305063.shtml](https://www.zyxel.com/dk/da/support/glossary_20101214_305063.shtml)
- [27] ZyXEL Communications Corporation. *USG110\_V4.30\_Ed1*. 2015. Dostupné také z: [https://www.ZyXEL.com/uploads/V4.21\\_AN\\_Smart\\_Client\\_Steering.pdf](https://www.ZyXEL.com/uploads/V4.21_AN_Smart_Client_Steering.pdf)



**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

2T2R	2 transmit 2 receive antens
DFS	Dynamic Frequency Selection
DSSS	Direct Sequence Spread Spectrum
ETSI	European Telecommunications Standards Institute
FCC	Federal Comunication Comission
FCS	Frame Check Sequence
IEEE	Institute of Electrical and Electronics Engineers
MU-MIMO	Multi-User Multiple Input – Multiple Output
OFDM	Orthogonal frequency division multiplexing
PD	Powered Devices
PoE	Power Over Ethernet
PSE	Power sourcing Equipment
QoS	Quality of Service
RSSI	Received Signal Strength Indicator
SHF	Super High Frequency
SSID	Service Set Identifier
SU-MIMO	Single-User Multiple Input – Multiple Output
UHF	Ultra High Frequency
VLAN	Virtual Local Area Network
VMPS	VLAN Membership Policy Server
VMPS	VLAN Membership Policy Server
WDS	Wirelss distribution systém
WLAN	Wireless local area network
WMM	Wifi multi media

**SEZNAM OBRÁZKŮ**

Obr. 1. Elektromagnetické spektrum [1]. .....	12
Obr. 2. 802.11 architektura (a) mód infrastruktury (b) ad-hoc mód [12]. .....	13
Obr. 3. Wired distribution systém [4]. .....	14
Obr. 4. Grafická reprezentace wi-fi kanálů v pásmu 2,4 GHz [8]. .....	15
Obr. 5. Srovnání SU-MIMO a MU-MIMO [13]. .....	18
Obr. 6. Vyzařovací charakteristiky dipólu se ziskem 2,16 dBi [14]. .....	21
Obr. 7. Vyzařovací charakteristika dipólu s větším ziskem [14]. .....	21
Obr. 8. Vyzařovací charakteristiky panelové směrové antény [15]. .....	22
Obr. 9. Vyzařovací charakteristika 90° sektorové antény [15]. .....	23
Obr. 10. Vyzařovací charakteristika parabolické antény [17]. .....	23
Obr. 11. Počet použitelných portů pro PoE na 130 W přepínači [18]. .....	26
Obr. 12. PoE Injektor [20]. .....	26
Obr. 13. Ukázka VLAN [21]. .....	27
Obr. 14. Struktura tagu [21]. .....	30
Obr. 15. Registrace směrovače. ....	40
Obr. 16. Náhled registrovaných zařízení. ....	40
Obr. 17. Aktualizace firmware. ....	41
Obr. 18. Změna hesla u administrátora. ....	41
Obr. 19. Nahrání nového startup konfiguračního souboru. ....	42
Obr. 20. Přiřazení portů k interface. ....	42
Obr. 21. Přidělení IP adresy k interface lan 1. ....	43
Obr. 22. Konfigurace WAN interface. ....	44
Obr. 23. Vytvoření VLAN200. ....	45
Obr. 24. Přiřazení IP adresy interface. ....	45
Obr. 25. Nastavení DHCP pro VLAN200. ....	46
Obr. 26. Vytvoření bezpečnostního profilu. ....	47
Obr. 27. Vytvořené bezpečnostní profily. ....	48
Obr. 28. Vytvoření bezpečnostního profilu pro žáky. ....	49
Obr. 29. Vytvoření Radio profilu SKOLA_2G. ....	50
Obr. 30. Vytvoření Radio profilu SKOLA_5G. ....	51
Obr. 31. Nastavení AP Group SKOLA, část 1. ....	51
Obr. 32. Nastavení AP Group ŠKOLA, část 2. ....	52

---

Obr. 33. Vytvoření nové politiky pro filtrování obsahu. ....	53
Obr. 34. Nastavení filtru webového obsahu pro žáky.....	54
Obr. 35. Přiřazení nově připojeného přístupového bodu do skupiny. ....	55
Obr. 36. Rozšíření licence pro více přístupových bodů na myZyXEL.com.....	56
Obr. 37. Refresh licencí na směrovači USG 110.....	56
Obr. 38. Vytvoření Capwap záznamu na DNS serveru. ....	57
Obr. 39. Přiřazení IPv4 Capwap záznamu. ....	58
Obr. 40. Nastavení IP adresy, brány a DNS. ....	59
Obr. 41. Editace uživatelů.....	59
Obr. 42. Definice nových VLAN.....	59
Obr. 43. Nastavení přenosu tagovaných rámců na všech portech v síti VLAN100. ....	60

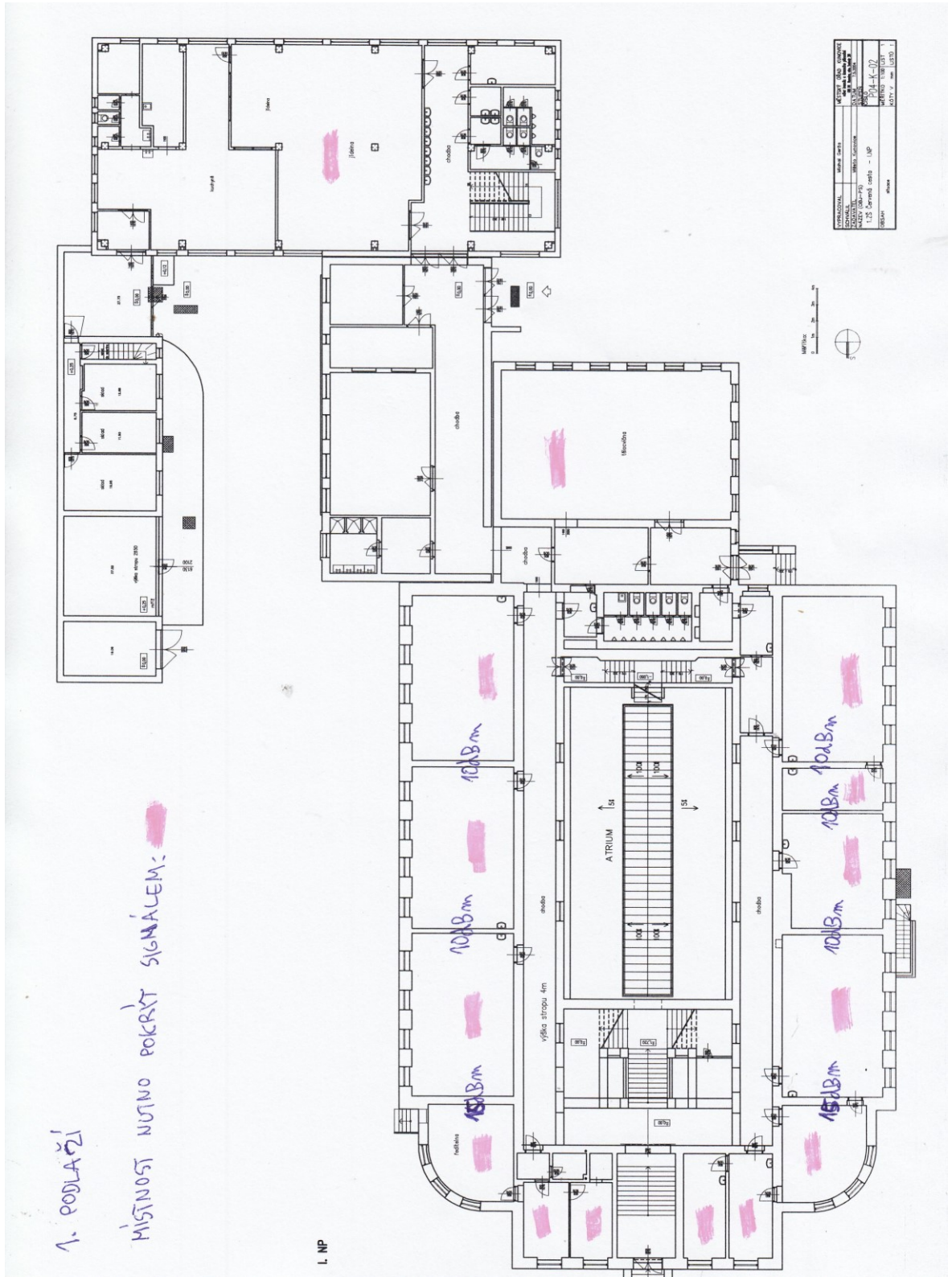
**SEZNAM TABULEK**

Tab. 1. Rychlosti na aplikační vrstvě versus rychlosti na fyzické vrstvě [12]. .....	19
Tab. 2. Seznam potřebných síťových prvků a materiálu. ....	38
Tab. 3. Rozvržení IP adres v defaultní síti.....	38
Tab. 4. Rozvržení IP adres sítím VLAN.....	39

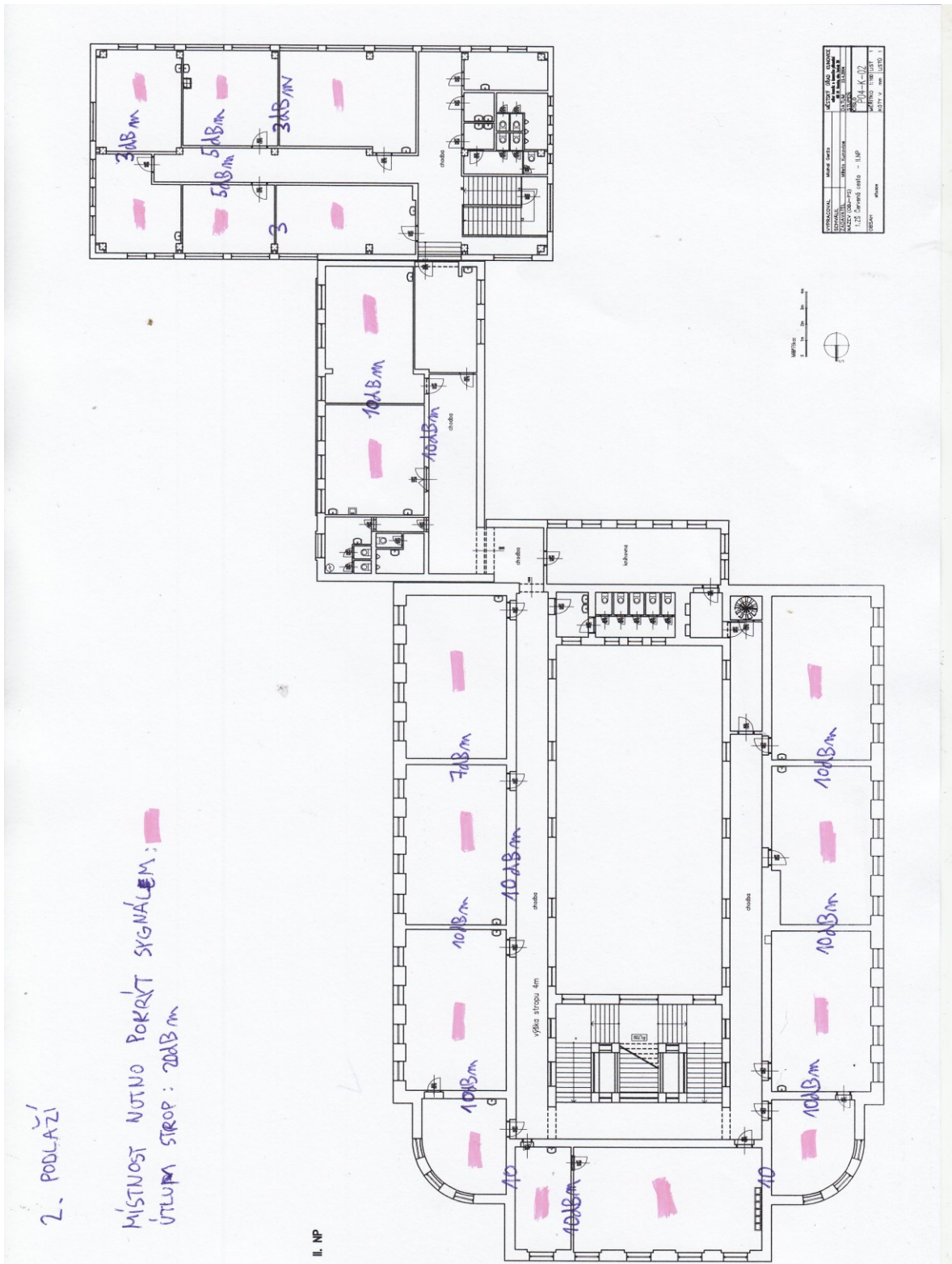
**SEZNAM PŘÍLOH**

P I	Útlumy zdí 1. patro
P II	Útlumy zdí 2. Patro
P III	Simulace pokrytí 1. patro pro 2,4 GHz
P IV	Simulace pokrytí 2. patro pro 2,4 GHz
P V	Simulace pokrytí 1. patro pro 5 GHz
P VI	Simulace pokrytí 2. patro pro 5 GHz
P VII	Definitivní umístění AP 2. Patro
P VIII	Definitivní umístění AP 1. patro

# PŘÍLOHA P I: ÚTLUMY ZDÍ 1. PATRO



# PŘÍLOHA P II: ÚTLUMY ZDÍ 2. PATRO



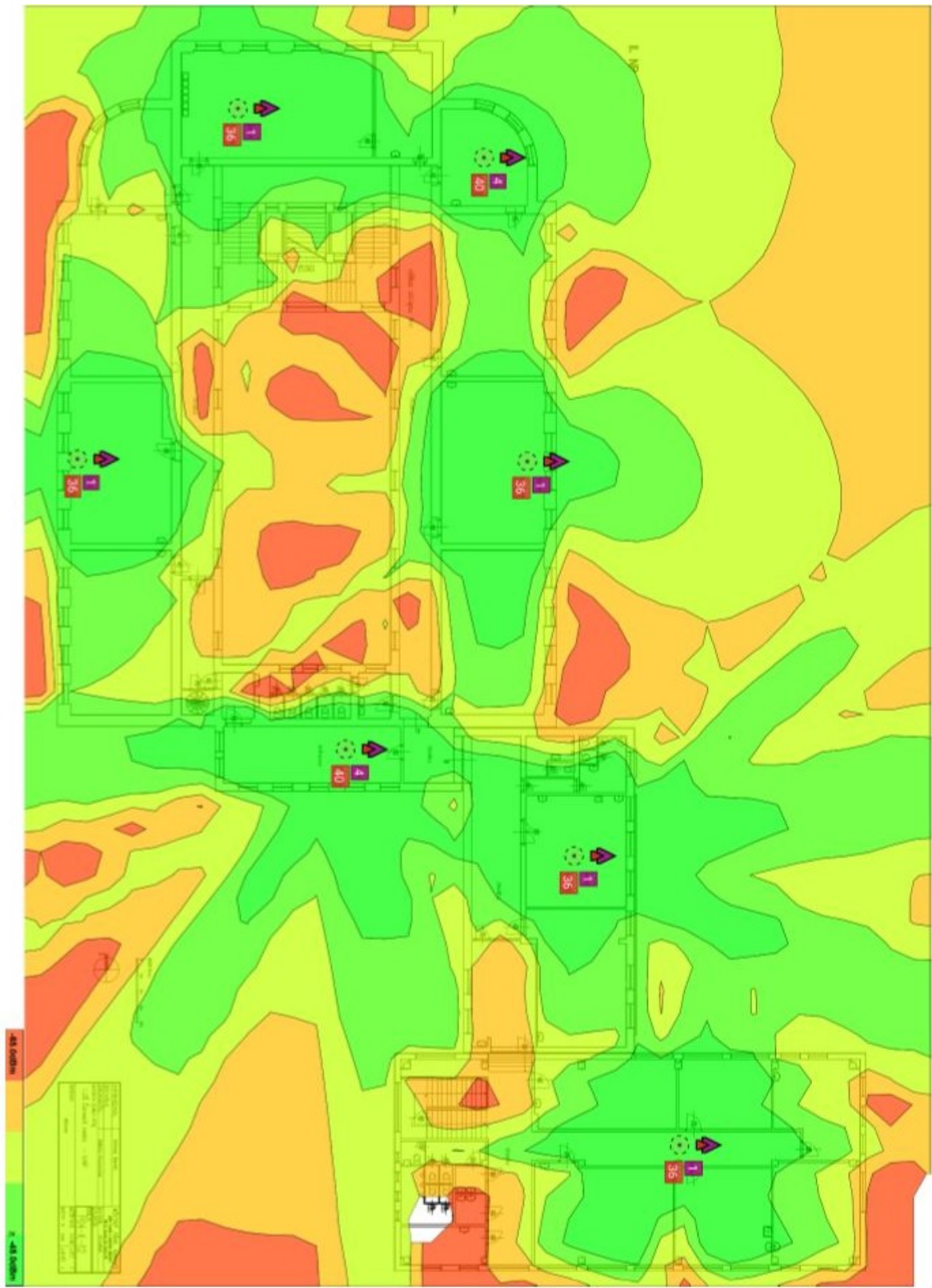


# PŘÍLOHA P III: SIMULACE POKRYTÍ 1. PATRO PRO 2,4 GHZ





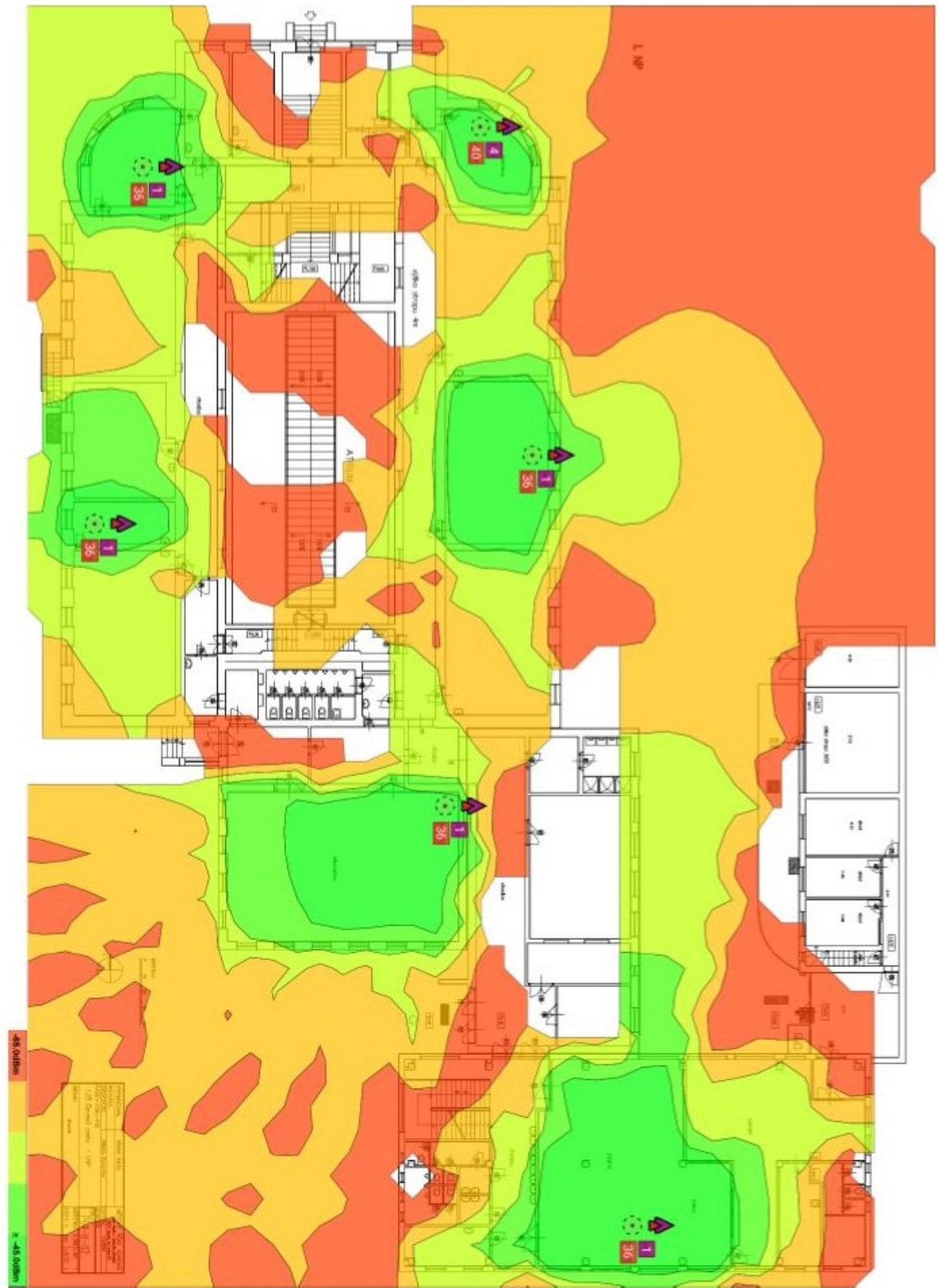
## PŘÍLOHA P IV: SIMULACE POKRYTÍ 2. PATRO PRO 2,4 GHZ



-65.0dBm

~ -45.0dBm

# PŘÍLOHA P V: SIMULACE POKRYTÍ 1. PATRO PRO 5 GHZ



**-65.0dBm** **-45.0dBm**



## PŘÍLOHA P VI: SIMULACE POKRYTÍ 2. PATRO PRO 5 GHZ

