



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV AUTOMATIZACE A INFORMATIKY

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF AUTOMATION AND COMPUTER SCIENCE

OPTIMALIZACE BEZDRÁTOVÝCH WIFI DISTRIBUOVANÝCH SÍTÍ

OPTIMIZATION OF WIFI DISTRIBUTED NETS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. IVAN ŽLŮVA

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. RADOMIL MATOUŠEK, Ph.D.

BRNO 2010

Vysoké učení technické v Brně, Fakulta strojního inženýrství

Ústav automatizace a informatiky

Akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

student(ka): Bc. Ivan Žlůva

který/která studuje v **magisterském navazujícím studijním programu**

obor: **Aplikovaná informatika a řízení (3902T001)**

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Optimalizace bezdrátových WiFi distribuovaných sítí

v anglickém jazyce:

Optimization of WiFi Distributed Nets

Stručná charakteristika problematiky úkolu:

Diplomová práce je velmi komplexní úlohou v dosud ne příliš probádané oblasti budování WDS sítí. Cílem práce bude navrhnout a implementovat metodiku budování tohoto typu sítě s využitím mobilních AP, jejichž poloha je známá a řiditelná. Vzhledem k rozsahu i povaze zadání, resp. následné realizace, se předpokládá částečná spolupráce s řešitelem zadání DP – Připojení koncového zařízení pomocí mobilních AP jednotek.

Cíle diplomové práce:

- 1) Stručný a vzhledem k práci problémově orientovaný popis norem 802.11abgn a případných proprietárních řešení jednotlivých výrobců.
- 2) Popis použitých bezdrátových zařízení.
- 3) Návrh metodiky i praktické ověření v rámci realizace vícebodové bezdrátové sítě, se scénáři:
 - a, Optimální propojení dvou stanovišť.
 - b, Optimální pokrytí daného prostoru.

Seznam odborné literatury:

Norma 802.11 a/b/g/n (RFC dokumenty)

Vedoucí diplomové práce: Ing. Radomil Matoušek, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2010/2011.

V Brně, dne

L.S.

Ing. Jan Roupec, Ph.D.
Ředitel ústavu

prof. RNDr. Miroslav Doupovec, CSc.
Děkan fakulty

Abstrakt

Práce se zabývá teoretickým návrhem a následnou praktickou realizací vícebodové bezdrátové sítě, pro variantu spoje dvou míst a pokrytí strukturovaného prostoru WiFi signálem. Síť je realizována pomocí zařízení fungujících v bezlicenčním pásmu 2,4 GHz a 5 GHz. Jednotlivá zařízení jsou konfigurována v módech WDS, WDS bridge případně AP. V práci je stručný popis norem IEEE 802.11a/b/g/n a proprietárních řešení přidružených k těmto normám. Praktická část je tvořena popisem jednotlivých variant zapojení a naměřenými hodnotami propustnosti WiFi sítě v závislosti na vytvořené topologii

Diplomová práce vznikla jako součást řešení výzkumného záměru *Intelligentní systémy v automatizaci* podporovaného MŠMT ČR pod registračním číslem MSM 0021630529.

Abstract

This thesis describes theoretic proposal and two practical realization of multi - point wireless network, first for communications between two endpoints and second for wireless signal coverage of a structured space. The wireless network is realized by the equipment working in unlicensed 2,4GHz and 5GHz ISM band. The wireless device are configured in three different wireless mods: WDS, WDS bridge and AP. This paper contains short information about IEEE 802.11a/b/g/n standard and associated proprietary wireless specifications. Practical workshop describes several variants connections and present the result of throughput measurements, depending on wireless network topology.

This research has been supported by the Czech Ministry of Education in the frame of MSM 0021630529 Research Intention *Intelligent Systems in Automation*.

Klíčová slova

IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, bezdrátová síť, WDS, síla signálu, propustnost, šířka pásma

Keywords

IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, Wireless Network, WDS, Signal strength, transmissivity, bandwidth

VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci vypracoval samostatně na základě uvedené literatury pod vedením vedoucího bakalářské práce.

.....

V Brně 5.10.2010

VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

Poděkování

Děkuji tímto zastoupení firmy OvisLink corp. v ČR, za zapůjčení testovacích vzorků, na nichž byla prováděna jednotlivá měření. Dále, tímto děkuji Ing. Radmilu Matouškovi, Ph.D. za cenné připomínky a rady při vypracování diplomové práce.

Obsah	str.
Obsah	7
1 Úvod	9
2 Technologie WiFi – standard IEEE 802.11a,b,g,n a proprietární řešení	11
2.1 Bezlicenční přenos ve frekvenčním pásmu 2,4GHz	11
2.1.1 Standard 802.11	11
2.1.2 Standard IEEE 802.11b	12
2.1.3 Standard IEEE 802.11g	13
2.2 Bezlicenční přenos ve frekvenčním pásmu 5GHz	17
2.2.1 Standard IEEE 802.11a	17
2.3 Kombinovaný bezlicenční přenos v pásmech 2,4GHz nebo 5GHz	19
2.3.1 Standard IEEE 802.11n	19
2.4 Proprietární řešení	21
3 Doplnky k normě IEEE 802.11	23
4 Zabezpečení bezdrátových sítí	25
4.1 Základní zabezpečení pomocí SSID a filtrace MAC	25
4.2 Zabezpečení WEP a WEP2	27
4.3 Zabezpečení WPA	27
4.3.1 Zabezpečení WPA-PSK	27
4.3.2 Zabezpečení WPA – spolupráce s 802.1X	29
4.4 Zabezpečení WPA2 – standard IEEE 802.11i	30
5 Antény pro příjem WiFi signálu a jejich příslušenství	31
5.1 Hlavní parametry antén	31
5.1.1 Polarizace signálu	31
5.1.2 Frekvence	32
5.1.3 Vyzařovací diagram – vyzařovací úhel	32
5.1.4 Směrovost antén	33
5.1.5 Zisk a výkon antén	34
5.2 Přepět'ové ochrany, kabely pro přenos signálu 2,4GHz a 5GHz	34
6 Přenosová trasa	37
6.1 Zarušení signálu	39
6.1.1 Vliv počasí na venkovní trasy	40
6.1.2 Vliv prostředí u indorových WiFi sítí	40
6.2 Přímá viditelnost	41
6.3 Nepřímá viditelnost	41
7 Možnosti konfigurace WiFi zařízení	43
7.1 Klient v módu AD-Hoc	43
7.2 Klient	43
7.3 Bridge	44
7.4 WD opakovač	45
7.5 Univerzální opakovač	47
7.6 WISP mód	47
7.7 WISP mód + univerzální opakovač	47
7.8 Režim brána	48
8 Popis použitých zařízení	49

8.1 multifunkční zařízení WL-5460AP v2	49
8.2 multifunkční zařízení WLA-5000AP v3	52
8.3 multifunkční zařízení WLA-5200AP	54
8.4 multifunkční zařízení AirMax5	56
8.5 multifunkční zařízení WLA-9000	58
8.6 multifunkční zařízení WN-300R	60
8.7 multifunkční zařízení WN-301R	62
8.8 usb dongle WN-300USB	64
8.9 Ostatní zařízení použita při měření	66
9 Návrh řešení pro propojení dvou stanovišť	67
9.1 Volba pásma a volba zařízení	67
9.2 Volba módu zařízení.	69
9.3 Praktický návrh spoje	69
9.4 Obecné řešení pro mobilní jednotky rozmisťující jednotlivá zařízení	69
10 Návrh řešení pro strukturovaný prostor	71
10.1 Volba zařízení a varianty zapojení	71
10.2 Rozmístění zařízení	73
10.3 Měření síly signálu pro různé normy z řady IEEE 802.11	74
10.4 Měření propustnosti mezi jednotlivými body WiFi sítě	75
10.5 Alternativní řešení pro pokrytí strukturovaného prostoru s jedním vysílaným SSID	76
10.6 Obecné řešení pro mobilní jednotky rozmisťující jednotlivá zařízení	76
11 Závěr	79
12 Seznam zkratk	81
13 Literatura	85
 Přílohy	
A Popis použitého software	87
B Nastavení zařízení WL-5460AP v2 do módu AP, bridge a WDS	92
C Nastavení WLA-5000AP v3 a WLA-9000 pro mód WDS bridge	103
D Naměřené hodnoty propustností pro spoje typu most	114
E Naměřené hodnoty propustnosti pro distribuovanou WiFi síť	120
F Měření síly signálu	123
G Plánek strukturovaného prostoru	124
H Obsah příloženého disku CD-ROM	125

1. Úvod

V dnešní, poměrně technicistní době, je stále více kladen důraz na přístup k informacím pomocí mobilních technologií. Patrně nejrozšířenější z celosvětového pohledu je použití mobilních telefonů s datovými moduly, které nám umožňují přístup k internetu, potažmo k již zmíněným informacím. Druhou nejrozšířenější skupinou umožňující mobilní přístup k informacím jsou bezdrátové sítě. Právě touto problematikou, zúženou na provoz v bezlicenčních pásmech 2,4GHz a 5 GHz, se budu v práci zabývat.

Původní koncepce využití pásma 2,4GHz byla pro vědecké a lékařské účely, kde se tohoto pásma užívá dodnes. Ovšem tlak a nutnost používání bezdrátových sítí způsobil uvolnění tohoto pásma pro dnes známé WiFi sítě. Následně pod vlivem EU došlo k přechodu pásma 5GHz z licencovaného do bezlicenčního.

Rozvoj technologie WiFi byl od počátku standardizace poměrně rychlý, ovšem nejrazantnější rozšíření této technologie přišlo po roce 2003, kdy začaly být standardně osazovány notebooky bezdrátovými WiFi síťovými kartami. Z oblasti výjimečného použití se tedy WiFi sítě dostali mezi masovou veřejnost. V dnešní době se zcela běžně setkáváme s volnými přístupy k WiFi sítím, a následně i k internetu, v restauracích, školách, na letištích a mnoha dalších místech. Miniaturizace WiFi přijímačů dnes umožňuje příjem WiFi signálu i v již běžných mobilních telefonech.

Obsah diplomového projektu se zabývá návrhem strukturovaných typů WiFi sítí, jak pro použití pouze jako propoj mezi koncovými body, tak i strukturou řešící pokrytí WiFi konektivitou u strukturovaného prostoru uvnitř budov. Pro druhou variantu je předpokládána možnost připojení koncových zařízení k vytvořené WiFi síti. Jednotlivé typy zapojení byly realizovány do funkčních vzorků, pro možnost dalšího měření parametrů WiFi sítě, jako je propustnost sítě a síla signálu v okolí bezdrátových jednotek. Z těchto naměřených hodnot je následně možno vytvořit strategii pro rozmístění bezdrátových zařízení pomocí říditelných robotických jednotek.

Při návrhu jednotlivých řešení WiFi sítí, bylo použito popisu jednotlivých norem IEEE 802.11 a/b/g/n a zapůjčených testovacích vzorků od firmy OvisLink, jenž, byly zapůjčeny na omezenou dobu právě pro účely jednotlivých měření.

První část diplomové práce pojednává o teorii WiFi sítí a je ji možno rozdělit do pěti na sebe navazujících kapitol. Jedná se o teoretický základ, bez něž se neobejdeme při návrhu vlastní struktury WiFi sítě a volbě jednotlivých prvků. První z kapitol je věnována normám IEEE 802.11 a/b/g/n a proprietárním řešením navazující na tyto normy. Na tuto kapitolu navazuje další část, kde je uvedeno množství dodatků k uvedeným normám a jejich stručný popis. Další část je věnována seznámení s problematikou zabezpečení WiFi sítí. Kapitola 5 pojednává o problematice WiFi antén a jejich příslušenství. Poslední z teoretických kapitol pak seznamuje s problematikou přenosových tras a případnými vlivy prostředí na tyto trasy.

Druhá část je věnována popisu použitých zařízení a vlastním návrhům struktury WiFi sítí s ohledem na jejich následnou aplikovatelnost pro běžný provoz. V této části je také zmíněna problematika měření propustnosti ve WiFi sítích a měření síly signálu.

2. Technologie WiFi – standard IEEE 802.11a,b,g,n a proprietární řešení

Prvotní návrhy pro bezdrátový přenos v bezlicenčním pásmu 2,4 GHz najdeme již v roce 1997. Tento návrh byl koncipován jako prvotní standard pro přenos dat 802.11 někdy také milně označovaný jako IEEE 802.11.

Pásmo 5GHz v prvotním návrhu bylo koncipováno jako licencované (z pohledu české legislativy), až později bylo uvolněno pro bezlicenční provoz.

2.1 Bezlicenční přenos ve frekvenčním pásmu 2,4GHz

Bezlicenční pásmo 2,4 GHz, tak jak je bráno širší veřejností, se rozprostírá mezi kmitočty 2,400-2,474 GHz (dle normalizace ČTÚ). Norma IEEE 802.11b ovšem specifikuje pásmo pro přenos dat od 2,300 GHz do 2,744 GHz, což je celkem 39 kanálů s šířkou každého kanálu 5MHz.

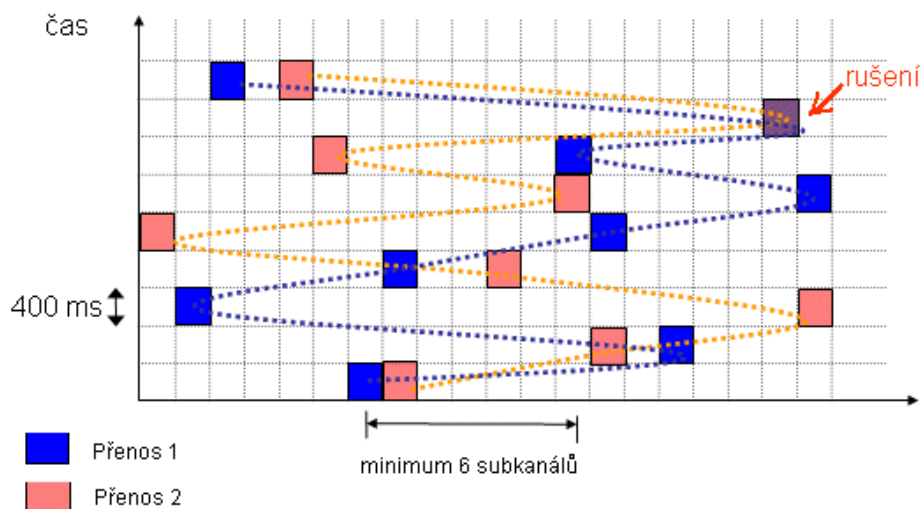
Pro již zmíněné užší pásmo je však uvažován kanál s šířkou pásma 20 MHz (maximálně 24 MHz), proto je v celém spektru možno nalézt maximálně 3 nepřekrývající se kanály, vyhovující tomuto požadavku. Jedná se o kanály číslo 1, 6 a 11.

Dle platné legislativy v ČR se užívá již zmíněné užší pásmo, které je děleno na 13 přenosových kanálů. Toto pásmo je shodné se zeměmi EU mimo Francii a Španělsko kde je povolen pouze kanál 10 a 11. V praxi se můžeme setkat ještě s frekvencemi určenými pro USA a Kanadu, kde je možno použít pouze 11 kanálů, případně s frekvencemi pro Japonsko, kde je použito o jeden kanál více než v ČR.

2.1.1 Standard 802.11

Koncepce byla navrhována již v roce 1997. Pro tuto normu jsou definovány tři různé fyzické vrstvy. První dvě jsou určeny pro rádiový přenos a třetí je určena pro IR přenos. Šlo o koncepci pro přenosy s rychlostí 1 Mbit nebo 2 Mbit na linkové vrstvě, potažmo s kapacitou 0,9 Mbit na vrstvě MAC pro vyšší rychlost fyzické vrstvy. Rádiová komunikace probíhala v pásmu ISM. Pro ČR je toto pásmo mezi frekvencemi 2,400 až 2,4835 GHz. Pro rádiové přenosy byl předpokládán dosah 100m pro otevřený prostor a 20 m pro uzavřený prostor, za předpokladu přímé viditelnosti vysílače a přijímače.

Pro první variantu rádiového přenosu byla použita modulace FHSS. Tento typ modulace je velmi nenáročný na zpracování vlastního signálu, ovšem má obrovskou náročnost na časovou synchronizaci. Jde o modulaci na principu frekvenčních proskoků. Pravidelně za cca 400 ms dojde k přeskočení na předem stanovený kanál, ze 79 užitých kanálů. Šířka každého kanálu je 1 MHz. Toto má za následek vysokou odolnost proti rušení ovšem velmi nízkou přenosovou rychlost, již uvedené 2 Mbity. Schematický princip modulace FHSS je vyobrazen na obrázku číslo 1.



Obrázek 1- princip modulace FHSS

Druhá varianta užívala modulace DSSS. Použito bylo 14 kanálů. Možnost užití jednotlivých kanálů již bylo popsáno výše. Modulace probíhá ve dvou krocích. V prvním kroku je datová posloupnost vynásobena pseudonáhodnou posloupností s mnohonásobně vyšší chipovou rychlostí, než je bitová rychlost dat. Ve druhém kroce je tato posloupnost modulována na nosnou frekvenci pomocí modulace PSK.

Třetí možnost používala IR záření na vysokých frekvencích. Tento princip přinášel bezpečnější komunikaci z pohledu rušení a případného odposlechu.

Jednotlivé metody modulace FHSS a DSSS jsou naprosto odlišné a proto mezi nimi není možná přímá spolupráce.

Toto řešení s užitím rádiového přenosu se používalo do cca roku 2000, kdy bylo nahrazeno standardizovanou normou IEEE 802.11b. Nejznámějším výrobcem zařízení typu 802.11 byl BreezNet.

2.1.2 Standard IEEE 802.11b

Původní návrh z roku 1997 došel k finální standardizaci v roce 1999. Došlo ke změně modulace z FHSS na DSSS. Norma uvažovala přenos 11 Mbit na fyzické vrstvě, respektive 4,3 Mbit na MAC vrstvě. Tato norma byla určena pro datové přenosy do 140 m ve volném prostoru a 38 m v uzavřeném prostoru.



Obrázek 2 – OvisLink WL-1120AP – patrně nejznámější představitel zařízení 802.11b

Pro zajištění vyšší přenosové rychlosti užívá doplňkové kódové klíčování CCKP v rámci DSSS na fyzické vrstvě.

Tento model specifikuje, že podle momentální velikosti zarušení přenosové trasy dochází k dynamickému snižování případně zvyšování rychlosti. Rychlost se tedy může pohybovat ve skocích od 1 Mbit až do 11 Mbit. Přesněji se jedná o rychlosti 1 Mbit, 2 Mbit, 5,5 Mbit a 11 Mbit.

Uvedená norma nebyla původně vhodná k přenosu hlasu. Až s postupem času byly dopracovány dodatky, které zlepšují parametry pro přenos jednotlivých služeb.

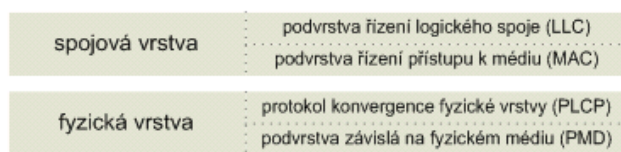
2.1.3 Standard IEEE 802.11g

Jedná se o normu velmi podobnou normě IEEE 802.11a, řešenou ovšem v pásmu 2,4 GHz. V dnešní době patří patrně k nejužívanějším. Normalizační institut IEEE tuto normu přijal v roce 2003. Jedná se o navázání na předchozí normu IEEE 802.11b a z toho vyplývající i zpětná kompatibilita se zařízeními splňující tuto starší normu.



Obrázek 3 – Airlive WL-5460AP – představitel zařízení splňující normu IEEE 802.11g

Přebírá první dvě vrstvy z modelu OSI normovaného v IEEE 802.11. Jedná se o fyzickou a spojovou vrstvu.

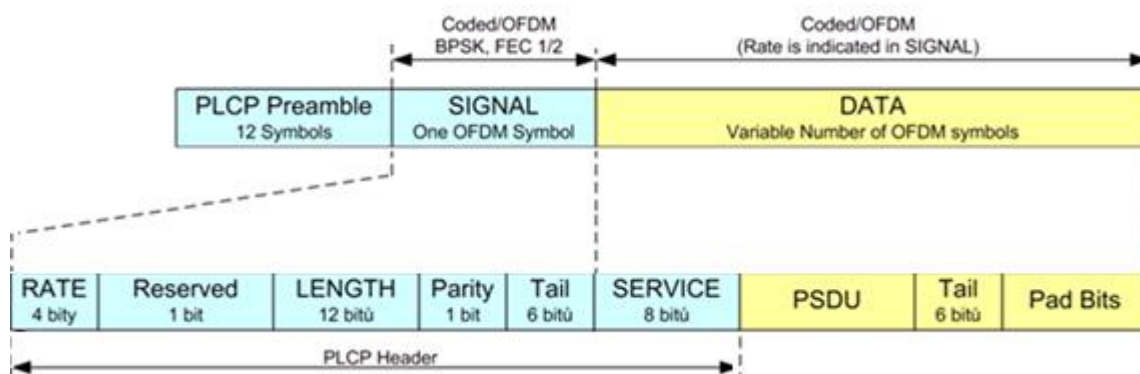


Obrázek 4 - rozdělení PHY vrstvy dle OSI v IEEE 802.11

Fyzická vrstva (PHY) je rozdělena na dvě subvrstvy:

PMD podvrstva je přímo závislá na fyzickém médiu. Tato subvrstva předává data z podvrstvy PLCP do rádiového prostoru, v případě příjmu opačně. Tyto podvrstvy spolu komunikují na základě přenosového mechanismu. V tomto případě se užívá OFDM. Jedná se o metodu ortogonálního multiplexu s kmitočtovým dělením. Kvůli zpětné kompatibilitě užívá ještě HR/DSSS modulaci.

PLCP podvrstva přímo spolupracuje s podvrstvou MAC spojové vrstvy. Při komunikaci mezi podvrstvami dochází k přidání informací o užitém přenosovém mechanismu a o modulaci. PLCP může dle normy nabývat dvou různých struktur. Jedná se o struktury preamble. Je možno se setkat s krátkou a dlouhou preambulí. Krátká preamble byla doplněna z důvodů zvýšení propustnosti specifických dat, jako je hlas, video a další.



Obrázek 5 PPDU rámec

PPDU rámec je rozdělen na 3 části:

- PLCP preamble – skládá se z 10 krátkých a 2 dlouhých OFDM symbolů
- PLCP hlavička – lze rozdělit na několik částí. Prvotní dělení je na signálovou část. Ta obsahuje 24 bitů a lze ji dále rozdělit na Rate (určuje nastavení rychlosti přenosu dat) a Length (určení velikosti dat). Ostatní části signálové části se užívají pro synchronizaci a řízení komunikace jednotlivých zařízení. Druhá, servisní část obsahuje 8 bitů.

- DATA – tato část PPDU paketu přenáší uživatelská data a servisní informace. Obojí se přebírá z vyšších komunikačních vrstev.

OFDM – Ortogonální frekvenční multiplex

Jedná se o mechanismus, který řeší v rámci IEEE 802.11g (i pro IEEE 802.11a) modulaci a demulaci výstupního a vstupního vysokofrekvenčního signálu, který se užívá pro přenos dat mezi jednotlivými zařízeními. Šířka pásma pro modulaci OFDM je použita 20 MHz. Jak již bylo zmíněno výše, tato šířka pásma umožňuje realizaci maximálně tří nepřekrývajících se kanálů, reálně je použito více kanálů, které se částečně vždy překrývají. Vzhledem k této skutečnosti je implementován v koncových zařízeních normy IEEE 802.11g mechanismus pro automatickou změnu kanálu v závislosti na zarušení přenosového prostředí. Tento mechanismus zvyšuje stabilitu připojení a rychlost přenosu dat.

Jednotlivé subkanály jsou modulovány dvou či vícecestavovou digitální modulací. Hlavním představitelem dvoustavové digitální modulace je klíčování fázovým posuvem PSK případně modifikovaným BPSK. Představitelem vícecestavových modulací je čtyřstavová digitální modulace s klíčovaným fázovým posuvem QPSK, případně čtyřstavová amplitudová modulace QAM (16-QAM, 64-QAM). Při komunikaci je do přenosu v každém subkanálu přidán ochranný konvulzní kód s kódovým poměrem. Jedná se o poměr počtu bitů užitečné informace, ku počtu všech bitů včetně redundantních (i nadbytečně redundantních).

Vzhledem k již zmíněné zpětné kompatibilitě normy IEEE 802.11g s normou 802.11b se používá dalších tří typů modulací. Jedná se o DBPSK, DQPSK a CCK. Je nutno podotknout, že zařízení splňující IEEE 802.11g při připojení zařízení splňující normu IEEE 802.11b snižuje svoji propustnost, v krajním případě až na 11,8 Mbit. Není tedy zcela ideální používat kombinaci obou standardů dohromady.

Tabulka 1 – závislost přenosové rychlosti na typu modulace a použitém kódovém poměru

Typ modulace	Kódový poměr	Přenosová rychlost pro subkanál s šířkou 20MHz [Mbit/s]
DBPSK	--	1
DQPSK	--	2
CCK	--	5,5 a 11
BPSK	$\frac{1}{2}$	6
BPSK	$\frac{3}{4}$	9
QPSK	$\frac{1}{2}$	12
QPSK	$\frac{3}{4}$	18
16-QAM	$\frac{1}{2}$	24
16-QAM	$\frac{3}{4}$	36
64-QAM	$\frac{2}{3}$	48
64-QAM	$\frac{3}{4}$	54

Spojová vrstva se dělí na dvě subvrstvy (viz obrázek 4):

Podvrstva LLC – jedná se o podvrstvu pro řízení logického spoje. Je normalizována standardem IEEE 802.2. Je naprosto nezávislá na fyzikální implementaci sítě (optická, metalická, rádiová, ...) a je pro všechny technologie vycházející z IEEE 802 shodná. Na referenčním modelu OSI zprostředkovává komunikaci mezi vyššími a nižšími vrstvami.

Podvrstva řízení přístupu MAC - je pro různé technologie různá a je přímo závislá na fyzikální implementaci sítě, případně spoje. Pro normu IEEE 802.11g je přesně specifikován formát MAC rámce a koordinace přístupu k médium. Z této specifikace vychází problematika skrytého uzlu a předcházení kolizím.

MAC rámec se dá definovat dvěma základními vlastnostmi. První je kontrolní součet CRC. Z kontrolního součtu lze zjistit, zda byl rámec poškozen případně změněn. Druhá vlastnost se týká fragmentace rámce.

V normě je ještě specifikována mezirámcová mezera ISF. Ta slouží ke koordinaci přístupu k médium. Jsou známy čtyři různé definice mezer mezi rámci.

- SIFS – nejkratší ISF. Užívá se pro odpověď typu ACK příjemce od odesílatele. Je to odpověď o doručení rámce a odpověď na dotaz CTS.
- PIFS – ISF se střední délkou. Užívá se pro výzvy.
- DIFS – ISF s největší délkou. Udává čas DCF, po který musí odesílatel čekat po přidělení média, než začne vysílat data.
- EIFS – nemá pevný interval. Užívá se při chybném přenosu rámce.

Aby nedocházelo k současnému vysílání více stanic, používá se koordinace přístupu k médium. Tímto se potlačí poškození původního signálu a je možno koordinovat vysílání jednotlivých zařízení. Dle IEEE 802.11g existují dvě funkce koordinující přístup k médium.

- DFS – funkce distribuované koordinace je součástí přístupové metody k médium CSMA/CA.
- PCF – funkce koordinace jedním bodem. Tato funkce je vhodná pro přenosy v reálném čase (např. video, hlas). V praxi se však neužívá.

Přístupová metoda k médium CSMA/CA je koncipována tak, aby eliminovala problém kolizí a skrytého uzlu. Ke kolizím může dojít, pokud se více jak jeden klient snaží přistoupit k médium ve stejný časový okamžik. V tomto případě, by mohlo dojít ke znefunkčnění sítě. Se skrytým uzlem se v běžné praxi můžeme setkat u venkovních sítí, pokud jsou používány směrové antény. Proto je nutné použít nástroje jak těmto stavům předcházet.

Pro předcházení kolizím, v normě CSMA/CA, je užito tří typů rámců a doplňkového registru:

- RTS – jedná se o žádost o vysílání. Vysílá se ještě před začátkem přenosu. Obsah rámce je čas potřebný pro přenos dat.

- CTS – potvrzení připravenosti pro příjem dat. Vysílá jej stanice po příjmu RTS. V rámci je obsažen čas, po který bude probíhat přenos dat.
- ACK – tento rámec je vyslán stanicí po úspěšném přijetí dat se správným součtem CRC.
- NAV – registr, do nějž ostatní stanice zapisují čas, po který nemají provádět vysílání. Jeho hodnota vychází z odposlechu RTS.

Norma IEEE 802.11 byla prvotně koncipována pro segment SOHO. V prostředí se předpokládá přímá viditelnost všech zařízení a možnost odposlechu RTS. S přechodem této technologie do segmentu ISP došlo k tomu, že jednotlivá zařízení na sebe „nevidí“. Tento stav se nazývá skrytý uzel. Příkladně máme zařízení A, B a C. Zařízení A řídí celou komunikaci, zařízení B a C jsou stanice. Pokud se stanice B a C „neslyší“ dochází při vyslání rámce RTS ze stanice B k tomu, že stanice C tento rámec nezachytí a nemůže si správně nastavit registr NAV. Toto má za následek zvýšení počtu kolizí. Proto se v outdoorovém prostředí při použití silnějších směrových antén připojuje cca 10 klientů k jednomu řídicímu bodu.

2.2 Bezlicenční přenos ve frekvenčním pásmu 5GHz

První zmínky o přenosech v bezlicenčním pásmu 5 GHz, tak jak je nyní širší veřejností znám, lze nalézt již z roku 1999. Tehdy byl schválen standard IEEE 802.11a. Toto pásmo někdy také můžeme najít pod zkratkou U-NII. Bohužel česká legislativa uznala toto pásmo za bezlicenční až v roce 2005 pod všeobecným opatřením VO-R/12/08.2005-34. Než bylo schváleno všeobecné opatření, pro již uvedené pásmo, užívali se v Evropě standardy WLAN, a Hyperlan2. Ty byly následně sloučeny do jediné licence dnes známé jako pásmo pro přenos dat na frekvenci 5GHz.

Obecně lze rozdělit toto pásmo na dvě části (bráno z pohledu legislativy ČR):

- Část vhodnou pouze pro použití uvnitř budov, s použitými frekvencemi 5150 – 5350 MHz a s maximálním výkonem EIRP 200mW.
- Druhá část je určena pro venkovní aplikace. Užívá frekvencí 5470 - 5725 MHz. Maximální použitelný výkon EIRP je 1W.

Pro kompletní pásmo musí ještě zařízení splňovat podmínky implementace automatické regulace výkonu TPC s činitelem potlačení minimálně 3 dB, dynamickou volbou kmitočtu DFS s mechanismem automatického výběru kmitočtu s šířkou pásma 330 MHz pro indoor aplikace a 225 MHz pro outdoor aplikace.

2.2.1 Standard IEEE 802.11a

Tento standard byl přijat normalizačním institutem IEEE v roce 1999. Práce na normě začaly vznikat dříve než na normě IEEE 802.11b. Ze standardu pro přenos dat na fyzické vrstvě následně vzešla norma IEEE 802.11g, která byla již popisována výše. Dále již bude popisována pouze norma s návazností na legislativu platnou v ČR a budou popisovány odlišnosti od normy IEEE 802.11g.

VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky



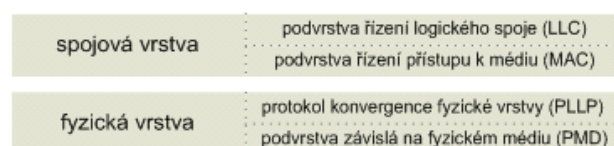
Obrázek 6 – Airlive – WLA-5000AP v3 – představitel zařízení pro normu IEEE 802.11a

Dle specifikace se jednalo o technologii koncipovanou k datovému přenosu do 35 m v uzavřeném prostoru a do 120 m ve volném prostoru. Pro jednotlivá pásma (indoor a outdoor) jsou definovány kanály, které se dají v ČR použít, viz tabulka 2.

Tabulka 2 – seznam povolených kanálů v ČR, pro IEEE 802.11a, žlutá část indoor, červená část outdoor

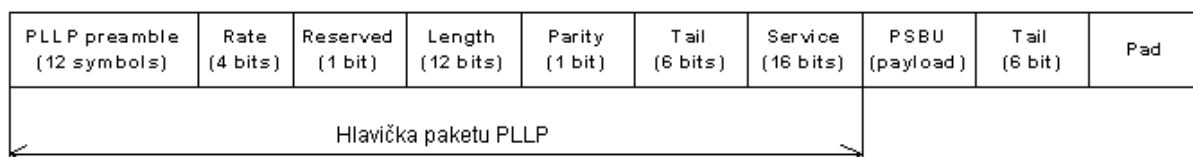
Číslo kanálu	36	40	44	48	52	56	60	64			
Střední frekvence [MHz]	5180	5200	5220	5240	5260	5280	5300	5320			
Číslo kanálu	100	104	108	112	116	120	124	128	132	136	140
Střední frekvence [MHz]	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700

Norma přebírá první dvě vrstvy z modelu OSI normovaného v IEEE 802.11 tak jako u normy IEEE 802.11g. Ovšem rozdílná je vyšší subvrstva ve fyzické vrstvě. Jedná se o subvrstvu PLLP viz obrázek 7.



Obrázek 7 - rozdělení PHY vrstvy dle OSI v IEEE 802.11 a poloha PLLP subvrstvy

PLLP subvrstva je téměř totožná se subvrstvou PLCP u IEEE 802.11g až na drobný rozdíl ve velikosti servisní části v hlavičce PLLP paketu. Ta má místo 8 bitů použito 16 bitů. Viz obrázek 8.



Obrázek 8 - rozdělení PLLP paketu na jednotlivé části

Po stránce přístupu k médiu je opět užita norma CSMA/CA s použitou modulací OFDM. Pro jednotlivé subkanály se již neužívají modulace DBPSK, DQPSK a CCK, proto může přenos dosahovat rychlostí, jenž jsou uvedeny v tabulce 3. Popis kódového poměru a typů modulací je shodný s normou IEEE 802.11g.

Tabulka 3 – závislost přenosové rychlosti na typu modulace a použitém kódovém poměru

Přenosová rychlost (Mbps)	Typ modulace	Kódový poměr	Kódované bity na jeden subkanál	Kódované bity v OFDM symbolu	Bitová rychlost v OFDM symbolu
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	16-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Další parametry jako je popis podvrstev LLC a MAC jsou zcela shodné s IEEE 802.11g.

2.3 Kombinovaný bezlicenční přenos v pásmech 2,4GHz nebo 5GHz

V praxi se můžeme setkat s technologiemi pro přenos dat, které užívají více antén pro příjem a vysílání signálu. Tato technologie je nazývána technologií MIMO. Tyto technologie jsou specifikovány pro bezlicenční provoz a to v pásmu 2,4 GHz, případně 5 GHz.

2.3.1 Standard IEEE 802.11n

Předpokládané schválení normalizačním institutem IEEE je pro tuto normu předpokládáno na konec roku 2010. Pracovní název nového standardu je někdy také označován jako IEEE 802.11-2007.

Do doby, než bude plně schválen nový standard, budou se užívat „předstandardy“ v podobě draft1, draft2 Od zařízení Draft 1 se velmi rychle ustoupilo kvůli nedokonalosti v implementaci technologií MIMO. Ve verzi Draft2 je již vše opraveno a všechna zařízení splňují i plnou zpětnou kompatibilitu s normami IEEE 802.11g a IEEE 802.11b. V dnešních dnech se již na internetu dá nalézt i popis Draft6, ale nemá zásadní odlišnosti od Draft2. Proto zařízení, s nimiž se nyní běžně setkáme, jsou typu Draft2.

Cílem této normy je docílit fyzické propustnosti 100 Mbit/s a vyšší. Toto je realizovatelné za přispění technologie MIMO s konfigurací až 4 vysílačích a až 4 přijímacích antén. Při této konfiguraci se dá dosáhnout rychlosti 600 Mbit/s na L1 vrstvě, což odpovídá rychlosti 400 Mbit/s na L2 vrstvě.

U verze Draft 2 se běžně setkáváme se zařízeními s konfigurací 2x2 antény pro příjem a vysílání, případně 2x3 nebo 3x3 antény pro příjem a vysílání.



Obrázek 9 - Airlive WN-5000R s konfigurací 2R3T a Airlive WN-300R s konfigurací 2R2T

Uvedený standard předpokládá i užití širšího kanálu a to až 40 MHz, na rozdíl od IEEE 802.11b a IEEE 802.11g, kde je užit kanál s šířkou pásma 20 MHz. U zařízení typu 802.11n Draft2 se ale setkáváme s možností nastavení šířky kanálu striktně na 20 MHz, nebo na 20 MHz s automatickým rozšířením na 40 MHz. Při užití pásma 40 MHz mohou být data posílána dvěma nezávislými kanály, což samo o sobě umožňuje zdvojnásobit propustnost oproti technologii IEEE 802.11b nebo IEEE 802.11g, přičemž toto je uvažováno bez užití technologie MIMO pro IEEE 802.11n Draft2. Návrh je koncipován na přenos rychlostí 144 Mbit/s pro pásmo 20 MHz na kanál a 300 Mbit/s pro kanál se šířkou 40 MHz. U jednotek AP je tedy nutno nastavit zda bude souběžně s definovaným kanálem, který se užívá pro přenos v kompatibilním módu s normou IEEE 802.11b a IEEE 802.11g, použit kanál vyšší nebo nižší a tím se umožní zvýšení šířky pásma.

Pro zvýšení rychlosti, ale i dosahu, je použita technologie MIMO. Tato technologie využívá vícečetných signálů, jejich odrazů a případných interferencí. U předchozích norem byl tento stav nežádoucí a byl hodnocen jako rušivý element. MIMO technologie je schopna za podpory SDM signál vyhodnotit korektně, v případě neúplnosti signálu se použije právě zmiňovaný odražený signál. Takto přenášená informace je doručena mezi zařízeními „korektněji“ než u předchozích norem.

Jednotlivé signály, jenž se přenášejí, potřebují pro vysílání ale i příjem každý svoji diskrétní anténu. Proto je uspořádání příkladně 2R2T, nebo 3R3T. Pro korektní fungování této technologie je nutno zabezpečit vlastní VF člen zpracovávající datový stream na každou vysílací nebo přijímací anténu. Toto má za následek vyšší pořizovací cenu jednotek splňující pre IEEE 802.11n normu.

Doposud byla zběžně popisována část pre normy týkající se frekvencí 2,4 GHz. Norma je ovšem od prvopočátku koncipována i pro pásmo 5 GHz. Toto pásmo se po schválení normy normalizačním institutem IEEE jeví jako perspektivnější než pásmo 2,4 GHz. Důvod je více oddělených kanálů a méně zarušené pásmo. Bohužel pro toto pásmo zatím nejsou k dispozici zařízení, které by byly běžně v prodeji.

2.4 Proprietární řešení

Od počátku standardizace norem IEEE 802.11b se můžeme setkávat s proprietárními technologiemi různých firem.

802.11b+	proprietární řešení z roku 2002. S řešením přišla firma Texas Instrument. Technologie vychází z principu DSSS, proto je s ním i zpětně kompatibilní. Užívá se 2x větší šířky pásma než u IEEE 802.11b. Tímto řešením můžeme dosáhnout rychlostí až 44 Mbit/s.
802.11G+	proprietární řešení, poměrně hojně užívané firmami Asus, Dlink, Zyxel, OvisLink a dalšími. Opět je použito větší šířky pásma pro přenos informací. Maximální dosahovaná rychlost na fyzické vrstvě dosahuje 108 Mbit/s.
G+	Proprietární řešení firmy Zyxel. Maximální rychlost na L1 vrstvě je až 125 Mbit/s. Obdobou je SpeedBooster firmy Linksys, případně 125M firmy Asus. Řešení jsou vystavěna na čipech Broadcom.
SuperG	obdoba 802.11G+. Uvedené řešení je vyvinuto firmou Atheros. Užívá se ještě komprese paketů. Reálná přenosová rychlost může dosahovat 40-60 Mbit/s.
MIMO G	proprietární řešení od AirGo Networks. Zařízení pracuje v pásmu 2,4 GHz. Používá větší šířku pásma a technologii MIMO. Umožňuje přenos 108 Mbit/s na L1 vrstvě a dvojnásobný dosah než klasické zařízení s IEEE 802.11g.
Turbo A	proprietární řešení vyvinuté firmou Atheros. Používá se dvakrát širší pásmo kanálu. Umožňuje dvakrát rychlejší přenos než standardní IEEE 802.11a.
Super A	Shodné řešení s Turbo A, opět od firmy Atheros, vedeno pouze pod jiným názvem
XR	proprietární řešení vyvinuté firmou Atheros. Používá nestandardní rychlosti, při slabším signálu. Má větší citlivost (-105dBm) než zařízení s normou IEEE 802.11a (-85dBm). Při použití této technologie může dojít u krátkých spojů k přebuzení jednotlivých zařízení, případně k nežádoucím interferencím na anténách.

3. Doplnky k normě IEEE 802.11

V běžné praxi se nesetkáváme pouze s IEEE 802.11, případně IEEE 802.11a/b/g/n, ale i s dalšími písmeny. Tyto písmena se nazývají dodatky normy IEEE 802.11. Pro přehled zde bude uveden kompletní seznam se stručným popisem.

IEEE 802.11	- vlastní norma přebírající počáteční řešení označované jako 802.11. Řešení s rychlostmi 1 a 2 Mbit/s.
IEEE 802.11a	- doplněk z roku 1999, pásmo 5 GHz, rychlost 54 Mbit/s
IEEE 802.11b	- doplněk z roku 1999, pásmo 2,4 GHz, rychlosti 5,5 a 11 Mbit/s
IEEE 802.11c	- bezdrátový bridge
IEEE 802.11d	- mezinárodní roamingový dodatek z roku 2001, obsahuje i IEEE 802.11c
IEEE 802.11e	- dodatek z roku 2005. Obsahuje vylepšení QoS
IEEE 802.11f	- dodatek platný od roku 2003 do března 2006. Pojednává o komunikaci mezi bezdrátovými přístupovými body
IEEE 802.11g	- již zmíněný standard v pásmu 2,4 GHz, s rychlostí 54 Mbit/s se zpětnou kompatibilitou s IEEE 802.11b
IEEE 802.11h	- dodatek z roku 2004. Upravuje spektrum 5 GHz vztažené k IEEE 802.11a pro region Evropy
IEEE 802.11i	- dodatek z roku 2004. Zlepšení šifrovacího a autentifikačního algoritmu, známo jako WPA2.
IEEE 802.11j	- dodatek z roku 2004 pro region Japonsko. Upravení a rozšíření frekvenčních pásem pro multimedia.
IEEE 802.11k	- vylepšení správy rádiových zdrojů pro vysoké frekvence. Navazuje přímo na IEEE 802.11j.
IEEE 802.11l	- rezervováno, bez dalšího využití
IEEE 802.11m	- upravení standardu po stránce přenosových metod a k nim vztažených drobných úprav
IEEE 802.11n	- ještě neschválený dodatek. Úprava pro přenos vyšší rychlostí, přidání MIMO technologie.
IEEE 802.11o	- rezervováno, bez dalšího využití
IEEE 802.11p	- dodatek specifikující přístup pro pohyblivá prostředí (auta, vlaky, ...)
IEEE 802.11q	- rezervováno, bez dalšího využití
IEEE 802.11r	- dodatek z roku 2008 upravující rychlý roaming mezi jednotlivými přístupovými body
IEEE 802.11s	- dodatek pro samoorganizující se sítě ESS Mesh
IEEE 802.11t	- dodatek pokrývající testovací metody pro bezdrátové sítě
IEEE 802.11u	- dodatek definující spolupráci sítě typu IEEE 802.11 se sítěmi mimo standard IEEE 802.11. Příkladem spolupráce se sítěmi mobilních operátorů.
IEEE 802.11v	- dodatek řešící správu bezdrátových sítí, přesněji konfigurace klientských zařízení během probíhajícího připojení
IEEE 802.11w	- dodatek ošetřující chráněné servisní rámce
IEEE 802.11x	- rezervováno, bez dalšího využití. Milně se zaměňuje za IEEE 802.1x
IEEE 802.11y	- dodatek ošetřující bezlicenční pásmo 3650-3700 MHz pro region USA

IEEE 802.11z	- rozšíření pro konfiguraci zařízení během navázané komunikace (DLS)
IEEE 802.11aa	- rozšíření pro širokopásmový přenos audio a video signálu
IEEE 802.11mb	- rozšíření připravované na rok 2010 až 2011. Mělo by revidovat nepoužívající rozšíření.
IEEE 802.11ac	- rozšíření s předpokládaným schválením koncem roku 2012. Řeší zvýšení propustnosti.
IEEE 802.11ad	- rozšíření s předpokládaným schválením koncem roku 2012. Řeší extrémní zvýšení propustnosti pro krátké vzdálenosti.

4. Zabezpečení bezdrátových sítí

Při přenosu dat pomocí technologie WiFi je nutno zabezpečit jejich ochranu před zneužitím. Hlavní hrozbou je odposlech dat s následným získáním přístupů ke chráněným aplikacím, v krajním případě zablokování kompletní komunikace v rámci bezdrátové sítě. Z těchto důvodů byly od prvopočátku řešeny mechanismy, které by těmto hrozbám účinně zabránily.

Obecně lze hrozby z pohledu celé infrastruktury WiFi sítě a návazných systémů, rozdělit na 3 části:

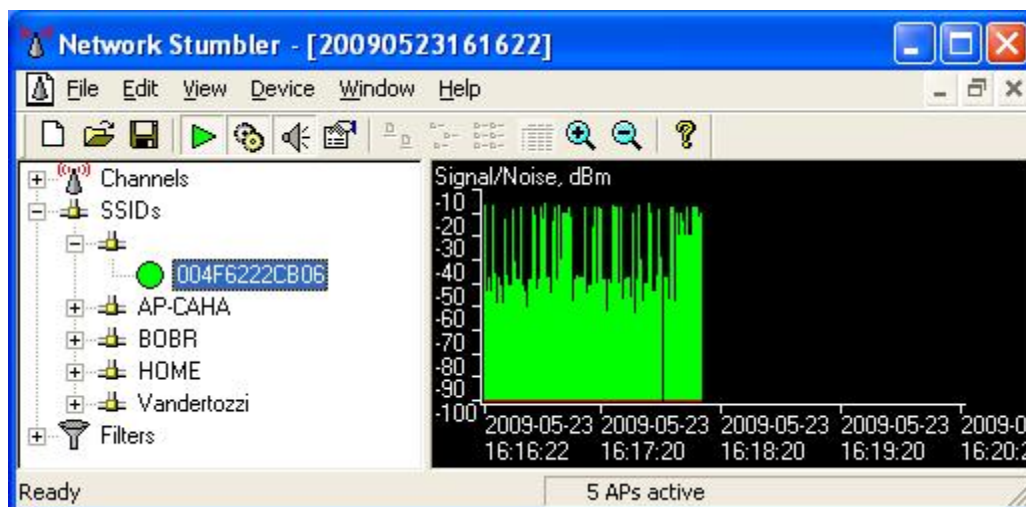
- Neoprávněný přístup do sítě.
- Neoprávněný únik dat způsobený odposlechem a vyčtením přenášených dat.
- Neoprávněná modifikace přenášených dat.

Proto jsou vyvíjeny zabezpečovací mechanismy, které těmto hrozbám mají zabránit. Běžně se setkáváme tedy se třemi mechanismy:

- *Autentizace* – ověření identity na straně odesílatele a příjemce dat
- *Kryptování* – ochrana proti vyčtení dat při odposlouchání komunikace
- *Integrita* – kontrola, při níž se vyhodnocuje, zda nebyla data během přenosu modifikována

4.1 Základní zabezpečení pomocí SSID a filtrace MAC

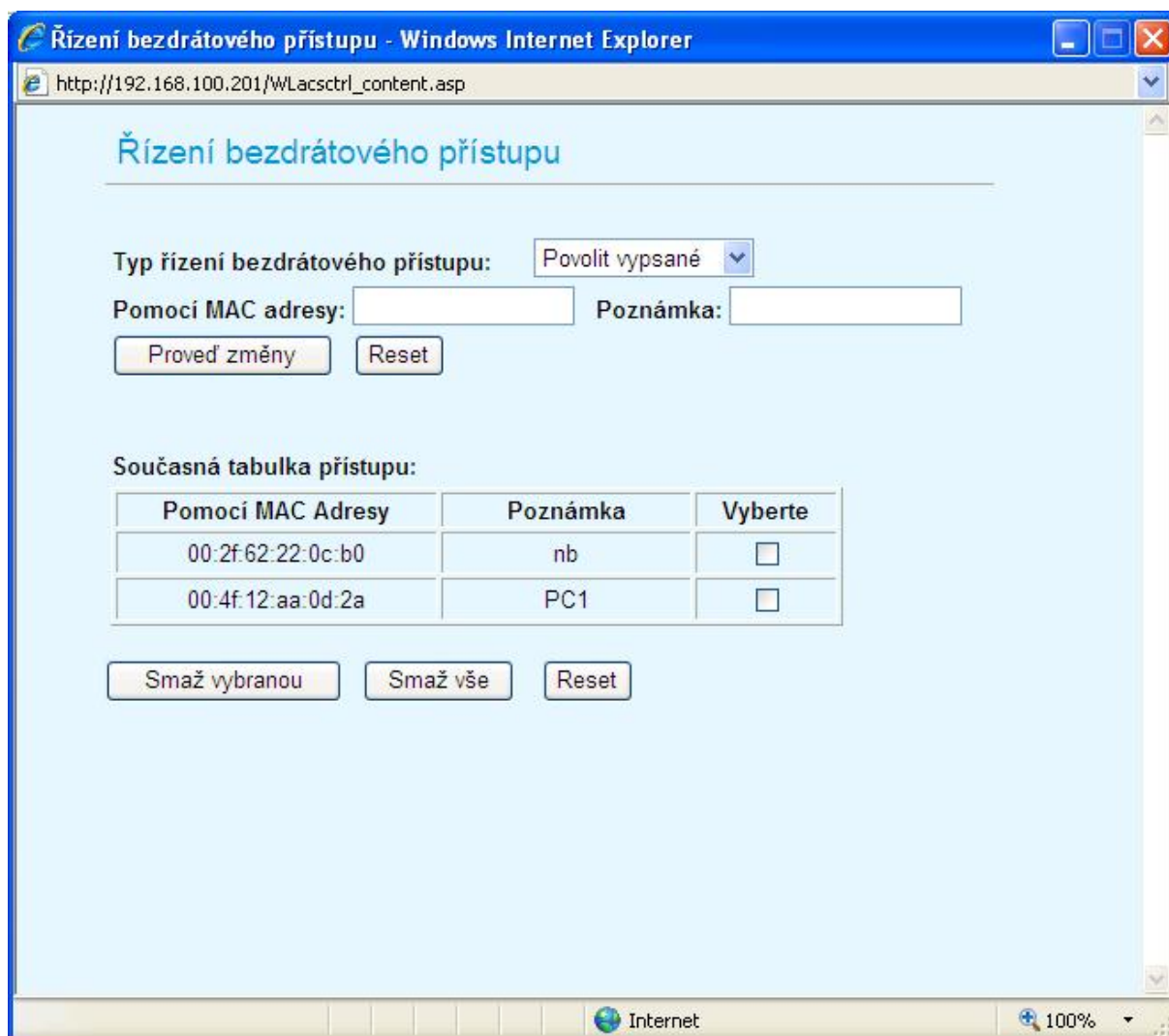
Jedno ze základních zabezpečení užívané pro autentizaci klienta vůči řídicímu prvku je použití skrytého SSID. Každé řídicí zařízení, jednotka AP, vysílá v pravidelných intervalech řídicí rámec s jednoznačným označením sítě, SSID. Tento rámec je možno u většiny dnes dostupných zařízení skrýt, pak mluvíme o skrytém SSID. Pro možnost připojení klienta k AP je tedy nutno toto SSID, ač je skryto, znát. V případě, že je použit jiný řetězec u klienta, než je použit v jednotce AP, nedojde k připojení. Na obrázku 6 je znázorněno zobrazení sítě se skrytým SSID a naopak v programu NetStumbler.



Obrázek 10 – zobrazení jednotlivých SSID v programu NetStumbler
VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

Tento rámec se dá za určitých předpokladů velmi jednoduše odposlechnout při asociační komunikaci jiných klientů s AP, případně lze vynutit tuto komunikaci podvrženým rámcem. Řídící rámec je vždy nekryptovaný, proto z něj lze velmi jednoduše název SSID získat.

Další z možností je filtrování MAC adres přistupujících k AP. Každé síťové zařízení jasně identifikovatelné pomocí MAC adresy, to platí i pro WiFi zařízení. Na straně AP je aplikován mechanismus kontroly přístupu zařízení s unikátní MAC adresou. V ovládacím software běžných AP tedy můžeme nastavit kontrolu jednotlivých zařízení pomocí MAC adres a následně jim umožnit, případně zakázat, přístup k dalším síťovým službám. Ilustrační tabulka se záznamy jednotlivých MAC adres je na obrázku 6.



Obrázek 11 – řízení přístupu u zařízení WL-5460AP v2 pomocí filtrování MAC adres

Bohužel i tato komunikace, kde je zakomponována MAC adresa klienta, probíhá nekryptovaně. Proto při odposlechu komunikace lze opět řetězec s MAC adresou získat.

Následně tuto adresu můžeme vložit do klienta, s nímž chceme komunikovat ve WiFi síti. To nám pak umožní připojit se k AP a následně i k ostatním síťovým službám, pokud není použito dalšího zabezpečení.

Uvedená zabezpečení jsou velmi jednoduchým a velmi zranitelným řešením. Prolomení těchto zabezpečení, v běžné WiFi síti, je otázkou několika minut při použití běžného WiFi klienta (například integrovaná WiFi karta v notebooku) a vhodného programového vybavení pro odchyťování paketů.

4.2 Zabezpečení WEP a WEP2

Součástí standardu IEEE 802.11b je od roku 1999 i mechanismus zabezpečení bezdrátových sítí WEP. Metoda používá proudovou šifrovací metodu RC4 pro utajení přenášené informace a metodu CRC-32 pro ověření korektnosti přenesených dat.

Běžně se setkáváme s 64 bitovým, 128 bitovým případně 256 bitovým WEP klíčem. Klíč se vždy skládá ze dvou částí. Vlastní klíč, který je o délce 40, 104 nebo 232 bitů a inicializačního vektoru vždy o délce 24 bitů. Obě části dávají dohromady kompletní RC4 klíč.

Toto zabezpečení má řadu vad, kvůli kterým je velmi jednoduše prolomitelné. Jedná se především o časté užívání stejného inicializačního vektoru, kolize inicializačního vektoru a statický klíč. Proto se jeho použití do produktivního prostředí nedoporučuje.

U starších zařízení od firmy Agere System se můžeme setkat se zabezpečením WEP plus. Toto zabezpečení je proprietárním řešením, kde jsou odstraněny takzvané slabé inicializační vektory, za jejichž pomoci lze mechanismus prolomit. Toto řešení má výhody pouze za předpokladu, že všechna zařízení komunikující v bezdrátové síti používají WEP plus.

Pozdějším řešením bylo zabezpečení označované jako WEP2. Snaha byla o rozšíření délky inicializačního vektoru a s tím spojeno i jeho více kombinací, a o zesílení šifrování silnějším šifrovacím algoritmem. Bohužel i přes toto rozšíření je mechanismus prolomitelný. Pouze je potřebný delší čas a více odchyťaných paketů. Tak jako u technologie WEP se nedoporučuje použití tohoto zabezpečení v produktivním prostředí.

4.3 Zabezpečení WPA

Po prolomení mechanismů WEP a WEP2, se nároky na zabezpečení WiFi sítí rapidně zvedli. Odezvou tohoto tlaku byl vznik pracovní skupiny řešící doplněk IEEE 802.11i. Tato skupina intenzivně začala řešit nový mechanismus pro kódování přenášených dat v bezdrátových WiFi sítích. Kompletní standard byl schválen v roce 2004, ale již v roce 2002 byl zveřejněn mechanismus pod názvem WPA.

4.3.1 Zabezpečení WPA-PSK

Metoda předsdíleného klíče (PSK) je někdy označována jako „osobní WPA“. Metoda je vhodná pro SOHO segment, tedy malé kanceláře a domácnosti. Pro přístup do sítě se musí

WPA-PSK AES je rozšířením WPA-PSK TKIP. Jedná se o rozšíření o symetrickou blokovou šifru Rijndael. Je užito symetrických klíčů na straně šifrované i na straně pro dešifrování. Délka jednotlivých klíčů může být 128, 192 nebo 256 bitů. Při šifrování se šifrují vždy bloky o velikosti 128 bitů. Doposud není znám případ prolomení tohoto typu kódu při použití silného hesla.

4.3.2 Zabezpečení WPA – spolupráce s 802.1X

Tato metoda zabezpečení předpokládá přímo spolupráci s autentizačním serverem, který splňuje normu IEEE 802.1x. Vzhledem k těmto podmínkám je zřejmé, že není vhodná pro SOHO segment a to z důvodu technické, potažmo finanční náročnosti.

Protokol 802.1X vychází z protokolu PPP, který je pro bezdrátové sítě rozšířen a nazývá se EAP. Pro vysvětlení zavedeme tři oddělené prvky:

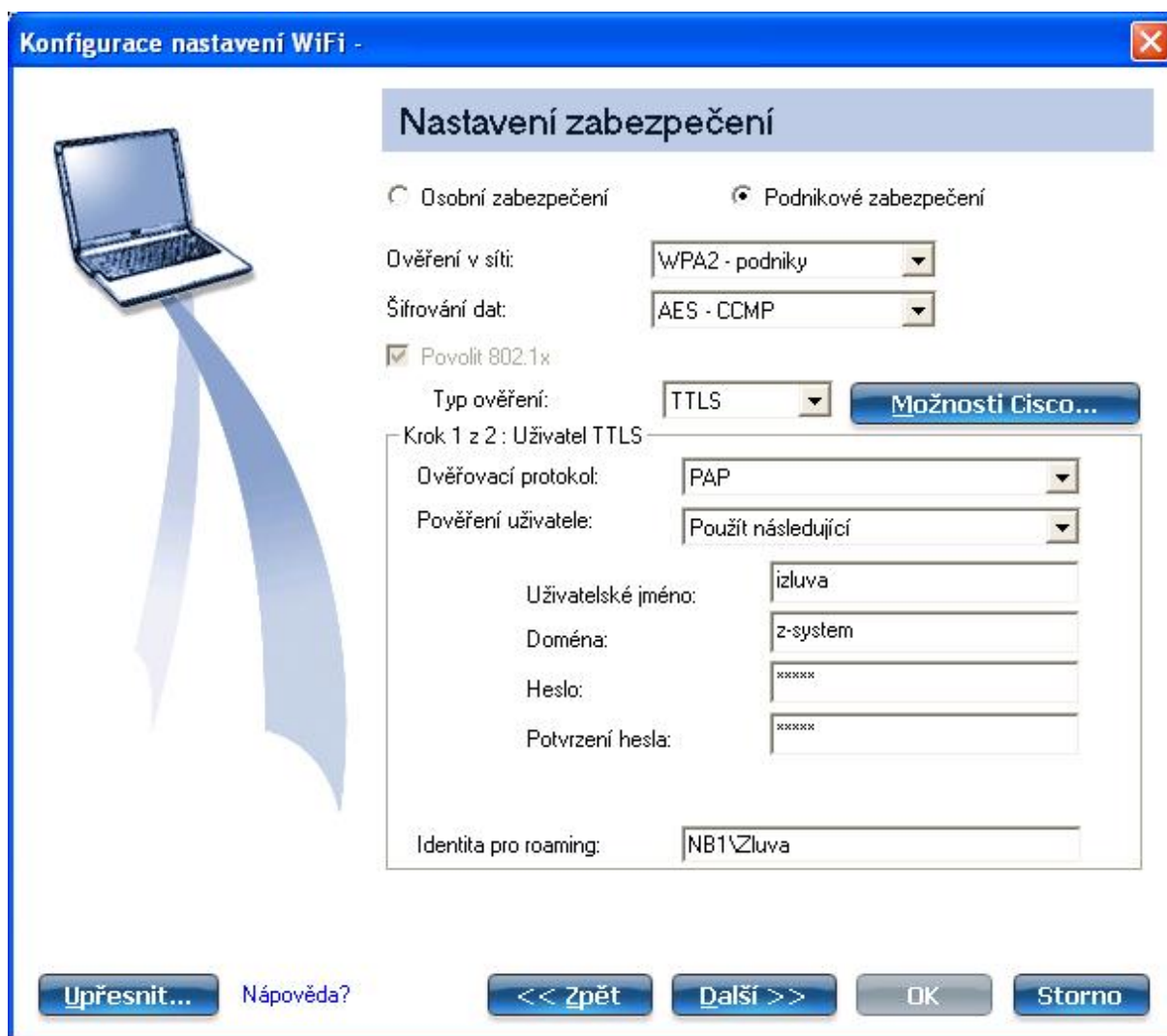
- Žadatel o přístup – klient žádající přístup do WiFi sítě
- Autentizátor – AP, případně specializovaná brána připojená před AP jednotkami. Na tomto prvku dochází k povolení, případně k blokování přístupu do sítě.
- Autentizační server- systém udržující informace potřebné k autentizaci. V praxi se setkáváme nejčastěji s RADIUS servery.

V běžné praxi se můžeme setkat s následujícími typy ověřovacích mechanismů:

- EAP-MD5 – bližší popis můžeme najít v normě RFC 1994 a RFC 2284. Pro ověření uživatele je použito unikátní jméno a heslo. Údaje jsou hašovány pomocí metody MD5 a následně jednoduše ověřeny. Proto není tato metoda vhodná pro WiFi sítě.
- EAP-TLS – bližší popis lze nalézt ve specifikaci RFC 2716. Pro ověření je užito PKI a SSL. Ověření probíhá na základě mechanismu ověření serverového a klientského certifikátu. Klíče jsou generovány dynamicky, následná komunikace probíhá TLS tunelem. Toto řešení je vhodné i pro bezdrátové sítě, ovšem musíme počítat s náročnějším udržováním aktivních PKI certifikátů pro server a klienty.
- EAP-TTLS- tunelované TLS, jedná se o rozšířenou metodu EAP-TLS bez použití ověřovacích certifikátů. Pro ověření je užito unikátní jméno a heslo. Tato metoda je vhodná pro WiFi sítě a nemá potřebu použití PKI certifikátů.
- EAP-PEAP- zabezpečený EAP, opět se jedná o rozšířenou modifikaci EAP-TLS. Užívá druhého TLS tunelu pro ověřovací algoritmus typu EAP.
- EAP-LEAP – řešení bylo navrženo firmou CISCO. Při ověření dochází k ověření klienta a sítě. Princip je obdobný jako u EAP-TLS, ale pro ověření se používá kombinace unikátního jména a hesla místo PKI certifikátu.

4.4 Zabezpečení WPA2 – standard IEEE 802.11i

Do června roku 2004 byly předchozí formy zabezpečení používány pouze jako prozatímní. Až se schválením normy IEEE 802.11i došlo k plné standardizaci, někdy známé jako WPA2. Opět je umožněno fungování s předsdíleným klíčem nebo ve spolupráci se zařízením pro ověření klienta dle IEEE 802.1x. V normě IEEE 802.11i je již zcela výhradně použito normy AES.



Obrázek 13 – nastavení zabezpečení pro síťové karty Intel

5. Antény pro příjem WiFi signálu a jejich příslušenství

Pro lepší příjem, ale i vysílání WiFi signálu, je zapotřebí kvalitnější antény, než bývá standardně dodávané se zařízením. Běžně se k zařízením dodávají antény se ziskem 2 dB. Toto je ovšem pro určitý typ použití zařízení připojeného k anténě naprosto nedostačující. Pro určité typy zapojení se neobejdeme i bez dalších drobností, jako jsou konektory, kabely, propojovací kusy, přepětové ochrany a další.

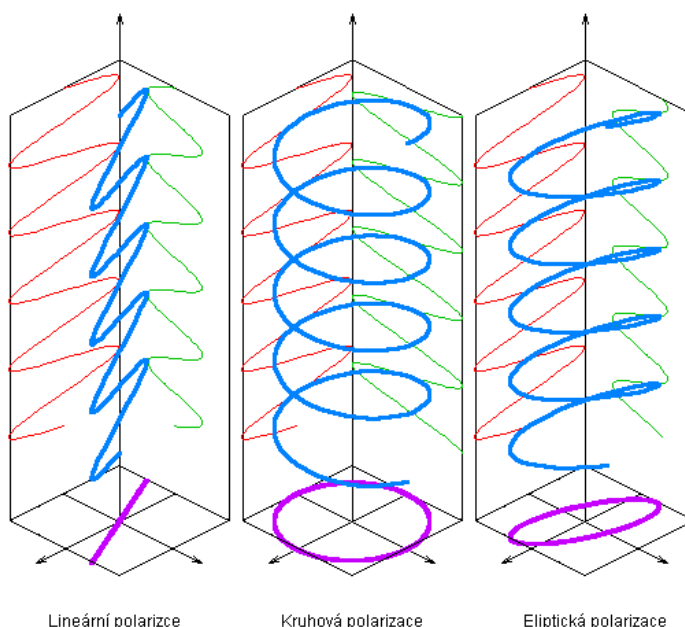
5.1 Základní parametry antén pro WiFi signál

Základními parametry pro specifikaci antén pro WiFi signál jsou především frekvence, pro kterou je anténa určena, zisk antény, pro jaký účel je anténa určena (směrové, všesměrové, sektorové), vyzařovací úhel a zisk.

5.1.1 Polarizace signálu

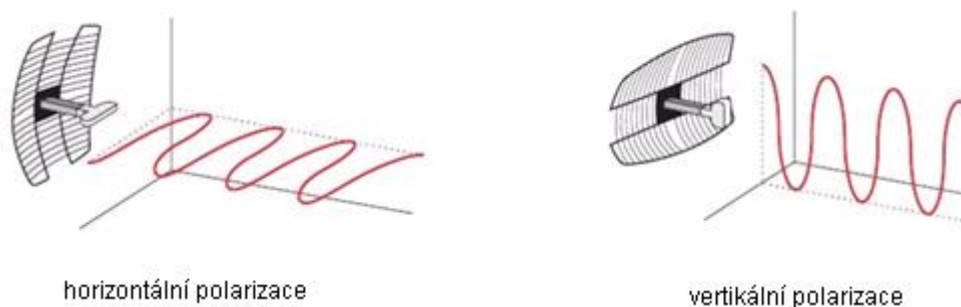
Každý vysílaný signál je specifikován mimo řady parametrů i polarizací. U WiFi sítě se tento parametr uplatňuje velmi podstatně.

Obecně se setkáváme se třemi typy polarizací, lineární, kruhovou a eliptickou. Schematické šíření vln u jednotlivých typů polarizací je znázorněno na obrázku 14. U WiFi sítě se používá výhradně polarizace lineární a to buď horizontální, nebo vertikální (viz obrázek 15). Pro všesměrové antény, bude o nich zmínka později, se uplatňuje výlučně vertikální polarizace. Pro spoje typu bod - bod používáme ryze směrových antén, kde můžeme s výhodou využít jednoho typu polarizace pro jeden spoj a druhého typu polarizace pro druhý spoj, na kanálech, které jsou relativně blízko sebe. Tímto jsme schopni docílit nižšího rušení mezi kanály.



Obrázek 14 – typy polarizací signálu – zdroj Wikipedia

Pro korektní fungování bezdrátového spoje musí být na obou koncích použita shodná polarizace, proto je na zadní straně směrových antén vždy vyobrazen směr polarizace pomocí šipek.



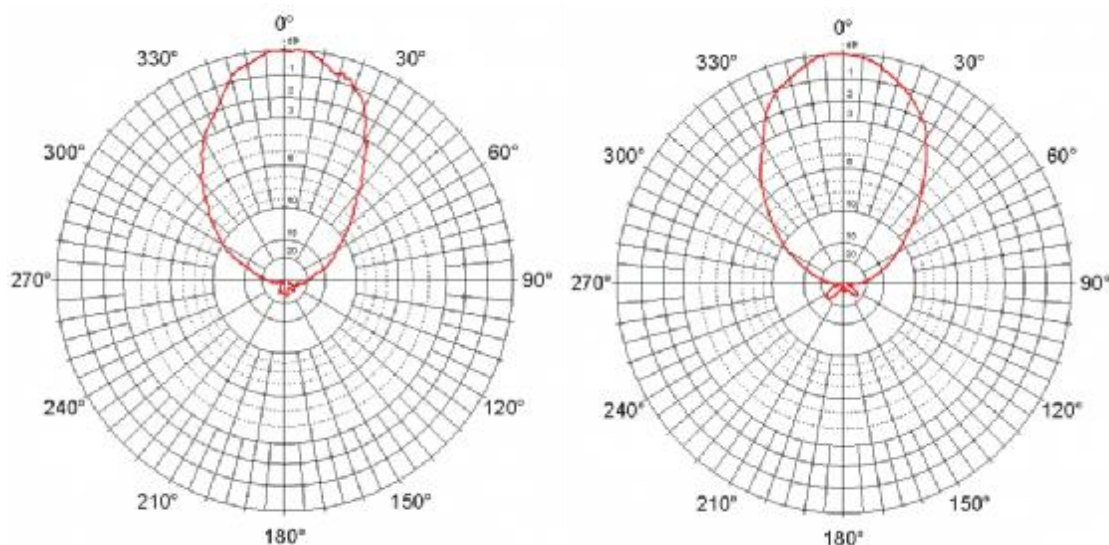
Obrázek 15 – lineární polarizace

5.1.2 Frekvence

Každá anténa je vždy navrhována a koncipována pro jasně definovanou frekvenci. Následně je tato frekvence uvažována jako střední a uvažují se parametry pro krajní frekvence pásma. Proto všechny kvalitní antény mají nejlepší charakteristiku pro 6 kanál u spektra 2,4 GHz. Obdobně toto platí i pro outdoorové subpásmo 5 GHz. Není tedy možné použít anténu pro pásmo 2,4 GHz, pro pásmo 5 GHz a opačně.

5.1.3 Vyzařovací diagram – vyzařovací úhel

Každá anténa má svůj definovaný vyzařovací diagram. Z tohoto diagramu lze odečíst vyzařovací úhel, respektive úhly. Vždy se setkáváme s vertikálním a horizontálním vyzařovacím úhlem. Jedná se o úhel vyzařování elektromagnetických vln, kdy je ještě splněn parametr zisku antény. Příklad vyzařovacího diagramu je na obrázku 16.



Obrázek 16 – vyzařovací diagram pro panelovou anténu JPA-10s vyzařovacím úhlem 60°/60°

5.1.4 Směrnost antén

Parametr směrovosti nám udává pro jaký účel se anténa hodí. Zda pro všesměrové vysílání, ryze směrové nebo sektorové.

Všesměrové antény

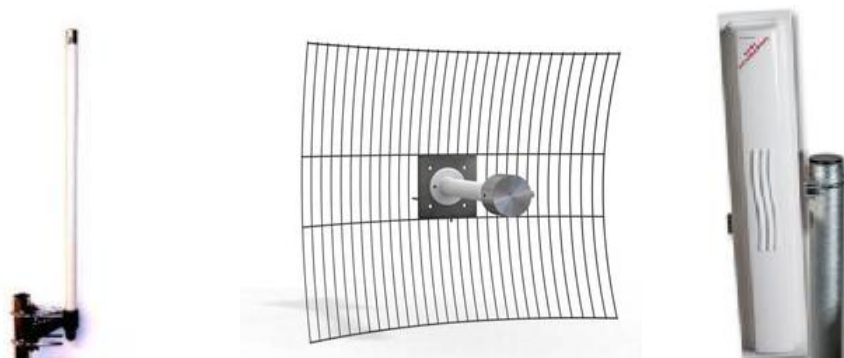
- vyzařovací úhel je 360° v horizontálním směru
- jsou vhodné pro pokrytí většího prostranství ve všech směrech, ideálně se umísťuje do středu prostoru, jenž potřebujeme pokrýt
- mají nejnižší zisk
- dodávají se všemi běžnými AP norem IEEE 802.11a/b/g

Směrové antény

- vyzařovací úhel je většinou velmi úzký v obou rovinách
- jsou vhodné pro spoje typu bod – bod na větší vzdálenosti

Sektorové antény

- antény vhodné pro vykrytí určitého sektoru



Obrázek 17 – ilustrační ukázka typů antén. Zleva všesměrová, uprostřed směrová a zprava sektorová anténa

5.1.5 Zisk a výkon antén

Zisk jako takový, je poměr, mezi výstupním a vstupním výkonem. Je udáván v dB, případně v dBi nebo dBd. Anténa se při vysílání chová pouze jako zářič VF signálu. V anténě při vysílání nedochází k zesílení signálu.

Anténa s kladným ziskem je vždy nějakým způsobem směrová. To znamená, že svoji vysílací/přijímací schopnosti soustředí do nějakého místa, zatímco ostatní místa jsou „hluchá“. Pak zisk antény, je vyjádřen jako poměr, kolikanásobně je zvýhodněn preferovaný směr, oproti tomu, kdyby se anténa chovala ve všech směrech úplně stejně (vyzařovací charakteristika v 3D prostoru by byla koule). Uvažujeme tedy 3D pohled na kompletní vyzařovací charakteristiku antény. Příkladně, pro všesměrovou anténu je zisk kladný v rovině kolmé na zářič, avšak ve vertikální rovině vidíme, že diagram je pokřivený prostorový hyperboloid. Z tohoto důvodu všesměrová anténa nefunguje dobře v prostoru nad sebe ani pod sebe.

Jak již bylo zmíněno, výkon se může udávat v několika jednotkách. Jednotka dBi je vztažená k izotropickému zářiči a jednotka dBd je vztažena k výkonu půleného dipólu. Většinou najdeme zisk udávaný v dBi.

U jednotek AP se setkáváme s maximálním vyzářeným výkonem. Ten je stanoven generální licencí GL-12/R/2000 (doplněna v roce 2003) vydanou ČTÚ. Tento vyzářený výkon, má maximální hodnotu 100 mW, což odpovídá 20 dB. Ovšem je nutno ještě říci, že v této licenci je také zakotvena takzvaná spektrální hustota. Vychází z poznatků, že vysílání neprobíhá na jediné frekvenci, ale v rozprostřeném spektru. Pak se vztahuje část vyzářeného výkonu na každý 1 MHz spektra. Z těchto poznatků ovšem vychází vyzářený výkon na maximálně +17 dBm. Výše uvedený výkon, ale nemá nic společného s výkonem antény. Ten je udáván v jednotkách až desítkách wattů.

Hlavním parametrem je tedy zisk antény uváděný v dB.

5.2 Přepěťové ochrany, kabely pro přenos signálu 2,4GHz a 5GHz

Pro bezpečné připojení antény k AP, případně klientské kartě či AP přepnutého do módu klient potřebujeme další prostředky, jako jsou konektory, kabely případně bleskojistky.

Pokud již máme vybranou jednotku AP a anténu, potřebujeme tyto dvě části spolehlivě spojit. Pro spojení tedy potřebujeme vhodný kabel zakončený VF konektory. Pokud jsou na zařízení a kabelu konektory různé je zapotřebí takzvaný pigtail, nebo-li propojovací kus (viz obrázek číslo 18). Na koncích kabelu jsou osazeny různé typy konektorů.

V dnešní době je patrně na koncových zařízeních nejrozšířenější konektor SMA, případně jeho reverzní varianta označovaná jako RSMA. U starších produktů a u prodlužovacích kabelů se nejčastěji používá konektor typu N. Pro ilustraci jsou konektory vyobrazeny na obrázku číslo 19.

Každý propoj (AP s pigtailem, pigtail s prodlužovacím kabelem atd.) má vždy přesně definovaný útlum daný výrobcem konektoru. Jednotlivé útlumy jsou potom uplatňovány při výpočtech přenosových tras, respektive při následném nastavování vysílacího výkonu na jednotce AP.



Obrázek 18 – PigTail s konektory SMA a konektor typu N



Obrázek 19 – Konektor RSMA a konektor typu N

Konektor je vždy připevněn k VF kabelu. Každý VF kabel je definován jeho hlavním parametrem a to je útlum na jeden metr běžné délky při dané frekvenci. Z toho je zřejmé, že určité typy kabelů jsou vhodné pro spektrum 2,4 GHz, některé pro pásmo 5 GHz. Pro hrubý přehled je v tabulce číslo 4 uvedeno několik nejpoužívanějších koaxiálních kabelů pro pásmo 2,4 GHz včetně jejich vybraných parametrů. Opět se tohoto parametru užívá při výpočtech přenosové trasy.

Tabulka 4 – parametry nejběžnějších kabelů pro pásmo 2,4 GHz

Typ kabelu	Průměr kabelu [mm]	Útlum na 1m délky [dB/m]
MWC 10/50	10	0,24
MWC 6/50	6	0,42
RF240TI	6	0,41
RG-213	11	0,37
H155	5,4	0,48
RG58V	5	0,79

Jako další pasivní prvek, standardně používaný při připojení venkovní antény ke koncovému zařízení, se uplatňuje přepětová ochrana, někdy označovaná jako bleskojistka. Jedná se o pasivní prvek, který má ochránit koncové zařízení před atmosférickou elektřinou. Zpravidla se instaluje na místo přechodu koaxiálního kabelu z vnějších do vnitřních prostor.

Principiálně fungují jako pásmová propust (laděný rezonátor). Všechny nežádoucí frekvence zkratuje, z toho je zřejmé žebleskojistka je opět pro pásmo 2,4 GHz, nebo pásmo 5 GHz. Obecně sebleskojistky testují proudovým nárazem o velikosti 3 kA a délce trvání impulsu 350 μ s. Dalšími technologickými variantami jsou plynovébleskojistky a jiskřiště.



Obrázek 20 – zkratová přepěťová ochrana PKO-N (2,4 GHz)

Dalším prvkem, se kterým se můžeme setkat, je asymetrický útlumový člen. Tento člen se používá při použití starších WiFi zařízení, která neumí regulovat výstupní výkon. Pokud, bychom u takového zařízení použili anténu s vyšším ziskem, dostali bychom se nad povolený limit ČTÚ pro vyzářený výkon. Tyto asymetrické útlumové členy mají velmi nízký útlum směrem od antény k zařízení, typicky 1 dB. Ve směru druhém se útlum pohybuje od 3 do 15 dB dle typu členu.



Obrázek 21 – asymetrický útlumový člen pro 2,4 GHz, s útlumem 13 dB

6. Přenosová trasa

Na přenosovou trasu je možno pohlížet ze dvou stran. Teoretický pohled, založený na matematických výpočtech a reálný pohled, kde je uplatněno matematických výpočtů a zkušeností z reálného provozu WiFi sítí.

Teoretický pohled zahrnuje celou trasu od aktivního koncového zařízení na straně vysílače po aktivní zařízení na straně přijímače. Vždy je zohledněna kompletní trasa, tedy část od VF konektoru po anténu u vysílací strany, část zohledňující prostředí mezi anténami a část od antény po VF konektor na straně přijímací.

Části pasivních prvků jako jsou konektory, kabely,bleskojistky a antény jsme si již popsali. Definici maximálního vyzářeného výkonu na anténě jsme již definovali výše. Jedná se o 17 dB. Pro teoretické výpočty tedy potřebujeme ještě hodnoty útlumu prostředí v závislosti na vzdálenosti vysílací a přijímací části (viz tabulka 5).

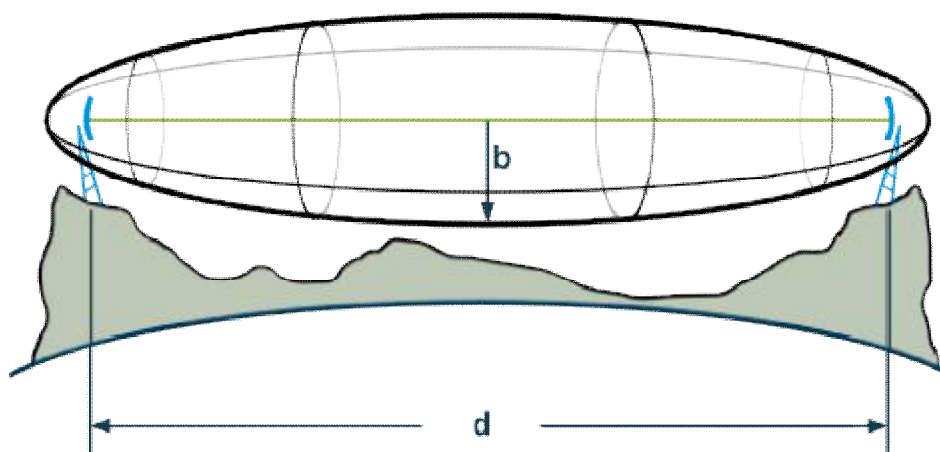
Tabulka 5 – závislost útlumu trasy na vzdálenosti při přímé viditelnosti

Vzdálenost [m]	50	100	200	300	400	500	600	1000
Útlum [dB]	74	80	86	90	92	94	96	100

Vzdálenost [m]	1500	2000	3000	4000	5000
Útlum [dB]	103	106	109	112	114

Hodnoty z tabulky 5 jsou platné za předpokladu přímé viditelnosti mezi přijímačem a vysílačem a za předpokladu zcela volné první Fresnelovy zóny.

První Fresnelova zóna je prostorový elipsoid, v jehož prostoru dochází k šíření vln, na nichž jsou modulována data. Proto by tato zóna měla být pro ideální případ zcela volná a neměly by do ní ani částečně zasahovat překážky (stromy, střechy domů ...). Na obrázku číslo 22 je zobrazena schematicky První Fresnelova zóna. Pro praktickou implementaci trasy je nutné znát vzdálenost jednotlivých aktivních zakončení d [m]. Poloměr zóny b [m] je pro vybrané vzdálenosti možno odečíst z tabulky číslo 6.



Obrázek 22 – První Fresnelova zóna – zdroj Wikipedia

Tabulka 6 – poloměr První Fresnelovy zóny

Vzdálenost d [m]	100	200	300	500	700	1000	1200	1500
Poloměr b [m]	0,9	1,25	1,55	2	2,35	2,8	3,1	3,45

Vzdálenost d [m]	2000	2600	3000	4000
Poloměr b [m]	4	4,55	4,9	5,65

Fresnelova zóna je rotační elipsoid, jak již bylo uvedeno. Má poměrně strmý nástup, takže pro vzdálenost 1000m sice máme průměr zóny 5,6 m, ale již ve vzdálenosti 100 m od vysílače, či přijímače je průměr zóny 3,4 m. S touto skutečností je nutno při návrhu trasy počítat.

Narušení První Fresnelovy zóny nemá většinou za následek extrémní snížení úrovně signálu, ale nárůst rušivých odrazů, čímž dochází ke zvýšení latence, případně ztrátivosti paketů. Při zastínění Fresnelovy zóny ze 40% dochází již k velmi těžké degradaci spoje. V praxi může dojít k narušení Fresnelovy zóny třeba výstavbou nového domu, růstem zeleně, průjezdem automobilu atd.

Dalším parametrem nutným pro vyhodnocení možné přenosové rychlosti je citlivost WiFi zařízení. Tabulka vyjadřující vztah přenosové rychlosti a velikosti útlumu je dodávána vždy výrobcem zařízení. Pro ilustraci jsou v tabulce 7 uvedeny hodnoty pro zařízení WL-5460 AP v2 a v tabulce 8 hodnoty pro zařízení WLA-5000AP v3.

Tabulka 7 – Závislost přenosové rychlosti na citlivosti (útlumu) pro WL-5460AP v2

Útlum [dBm]	-91	-90	-90	-86				
Rychlost při IEEE 802.11g [Mbps]	1	2	5	11				
Útlum [dBm]	-87	-87	-86	-84	-82	-78	-73	-70
Rychlost při IEEE 802.11g [Mbps]	6	9	12	18	24	36	48	54

Tabulka 8 – Závislost přenosové rychlosti na citlivosti (útlumu) pro WLA-9000

Útlum [dBm]	-90	-89	-88	-86	-82	-79	-73	-71
Rychlost při IEEE 802.11a [Mbps]	6	9	12	18	24	36	48	54
Útlum [dBm]	-89	-88	-88	-86	-82	-79	-75	-73
Rychlost při IEEE 802.11a [Mbps]	6	9	12	18	24	36	48	54

S těmito parametry již lze provést teoretický výpočet přenosové trasy. Při výpočtu postupujeme následujícím způsobem:

- +výstupní výkon vysílače (nutno regulovat kvůli limitu ČTÚ)
- útlum pigtailu (redukce SMA/N, typicky 2 dB)
- útlum bleskojistky (2 dB)
- útlum dvou konektorů (2 x 1dB)
- útlum kabelu na vysílací straně ("měrný útlum kabelu" x délka kabelu v metry)
- + zisk vysílací antény

mezisoučet (vysílací výkon – nesmí přesáhnout zmiňovaných 17 dB)

VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

- útlum trasy
- + zisk přijímací antény
- útlum kabelu na přijímací straně ("měrný útlum kabelu" x délka kabelu v metry)
- útlum dvou konektorů (2 x 1 dB)
- útlum bleskojistky (2 dB)
- útlum pigtailu (redukce N/SMA, typicky 2 dB)

výsledek (hodnota musí být vždy větší než je citlivost přijímače)

Tento postup opakujeme pro oba směry. Je to z důvodu různých komponent na každé straně.

6.1 Zarušení signálu

O zarušení signálu můžeme hovořit v různých pohledech. Jedná se vlastně o vliv prostředí na kvalitu signálu. Vlivy mohou mít různý charakter, od počasí, přes překážky v přímé trase, vliv zařízení fungujících na obdobné frekvenci jako WiFi, až po jiné WiFi sítě komunikující v blízkém pásmu.

Patrně největším rušivým elementem jsou zařízení pracující na obdobné frekvenci. Jedná se například o starší typy mikrovlnných trub a Bluetooth zařízení. U většiny modernějších WiFi zařízení je už zcela eliminován vliv signálů zprostředkovávající přenos dat mezi jednotlivými Bluetooth zařízeními. Dalším, asi nejčastějším vlivem rušení je koexistence mnoha WiFi sítí. Jak již bylo zmíněno, existují pouze tři nepřekrývající se kanály. Při koexistenci právě tří sítí na právě zmíněných kanálech ještě nedochází k rušení. Pokud je ovšem použito více kanálů, které jsou blízko sebe při využití více sítěmi, pak dochází k rušení mezi jednotlivými sítěmi. Toto se může projevovat delšími latencemi, výpadky komunikace, nebo kompletním znefunkněním WiFi sítě, v případě použití stejného kanálu pro více jak jednu síť. Rušení signálu způsobuje odraz signálu vznikající na rozhraní materiálů, při prostupu pevnými látkami. Následně dochází k rušivým interferencím signálu, který nemusí být korektně vyhodnocen.

K rušení dochází při koexistenci příkladně dvou WiFi sítí ač od sebe dostatečně vzdálených, fungujících na stejném kanálu. K této situaci dochází za předpokladu špatně zvolených typů antén a špatně volené velikosti vyzářeného výkonu. Pak může jedna síť fungovat zcela bez problémů a druhá nemusí fungovat v extrémním případě vůbec.

MAC	SSID	Name	Chan
0013D424F147	TUMA		6
001FC65304F3	ASUS		1
0022151B7CEA	Simaci		1
00221521B491	Persefone		1
0015F26AD919	bohunka		4
004F6701F348	bel20w		6
0002CFB3FB4B	Prichy		1
0021298321AC	senkovi		3
00120EA04D60	APKORCOVI		1
004F62048EF6	BOBR		3
0018F3A8DC91	MAL		6
0018F3DA094A	sergis		7
0023546DD6B6	-doma-		1+
004F6702AE01	HOME		4*

Obrázek 23 – výstup z programu NetStumbler – koexistence WiFi sítí na stejných kanálech

6.1.1 Vliv počasí na venkovní trasy

Pásmo 2,4 GHz a 5 GHz spadá do spektra takzvaných mikrovln. Mikrovlny se přeměňují ve vodě a organických hmotách na teplo.

Počasí jako takové má vliv na rušení signálu z pohledu množství a skupenství vody obsažené na venkovní přenosové trase. Za příliš hustého sněžení nebo deště může dojít k drobné degradaci signálu, tím i ke zhoršení propustnosti sítě. Pro hustý déšť (150 mm / h) dochází k útlumu cca 0,02 dB/km.

Dá se tedy říci, že spolehlivost WiFi sítí je z velmi malé míry závislá na dešti či sněžení.

6.1.2 Vliv prostředí u indoorových WiFi sítí

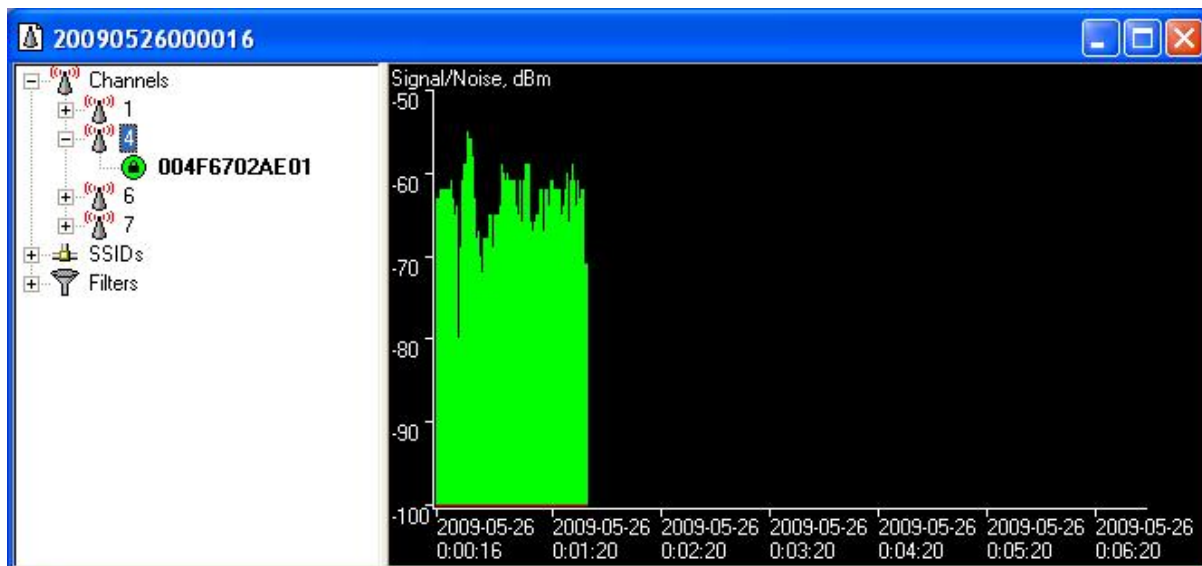
Indoorové sítě malých velikostí jsou stále rozšířenější. Řada uživatelů internetu má sice pevné připojení DSL linkou nebo pomocí kabelového operátora, ale chtějí využít „volnost pohybu“ po svém bytě nebo domě se svým notebookem.

Málo tvůrců a uživatelů, těchto drobných, především domácích WiFi sítí, ovšem uvažuje nad tím, že každý vstup pevnou látkou (zdivo, dveře ...) způsobí přinejmenším útlum přenášeného signálu. Příkladně u panelové zástavby je v každé stěně, podlaze i stropu použit kov, který se v určité míře chová jako Faradayova klec. Z druhého pohledu při průchodu WiFi signálu touto ocelovou výztuží, dochází k jeho deformacím a odrazům.

Tyto rušivé vlivy se pak nezkušený tvůrce WiFi sítě snaží potlačit co nejvyšším vyzářeným výkonem na straně vysílače, což má za následek, že v blízkosti vysílače dochází k přebuzení přijímače (opět způsobí špatný příjem) a v blíže nespecifikovaných místech dochází ke vzniku míst bez pokrytí signálu (způsobeno odrazy a interferencemi).

Například při vyzářeném výkonu 22 dB (mimo limit ČTÚ) a následnému prostupu jednou železobetonovou zdí o šířce 15 cm je síla signálu ve vzdálenosti 8 m od vysílače mezi

-60 a -70 dB. Na obrázku 24 je pro tento případ vyobrazena charakteristika z programu NetStumbler.



Obrázek 24 – síla signálu ve vzdálenosti 8m od AP, za nosnou železobetonovou zdí

6.2 Přímá viditelnost

Jak již bylo zmíněno výše, pro kvalitní přenos WiFi signálu je potřeba ideálně přímá viditelnost a prostor odpovídající První Fresnelově zóně. Často se druhý aspekt pomíjí. Příkladně při výstavbě WiFi sítě v zimním období jsou všechny stromy bez listů a při měření síly signálu a propustnosti je spoj v naprostém pořádku. Ovšem se změnou ročního období dojde k olistění, které způsobí zvýšení útlumu na trase mezi anténami. Pokud se k tomuto přidá déšť a listů na stromě je mokré, může dojít v krajním případě až ke ztrátě spojení mezi koncovými body (záleží z kolika procent je Fresnelova zóna zastíněna olistěným stromem).

V určitých případech se setkáme s anténou umístěnou za oknem. Bohužel takto umístěná anténa, i když má „přímou viditelnost“, tak z pohledu WiFi signálu se jedná o umístění za překážkou. Signál se tedy musí šířit skrz zasklení okna. Bohužel moderní zasklení používá kvůli splnění parametrů tepelného prostupu sklem látky, které zabraňují šíření WiFi signálu. Proto je nutno počítat i s touto eventualitou.

6.3 Nepřímá viditelnost

Obecný princip WiFi sítí vůbec nepředpokládá přenos signálu bez přímé viditelnosti. Ovšem zcela běžně se tento jev vyskytuje u již zmíněných indoorových WiFi sítí.

Pokud se jedná o venkovní síť, uplatňují se fyzikální vlastnosti vlnění. Vlna pro frekvenci 2,4 GHz má délku zhruba 12,5 cm, pro frekvenci 5 GHz se jedná o délku vlny cca 6 cm. Tyto vlny se zcela odrazí od překážky, která je větší, než je velikost vlny. V případech

průchodu vodou nebo organickými látkami jsou měněny na teplo, jak již bylo zmíněno dříve. Z tohoto důvodu můžeme WiFi signál detekovat i na místě kde není vůbec vidět na vysílač. Bohužel tento signál bývá často velmi deformovaný, takže je nevhodný pro připojení WiFi signálu v normách IEEE 802.11 a/b/g. Pro normu IEEE 802.11n se právě zmíněných odrazů využívá pro zvýšení kvality přenosu a ke zvýšení dosahu WiFi sítě využívající tuto normu.

Další jev, se kterým se můžeme běžně setkat, je difrakce na hraně.

Některá speciální zařízení, jako je třeba Motorola Canopy, využívá právě zmíněných jevů, odrazu a difrakce. Na běžném zařízení normy IEEE 802.11 b/g je sice uvedené zařízení detekováno jako zařízení s normou IEEE 802.11b, ale nelze se k němu připojit. To je způsobeno proprietárním řešením implementovaným firmou Motorola.

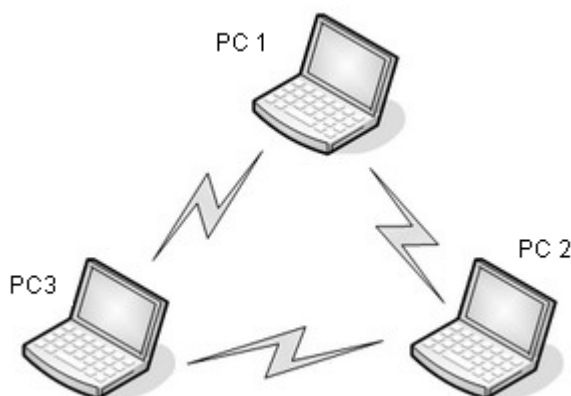
7. Možnosti konfigurace WiFi zařízení

Nyní se budeme zabývat možnostmi konfigurace WiFi zařízení z pohledu koncových zařízení a z pohledu možností konfigurace u univerzálních WiFi zařízení. Další popis je platný pro většinu dostupných WiFi multifunkčních zařízení podporující normy IEEE 802.11a/b/g.

7.1 Klient v módu Ad-hoc

Tento mód WiFi zařízení nám umožňuje spojení několik koncových zařízení mezi sebou v režimu rovný s rovným. Všechna zařízení komunikují se všemi ostatními, tento stav se nedá měnit. V síti tedy není definován řídicí bod. Tento mód je výlučný pouze pro koncová zařízení, případně pro univerzální zařízení nastavená do módu klient s nastavením komunikace v sítích AD-hoc. S tímto řešením se v praxi setkáváme velmi okrajově. Důvod je především nutnost přímé viditelnosti mezi všemi klienty.

Pro zabezpečení takové sítě je možno použít některý z typu již uvedených zabezpečení WiFi sítí po stránce krytování signálu. Není možné použít funkce filtrování přístupů pomocí MAC adres.



Obrázek 25 – schéma sítě Ad-hoc

7.2 Klient

Uvedený mód můžeme najít ve všech koncových WiFi zařízeních (např. síťové karty, VoIP telefony, WiFi print servery, WiFi IP kamery ...). Tato funkce umožňuje připojení klienta (koncového zařízení) k řídicí jednotce AP. V síti tedy musí být alespoň jedna jednotka AP, bez ní nelze síť vytvořit. Dle nastavení jednotky AP mohou klienti komunikovat mezi sebou, případně mohou být od sebe izolováni. V tomto případě není nutná přímá viditelnost mezi jednotlivými klienty je možno komunikovat na větší vzdálenosti s použitím směrových antén. Pro zabezpečení sítě je možno použít jedno z již uvedených zabezpečení, případně jejich kombinace (filtrace dle MAC adresy + kódování typu PSK WPA-TKIP). Tento model

se někdy nazývá infrastrukturální. Některá AP se v módu AP dají přepnout na fungování v sítích Ad-Hoc. Tímto nastavením dojde k přepnutí AP do módu klient typu Ad-Hoc. Na obrázku 26 je vyobrazen princip komunikace v síti s jednotkou AP a koncovými zařízeními typu klient, případně univerzálními WiFi zařízeními konfigurovanými pomocí SW jako klient.



Obrázek 26 – struktura sítě s AP s jednotlivými klienty

7.3 Bridge

Tento mód lze konfigurovat u multifunkčních WiFi zařízení. Správnou konfigurací dosáhneme vytvoření transparentního mostu mezi koncovými zařízeními. Nejrozšířenější je spoj typu point to point. Jedná se pouze o most mezi dvěma zařízeními. Lze ovšem konfigurovat i spoje typu hvězda. V případě této konfigurace ovšem dochází k nepříjemným vlivům, dělení přenosové rychlosti. To bude popsáno níže v části reálných měření.

Pro konfiguraci tohoto módu pro dvě zařízení je nutné znát MAC adresy WiFi síťových rozhraní protějšního prvku. Most se navazuje pouze na základě kontroly MAC adres. Pro funkci není vyžadováno zadání SSID, to také není vysíláno. V zaručenějších oblastech se doporučuje použít pevně nastaveného kanálu.

Pokud je most dobře nakonfigurovaný je poměrně velmi složité komunikaci odposlouchávat. Jak již bylo zmíněno SSID není vysíláno a nelze ani tento spoj nalézt pomocí běžných programů, jakou jsou ovládací programy pro WiFi karty nebo program NetStumbler. Pokud by měl takový spoj nabourán z vnějšku, muselo by dojít k odchytní paketů s následným vyčtením MAC adres koncových zařízení mostu, odstínění jednoho konce mostu a nahrazení zařízením s naklonovanou MAC adresou, která před tím patřila koncovému bodu, který je již odstíněn. Toto se v reálném provozu poměrně velmi problematicky realizuje, proto se na tyto spoje ani nepoužívá zabezpečení typu krytování WPA případně WPA2, ač je to možné u většiny zařízení.

Přenos dat probíhá zcela transparentně, používá se například na spoje mezi dvěma LAN.



Obrázek 27 – struktura most

7.4 WDS opakovač

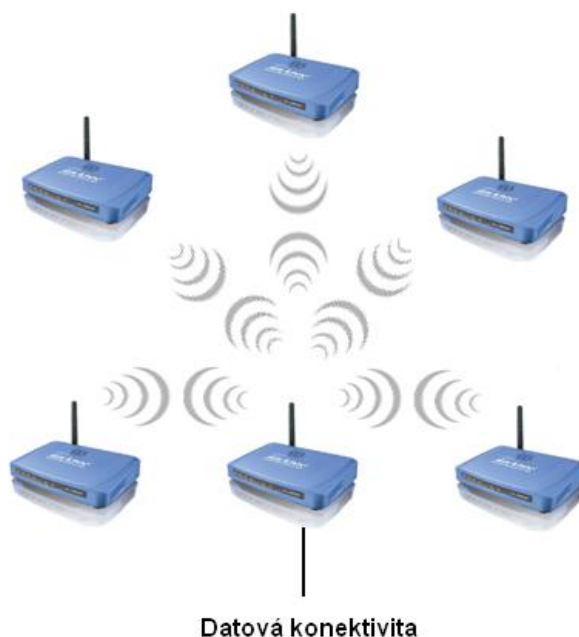
Bezdrátový distribuční systém je systém pro distribuci WiFi signálu. Technologie WDS provádí tedy komunikaci mezi jednotlivými jednotkami, které jsou mezi sebou svázány pomocí kontroly MAC adres, tak jak je tomu u zapojení typu most. Navíc každá jednotka dále distribuuje WiFi signál v módu AP. Celá struktura funguje na jednom jasně definovaném WiFi kanálu s jedním SSID. U jednotlivých WDS zařízení je možno zapnout podporu IAPP, pak se celý systém chová jako plně roamingový.

Pro řešení WDS systému lze použít tři základních typů zapojení jednotlivých WDS zařízení. Jedná se o:

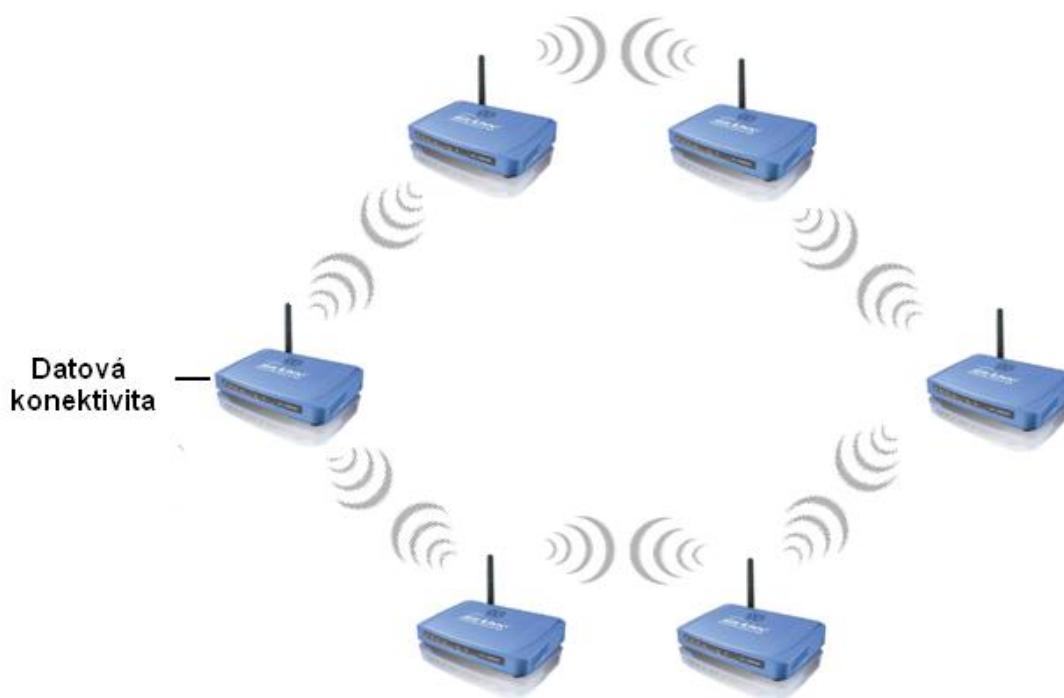
- 1) řetězec – jednotlivá zařízení jsou zapojena jako řetěz za sebou (viz obrázek 28)
- 2) hvězda – na jednu centrální jednotku je napojeno více dalších jednotek (viz obrázek 29)
- 3) kruh – jednotky jsou zapojeny do kruhu, pro funkčnost je potřebná podpora protokolu STP. Struktura je ilustračně vyobrazena na obrázku 30.



Obrázek 28 – schematické zapojení WDS zřetěžení



Obrázek 29 – schematické zapojení WDS hvězda



Obrázek 30 – schematické zapojení WDS kruh

Každá z těchto technologií má své výhody i nevýhody. U zapojení do řetězce dochází ke snižování propustnosti v exponenciální řadě s každým zapojeným dalším WDS bodem. Příkladně na první AP v módu WDS získáme propustnost o velikosti X . Na dalším bodu už je to pouze zhruba jedna polovina této přenosové rychlosti. Na dalším bodu už jen jedna čtvrtina X . Při výpadku některého prvku v zapojení typu řetěz je znefunkčnena část od tohoto prvku dále. Pokud dojde k výpadku hned prvního AP v módu WDS, ke kterému je připojena další datová konektivita, dojde k odpojení všech klientů připojených na tento systém k této konektivitě.

Pro zapojení do hvězdy použijeme s výhodou terminologii pro síťové grafy. Přenosová rychlost mezi AP umístěným na kmenu grafu a každým dalším AP (list grafu) je ve výši X . Ovšem pokud mezi sebou komunikují klienti připojení ke koncovým AP (na listech grafu), je přenosová rychlost pouze polovina X . Při výpadku koncového AP v módu WDS přichází o konektivitu, která je připojena k centrálnímu AP, pouze ti klienti, co se připojují k AP, který má výpadek. Pokud ovšem vypadne AP na kmeni grafu, dochází k celkovému výpadku sítě.

U kruhové topologie je nutno použít navíc STP protokol. Ten zabrání vzniku redundantních spojení v síti. Následně tedy vzniká z kruhové topologie kombinace topologie hvězda a řetěz, s upřesněním že se jedná maximálně o dvě větve, případně pouze o jednu. Pak jde přímo o strukturu řetěz. Následky výpadku WDS zařízení se pak vztahují pouze na tuto jednotku. V případě výpadku WDS jednotky, ke které je připojena konektivita, má za následek výpadek u všech uživatelů.

Všechna tato zapojení mají jednu velkou nevýhodu pro reálný datový provoz. Struktura WDS sítí není uvnitř routována. Pokud dochází k nežádoucí komunikaci od klientů (zavírované PC, špatně konfigurované dotazování na browsermastering, ...), pak tato se šíří po všech WDS prvcích a následně i ke všem klientům a může způsobovat nežádoucí trafik.

7.5 Univerzální opakovač

Zařízení nakonfigurované do tohoto módu funguje jako klient vůči AP, ke kterému se připojuje a následně samo jako AP, se kterým komunikují už koncoví klienti. Pro konfiguraci „klientské části“ je potřeba zadat kanál, na kterém se přijímá WiFi signál, SSID sítě, ke které se připojuje, eventuálně zabezpečení které je ve WiFi síti použito (WPA, WPA2). Pro konfiguraci „vysílací“ části už zadáváme pouze SSID jenž bude použito. Číslo kanálu a zabezpečení se přebírá z klientské části. Teoretické opodstatnění je v rozšíření rozsahu sítě, to je ovšem poměrně diskutabilní. Pokud je použita jediná anténa, která přijímá WiFi signál od ISP, tak vysílání z virtuálního AP pak zase probíhá za pomoci této antény. Z tohoto pohledu tedy toto nastavení není vhodné pro příjem WiFi signálu od providera a následné šíření WiFi signálu v rámci domu nebo bytu. Následkem tohoto nastavení je povětšinou rušení signálu ve WiFi síti ISP a tím i ke zhoršení přijímaného signálu. Na obrázku 31 je uvedeno schematicky zapojení pro tuto konfiguraci.



Obrázek 31 – schematické zapojení pro mód univerzální opakovač

7.6 WISP mód

Tento mód byl vyvinut firmou OvisLink pro jejich multifunkční bezdrátová zařízení. V nynější době se tento název s téměř stejnou vnitřní konfigurací používá u řady dalších výrobců. Jak název napovídá, jedná se o WiFi klienta s následným routováním na porty LAN.

V tomto módu je tedy WAN port routeru zprostředkován WiFi částí. Zde tedy pro WiFi část musíme zadat parametry od ISP (pevná IP, dynamicky přidělovaná IP případně naklonovaná MAC adresa, typ zabezpečení ...). Pro LAN část je pak možnost zapnout překlad adres NAT, rozsah IP adres pro přidělování DHCP serverem a další. Pokud použijeme takto nakonfigurované zařízení pro koncové klienty, zbavíme se již zmiňovaného nežádoucího trafiku v páteři WiFi sítě.



Obrázek 32 – schematické zapojení zařízení s WISP módem

7.7 WISP + univerzální opakovač

Tento mód je sloučením předchozích dvou možných nastavení. V podstatě bychom jedním zařízením vytvořili klienta pro WiFi od ISP, router s WAN částí zprostředkovanou WiFi routující na LAN porty zařízení a na „virtuální AP“. Bohužel pro virtuální AP je definován kanál pro komunikaci od ISP. Tento kanál nelze změnit, protože by došlo ke znefunkčnění přístupu ke službám od ISP. Shodná definice jak pro ISP klienta tak pro vzniklé „virtuální AP“ je i pro zabezpečení. Pokud tedy ISP zabezpečení na straně klienta nepoužívá, nemůžeme ho zapnout ani pro nově vzniklé AP. Opět by došlo ke znefunkčnění koncového bodu. Další nevýhody jsou popsány v bodu 6.5.



Obrázek 33 – schematické zapojení zařízení nakonfigurovaného jako WISP + universal repeater

7.8 Režim brána

Tento režim patří k hojně využívaným u koncových zákazníků, kteří si sami staví domácí bezdrátovou síť. Například u uživatelů kabelových operátorů, kdy je do domácnosti dovedeno připojení s jednou IP adresou.

Jeden z portů LAN, je v tomto módu nakonfigurován jako WAN port routeru. Následně je možno zapnout překlad adres NAT na druhý LAN port a do WiFi části, která je nakonfigurována jako AP. Pro WiFi část je možno nastavit jedno z možných zabezpečení, které zvládá zařízení, případně jejich kombinaci (WPA2 a kontrola MAC adres). Vyspělejší zařízení umí například filtraci URL adres, realizovat demilitarizovanou zónu na základě definice IP v lokální síti pro případné připojení serveru a mnoho dalších funkcí.



Obrázek 34 – schematické zapojení zařízení v módu gateway

8. Popis použitých zařízení

Z pohledu zadání práce byla volena zařízení splňující normu IEEE 802.11a, IEEE 802.11g a IEEE 802.11n Draft2. Zařízeními typu IEEE 802.11b již nejsou běžně dostupná, proto tato zařízení nebyla použita pro jednotlivá měření.

8.1 multifunkční zařízení WL-5460AP v2

Uvedené zařízení podporuje normy IEEE 802.11b a IEEE 802.11g. Je určeno pro provoz v bezlicenčním pásmu 2,4 GHz. WL-5460AP v2 lze konfigurovat v režimech: AP, klient, Bridge, WDS, universal repeater, WISP, WISP + universal repeater a gateway. Toto zařízení je určeno především jako koncové zařízení v režimu klient, případně WISP. Lze jej, ale bez problému použít i pro menší síť v módu AP, nebo v módu bridge pro propojení dvou sítí LAN. Použití tohoto zařízení je nutno zvážit s ohledem na množství provozovaných bezdrátových sítí v normě IEEE 802.11b/g.

Zařízení je koncipováno pro napájení napětím 12 V s proudovým odběrem 800 mA. PCB deska je umístěna v plastovém boxu s možností montáže na zeď za pomoci dvou dodávaných kotevnických šroubů. V balení dále najdeme anténu se ziskem 2 dB, UTP kabel kategorie 5 o délce 1 m a napájecí spínaný zdroj 12 V / 1A.

Na zadní straně boxu jsou vyvedeny 2 konektory RJ45, konektor R-SMA pro připojení antény a konektor JACK 3,5 mm pro připojení napájení. Vedle těchto konektorů je umístěno tlačítko pro reset zařízení do továrního nastavení.

Na předním panelu jsou umístěny indikační LED. Význam jednotlivých LED je uveden v tabulce 9.

Shrnutí všech základních funkcí zařízení WL-5460AP v2 je v tabulce 10.



Obrázek 35 – multifunkční WiFi zařízení WL-5460AP

Tabulka 9 – význam svitu jednotlivých LED na předním panelu WL-5460AP v2



Číslo LED	Indikátor	Barva	Význam
1	Power	zelená	Svítí-li, je zařízení v provozu.
2	Status	červená	Svítí-li, zařízení načítá nastavení z paměti.
3	Link/Act.	zelená	Svítí-li, je bezdrátové připojení aktivní. Svítí-li přerušovaně, přenáší se přes WiFi rozhraní data.
4	WEP/WPA	oranžová	Svítí-li, je zabezpečení bezdrátové komunikace aktivní.
5	MAC Ctrl	oranžová	Svítí-li, je aktivní funkce filtrování MAC adres.
6	Bridge/Repeater	oranžová	Svítí-li, je aktivní režim mostu či opakovače.
7	LAN1	Zelená	Svítí-li, je připojen síťový kabel. Svítí-li řerušovaně, přenáší se data.
8	LAN2		

Tabulka 10 – specifikace základních parametrů WL-5460AP v2

Podporované módy	AP Client Bridge, WDS Repeater Universal Repeater WISP , WISP + Universal Repeater Gateway
Výběr nejvýznamnějších funkcí	SSID (název bezdrátové sítě) Hide ESSID (skrytí názvu bezdrátové sítě) Access Control (filtrace MAC adres) DHCP server a Relay agent WatchDog ACK (Acknowledge character, 0~255) 8 úrovní vysílacího výkonu (0~18dBm) Podpora STP izolace WiFi klientů

Hardwarové prostředky	čipová sada Realtek RTL 8186 16 MB SDRAM vnitřní paměti, 2 MB Flash 2x 10/100 LAN port RJ-45 R-SMA konektor pro připojení antény verze firmwaru: 5460APv2_e15_czech			
Anténa	Odpojitelná			
Frekvenční pásmo	USA (FCC) 11 kanálů: 2,412 GHz~2,462 GHz Evropa (ETSI) 13 kanálů: 2,412 GHz~2,472 GHz Asie (TELEC) 14 kanálů: 2,412 GHz~2,483 GHz			
Přenosová rychlost v závislosti na citlivosti	IEEE 802.11b	min (dBm)	1 Mb/s	-91
			2 Mb/s	-90
			5 Mb/s	-90
			11 Mb/s	-86
	IEEE 802.11g	min (dBm)	6 Mb/s	-87
			9 Mb/s	-87
			12 Mb/s	-86
			18 Mb/s	-84
			24 Mb/s	-82
			36 Mb/s	-78
			48 Mb/s	-73
			56 Mb/s	-70
Použité modulace	802.11b DSSS (CCK, DQPSK, DBPSK) 802.11g OFDM (64-QAM, 16-QAM, QPSK, BPSK)			
Zabezpečení datového přenosu, autentizace	64/128-bit WEP WPA/WPA2-PSK 802.1x			
Podporované protokoly	Všechny známé protokoly			
Konfigurace	WEB rozhraní, telnet			
Verze FW	e15_czech			
Provozní podmínky	teplota: 0~60°C vlhkost: 20~80 % - nekondenzující			
Skladovací podmínky	teplota: -20~65°C vlhkost: max. 95% - nekondenzující			
Napájecí napětí	12 V DC/0,8A			
Hmotnost	180 g			
Rozměry (d x š x v)	135 x 100 x 26 mm			

8.2 multifunkční zařízení WLA-5000AP v3

Multifunkční zařízení je určeno pro normu IEEE 802.11a a IEEE 802.11g. Z toho vyplývá, že zařízení je určeno pro provoz v bezlicenčních pásmech 2,4 GHz a 5 GHz. WLA-5000AP v3 lze konfigurovat v režimech: AP, klient, Bridge, WDS a WISP. Toto zařízení je vhodné pro použití jako most v páteřních spojích a AP pro distribuci WiFi signálu ke koncovým klientům

Zařízení je koncipováno pro napájení napětím 5 V s proudovým odběrem 2 A. PCB deska je umístěna v plastovém boxu s možností montáže na zeď za pomoci dvou dodávaných kotevních šroubů. V balení dále najdeme anténu se ziskem 2 dB, UTP kabel kategorie 5 o délce 1m a napájecí spínaný zdroj 5 V / 2 A.

Na zadní straně boxu je vyveden 1 konektory RJ45, konektor R-SMA pro připojení antény a konektor JACK 3,5 mm pro připojení napájení. Vedle těchto konektorů je umístěno zapuštěné tlačítko pro reset zařízení do továrního nastavení.

Na vrchním panelu jsou umístěny 3 indikační LED. Jedna indikuje napájení celého zařízení, další je určena pro indikaci aktivity LAN a poslední indikuje aktivitu WiFi. Shrnutí všech základních funkcí zařízení WLA-5000AP v3 je v tabulce 11.



Obrázek 36 – multifunkční zařízení WLA-5000AP

Tabulka 11 – specifikace základních parametrů WLA-5000AP v3

Podporované módy	AP Client Bridge, WDS Repeater WISP
Výběr nejvýznamnějších funkcí	Multi SSID Vlan tágování Hide ESSID (skrytí názvu bezdrátové sítě) Access Control (filtrace MAC adres) DHCP server a Relay agent WatchDog ACK (Acknowledge character, 0~255) vysílací výkon 20dB pro 802.11b, 17dB pro 802.11a/g Podpora STP izolace WiFi klientů
Hardwarové prostředky	čipová sada Atheros AR2312+AR5112 32 MB SDRAM vnitřní paměti, 4 MB Flash 1x 10/100 LAN port RJ-45 R-SMA konektor pro připojení antény verze firmwaru: 5000APv3_2.0e8
Anténa	odpojitelná
Frekvenční pásmo	USA (FCC) 11 kanálů: 2,412 GHz~2,462 GHz Evropa (ETSI) 13 kanálů: 2,412 GHz~2,472 GHz Asie (TELEC) 14 kanálů: 2,412 GHz~2,483 GHz USA (U-UNII) 12 kanálů: pásmo 5,15-5,35GHz a 5,725-5,825 Evropa (ETSI) 19 kanálů: 5,15-5,35GHz a 5,47-5,725GHz Asie (TELEC) 4 kanály: 4,9-5,0GHz, 5,03-5,091GHz a 5,15-5,25 GHz
Použité modulace	802.11a OFDM (64-QAM, 16-QAM, QPSK, BPSK) 802.11b DSSS (CCK, DQPSK, DBPSK) 802.11g OFDM (64-QAM, 16-QAM, QPSK, BPSK)
Zabezpečení datového přenosu, autentizace	64/128-bit WEP WPA/WPA2-PSK 802.1x
Podporované protokoly	Všechny známé protokoly
Konfigurace	WEB rozhraní, SNMP v, v2, v2c , UpNP
Verze FW	2.0e8
Provozní podmínky	teplota: 0~40°C vlhkost: 10~80 % - nekondenzující
Skladovací podmínky	teplota: -20~65°C vlhkost: max.80% - nekondenzující
Napájecí napětí	5 V DC/2A
Hmotnost	210 g
Rozměry (d x š x v)	160 x 115 x 30 mm

VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

8.3 multifunkční zařízení WLA-5200AP

Toto zařízení je určeno pro normu IEEE 802.11a a IEEE 802.11g. Z toho vyplývá, že zařízení je určeno pro provoz v bezlicenčních pásmech 2,4 GHz a 5 GHz. WLA-5200AP lze konfigurovat v režimech: AP, klient, Bridge, WDS, universal repeater, WISP, WISP + universal repeater a gateway. WLA-5200AP se většinou v praxi používá jako koncové zařízení v módu klient případně v módu WISP.

Zařízení je koncipováno pro napájení napětím 12 V s proudovým odběrem 1 A. PCB deska je umístěna v plastovém boxu s možností montáže na zeď za pomoci dvou dodávaných kotevních šroubů. V balení dále najdeme anténu se ziskem 2 dB, UTP kabel kategorie 5 o délce 1m a napájecí spínaný zdroj 12 V / 1 A.

Na zadní straně boxu jsou vyvedeny 2 konektory RJ45, konektor R-SMA pro připojení antény a konektor JACK 3,5mm pro připojení napájení. Vedle těchto konektorů je umístěno zapuštěné tlačítko pro reset zařízení do továrního nastavení.

Na předním panelu jsou umístěny 4 indikační LED. Indikují stav napájení celého zařízení, aktivitu portů LAN1 a LAN2 a poslední LED indikuje aktivitu WiFi. Shrnutí všech základních funkcí zařízení WLA-5200AP je v tabulce 12.



Obrázek 37 – multifunkční zařízení WLA-5200AP

Tabulka 12 – specifikace základních parametrů WLA-5200AP

Podporované módy	AP Client Bridge, WDS Repeater Universal Repeater WISP , WISP + Universal Repeater Gateway
Výběr nejvýznamnějších funkcí	SSID (název bezdrátové sítě) Hide ESSID (skrytí názvu bezdrátové sítě) Access Control (filtrace MAC adres) DHCP server a Relay agent WathDog ACK (Acknowledge character, 0~255) vysílací výkon 20dB pro 802.11b, 17dB pro 802.11a/g Podpora STP izolace WiFi klientů
Hardwarové prostředky	čipová sada Realtek RTL 8651B 32 MB SDRAM vnitřní paměti, 4 MB Flash 2x 10/100 LAN port RJ-45 R-SMA konektor pro připojení antény verze firmwaru: 5200AP_e7
Anténa	Odpojitelná
Frekvenční pásmo	USA (FCC) 11 kanálů: 2,412 GHz~2,462 GHz Evropa (ETSI) 13 kanálů: 2,412 GHz~2,472 GHz Asie (TELEC) 14 kanálů: 2,412 GHz~2,483 GHz USA (U-UNII) 12 kanálů: pásmo 5,15-5,35GHz a 5,725-5,825 Evropa (ETSI) 19 kanálů: 5,15-5,35GHz a 5,47-5,725GHz Asie (TELEC) 4 kanály: 4,9-5,0GHz, 5,03-5,091GHz a 5,15-5,25 GHz
Použité modulace	802.11a OFDM (64-QAM, 16-QAM, QPSK, BPSK) 802.11b DSSS (CCK, DQPSK, DBPSK) 802.11g OFDM (64-QAM, 16-QAM, QPSK, BPSK)
Zabezpečení datového přenosu, autentizace	64/128-bit WEP WPA/WPA2-PSK, 802.1x
Podporované protokoly	Všechny známé protokoly
Konfigurace	WEB rozhraní, SNMP v, v2, v2c
Verze FW	E7
Provozní podmínky	teplota: 0~60°C vlhkost: 20~80 % - nekondenzující
Skladovací podmínky	teplota: -20~65°C vlhkost: max. 95% - nekondenzující
Napájecí napětí	12 V DC/0,8A
Hmotnost	210 g
Rozměry (d x š x v)	160 x 115 x 30 mm

8.4 multifunkční zařízení AirMax5

Uvedené zařízení je koncipováno pro outdoorové použití. Je postaveno na chipsetu Atheros pro normu IEEE 802.11a. Zařízení se dá konfigurovat v módech AP, klient, WDS, most, univerzální opakovač a WISP. Vzhledem k integrované směrové anténě se prvotně hodí pro použití v režimech most, klient a WISP.

Zařízení je napájeno pomocí PoE injektoru, který je spolu s UTP kabelem o délce 1m a spínaným zdrojem 12V / 1A, dodáván v balení. Zařízení je vybaveno sadou indikačních LED, které vyhodnocují sílu přijímaného signálu. Toto nám usnadní kvalitní nasměrování zařízení. Bližší popis indikačních LED je uveden v tabulce 13.

Shrnutí všech základních funkcí zařízení AirMAX5 je uvedeno v tabulce 15.



Obrázek 38 – multifunkční zařízení AirMAX5

Tabulka 13 - popis indikačních LED

Power	červená	Svítí-li, zařízení pracuje
Link	žlutá	Svítí-li, zařízení je připojeno, bliká-li, přenáší se data
Full	modrá	Svítí-li samostatně modrá LED, signál je slabý, v případě svitu zelené LED je signál dobrý, při svitu obou LED je signál v maximální výši. Při zhasnutých obou LED, není signál dostačující
	zelená	



Obrázek 39 - panel indikačních LED na boku zařízení

Tabulka 14 – specifikace základních parametrů zařízení AirMAX5

Podporované módy	AP Client WDS, Bridge Universal repeater WISP
Výběr nejvýznamnějších funkcí	Multi SSID (název bezdrátové sítě) Vlan tágování Hide ESSID (skrytí názvu bezdrátové sítě) Access Control (filtrace MAC adres) DHCP server a Relay agent WathDog ACK (Acknowledge character, 0~255) vysílací výkon 23dB pro 802.11a Podpora STP izolace WiFi klientů
Hardwarové prostředky	čipová sada Atheros AR2312+AR5112 32 MB SDRAM vnitřní paměti, 8 MB Flash 1x 10/100 LAN port RJ-45, s pasivním PoE (12-22V) Integrovaná směrová anténa 14 dBi R-SMA konektor pro připojení externí antény verze firmwaru: 5200AP_e7
Anténa	odpojitelná
Frekvenční pásmo	USA (FCC) 12 kanálů: pásmo 5,15-5,35GHz a 5,725-5,825GHz Evropa (ETSI) 19 kanálů: 5,15-5,35GHz a 5,47-5,725GHz Asie (TELEC) 4 kanály: 4,9-5,0GHz, 5,03-5,091GHz a 5,15-5,25 GHz
Použité modulace	802.11a OFDM (64-QAM, 16-QAM, QPSK, BPSK)
Zabezpečení datového přenosu, autentizace	64/128-bit WEP WPA/WPA2-PSK 802.1x
Podporované protokoly	Všechny známé protokoly
Konfigurace	WEB rozhraní, telnet, SSH2, SNMP v1/2
Verze FW	E7
Provozní podmínky	teplota: 0~60°C vlhkost: 20~80 % - nekondenzující
Skladovací podmínky	teplota: -20~65°C vlhkost: max. 95% - nekondenzující
Napájecí napětí	12 V DC/1A
Hmotnost	210 g
Rozměry (d x š x v)	210 x 100 x 32 mm

8.5 multifunkční zařízení WLA-9000

Uvedené zařízení je postaveno na dvou spojených radiových jednotkách. Jedna z jednotek je pro normu IEEE 802.11a a druhá pro normy IEEE 802.11a/b/g. Zařízení je tedy vhodné pro provoz v pásmech 2,4 GHz a 5 GHz.

WLA-9000 lze konfigurovat v režimech: dvojité AP, dvojitá WDS, dvojitý most, duplexní most, klient a AP, most + AP, WDS + router, AP + gateway, AP + WISP. Nebo v módech se zapnutou pouze jednou radiovou jednotkou. Pak je možno konfigurovat zařízení jako AP, klient, most, WDS, WISP, gateway.

Zařízení je možno napájet dvěma způsoby. Pomocí napájecího adaptéru s parametry 5,5 V / 2,5 A nebo pomocí PoE portu splňující normu IEEE 802.3af.

WLA-9000 je vhodné především pro výstavbu páteřních spojů, případně páteřních spojů se zapnutým AP pro koncové klienty.

PCB je vložena do plastového krytu. Na zadním panelu najdeme 2 konektory R-SMA pro připojení antén, 3 konektory RJ45 (prostřední port podporuje normu IEEE 802.3af) a konektorem JACK pro napájení pomocí adaptéru. Vedle napájecího konektoru je umístěno zapuštěné tlačítko pro reset zařízení do továrního nastavení.

Na předním panelu je umístěno 6 LED pro indikaci stavu zařízení. Popis jednotlivých LED je v tabulce 15.

V balení spolu se zařízením najdeme 1m dlouhý kabel UTP cat5, již zmiňovaný napájecí adaptér, 2 antény s výkonem 2 dB, instalační manuál a CD s manuálem v elektronické podobě.

Bližší popis základních parametrů zařízení najdete v tabulce 16.



Obrázek 40 – multifunkční dvourádiové zařízení WLA-9000

Tabulka 15 - popis indikačních LED u zařízení WLA-9000



Pořadí LED	Označení	Popis
1	Power	Svítí, pokud je zařízení v provozu
2	WLAN1	Svítí, pokud je zařízení napájeno, bliká, pokud jsou přenášena data. Nesvítí, pokud je jednotka vypnuta
3	WLAN2	
4	LAN 1	Svítí-li, je port připojen, při problikávání indikuje přenos dat. Pokud nesvítí, je port odpojen.
5	LAN 2	
6	LAN 3	

Tabulka 16 - specifikace základních parametrů zařízení WLA-9000

Podporované módy	Kombinace AP, Clie, WDS, Bridge, WISP a gateway pro obě rádiové jednotky
Výběr nejvýznamnějších funkcí	Multiply SSID Vlan tágování Hide ESSID (skrytí názvu bezdrátové sítě) Access Control (filtrace MAC adres) DHCP server a Relay agent WathDog ACK (Acknowledge character, 0~255) vysílací výkon 23dB pro 802.11a a 17dB pro 802.11b/g Podpora STP izolace WiFi klientů
Hardwarové prostředky	čipová sada Atheros 32 MB SDRAM vnitřní paměti, 8 MB Flash 3x 10/100 LAN port RJ-45, z toho 1x PoE dle normy IEEE 802.3af 2x R-SMA konektory pro připojení externích antén verze firmwaru: 9000_1.0e27
Anténa	odpojitelná
Frekvenční pásmo	WLAN2 (radio2) USA (FCC) 11 kanálů: 2,412 GHz~2,462 GHz Evropa (ETSI) 13 kanálů: 2,412 GHz~2,472 GHz Asie (TELEC) 14 kanálů: 2,412 GHz~2,483 GHz WLAN1 a WLAN2 USA (U-UNII) 12 kanálů: pásmo 5,15-5,35GHz a 5,725-5,825GHz

	Evropa (ETSI) 19 kanálů: 5,15-5,35GHz a 5,47-5,725GHz Asie (TELEC) 4 kanály: 4,9-5,0GHz, 5,03-5,091GHz a 5,15-5,25 GHz			
Použité modulace	802.11a OFDM (64-QAM, 16-QAM, QPSK, BPSK) 802.11b DSSS (CCK, DQPSK, DBPSK) 802.11g OFDM (64-QAM, 16-QAM, QPSK, BPSK)			
Přenosová rychlost v závislosti na citlivosti Přenosová rychlost v závislosti na citlivosti	IEEE 802.11a	min (dBm)	6 Mb/s	-90
			9 Mb/s	-89
			12 Mb/s	-88
			18 Mb/s	-86
			24 Mb/s	-82
			36 Mb/s	-79
			48 Mb/s	-73
			54 Mb/s	-71
	IEEE 802.11g	min (dBm)	6 Mb/s	-89
			9 Mb/s	-88
			12 Mb/s	-88
			18 Mb/s	-86
			24 Mb/s	-82
			36 Mb/s	-79
			48 Mb/s	-75
			54 Mb/s	-73
Podporované protokoly	Všechny známé protokoly			
Konfigurace	WEB rozhraní, telnet, SNMP v1/2			
Verze FW	1.0e23			
Provozní podmínky	teplota: 0~40°C vlhkost: 10~90 % - nekondenzující			
Skladovací podmínky	teplota: -20~65°C vlhkost: max.90% - nekondenzující			
Napájecí napětí	5,5 V DC/2,5A nebo PoE dle IEEE 802.3af 48V / 0,4A			
Hmotnost	341 g			
Rozměry (d x š x v)	191 x 145,5 x 29 mm			

8.6 multifunkční zařízení WN-300R

Uvedené zařízení odpovídá definici pre IEEE 802.11n ve verzi Draft2. Je zpětně kompatibilní s normou IEEE 802.11b/g. Z těchto parametrů je tedy zřejmé že se jedná o zařízení pracující v bezlicenčním pásmu s frekvencí 2,4 GHz. WN-300R lze konfigurovat v módech: router + AP, AP, WDS, most a univerzální opakovač. Je navrženo především pro použití v módu router + AP.

Koncepce zařízení je definována pro napájení adaptérem 12 V / 1 A. Spolu s napájecím adaptérem, dvěma anténami se ziskem 2 dB v balení najdeme ještě UTP kabel kategorie 5 o délce 1m, instalační manuál a CD s manuálem v elektronické podobě.

PCB je vložena do plastové krabičky. Na zadním panelu je umístěno 5 LAN portů (1x WAN a 4x LAN), konektor JACK 3,5 mm pro připojení napájecího adaptéru a dva R-SMA konektory pro připojení antén. Na předním panelu najdeme 6 indikačních LED a dvě tlačítka. Bližší popis předního panelu je v tabulce 17.

Zařízení využívá pro komunikaci v módu 802.11n model 2R2T pro antény.

Bližší popis základních parametrů zařízení najdete v tabulce 18.



Obrázek 41 – multifunkční WiFi zařízení WN-300R s podporou IEEE 802.11n Draft2

Tabulka 17 - popis předního panelu zařízení WN-300R

Pořadí	Označení	Popis
1	Power	Svítlí, pokud je zařízení v provozu
2	Tlačítko WPS	Tlačítko pro výměnu klíčů mezi zařízeními, pro rychlo konfiguraci sítě
3	WiFi aktivity	Svítlí, pokud je WiFi část aktivní, bliká při přenosu dat
4	LAN 1	Svítlí-li, je port připojen, při problikávání indikuje přenos dat. ,Pokud nesvítlí, je port odpojen.
5	LAN 2	
6	LAN 3	
7	LAN 4	
8	Reset	Tlačítko pro reset zařízení do továrního nastavení

Tabulka 18 - specifikace základních parametrů zařízení WN-300R

Podporované módy	AP Router + AP Bridge, WDS Repeater Univerzální repeater
Výběr nejvýznamnějších funkcí	Možnost dvou SSID Hide ESSID (skrytí názvu bezdrátové sítě) Access Control (filtrace MAC adres) DHCP server a Relay agent ACK (Acknowledge character, 0~255) vysílací výkon 20dB pro 802.11b, 17dB pro 802.11g/n izolace WiFi klientů
Hardwarové prostředky	1x 10/100 WAN 4x 10/100LAN porty RJ-45 2x R-SMA konektor pro připojení antén (2R2T) verze firmwaru: WN300_1.00
Anténa	Odpojitelné
Frekvenční pásmo	USA (FCC) 11 kanálů: 2,412 GHz~2,462 GHz Evropa (ETSI) 13 kanálů: 2,412 GHz~2,472 GHz Asie (TELEC) 14 kanálů: 2,412 GHz~2,483 GHz
Použité modulace	802.11b DSSS (CCK, DQPSK, DBPSK) 802.11g OFDM (64-QAM, 16-QAM, QPSK, BPSK) 802.11n OFDM (64-QAM, 16-QAM, QPSK, BPSK)
Zabezpečení datového přenosu, autentizace	64/128-bit WEP WPA/WPA2-PSK 802.1x MAC filtrace WPS tlačítko
Podporované protokoly	Všechny známé protokoly
Konfigurace	WEB rozhraní, UpNP
Verze FW	1.00
Provozní podmínky	teplota: 10~40°C vlhkost: 10~90 % - nekondenzující
Skladovací podmínky	teplota: -20~65°C vlhkost: max.80% - nekondenzující
Napájecí napětí	12 V DC/1A

8.7 multifunkční zařízení WN-301R

Uvedené zařízení je odvozeno od zařízení WN-300R. Jediný rozdíl je v nemožnosti připojit externí antény, ty jsou u tohoto modelu integrovány. Využití zařízení je především v kombinaci router + AP.

Balení obsahuje vlastní zařízení, napájecí adaptér, UTP kabel kategorie 5 o délce 1m, manuál a CD s manuálem v elektronické podobě.

PCB deska je vložena v plastové krabičce. Zadní panel obsahuje 5 portů RJ45 (1xWAN a 4xLAN) a JACK konektor pro připojení napájení. Přední panel obsahuje indikační LED a dvě tlačítka. Bližší popis předního panelu je uveden v tabulce 19.

Popis základních parametrů zařízení najdete v tabulce 20.



Obrázek 42 – multifunkční WiFi zařízení WN-301R s podporou IEEE 802.11n Draft2

Tabulka 19 - popis předního panelu zařízení WN-301R

Pořadí	Označení	Popis
1	Sekurity	Pokud tlačítko svítí, je použito zabezpečení
2	Tlačítko WPS	Tlačítko pro výměnu klíčů mezi zařízeními, pro rychlo konfiguraci sítě
3	WiFi	Svítí, pokud je zařízení připraveno k přenosu s klientem, bliká při přenosu dat, nesvítí, pokud není nikdo připojen prostřednictvím WiFi
4	LAN	Svítí-li, je alespoň jeden port připojen, při problikávání indikuje přenos dat. ,Pokud nesvítí, jsou porty odpojeny.
5	Power	Svítí, pokud je zařízení v provozu
6	WAN	Indikace zde je připojen WAN port, při problikávání je detekován přenos dat
7	Internet	Indikace zda je zařízení připojeno k síti Internet. Pokud LED problikává, dochází k přenosu dat.
8	Reset	Tlačítko pro reset zařízení do továrního nastavení

Tabulka 20 - specifikace základních parametrů zařízení WN-301R

Podporované módy	AP Router + AP Bridge, WDS Repeater Univerzální repeater
Výběr nejvýznamnějších funkcí	Možnost dvou SSID Hide ESSID (skrytí názvu bezdrátové sítě) Access Control (filtrace MAC adres) DHCP server a Relay agent ACK (Acknowledge character, 0~255) vysílací výkon 20dB pro 802.11b, 17dB pro 802.11g/n izolace WiFi klientů
Hardwarové prostředky	1x 10/100 WAN 4x 10/100LAN porty RJ-45 Dvě integrované antény (2R2T) verze firmwaru: WN301_1.00
Anténa	Dvě - integrované
Frekvenční pásmo	USA (FCC) 11 kanálů: 2,412 GHz~2,462 GHz Evropa (ETSI) 13 kanálů: 2,412 GHz~2,472 GHz Asie (TELEC) 14 kanálů: 2,412 GHz~2,483 GHz
Použité modulace	802.11b DSSS (CCK, DQPSK, DBPSK) 802.11g OFDM (64-QAM, 16-QAM, QPSK, BPSK) 802.11n OFDM (64-QAM, 16-QAM, QPSK, BPSK)
Zabezpečení datového přenosu, autentizace	64/128-bit WEP WPA/WPA2-PSK 802.1x MAC filtrace WPS tlačítko
Podporované protokoly	Všechny známé protokoly
Konfigurace	WEB rozhraní, UpNP
Verze FW	1.00
Provozní podmínky	teplota: 10~40°C vlhkost: 10~90 % - nekondenzující
Skladovací podmínky	teplota: -20~65°C vlhkost: max.80% - nekondenzující
Napájecí napětí	12 V DC/1A

8.8 USB dongle WN-300USB

Uvedené zařízení bylo použito pro měření WiFi sítě s podporou ještě neschválené normy IEEE 802.11n. Zařízení je konfigurované jako klient. Připojitelné k PC či notebooku pomocí USB 2.0 rozhraní. Podporuje normy IEEE 802.11b/g a pre normu IEEE 802.11n Draft2. Zařízení je určeno pro pásmo 2,4 GHz.

Bližší popis zařízení je uveden v tabulce 21.



Obrázek 43 – USB WiFi klient WN-300USB s podporou IEEE 802.11n Draft2

Tabulka 21 - specifikace základních parametrů zařízení WN-301R

Podporované módy	SW klient
Výběr nejvýznamnějších funkcí	SSID ACK (Acknowledge character, 0~255)
Hardwarové prostředky	1x USB 2.0 Číslo Ralink RT3070
Anténa	Integrovaná
Frekvenční pásmo	USA (FCC) 11 kanálů: 2,412 GHz~2,462 GHz Evropa (ETSI) 13 kanálů: 2,412 GHz~2,472 GHz Asie (TELEC) 14 kanálů: 2,412 GHz~2,483 GHz
Použitý výkon	802.11b 17dBm $\pm$ 1dBm 802.11g 14dBm $\pm$ 1dBm 802.11n 14dBm $\pm$ 1dBm
Použitá rychlost	802.11b: 1/2/5.5/11Mbps 802.11g 6/9/12/24/36/48/54Mbps 802.11n pásmo 20MHz MCS0-7 (až 72Mbps) 802.11n pásmo 40MHz MCS0-7 (až 150Mbps)
Zabezpečení datového přenosu, autentizace	64/128-bit WEP WPA/WPA2-PSK 802.1x WPS
Podporované protokoly	Všechny známé protokoly
Konfigurace	SW pro systémy Microsoft Windows XP a vyšší
Provozní podmínky	teplota: 0~40°C vlhkost: 10~95 % - nekondenzující
Skladovací podmínky	teplota: -20~65°C vlhkost: max.95% - nekondenzující
Napájecí napětí	Z USB portu max. 500mA

8.9 Ostatní zařízení použita při měření

Při jednotlivých měřeních byly použity dva notebooky HP typ Nx 6110 a dva notebooky HP 6730s. U typu NX 6110 je použita integrovaná síťová karta LAN BroadCom 440x 10/100 Mbps a WiFi miniPCI modul Intel 2915abg a Intel 2200bg. U modelu HP 6730s je použita integrovaná síťová karta LAN Marvel Yukon 88E8042 10/100/1000MBps a WiFi miniPCI modul Intel WiFi link 5100agn a Intel 3915abg.

9. Návrh řešení pro propojení dvou stanovišť

Problematika spojení dvou stanovišť pomocí WiFi signálu je takřka pravidelně řešena u ISP providerů používající WiFi technologii. Vždy se snažíme propojit bod s přístupem k datové konektivitě se vzdáleným bodem, kam tuto konektivitu potřebujeme přenést. Pro realizaci takového spoje využijeme informací uvedených v předchozím textu.

9.1 Volba pásma a volba zařízení

Vzhledem k velkému množství WiFi sítí je potřeba před započítím teoretických úvah nad řešením spoje provést kontrolní měření v lokalitě, kde chceme spoj realizovat. Měření můžeme provést například pomocí programu NetStumbler (krátký popis použitého SW je uveden v příloze A). Zjistíme tedy obsazené kanály pro normu IEEE 802.11 b/g, případně pro IEEE 802.11a. Sítě s pre normou IEEE 802.11n zatím vůbec pro venkovní použití neuvažujeme.

Výsledek naměřených hodnot můžeme vidět na obrázku 45. Tato měření byla prováděna v oblasti Brno - Bohunice, okolí ulic Gruzínská, Moldavská a Ukrajinská, mezi panelovou zástavbou, viz obrázek 44. Další měření bylo realizováno ve středu Brna mezi ulicemi Olomoucká a Štolcova. Bližší popis a naměřené hodnoty jsou v příloze D.



Obrázek 44 – výřez z mapy s určením koncových bodů pro výstavbu spoje a následné měření

MAC	SSID	Name	Chan
0013D424F147	TUMA		6
001FC65304F3	ASUS		1
0022151B7CEA	Simaci		1
00221521B491	Persefone		1
0015F26AD919	bohunka		4
004F6701F348	bel20w		6
0002CFB3FB4B	Prichy		1
0021298321AC	senkovi		3
00120EA04D60	APKORCOVI		1
004F62048EF6	BOBR		3
0018F3A8DC91	MAL		6
0018F3DA094A	sergis		7
0023546DD6B6	-doma-		1+
004F6702AE01	HOME		4*

Obrázek 45 – naměřené informativní hodnoty z programu NetStumbler- měřeno notebookem HP NX 6110 s kartou Intel 2915abg

Z přehledu je zřejmé, že oblast je poměrně dost zarušená v pásmu 2,4 GHz. Ale ještě stále je možné za použití velmi směrových antén a použití kanálů číslo 9-13 vytvořit bezdrátový spoj typu most. Případně lepší volba by byla použití zařízení fungujícího v pásmu 5 GHz.

S ohledem na zjištěný stav byly pro testování zvoleny zařízení WL-5460AP v2 pro pásmo 2,4 GHz a WLA-5000AP v3, WLA-9000, AirMAX5 pro pásmo 5 GHz.

9.2 Volba módu zařízení.

Jako výchozí bod bylo zvoleno místo na střeše garáží na Ulici Ukrajinská. Konektivita se měla přenášet z tohoto bodu přes bod umístěný na ulici Gruzínská do koncového bodu na roh ulice Moldavská.

Pro řešení tohoto modelu je možno použít několika variant.

- **varianta s použitím pasivní retranslace** – výchozí bod je v režimu AP koncový v režimu klient. Toto řešení bylo na počátku vyřazeno z dalšího testování kvůli velkému útlumu na pasivním retranslačním bodě. Pro korektní fungování takového spoje je nutno použít silné zabezpečení. Spoj je viditelný pro okolí. V případě dlouhých vzdáleností je toto řešení naprosto nekonceptní. Toto řešení má odůvodnění pouze v případě absence možnosti napájení v místě nutné retranslace.
- **varianta s nastavením WDS** – všechny body jsou v módu WDS. Jako nežádoucí jev je šíření konektivity do okolí. Tato varianta by se hodila, pokud bychom chtěli pokrýt větší území WiFi signálem. Nevýhodou je již zmiňované dělení propustnosti s každým přeskokem ve WDS síti. Při výstavbě WDS sítí, se můžeme setkat s nepříjemným jevem vzniklým rozdílným zarušením WiFi signálu v různých místech pokrytí. WDS systém předpokládá použití jednoho kanálu a jednoho SSID na všech jednotkách WDS. Bohužel jedna část spoje může na uvedeném kanálu fungovat zcela bez problému, ale další část spoje může již být

zcela nefunkční. Proto se i těchto typů sítí doporučuje dělení na jednotlivé segmenty. Bližší popis je v příloze E.

- **varianta propojení typu most** – tato varianta řešení je velmi podobná variantě předchozí, s tím rozdílem, že není WiFi signál šířen dál pro možnost připojení koncových klientů. Opět může vzniknout stejný problém jako u případu WDS sítě, je tedy lepší síť rozdělit celý propoj na několik segmentů. Tímto se eliminuje i nežádoucí efekt WDS systému ať v módu WDS nebo WDS bridge, kdy dochází na každé retranslaci k dělení propustnosti.

Při měření byla použita možnost s WDS prvky a s prvky nakonfigurovanými jako WDS most. Při měření vznikly modely s variantami jednoho prvku na retranslačním bodu, dvou jednorádiových prvků nebo jednoho dvourádiového zařízení na retranslačním bodu. Výsledky těchto měření jsou v příloze D.

9.3 Praktický návrh spoje

Při řešení této úlohy vycházíme z teoretického návrhu, kdy provedeme alespoň základní posouzení výběru antény na základě známých údajů zarušení a vzdáleností mezi jednotlivými body. Z pohledu kvality spoje byly vybírány úzce směrové antény se ziskem 6 dB pro koncová zařízení a všesměrová anténa se ziskem opět 6 dB pro retranslační bod, v případě použití jednoho zařízení s jednou rádiovou jednotkou pro retranslační bod. Další možností pro takto navržený retranslační bod je použití dvou antén a anténní slučovač. V praxi se ale toto řešení moc nepoužívá, protože je náročnější na stavbu a návrh. Pro případ dvou spojů s velmi odlišnou vzdáleností musíme použít navíc asymetrický útlumový člen.

V případě retranslačního bodu se dvěma zařízeními, nebo jedním dvourádiovým zařízením bylo použito dvou úzce směrových antén se ziskem 6 dB. Vždy byl navázán spoj na rychlosti 54 Mbit. Bližší popis je uveden v příloze D.

9.4 Obecné řešení pro mobilní jednotky rozmisťující jednotlivá zařízení

Pro rozmísťování jednotlivých WiFi zařízení je předpokládáno užití mobilních robotických jednotek. Proto byla jednotlivá zařízení vybírána s ohledem na napájení, kde je limitujících maximálně 12 V DC.

Pro kvalitní návrh spoje je za potřebí již zmíněné zmapování prostředí s ohledem na rušivé vlivy okolních WiFi sítí.

Abychom mohly použít mobilních jednotek pro rozmístění jednotlivých zařízení musíme provést úvahu nad zajištěním ještě funkční konektivity mezi jednotlivými body.

Jak již bylo zmíněno, pro optimální komunikaci je potřeba přímá viditelnost a alespoň 60% plochy z kolmého řezu Fresnelovou zónou.

Při použití mobilních jednotek pro rozmísťování WiFi zařízení, by v prvním kroku měla být anténa u stacionárního bodu všesměrová, případně sektorová. Mobilní jednotka by měla použít buď všesměrovou anténu, nebo případně směrovou anténu, ale tak aby stále směřovala přímo na stacionární vysílač. Jednotka by měla zařízení nakonfigurované v tuto chvíli jako klient a stacionární bod by byl konfigurován jako AP. V případě ztráty konektivity

mobilní jednotky s pevnou jednotkou, by musel být aplikován algoritmus pro provedení posledního kroku zpět, až do chvíle kdy opět konektivita bude navázána. Tímto způsobem se zajistí první propoj. Následně by mělo dojít k výměně antén u pevného a pohyblivého se bodu. Po prohození antén pohyblivý se bod zůstane stát na místě s konektivitou a již dále neprovádí žádný pohyb. Následně se pomocí konfiguračního programu přepne stacionární bod do módu most a zařízení na mobilní jednotce do módu WDS. Tím zaručíme konektivitu mezi prvními dvěma body. Další jednotka se pomocí WiFi zařízení, jenž je v módu klient připojí k zařízení v módu WDS a opakuje se postup jako u prvního spoje s tou výjimkou, že se mění nastavení bodu v módu WDS na mód bridge pro spoj s předchozím a následujícím bodem.

Tento postup se opakuje do té doby, dokud nedojde ke spojení obou koncových bodů, které se mají spojit. Dojde ke vzniku spoje na bázi mostu.

Toto řešení předpokládá vytváření spojů typu bod – bod (pro krajní zařízení), nebo bod – multi bod (pro všechna ostatní zařízení). Nevýhoda je v již zmíněném dělení propustnosti na každém retranslačním bodu. Tato nevýhoda se dá z velké části eliminovat za pomoci zařízení se dvěma rádiovými jednotkami, nebo pomocí dvou zařízení propojenými UTP kabelem. Dvourádiové, nebo dvě jednorádiové jednotky jsou umístěny na všech retranslačních bodech, tedy mimo koncových bodů spoje.

Princip spojení každých dvou jednotek je stejný s tím, že se nemusí prohazovat antény mezi jednotlivými zařízeními, protože každá z mobilních jednotek veze dvě vlastní antény, pro příjem je užita směrová a pro vysílání všesměrová nebo sektorová anténa. Po získání krajní hodnoty vzdálenosti mobilní jednotky tak přepínáme zařízení, jenž spolu komunikují do módu bridge. Musíme ovšem vždy dbát na co největší odstup mezi použitými kanály, abychom eliminovali co nejvíce rušení mezi jednotlivými zařízeními. Implementace řešení s dvourádiovou, případně dvěma jednorádiovými zařízeními je mnohem náročnější.

Zmíněným postupem získáme přemostění mezi dvěma koncovými body, ale rozhodně nebude zcela optimálně řešeno. To vyplývá z aspektu použití jednotlivých typů antén pro pokrytí určitého území. Při výstavbě spoje typu bod - bod, z nichž se celý spoj pak skládá, je použito vždy páru co nejsměrovějších antén s optimálním ziskem pro provedení spoje. Tímto je dosaženo mnohem větší vzdálenosti koncových bodů jednotlivých subspojů, než v případě kombinace směrové a sektorové případně všesměrové antény. V reálném prostředí je také uvažován vliv reliéfu krajiny. Tento vliv se bohužel, při rozmístování WiFi zařízení pomocí robotických jednotek, zohlednit nedá.

10. Návrh řešení pro strukturovaný prostor

Dalším možným návrhem je pokrytí WiFi signálem strukturovaný prostor uvnitř budov. Zde se můžeme potýkat s různými problémy, jakou jsou blíže nespecifikované útlumy při průchodu zdmi, odrazy signálu, nežádoucí interference a další.

Pro kontrolní měření bylo umožněno využít prostor v 7. NP v budově VUT fakulty strojní. Plánek těchto prostor s body kde byly rozmístěny jednotlivé jednotky WDS je uveden v příloze G.

10.1 Volba zařízení a varianty zapojení

Vzhledem k potřebám pokrýt prostor WiFi signálem tak, aby ke vzniklé síti bylo možno připojit jednotlivé klienty a zařízení, například WiFi IP kamery, byla pro šíření koncového signálu použita zařízení s normou IEEE 802.11g. Voleny tedy byly zařízení WL-5460AP v2 a WLA-5200AP. Pro variantu s eliminací nežádoucích efektů WDS systému byly pro spoje mezi koncovými zařízeními použity zařízení WLA-5200AP v módu WDS bridge konfigurována pro normu IEEE 802.11a. Poslední variantou bylo zapojení zařízení s normou IEEE 802.11n Draft2.

Varianty jednotlivých zapojení systému:

1. Všechna zařízení mají jedno SSID, fungují na jednom kanále a jsou nastavena jako WDS, jsou ve schématu zřetězení. Schéma zapojení s jednotlivými MAC adresami je uvedeno na obrázku 45. Toto zapojení je závislé na fungování WDS. Maximálně je tedy vhodné použít 5 zařízení kdy teoretická maximální propustnost na posledním zařízení je 3 Mbps. Další zařízení by mělo teoretickou maximální propustnost pouze 1,5 Mbps, což při předpokladu reálného provozu s deseti klientskými stanicemi připojenými k jednomu AP, se jeví jako nedostačující. Příkladně WiFi IP kamera může při maximální kvalitě použít stream s šířkou pásma až 2 Mbps. Měření propustnosti pro toto schéma je uvedeno v příloze E.



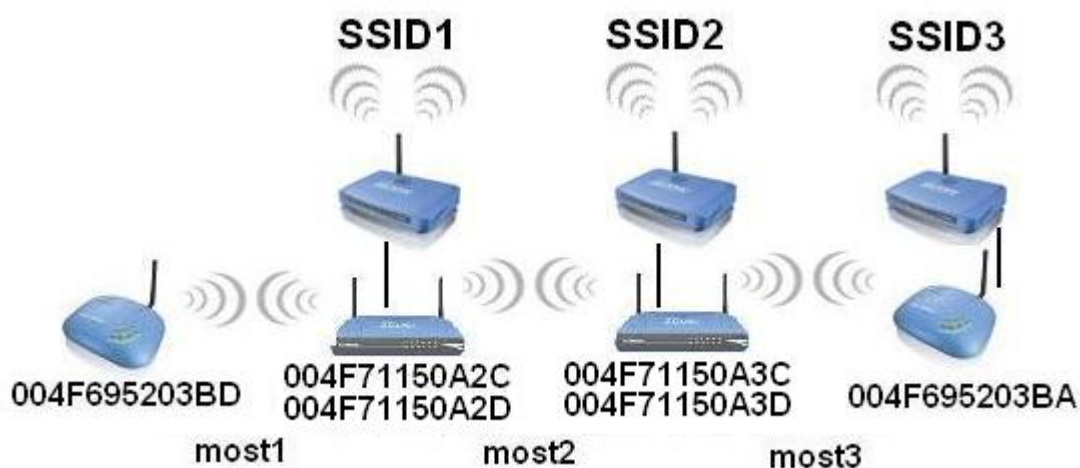
Obrázek 45 – schéma zapojení zařízení.

2. Vždy lichá zařízení jsou nastavena v módu bridge a sudá v módu WDS, tato konfigurace je možná pouze pro variantu se zařízeními WL-5460AP v2 a WLA-5200AP. Zapojení je ve schématu řetězení. Na jednotlivých retranslačních bodech jsou umístěna vždy 2 zařízení. Tímto zapojením je možno eliminovat nežádoucí efekt WDS zapojení s tím, že vždy sudé AP se chová jako zakončení mostu a zároveň jako AP. Nevýhodou tohoto zapojení je nutnost více volných kanálů pro kvalitní běh celé sítě. Další nedostatek je nutnost použít více SSID a jak již bylo zmíněno více kanálů. Pro koncové klienty se celý systém nechová jako jeden přístupový bod, ale jako n přístupových bodů s n BSSID a m použitými kanály. Počet použitých kanálů a SSID je závislý na rušení se jednotlivých WiFi subsítí mezi sebou. Teoreticky na posledním zařízení, můžeme dosáhnout teoretické propustnosti až 23 Mbps, pokud předchozí části WiFi sítě nejsou zatíženy. Schéma zapojení včetně jednotlivých MAC adres, módu zařízení a možných SSID je na obrázku 46. Měření propustnosti pro toto schéma je uvedeno v příloze E.



Obrázek 46 – schéma zapojení zařízení s použitím WiFi „subsítí“

3. Páteří rozvod je tvořen systémem fungujícím v normě IEEE 802.11a. Je dělen na jednotlivé spoje v módu bridge. Na retranslačních bodech jsou vždy umístěna 2 zařízení a to WLA-9000 a druhé, které zabezpečuje šíření WiFi signálu dle normy IEEE 802.11b/g (WL-5460AP v2, WLA-5200AP nebo WLA-5000AP). Zařízení s normou IEEE 802.11a jsou konfigurována vždy jako bridge a je použito schéma point to point. Zařízení WLA-9000 je konfigurováno jako dual WDS bridge a je k němu pomocí LAN portu připojeno zařízení v módu AP s normou IEEE 802.11g. Maximální teoretická propustnost na páteří WiFi síti je 26 Mbps a to v libovolném bodě sítě. Páteří rozvod je koncipován opět jako řetěz. Nevýhodou tohoto systému je opět nutnost použití více kanálů jak v normě IEEE 802.11a tak v normě IEEE 802.11g. Celý systém se opět chová pro koncového klienta jako více WiFi sítí s různými SSID. Schéma zapojení včetně jednotlivých MAC adres, módu zařízení a možných SSID je na obrázku 47.



Obrázek 47 – schéma zapojení zařízení s použitím WiFi „subsítí“

4. Celý systém je tvořen zařízeními splňující IEEE 802.11n Draft2. Spoje mezi jednotlivými AP jsou konfigurovány jako WDS. Jsou použita pouze 3 zařízení (tento počet byl zapůjčen firmou OvisLink), s konfigurací rozšířené šířky kanálu. Vzhledem k rapidně větší propustnosti této WiFi sítě je možno použít i více zařízení za sebou. Pokud ovšem nechceme celý systém degradovat je nutno použít klientů s pre normou IEEE 802.11n draft2. Schéma zapojení včetně jednotlivých MAC adres zařízení je na obrázku 48.



Obrázek 48 – schéma zapojení pro IEEE 802.11n Draft2

10.2 Rozmístnění zařízení

Jednotlivá zařízení byla rozmístněna tak, aby bylo možno porovnávat průběhy při přímých viditelnostech mezi jednotlivými zařízeními v určité části WiFi sítě a průběhy při nutném průchodu WiFi signálu překážkami. Vyobrazení míst rozmístnění jednotlivých zařízení je zaznačeno v příloze G.

VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

10.3 Měření síly signálu pro různé normy z řady IEEE 802.11

Orientační měření síly signálu okolních WiFi vysílačů nám umožní každé z použitých zařízení. Přehledné zobrazení síly je možno zobrazit ve webovém prohlížeči. Jednotlivá zobrazení jsou uvedena na obrázcích 48 až 50. Vybraná zařízení, jako třeba WL-5460AP v2 nám umožní orientační měření signálu i v programu telnet, přes který je možno zařízení i konfigurovat. Ilustrační odečet je vyobrazen na obrázku 51. Toto měření je ale pouze orientační a je závislé na okolních podmínkách (průchod osoby mezi zařízeními atd.). Pro přesnější měření s časovým průběhem bylo použito jednoho z notebooku s WiFi kartou pro všechny použité normy a program NetStumbler. Jedná se opět pouze o orientační měření, které je závislé na kvalitě antény v notebooku a na citlivosti použité WiFi karty. Tato měření jsou vyobrazena v příloze F.

SSID	BSSID	Kanál	Typ	Šifrovat	Signál	Vyberte
DP_VUT AP_WDS4	00:4f:62:23:8d:d8	13 (G)	AP	no	93	☐
DP_VUT AP_WDS1	00:4f:62:22:cb:06	13 (G)	AP	no	78	☐
DP_VUT AP_WDS2	00:4f:62:22:cb:4e	13 (G)	AP	no	63	☐
DP_VUT AP_WDS5	00:4f:62:0f:0d:88	13 (G)	AP	no	50	☐

Obrázek 48 – odečet síly signálu okolních zařízení pro WL-5460AP v2 z webového rozhraní

	ESSID	MAC Address	Conn Mode	Channel	Turbo	Super	XR	WME	Signal Strength (dbm)	Security	Network
☐	Hrad120h	00:0c:42:23:6b:80	A	36	-	-	-	*	-89	WPA2 PSK	AP
☐	tep8	00:0b:6b:81:c3:03	A	44	-	-	-	-	-83	None	AP
☐	5hrad	00:80:48:36:82:f1	A	56	-	-	-	-	-89	WEP	AP
☐	preSSopEr	00:0b:6b:86:29:60	A	64	-	-	-	-	-83	WEP	AP
☐	IPEX-AP-163	00:0c:42:26:95:b0	A	120	-	-	-	-	-89	WPAPSK-AUTO	AP
☐	ErstAp	00:0b:6b:36:bc:b6	A	132	-	*	-	*	-79	WEP	AP

Obrázek 49 – ilustrační odečet síly signálu okolních zařízení pro WLA-5000AP v3 – pro normu 802.11a

	ESSID	MAC Address	Conn Mode	Channel	Turbo	Super	XR	WME	Signal Strength(dbm)	Security	Network
○	CZFree.Net.Cern	00:02:72:4b:96:ed	B	1	-	-	-	-	-89	None	AP
○	CERNOVICE1	00:0b:6b:37:34:13	B	1	-	-	-	-	-92	WEP	AP
○	RyWa.H01	00:0e:8e:7f:9c:23	G	4	-	-	*	*	-83	None	AP
○	KR001	00:13:f7:7f:cc:e0	G	5	-	-	-	*	-91	WPA2 PSK	AP
○	J&J	00:23:cd:c3:ab:8c	G	6	-	-	*	-	-88	WEP	AP
○	02	00:02:cf:50:84:8c	G	6	-	-	-	-	-86	WEP	AP
○	YVNET	00:19:e0:6e:95:4a	G	6	-	-	*	*	-86	None	AP
○	SAS144	00:0b:6b:db:fe:24	B	7	-	-	-	-	-74	None	AP
○	CERNOVICE	00:0b:6b:dd:be:c5	B	8	-	-	-	-	-83	WEP	AP
○	TP-LINK	00:1d:0f:e4:87:fe	B	10	-	-	-	-	-89	WPAPSK-AUTO	AP
○	Olomoucka.Brnet.cz	00:0b:6b:81:37:f8	G	10	-	-	-	-	-86	None	AP
○	Jura	00:0e:2e:64:67:4c	G	11	-	-	-	-	-92	WEP	AP
○	moje_doma_sit	00:23:54:02:24:ee	G	11	-	-	-	-	-92	WPA PSK	AP

Obrázek 50 – odečet síly signálu okolních zařízení pro WLA-5000AP v3 – pro normu 802.11g

```

WL-5460AP> wlan survey
=====
ID      SSID      BSSID      Channel Type      Encrypt Signal      no      83
0       DP_UUT    00:4f:62:0f:0d:88    13 <G>    AP              no      73
1       DP_UUT    00:4f:62:21:f2:0e    13 <G>    AP              no      60
2       DP_UUT    00:4f:62:22:cb:4e    13 <G>    AP              no      58
3       wifi_8np_ofi1 00:11:d8:8d:53:08    1 <B+G>    AP              no
4       DP_UUT    00:4f:62:22:cb:06    13 <G>    AP              no
=====

```

Obrázek 51 – odečet síly signálu okolních zařízení pro WL-5460AP v2 v programu telnet

10.4 Měření propustnosti mezi jednotlivými body WiFi sítě

Jeden z kvalitativních prvků pro posuzování počítačových sítí je propustnost. U WiFi toto platí také. Proto vždy pro danou konfiguraci sítě byla prováděna měření mezi jednotlivými uzly sítě, případně mezi WiFi klientem a zvoleným uzlem. Uzlem je myšlen retranslační bod WiFi sítě.

Pro měření bylo použito dvou programů. NetStress a IPERF. Jejich bližší popis je uveden v příloze A.

Pro relevantní měření u prvků, které mají více jak jeden LAN port, bylo nutné změřit i propustnost mezi těmito porty, z důvodu případného dalšího propojení některých zařízení mezi sebou. Pro eliminaci náhodné chyby způsobené špatnou síťovou kartou LAN bylo provedeno i kontrolní měření pouze mezi oběma notebooky bez přítomnosti dalšího zařízení. Další z testů, byl prováděn v prostředí bez rušení, kdy spolu komunikovaly notebooky

VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

připojené k zařízení, jenž bylo používáno v módu AP. Tímto se ověřila propustnost bezdrátové části, která byla srovnávána s hodnotami uváděnými výrobcem.

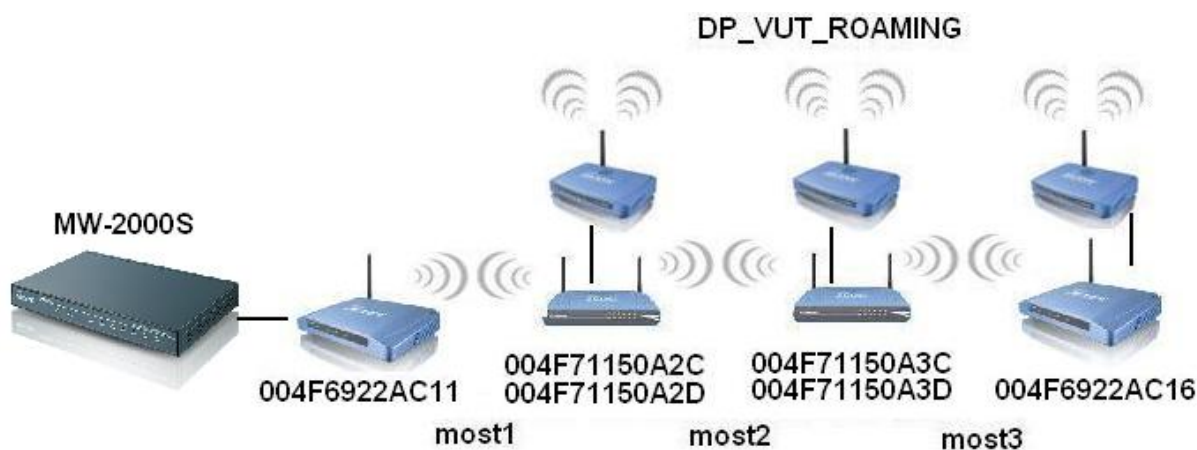
Po těchto prvotních testech vždy byla prováděna měření mezi jednotlivými uzly, jak již bylo zmíněno výše. Jednotlivé hodnoty pro různé konfigurace WiFi sítě jsou uvedeny v příloze E.

10.5 Alternativní řešení pro pokrytí strukturovaného prostoru s jedním vysílaným SSID

Jednou z možných alternativ pokrytí strukturovaného prostoru s použitím jednoho SSID a zachováním maximální propustnosti z libovolného bodu WiFi sítě, je použití struktury z bodu 9.1 varianta 3 s následnou auto konfigurací koncových zařízení za pomoci brány MW-2000s. Bránu je možno spojit se zařízeními WLA-5000AP nebo WL-5460AP v2, proto tato zařízení nemohou být použita v páteřním rozvodu. Maximální počet obsluhovaných AP touto branou je 12 zařízení, při použití pouze jednoho typu připojených koncových AP.

Zařízení MW-2000s nám umožní vytvoření roamingového systému s více AP za použití jednoho SSID. Brána automaticky volí i kanály pro koncová AP tak, aby nedocházelo k rušení mezi jednotlivými koncovými AP, v našem případě WL-5460AP v2. Zabezpečení koncových bodů přebírá pod svoji správu také tato brána, kdy mimo již zmíněných typů jako je WEP, WPA-PSK, umí brána transparentní ssl VPN.

Schéma celého zapojení za použití struktury zřetězení páteřních zařízení je uvedeno na obrázku 52.



Obrázek 52 – schéma zapojení WiFi sítě s bránou MW-2000S řídící koncová AP pro roaming

10.6 Obecné řešení pro mobilní jednotky rozmisťující jednotlivá zařízení

Jak bylo zmíněno výše, pro rozmisťování jednotlivých zařízení budou použity robotické jednotky s dálkovým řízením.

Před započítáním rozmisťování WiFi jednotek je doporučeno provést první měření prostorů s následným vyhodnocením vlivu okolních WiFi sítí. Z vyhodnocení pak bude

VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

zřejmé, kterou normu je vhodné použít pro nově vznikající WiFi síť. Předpokládaná topologie může být řetězec, hvězda, případně kombinace obou. Vzhledem k tomuto předpokladu bych doporučil zvolit strategii tvorby topologie uvedenou v bodu 9.1 bod 3. Tedy, každá jednotka poveze dvě WiFi zařízení, jedno dvourádiové pro normu IEEE 802.11a a druhé pro šíření WiFi signálu dle normy IEEE 802.11g

Předpokládáme, že datová konektivita bude vztažena k pevnému bodu, který se nebude pohybovat.

Pro pokrytí páteřní WiFi sítě si musíme stanovit kvalitativní požadavky na tuto část. Nejjednodušší požadavkem pro následný návrh může být síla signálu přijímaná od předchozí WiFi jednotky. Na základě tohoto vyhodnocení se dá následně stanovit i teoretická maximální propustnost sítě.

Pro model ve strukturovaném prostoru (budově) budou u zařízení aplikovány všesměrové antény dodávané výrobcem. Pokud bychom chtěli zvýšit dosah, je možno použít antény s vyšším ziskem, ovšem pak je nutné regulovat výstupní výkon Tx na jednotlivých zařízeních tak, aby nebyl překročen limit pro maximální vyzářený výkon. Nevýhodou tohoto řešení je, že zařízení, která jsou v bezprostřední blízkosti mohou díky anténám s vyšším ziskem přebudit vstupní člen a následkem toho dojde k výpadku spojení, případně neúměrně dlouhým latencím.

Nyní tedy popíši kroky výstavby sítě:

1. Pevný bod je nastaven jako AP, tak aby bylo možno připojit WiFi zařízení v módu klient (pro zařízení s normou IEEE 802.11a). Toto je výchozí bod pro pohyb mobilních jednotek.
2. Robot s tímto zařízením se dává do pohybu, přičemž je vyhodnocována síla signálu. Pokud překročíme vzdálenost, kdy se signál dostane pod určenou hranici, robot se vrací až k hranici, kdy je signál vyhovující. Robot zůstane stát.
3. Na tomto stojícím robotu se zapíná WiFi zařízení s normou IEEE 802.11g, to je nastaveno již jako AP.
4. Další robot se dává do pohybu a má nastaveno zařízení normy IEEE 802.11a do módu klient a je připojeno k pevnému bodu s konektivitou. Zároveň je zapnuto zařízení s normou IEEE 802.11g tak aby sledovalo sílu signálu již vysílajících zařízení. Vyhodnocují se síly signálu obou zařízení. Pokud je dosažena hranice, kde je signál pro zařízení IEEE 802.11a limitním, robot se vrací a kopíruje hranici, která vyhovuje síle signálu od výchozího bodu. Zároveň vyhodnocuje síly signálu od zařízení IEEE 802.11g, kde je obdobně definována minimální síla signálu. Pokud je této hranici dosaženo, robot zastaví. Následně se přejde zpět na počátek bodu 3. Pokud nemůže robot takové místo najít (omezení hranicemi prostoru), přecházíme k bodu 5.
5. Stojící robot zapíná druhou rádiovou jednotku v normě IEEE 802.11a do módu AP.
6. Mobilní jednotka, která nenašla vyhovující bod pro zastavení, se připojuje ke stojící jednotce s nejsilnějším signálem v normě IEEE 802.11a, případně se k ní automaticky vrátí.
7. Spoje typu AP klient, mezi stojícími jednotkami a pevným bodem, přepneme do módu bridge. Vzniká první vrstva páteřní struktury WiFi sítě.
8. Každou ze stojících jednotek prohlásíme za pevný bod. Přecházíme k bodu 1 a necháme další jednotky vytvářet další vrstvu páteřní WiFi sítě.

VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

Uvedené kroky aplikujeme opakovaně pro stacionárně stojící robotické jednotky tak, aby došlo k optimálnímu pokrytí strukturovaného prostoru WiFi signálem normy IEEE 802.11g a následně k této struktuře bylo možno připojovat koncové klienty, případně WiFi IP kamery.

11. Závěr

Byla provedena řada venkovních měření pro typ spoje point to point a point to multipoint. Z výsledků je jasné zřejmé, že pro výstavbu kvalitnějšího spoje je vhodné volit pásmo s nižším zarušením, což je v dnešní době jednoznačně pásmo 5 GHz. Dalším zcela zřejmým výsledkem je použití dělených tras na jednotlivé segmenty. Pro jednotný segment za použití WDS technologie dochází k nepříjemnému dělení propustnosti. Tato se dá velice dobře eliminovat právě zmíněným rozdělením na jednotlivé zcela samostatné segmenty. Dále lze jednoznačně doporučit toto řešení pro případy velkých rozdílů vzdáleností mezi jednotlivými koncovými body v zapojení point to multipoint. Rozdělením na jednotlivé zcela samostatné segmenty je zcela eliminován vliv hodnot ACK pro spoje, kde tento parametr již neodpovídá vzdálenosti zařízení od přístupového bodu.

Ze zkušeností lze doporučit pro spoje point to point použití venkovního zařízení AirMAX5. Aplikace těchto zařízení pro spoje do 3 km je naprosto bezproblémová a je možno vytvořit velice kvalitní spoj bez nutnosti použití více komponent pro každou stranu spoje. Pro výstavbu jednoduchého retranslačního bodu je opět výhodnější použít dvou venkovních zařízení, než dvou antén s odpovídajícími svody připojenými do zařízení WLA-9000, které je umístěno tak, aby umístění vyhovovalo specifikaci tohoto produktu.

Z jednotlivých měření pro koncepci WDS a WDS most byla ověřena teoretická znalost nežádoucích vlivů těchto zapojení. Jde především o dělení přenosové rychlosti na každém retranslačním bodě a o nevhodnost aplikace těchto zapojení pro rozsáhlé celky s aktivním WiFi provozem v okolních WiFi sítích s ohledem na možnost zarušení části WDS sítě okolními bezdrátovými sítěmi.

Z jednotlivých měření, která byla prováděna uvnitř budov, bylo zjištěno, že útlum signálu při průchodu překážkou je pro normy IEEE 802.11a a IEEE 802.11g velmi podobný. Rozdíly pro pásmo 2,4 GHz a 5 GHz jsou zanedbatelné. Této skutečnosti bylo využito při úvaze nad principem rozmisťování jednotlivých zařízení pomocí říditelných robotických jednotek. Pro bezproblémový chod WiFi sítě lze jednoznačně doporučit stejný postup jako v případě venkovních distribuovaných sítí. Jedná se především o použití pásma 5 GHz pro páteřní spoje v distribuované síti a jejich dělení na jednotlivé segmenty. Konečné pokrytí WiFi signálem je následně řešeno již technologií 2,4 GHz, která je v dnešní době podstatně dostupnější než technologie pro pásmo 5 GHz. Tento pohled je brán z pohledu dostupnosti koncových zařízení připojujících se k WiFi síti.

Z pohledu nově nastupující technologie 802.11n, která nemá ještě pevně určený standard, lze doporučit její využití, ale pouze za předpokladu použití koncových zařízení koncipovaných také pro tuto normu. Při měřeních síly signálu a propustnosti, za použití zařízení 802.11n Draft 2, bylo dosahováno větších vzdáleností a větších propustností pro jednotlivých spojů, než-li za použití stejně umístěných zařízení, ale se staršími normami IEEE 802.11a nebo IEEE 802.11g. Z naměřených hodnot je zcela jasné vidět, že propustnost spojů realizovaných pomocí technologie 802.11n je 2x větší než při použití starších standardů. Bohužel toto kvalitativní navýšení spoje je realizovatelné pouze za předpokladu užití obou koncových zařízení v normě IEEE 802.11n Draft2. Výhodou uvedených zařízení je zpětná kompatibilita s předchozími standardy, proto je vhodné s ohledem na budoucí provoz uvažovat nad použitím těchto zařízení pro koncové pokrytí prostoru WiFi signálem.

Z jednotlivých měření WDS technologie i pro zařízení IEEE 802.11n Draft2 je zřejmé, že tato technologie není vhodná pro realizaci páteřních spojů distribuované sítě za

předpokladu průchodu WiFi signálu překážkou mezi jednotlivými páteřními zařízeními WiFi sítě. Dochází k velmi značné degradaci spoje ve srovnání se staršími standardy.

Ze zkušeností lze tedy doporučit kombinaci jednotlivých WiFi technologií při rozmisťování pomocí říditelných robotických jednotek pouze pro problematiku pokrytí strukturovaného prostoru. Při použití ve venkovních podmínkách není možno eliminovat vliv reliéfu prostředí, proto tato technologie není zcela vhodná pro použití ve spolupráci s těmito jednotkami.

12. Seznam použitých zkratk

2R2T	2 transmit, 2 receive – model počtu vysílačích a přijímacích antén v poměru 2:2
3R3T	3 transmit, 3 receive – model počtu vysílačích a přijímacích antén v poměru 3:3
2R2T	2 transmit, 2 receive – model počtu vysílačích a přijímacích antén v poměru 2:2
ACK	Acknowledgment – potvrzuje příjem a správnost přijatých dat v rámci bezdrátové komunikace
AES	Advanced Encryption Standard – šifra, využívající symetrického klíče (tj. stejný klíč k šifrování i dešifrování)
AP	Access Point – přístupový bod
BPSK	Binary Phase-Shift Keying – typ dvoustavové modulace
BSS	Basic Service Set – základní soubor služeb
CAM	Content-Addressable Memory – tabulka fyzických adres a portů síťových rozhraní
CCK	Complementary Code Keying – digitální frekvenční modulace
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol – autentizační protokol, používaný v rámci WPA2
CD	Compact Disc – kompaktní disk
CRC	Cyclic Redundancy Check – redundantní kontrolní součet
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance – metoda vícenásobného přístupu k médiu s předcházením kolizí
CST	Common Spanning Tree – jiný název pro Spanning Tree Protocol (STP)
CTS	Clear To Send – potvrzení připravenosti příjmu dat v rámci bezdrátové komunikace
ČTÚ	Český telekomunikační úřad
DBPSK	Differential Binary Phase-Shift Keying – diferenciální dvoustavová digitální modulace
DC	Direct Current – stejnosměrné napětí (proud)
DCF	Distributed Coordination Function – distribuovaná koordinace přístupu k médiu
DIFS	Distributed Coordination Function Inter Frame Spacing – mezirámcové mezery největší délky
DP	Diplomová práce
DQPSK	Differential Quadrature Phase-Shift Keying – diferenciální čtyřstavová digitální modulace
DSSS	Direct Sequence Spread Spectrum – metoda frekvenční modulace
EAP	Extensible Authentication Protocol – autentizační protokol
EIFS	Extended Inter Frame Spacing – mezirámcové mezery libovolné délky
EIRP	equivalent isotropically radiated power, ekvivalentní izotropně vyzářený výkon
ESS	Extended Service Set – překrývající se soubor služeb
FHSS	Frequency Hopping Spread Spectrum – metoda frekvenční modulace
FIPS	Federal Information Processing Standards – Americký federální standard

VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

FTP	File Transfer Protocol – aplikační protokol, obstarávající přenos souboru mezi stanicemi, na kterých mohou být spuštěny různé operační systémy
HR/DSSS	High Rate/Direct Sequence Spread Spectrum – přenosový modulační mechanismus
IAP	Internet Access Provider – poskytovatel internetového připojení
IAPP	Inter-Access Point Protocol – podporuje plynulý pohyb klienta mezi přístupovými body
IBSS	Independent Basic Service Set - nezávislý základní soubor služeb
ICMP	Internet Control Message Protocol – slouží k signalizaci mimořádných situací v IP sítích (např. chybová hlášení)
ID	Identifikující
IEEE	Institute of Electrical and Electronics Engineers – Institut inženýrů elektrotechniky a elektroniky
IFS	Inter Frame Spacing – mezirámcové mezery
IP	Internet Protocol – internetový protokol
IR	Infrared – infračervené světlo (spektrum)
ISM	Industrial, Science and Medical band
ISP	Internet Service Provider – poskytovatel internetového připojení
LAN	Local Area Network – lokální počítačová síť
LEAP	Lightweight Extensible Authentication Protocol
LED	Light Emitting Diode – světlo emitující polovodičová dioda
LLC	Logical Link Control - podvrstva spojové vrstvy
MAC	Medium Access Control – podvrstva spojové vrstvy
MIMO	Multiple-input multiple-output – technologie označující použití více vstupů více výstupů
MSTP	Multiple Spanning Tree Protocol - protokol, který obstarává zacyklení aktivních prvků (switch, směrovač,...) v počítačových sítích
NAT	Network Address Translation – překlad síťových adres
NAV	Network Allocation Vector – délka doby, po kterou nebudou bezdrátová zařízení vysílat
NTP	network time protokol
OFDM	Orthogonaly Frequency Division Multiplexing – metoda frekvenční modulace
OSI	Open Systems Interconnection – propojení otevřených standardů - model síťové hierarchie, představující strukturu síťových protokolů jako řadu vertikálních vrstev
PAN	Personal Area Network – osobní síť
PBCC	Packet Binary Convolution Coding
PC	Personal Computer
PCF	Point Coordination Function – koordinace přístupu k médiu jedním bodem
PCI	Peripheal Component Interface – rozhraní přídavných zařízení počítače
PDM	Physical Dependent Medium – podvrstva fyzické vrstvy, závislá na daném fyzickém médiu
PEAP	Protected Extensible Authentication Protocol – rozšiřuje zabezpečení ostatních ověřovacích protokolů EAP
PHY	Physical Layer – fyzická vrstva

PIFS	Point Inter Frame Spacing – mezirámcové mezery střední délky
PLCP	Physical Layer Convergence Procedure – podvrstva fyzické vrstvy, nemusí být závislá na daném fyzickém médiu
PoE	Power over Ethernet – napájení zařízení pomocí ethernetového kabelu
PPDU	Physical Layer Packed Data Unit – paket fyzické vrstvy
PPP	Point-to-Point Protocol – obstarává telefonické připojení počítače k Internetu
PPTP	Point-to-Point Tunneling Protocol – bezpečná komunikace skrze Internet (nezabezpečené sítě) – virtuální privátní síť
PSK	Phase Shift Keying – digitální modulace
PSK	Pre-Shared Key – předsdílený klíč
QAM	Quadrature Amplitude Modulation – digitální čtyřstavová amplitudová modulace
QoS	Quality of Service – systém, pro řízení datových toků v počítačových sítích
QPSK	Quadrature Phase-Shift Keying – digitální čtyřstavová modulace
RAM	Random Access Memory – typ fyzické paměti (přepisovatelná)
RB	Root Bridge – kořenový most
RF	Radio Frequency – rádiová frekvence
RFC	Request for Comments – označení standardů a dokumentů pro oblast počítačů, Internetu a dalších systémů
ROM	Read-Only Memory – typ fyzické paměti (nepřepisovatelná)
RTS	Request to Send – žádost o vysílání
SDM	Spatial Division Multiplexing
SDRAM	Synchronous Dynamic Random Access Memory – typ fyzické paměti (přepisovatelná)
SIFS	Short Inter Frame Spacing – mezirámcové mezery nejmenší délky
SNMP	Simple Network Management Protocol – správa, konfigurace a informace o síťových zařízeních
SOHO	smalloffice and home office – vyjadřuje segment použití. Segment malých firem a domácností
SSID	Service Set Identifier – název bezdrátové sítě
SSL	Secure Socket Layer – zabezpečení komunikace šifrováním autentizací
STA	Spanning Tree Algorithm – algoritmus, použitý v protokolu STP
STP	Spanning Tree Protocol – protokol, který obstarává zacyklení aktivních prvků (switch, směrovač,...) v počítačových sítích
SW	Switch – přepínač - aktivní prvek počítačové sítě – propojuje počítače na různých segmentech sítě
TCP	Transmission Control Protocol – protokol, používaný pro „spolehlivý“ přenos datagramů v rámci počítačových sítí a Internetu
TKIP	Temporal Key Integrity Protocol – bezpečnostní protokol používaný v bezdrátových sítích
TLS	Transport Layer Security – zabezpečení komunikace šifrováním autentizací
TOS	Type of Service – část IP paketu, označující typ služby
TTL	Time-to-Live – hodnota, která omezuje průchodnost paketů přes aktivní prvky sítě nebo dobu jejich platnosti

TTLS	Tunneled Transport Layer Security – zabezpečená komunikace skrze Internet – vytvoření virtuální privátní sítě
U-NII	Unlicensed National Information Infrastructure
UDP	User Datagram Protocol – protokol, zajišťující „nespolehlivý“ přenos datagramů v rámci počítačových sítí a Internetu
UPnP	Universal Plug and Play – snadné rozpoznání a konfigurace hardware
USB	Universal Serial Bus – universální sériové rozhraní
VPN	Virtual private network
WDS	Wireless Distribution System – bezdrátový distribuční systém
WEP	Wired Equivalent Privacy – metoda šifrování komunikace
Wi-Fi	Wireless Fidelity – asociace pro bezdrátový standard; pojem pro bezdrátové sítě založené na standardu IEEE 802.11b/g
WISP	Wireless Internet Service Provider – provozní režim WiFi zařízení, které umí kombinovat příjem dat přes bezdrátovou část a nastavit směrovač pro LAN výstupy
WLAN	Wireless Local Area Network – bezdrátová lokální počítačová síť
WPA	Wi-Fi Protected Access – metoda šifrování komunikace
WPS	WiFi protected setup – funkce pro rychlou konfiguraci zabezpečení ve WiFi síti

13. LITERATURA

- [1] BARKEN, L.: *Jak zabezpečit bezdrátovou síť Wi-Fi*. Computer Press, Brno 2004. ISBN 80-251-0346-3.
- [2] DAVIS, H.: *Bezdrátové sítě Wi-Fi*. Grada, Praha 2006. ISBN 80-247-1421-3.
- [3] HABRAKEN, J.: *Počítačové sítě*. Grada, Praha 2006. ISBN 80-247-1422-1.
- [4] KABELOVÁ, A.; DOSTÁLEK, L.: *Velký průvodce protokoly TCP/IP a systémem DNS*. Computer Press, 3. vyd. Praha 2002. ISBN 80-7226-675-6.
- [5] PECHAČ, P.: *Modely šíření vln v zástavbě*. 1. vyd. BEN – technická literatura, Praha 2005. ISBN 80-7300-186-1.
- [6] ZANDL, P.: *Bezdrátové sítě WiFi – praktický průvodce*. Computer Press, Brno 2003. ISBN 80-7226-632-2.
- [7] KOCOUR, Z.; ŠAFRÁNEK, M. *Fyzická vrstva WiFi* [online]. Dostupné z: <<http://access.feld.cvut.cz/view.php?navezclanku=fyzicka-vrstva-wi-fi&cislocclanku=2008050006>>
- [8] KOCOUR, Z.; ŠAFRÁNEK, M. *Bezdrátové systémy v přístupové síti* [online]. Dostupné z: <<http://access.feld.cvut.cz/view.php?navezclanku=bezdratove-systemy-v-pristupove-siti&cislocclanku=2008020002>>
- [9] KOVÁŘ, P.; NOVOTNÝ, V. *Přístupové metody bezdrátových sítí* [online]. Dostupné z: <<http://access.feld.cvut.cz/view.php?navezclanku=pristupove-metody-bezdratovych-siti&cislocclanku=2008100003>>
- [10] OVISLINK corp., divize AIRLIVE. *Webové stránky výrobce* [online]. Dostupné z: <http://www.airlive.com>

PŘÍLOHY

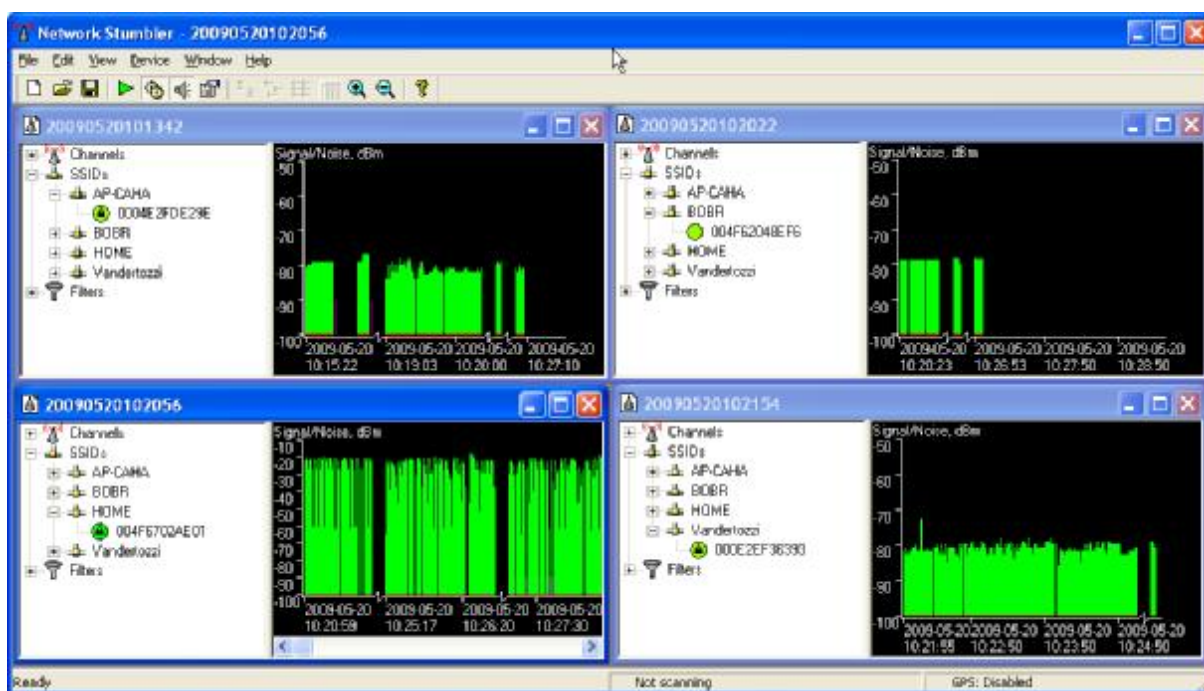
A Popis použitého software

NetStumbler

Jednou ze základních utilit pro kontrolu výskytu WiFi sítí je program NetStumbler. U většiny WiFi síťových karet, nám umožňuje provést scan frekvenčního pásma s následným rozlišením výskytu jednotlivých sítí na jednotlivých kanálech. Tato informace nám umožní vhodnou volbu kanálu u námi navrhované sítě, tak abychom co nejvíce eliminovali rušení v rámci překrývajících se kanálů.

Program nám umožňuje jednoduchou filtraci všech nascanovaných WiFi sítí dle jednoduchých kritérií jakou jsou například, zda je síť kryptovaná, zda je používáno defaultní SSID a další. Další drobností je možnost prohlížení přiřazených BSSID k jednotlivým vysílaným SSID. Toto se s výhodou používá u zapojení sítí s WDS opakovači. Celá síť se tváří že má pouze jedno SSID, ale je k ní přiřazeno několik BSSID, která odpovídají jednotlivým zařízením. BSSID ve skutečnosti odpovídá MAC adrese WiFi části zařízení.

Program nám mimo těchto základních údajů umožňuje měření síly WiFi signálu, zjištění procentní síly signálu, útlum na přijímači, IP adresu bodu a mnoho dalších parametrů. Pokud máme v dosahu více sítí, u kterých potřebujeme zjistit sílu přijímaného signálu, je možno provádět tento odečet u každé sítě zvlášť (viz obrázek 1A). Bohužel odečet probíhá vždy pouze u jedné sítě, kterou si zvolíme jako aktivní pro monitoring. Výsledky nasnímaných hodnot je možno uložit do souboru a dále je použít později pro vyhodnocení měření. Jednou dost podstatnou nevýhodou je, že program nedovede zachytit spoje typu most. Program spolupracuje s vybranými snímači GPS signálu, což se dá s výhodou využít při měření ve venkovním prostředí.



Obrázek 1A – rozložení oken pro více WiFi sítí

Iperf 1.7.0

Tento jednoduchý konzolový program byl používán při měřeních propustnosti jednotlivých spojů. Aplikaci je v možno použít jako klient nebo jako server. Pro měření tedy byly použity obě funkcionality Na obrázku 2A jsou zobrazeny jednotlivé možné parametry programu.

```
C:\>iperf --help
Usage: iperf [-s|-c host] [options]
       iperf [-h|--help] [-v|--version]

Client/Server:
  -f, --format [kmKM]    format to report: Kbits, Mbits, KBytes, MBytes
  -i, --interval #       seconds between periodic bandwidth reports
  -l, --len #[KM]        length of buffer to read or write (default 8 KB)
  -m, --print_mss        print TCP maximum segment size (MTU - TCP/IP header)
  -o, --output <filename> output the report or error message to this specific
  d file
  -p, --port #           server port to listen on/connect to
  -u, --udp              use UDP rather than TCP
  -w, --window #[KM]     TCP window size (socket buffer size)
  -B, --bind <host>      bind to <host>, an interface or multicast address
  -C, --compatibility    for use with older versions does not send extra msgs
  -M, --mss #            set TCP maximum segment size (MTU - 40 bytes)
  -N, --nodelay          set TCP no delay, disabling Nagle's Algorithm
  -U, --IPv6Version      Set the domain to IPv6

Server specific:
  -s, --server           run in server mode
  -D, --daemon           run the server as a daemon
  -R, --remove           remove service in win32

Client specific:
  -b, --bandwidth #[KM]  for UDP, bandwidth to send at in bits/sec
                        <default 1 Mbit/sec, implies -u>
  -c, --client <host>    run in client mode, connecting to <host>
  -d, --dualtest          Do a bidirectional test simultaneously
  -n, --num #[KM]        number of bytes to transmit (instead of -t)
  -r, --tradeoff          Do a bidirectional test individually
  -t, --time #           time in seconds to transmit for (default 10 secs)
  -F, --fileinput <name> input the data to be transmitted from a file
  -I, --stdin            input the data to be transmitted from stdin
  -L, --listenport #     port to receive bidirectional tests back on
  -P, --parallel #       number of parallel client threads to run
  -T, --ttl #            time-to-live, for multicast (default 1)

Miscellaneous:
  -h, --help             print this message and quit
  -v, --version          print version information and quit

[KM] Indicates options that support a K or M suffix for kilo- or mega-

The TCP window size option can be set by the environment variable
TCP_WINDOW_SIZE. Most other options can be set by an environment variable
IPERF_<long option name>, such as IPERF_BANDWIDTH.

Report bugs to <dast@nlanr.net>
```

Obrázek 2A – zobrazení položky help pro iperf

Pro měření tedy bylo použito dvou různých nastavení a to mód klient (použit parametr -c) a server (použit parametr -s). Při měření byly použity hodnoty pro velikost paketu o velikosti 64 KB a vyrovnávací paměť o velikosti 24 KB. Čas jednotlivých měření byl definován na 30 s.

Příklad pro nastavení aplikace v módu server:

IPERF – s –w 64K –l 24K

Příklad pro nastavení aplikace v módu server:

IPERF – c 192.168.100.12 –w 64K –l 24K –t 30

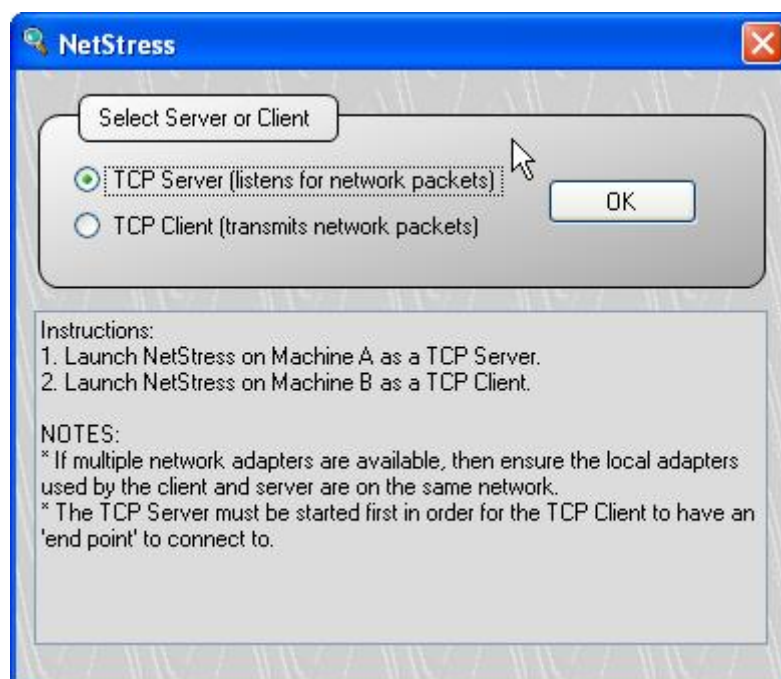
NetStress 1.0.8245

Program pro měření datové propustnosti mezi dvěma PC. Program je velmi jednoduchý a intuitivní. Po spuštění je uživatel vyzván k výběru módu, ve kterém se má program rozběhnout (viz obrázek 3A). Jako u předchozího programu je možno vybrat klient nebo server. Po výběru módu se musí vybrat síťové rozhraní na kterém bude program komunikovat. V našem případě to byly síťové adaptéry LAN nebo síťové adaptéry WiFi (vybíralo se dle typu měření). Tento výběr je shodný pro oba módy programu. Na obrázku 4A je vyobrazen mód server s již vybraným síťovým rozhraním.

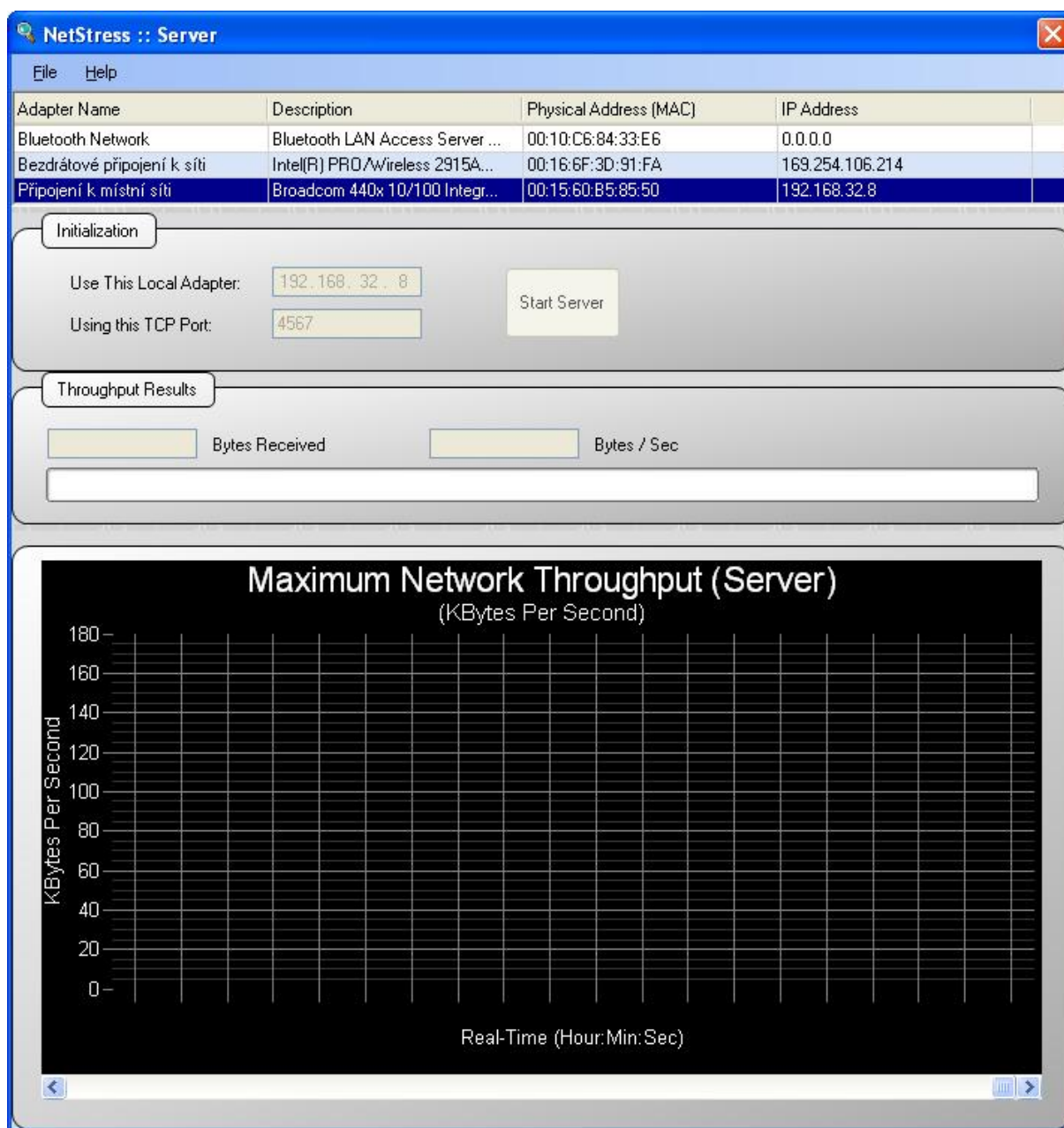
Pro mód klient je nutno ještě zadat IP adresu protějšního PC kde se spuštěn NetStress jako server (viz obrázek 5A).

Každé měření je potom automaticky vyhodnocováno a výsledky jsou zaznamenávány do zobrazovaného grafu. Dále je zobrazen počet přenesených dat a průměrná hodnota propustnosti, která se vypočítává z doby měření a přenesených dat. Tyto údaje, jsou zobrazovány jak na straně serveru, tak na straně klienta.

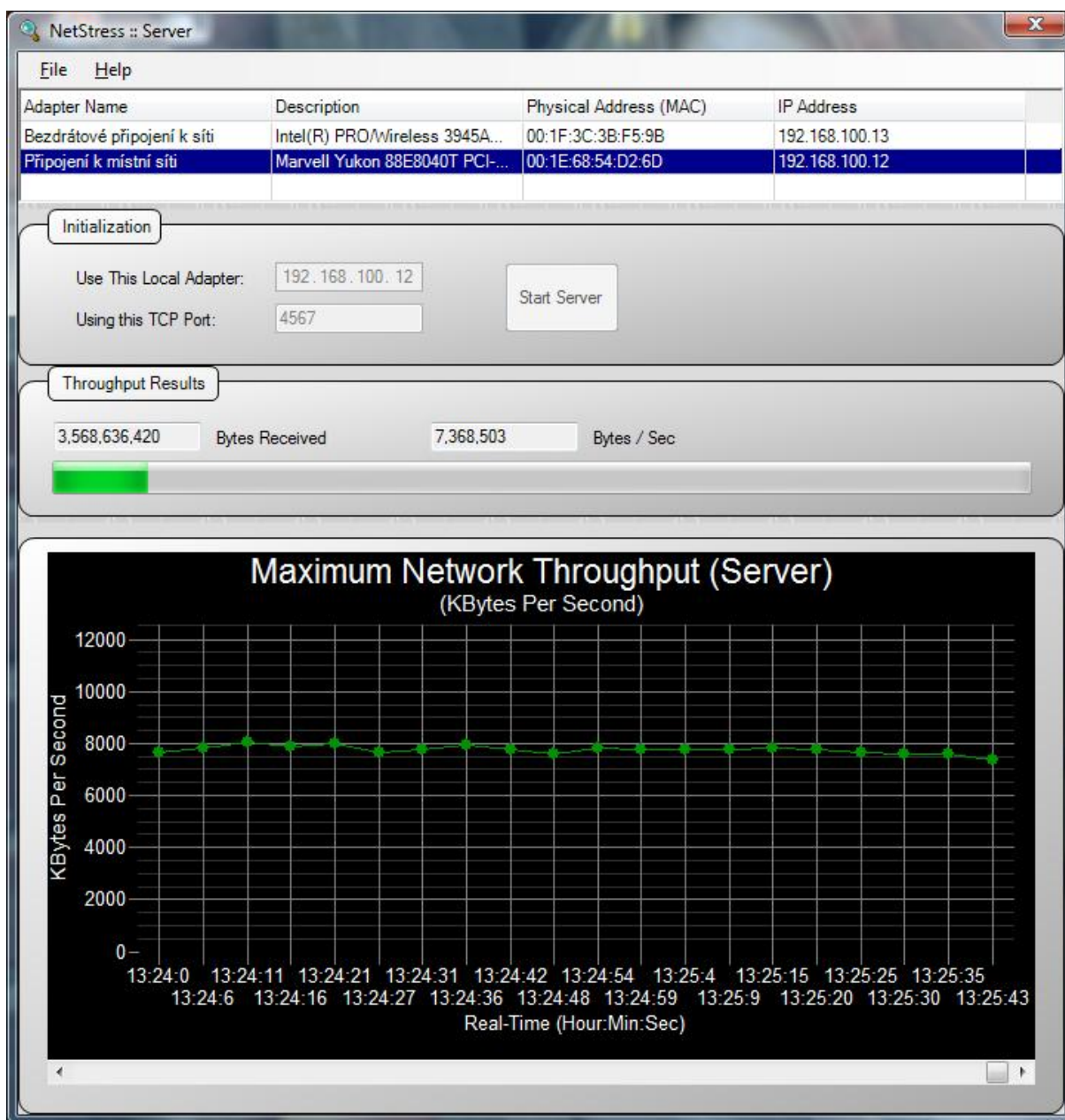
Měření se ukončí odchodem z programu. Z tohoto důvodu je tedy pro každé měření nutno spustit a nakonfigurovat program znovu, to se týká klientské části.



Obrázek 3A – výběr módu



Obrázek 4A – serverový mód s vybraným rozhraním LAN



Obrázek 5A – klientský mód se zobrazeným grafem a propustností

Příloha B

Nastavení zařízení WL-5460 – mód AP, bridge a mód WDS

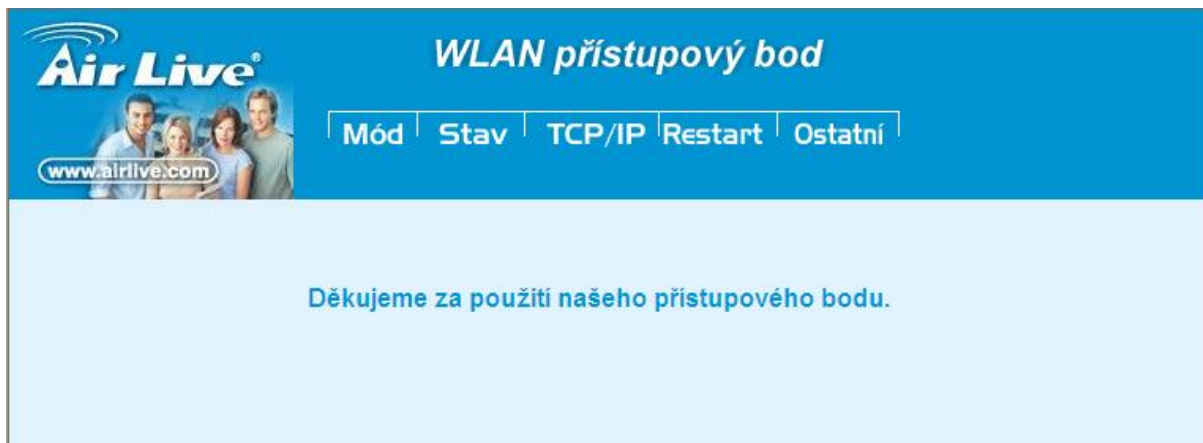
Uvedené zařízení patří patrně k jednomu z nejrozšířenějších multifunkčních WiFi zařízení typu IEEE 802.11b/g na Českém trhu. S ohledem na tuto skutečnost a s ohledem na množství koncových WiFi zařízení pracujících v normě IEEE 802.11b/g bylo vybráno právě toto zařízení pro módy AP, případně most a WDS.

Uvedené zařízení je konfigurováno s firmware 5460APv2_e15_czech_b2. Jiné verze firmware mohou být mírně odlišné!

Po vybalení nového zařízení z přepravního boxu je zařízení v továrním nastavení. Tedy na WiFi zařízení je použit kanál číslo 11, SSID s názvem airlive, kompatibilita pro IEEE 802.11b/g zařízení a není použito žádné zabezpečení pro WiFi AP. Pro LAN i WiFi část je zařízení nakonfigurováno s IP adresou 192.168.100.252 a maskou podsítě 255.255.255.0. Integrovaný DHCP server je vypnutý. K zařízení se tedy dá připojit pomocí libovolného LAN portu nebo pomocí WiFi za předpokladu, že bude zařízení, z něž se připojujeme mít nakonfigurováno síťové rozhraní v IP prostoru 192.168.100.x vyjma IP adresy, jenž je přiřazena WL-5460AP v2.

Jak již bylo zmíněno dříve, zařízení je možno konfigurovat do řady módu. Pro náš případ se vybírá nastavení pro mód AP, bridge nebo WDS. Uvedené konfigurace jsou prováděny pomocí webového prohlížeče. Dle výrobce je doporučen Internet Explorer 5.5 a vyšší.

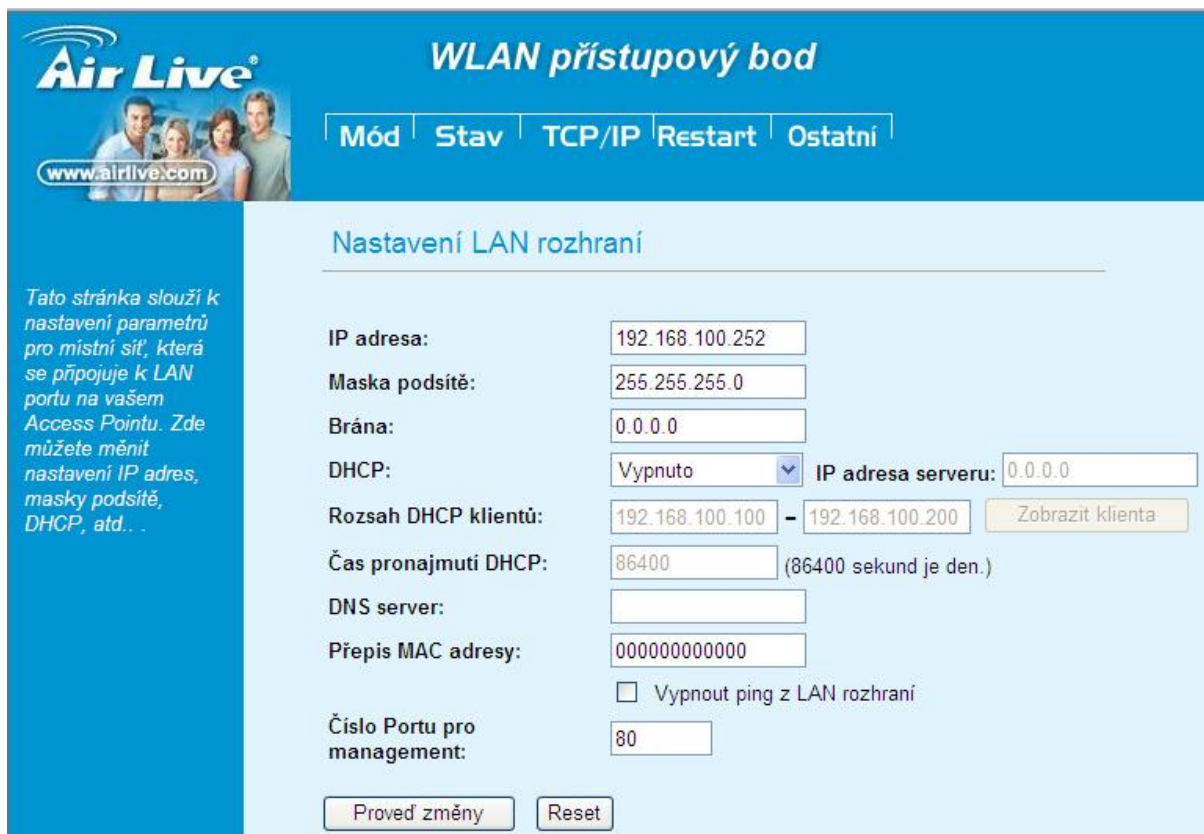
Po připojení pomocí internetového prohlížeče k adrese <http://192.168.100.252> je vyobrazena následující stránka:



Pokud potřebujeme zařízení zanést do námi zvoleného IP prostoru, zvolíme položku TCP/IP. Na stránce, která se zobrazí, můžeme změnit TCP/IP adresu rozhraní se všemi dalšími náležitostmi, jako jsou maska podsítě a výchozí brána. Případně můžeme nastavit v zařízení pohled na DHCP server. Zařízení můžeme nastavit jako klient, server, přenosový agent nebo že je DHCP vypnuto. Další možnost je zakázání odezvy ping z LAN rozhraní a port na němž je prováděn management zařízení. Standardně je použit port 80. Po provedení všech změn potvrdíme uložení tlačítkem *Proved' změny*. Případně můžeme vše uvést do původní podoby

VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

tlačítkem *Reset*. Po stlačení tlačítka jsme upozorněni, že změny se projeví až po restartu zařízení. To provedeme v menu *Restart*.



The screenshot shows the 'WLAN přístupový bod' (WLAN access point) configuration interface for 'Air Live'. The top navigation bar includes 'Mód', 'Stav', 'TCP/IP', 'Restart', and 'Ostatní'. The 'TCP/IP' tab is selected, leading to the 'Nastavení LAN rozhraní' (LAN interface settings) page.

On the left, a blue sidebar contains the text: 'Tato stránka slouží k nastavení parametrů pro místní síť, která se připojuje k LAN portu na vašem Access Pointu. Zde můžete měnit nastavení IP adres, masky podsítě, DHCP, atd...' (This page is used for setting parameters for the local network that connects to the LAN port on your Access Point. Here you can change the settings for IP addresses, subnet mask, DHCP, etc...).

The main configuration area includes the following fields and options:

- IP adresa:** 192.168.100.252
- Maska podsítě:** 255.255.255.0
- Brána:** 0.0.0.0
- DHCP:** Vypnuto (dropdown menu)
- IP adresa serveru:** 0.0.0.0
- Rozsah DHCP klientů:** 192.168.100.100 - 192.168.100.200 (with a 'Zobrazit klienta' button)
- Čas pronajmutí DHCP:** 86400 (86400 sekund je den.)
- DNS server:** (empty field)
- Přepis MAC adresy:** 000000000000
- ☐ Vypnout ping z LAN rozhraní
- Číslo Portu pro management:** 80

At the bottom, there are two buttons: 'Proved' změny' (Apply changes) and 'Reset'.

Pokud jsme tedy provedli změnu TCP/IP protokolu na rozhranních zařízeních, můžeme se pustit do nastavení potřebného módu WiFi zařízení.

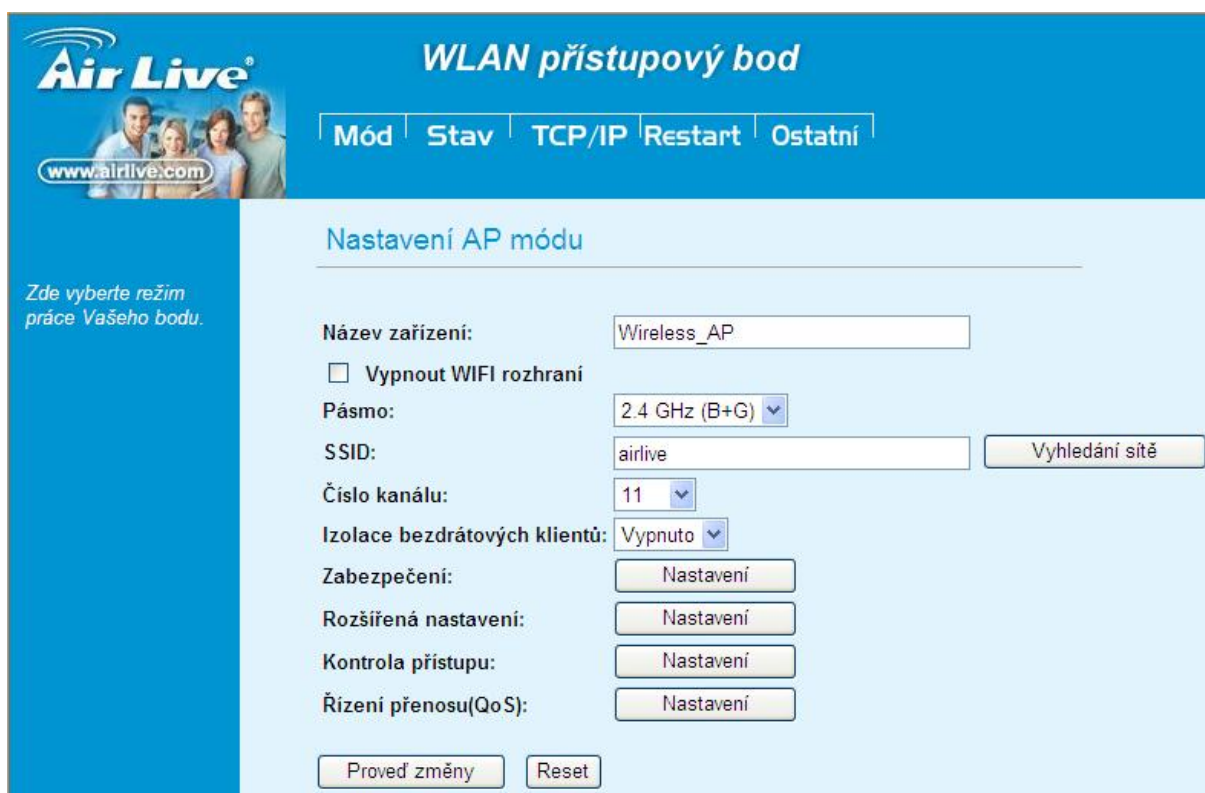
Pro možnost konfigurace Módu vybereme v menu položku *Mód*. Zobrazí se nám následující stránka kde je možno vybrat daný mód zařízení.



Pokud vybereme jiný mód, než je standardně nastaven, jsme vyzváni k potvrzení tohoto výběru. Po odsouhlasení je zařízení restartováno s již vybraným módem. Restart trvá cca 30 s. Musíme však brát na zřetel, že pokud zařízení konfigurujeme z továrního nastavení, tak při změně módu z AP může dojít ke stavu, kdy se již k zařízení nemůžeme připojit pomocí WiFi rozhraní (platí pro módy klient a most).

Nyní se budeme zabývat nastavením zařízení v módu AP.

Předpokládáme, že zařízení je nyní v módu AP. Klepneme na tlačítko *Nastavení*. Následně se objeví stránka s možnostmi nastavení zařízení v módu AP. Na této stránce (viz obrázek níže) můžeme nastavit název zařízení, kompatibilitu se zařízeními typu IEEE 802.11b, IEEE 802.11g nebo IEEE 802.11b/g. V našem případě volíme pouze 802.11g. Název SSID můžeme změnit, v našem případě byl použit DP_VUT. Pokud nemáme k dispozici zařízení, jímž bychom změřili WiFi síť v okolí kde má být AP použit, můžeme použít pro přehled možnost *Vyhledání sítě*. Pokud tuto funkci použijeme, bude zobrazena přehledná tabulka s okolními sítěmi, použitým kanálem, vysílaným SSID a silou přijímaného signálu. Toto nám umožní zvolit vhodný kanál pro toto AP. V našem případě byl volen kanál 1. Pro možnost izolace bezdrátových klientů je zde uvedena volba, kterou můžeme tuto funkci zapnout.



The screenshot shows the 'Air Live' logo and 'WLAN přístupový bod' (WLAN access point) title. Navigation tabs include 'Mód', 'Stav', 'TCP/IP', 'Restart', and 'Ostatní'. The 'Nastavení AP módu' section contains the following settings:

- Název zařízení: Wireless_AP
- ☐ Vypnout WIFI rozhraní
- Pásmo: 2.4 GHz (B+G)
- SSID: airtive
- Číslo kanálu: 11
- Izolace bezdrátových klientů: Vypnuto
- Zabezpečení: Nastavení
- Rozšířená nastavení: Nastavení
- Kontrola přístupu: Nastavení
- Řízení přenosu(QoS): Nastavení

Buttons at the bottom: 'Proveď změny' and 'Reset'. A 'Vyhledání sítě' button is next to the SSID field. A sidebar on the left says 'Zde vyberte režim práce Vašeho bodu.' (Select the operating mode of your point here).

V případě potřeb zabezpečení AP můžeme zvolit položku zabezpečení, kterou potvrdíme tlačítkem *Nastavení*. Zde je možno vybrat z možností žádné, WEP, WPA-PSK(TKIP), WPA-PSK(AES), WPA2-PSK(AES), WPA2-PSK Mix nebo 802.1x / Radius.



The 'Nastavení bezpečnosti bezdrátového spojení' section contains the following settings:

- Šifrování: WPA-PSK (TKIP)
- Formát před-sdíleného klíče: Heslo
- Před-sdílený klíč: (empty text field)
- Životnost skupinového klíče: 86400 sek

Buttons at the bottom: 'Proveď změny' and 'Reset'. A mouse cursor is pointing at the 'Reset' button.

V našem případě nebylo vybráno žádné zabezpečení. Pokud ovšem vybereme typ zabezpečení, musíme jej odsouhlasit pomocí tlačítka *Proveď změny*. Poté jsme informováni, že se změny projeví až po restartu zařízení. Následně můžeme zavřít okno s nastavením zabezpečení.

Další možnost je použít pokročilá nastavení pro WiFi část. Po potvrzení tlačítkem *Nastavení* se zobrazí následující stránka.

Pokročilé bezdrátové nastavení

Práh fragmentace:	2346	(256-2346)
Práh RTS:	2347	(0-2347)
Beacon interval:	100	(20-1024 ms)
Čas vyčkávání:	50000	(101-60480000 10ms)
Rychlost datové modulace:	Auto v	
Typ synchronizačního bloku:	☒ Dlouhý synchronizační blok ☐ Krátký synchronizační blok	
Zobrazovat SSID:	☒ Povolit ☐ Potlačit	
IAPP:	☒ Povolit ☐ Potlačit	
802.11g ochrana:	☒ Povolit ☐ Potlačit	
Vysílací výkon tx:	Výkon 2 (cca 16dB) v	
☐ Hlídní spojení		
Interval hlídání:	1	(1-60 minut)
Watch host:	0.0.0.0	
Časování ack:	0	(0-255, 0:Automatické řazení, jednotka: 4psec)
Defaultní (tovární) nastavení		
Proveď změny Reset		

Zde můžeme nastavit práh fragmentace, práh pro RTS, Beacon Interval a další. Všechny tyto položky mají vliv na výkon WiFi zařízení a na latence spojů. Položku rychlost spoje ponecháme na Auto, jelikož není jasné jakou maximální rychlostí se mohou jednotliví klienti připojit. Pokud nastavíme rychlost pevně, může docházet k výpadkům spojení nebo velkým latencím. Další důležitou položkou je vysílací výkon Tx. Tento se především nastavuje při použití externích antén. Toto bylo již zmíněno dříve. Jednotlivé možnosti pro vysílací výkon jsou 18, 16, 15, 11, 10, 7, 5 a 0 dB. Poslední možností pro nastavení je takzvaný Watch dog (hlídač spojení). Zde je možno nastavit časový interval, který udává, po jakém časovém intervalu se dotaz na průchod ping na adresu Watch host provádí. Toto se s výhodou využívá u hlídání dostupnosti ke konektivitě. Po nastavení všech parametrů opět potvrdíme tlačítkem a následně jsme informováni o tom, že opět pro provedení změn musí dojít k restartu zařízení.

Další možnost nastavení je kontrola přístupů na základě MAC adresy. Princip byl popsán již dříve. Na stránce je možno nastavit, zda se má systém vůbec používat, zda mají být zařízení s vypsanými MAC adresami povoleny nebo zakázány. MAC adresa se vkládá jako jeden řetězec bez obvyklých dvojteček, tedy například 004F8A622110. Pro uložení a následné použití je stejný dokončovací postup jako ve všech předchozích případech.

Řízení bezdrátového přístupu

Typ řízení bezdrátového přístupu: Povolit vypsané ▼

Pomocí MAC adresy: Poznámka:

Proveď změny Reset

Současná tabulka přístupu:

Pomocí MAC Adresy	Poznámka	Vyberte
00:16:6f:3d:91:fa	nb	☐

Smaž vybranou Smaž vše Reset

Poslední možnost pro konfiguraci AP módu je nastavení pravidel QoS. Tyto pravidla je možno konfigurovat na celkové zařízení (LAN a WLAN), nebo po třídách, kterým jsou přiřazeny jednotlivé adresy TCP/IP nebo MAC adresy. Kontrola TCP/IP adres a MAC adres je prováděna pouze na WLAN. Stránka s možnostmi nastavení je vyobrazena níže.

Kontrola přenosu IP/MAC/Rozhraní

*** VAROVÁNÍ: Změna nastavení se projeví až po restartu zařízení. Nezapomeňte restartovat AP po dokončení všech nastavení. ***

Pozn: Výstupní rychlost je vrchní limit šířky pásma.

POZN: Kontrola rozhraní má přednost před IP/MAC. Pokud chcete užívat IP/MAC řízení provozu, musíte vypnout kontrolu rozhraní.

Řízení provozu rozhraním ☐ Zapnuto ☒ Vypnuto

Výstupní rychlost LAN kbps

Výstupní rychlost WLAN kbps

Název třídy	Rychlost LAN	Výstupní rychlost WLAN	Poznámka
	kbps	kbps	

Aktuální tabulka tříd:

Název třídy	Rychlost LAN (Kbps)	WLAN rychlost (Kbps)	Poznámka	Vyberte
pokus	200	200	max	☐

Pozn: Jsou podporovány jen IP adresy klientů bezdrátové sítě LAN.

☐ Zapnout IP kontrolu

Název třídy	IP	Výstupní rychlost LAN	Výstupní rychlost WLAN	Poznámka
		kbps	kbps	

Současná tabulka kontroly IP:

Název třídy	IP adresa	Rychlost LAN (Kbps)	WLAN rychlost (Kbps)	Poznámka	Vyberte

Pozn: Jsou podporovány jen MAC klientů bezdrátové sítě LAN.

☐ Zapnout MAC kontrolu

Název třídy	MAC	Rychlost LAN	Výstupní rychlost WLAN	Poznámka
		kbps	kbps	

Současná tabulka MAC kontroly:

Název třídy	Pomocí MAC adresy	Rychlost LAN (Kbps)	WLAN rychlost (Kbps)	Poznámka	Vyberte

Nyní se budeme zabývat nastavením zařízení v módu bridge.

Předpokládáme, že zařízení je již do tohoto módu přepnutu a můžeme tedy začít s konfigurací. Pro konfiguraci je nutno, aby zařízení bylo připojeno pomocí LAN, nikoli pomocí WiFi!

Na stránce výběru módu potvrdíme mód Most. Objeví se následující stránka.

The screenshot shows the 'WLAN přístupový bod' (WLAN access point) configuration interface for 'Air Live'. The top navigation bar includes 'Mód', 'Stav', 'TCP/IP', 'Restart', and 'Ostatní'. The main heading is 'Nastavení bridge módu' (Bridge mode settings). On the left, a sidebar says 'Zde vyberte režim práce Vašeho bodu.' (Here select the operating mode of your point). The main content area contains the following settings:

- Název zařízení:** Most1
- ☐ Vypnout WIFI rozhraní
- Pásmo:** 2.4 GHz (G)
- Číslo kanálu:** 3
- 802.1d spanning tree:** Vypnuto
- Nastavení WDS zabezpečení:** Nastavení
- Rozšířená nastavení:** Nastavení
- Buttons:** Proved' změny, Reset
- MAC adresa AP:** [empty field] **Vyhledání sítě**
- Poznámka:** [empty field] **Vlož MAC adresu**, **Reset**, **Ukaž statistiku**
- Tabulka MAC adres:**

Pomocí MAC Adresy	Poznámka	Vyberte
00:4f:72:60:50:12	most2	☐

Buttons: Smaž vybranou, Smaž vše, Reset

Na této stránce nastavíme normu, pod kterou má být most spuštěn. Na výběr je opět možnost kompatibility s IEEE 802.11b, IEEE 802.11g nebo kombinací obou. Zpravidla vybíráme normu odpovídající IEEE 802.11g. Pokud si nejsme jisti okolními sítěmi WiFi a jejich využitím jednotlivých kanálů, můžeme použít již popsanou funkci pro vyhledání sítí.

Most jako takový nemá dle specifikace SSID, proto se zde nezadává. Zadává se protější strana, či strany ve formátu MAC adres (BSSID) protějších stran mostu. Toto zařízení dovede fungovat v módu most jako point to multipoint s omezením na 10 souběžných spojů. K danému BSSID můžeme přiřadit název a následně jej můžeme vložit do tabulky MAC adres. Potvrzení se opět provede stiskem tlačítka *Proved' změny*. Pro most je možno

konfigurovat i rozšířená nastavení. Toto nastavení je shodné jako u módu AP. Další položkou je možnost konfigurace zabezpečení spoje typu most. Princip je shodný jako v předchozím případě pro mód AP. Ovšem není praktický důvod zabezpečení používat z pohledu nabourání se do sítě s odběrem konektivity. Pro případ odposlechu je princip obdobný.

Pro plné vytvoření spoje typu most je nutné ještě nastavit druhé zařízení opět do módu most, na stejný kanál a stejnou normu. Ovšem do adresy MAC musíme zadat MAC prvního zařízení. Po provedení změn a restartu zařízení by měl most být automaticky navázán. Kontrola je možná provést v položce *Ukaž statistiku*, viz níže.

Tabulka WDS AP

MAC Adresa	Tx Pakety	Tx Chyby	Rx Pakety	Tx Hodnota (Mbps)
00:4f:62:17:0a:30	11858147	259	13367017	54

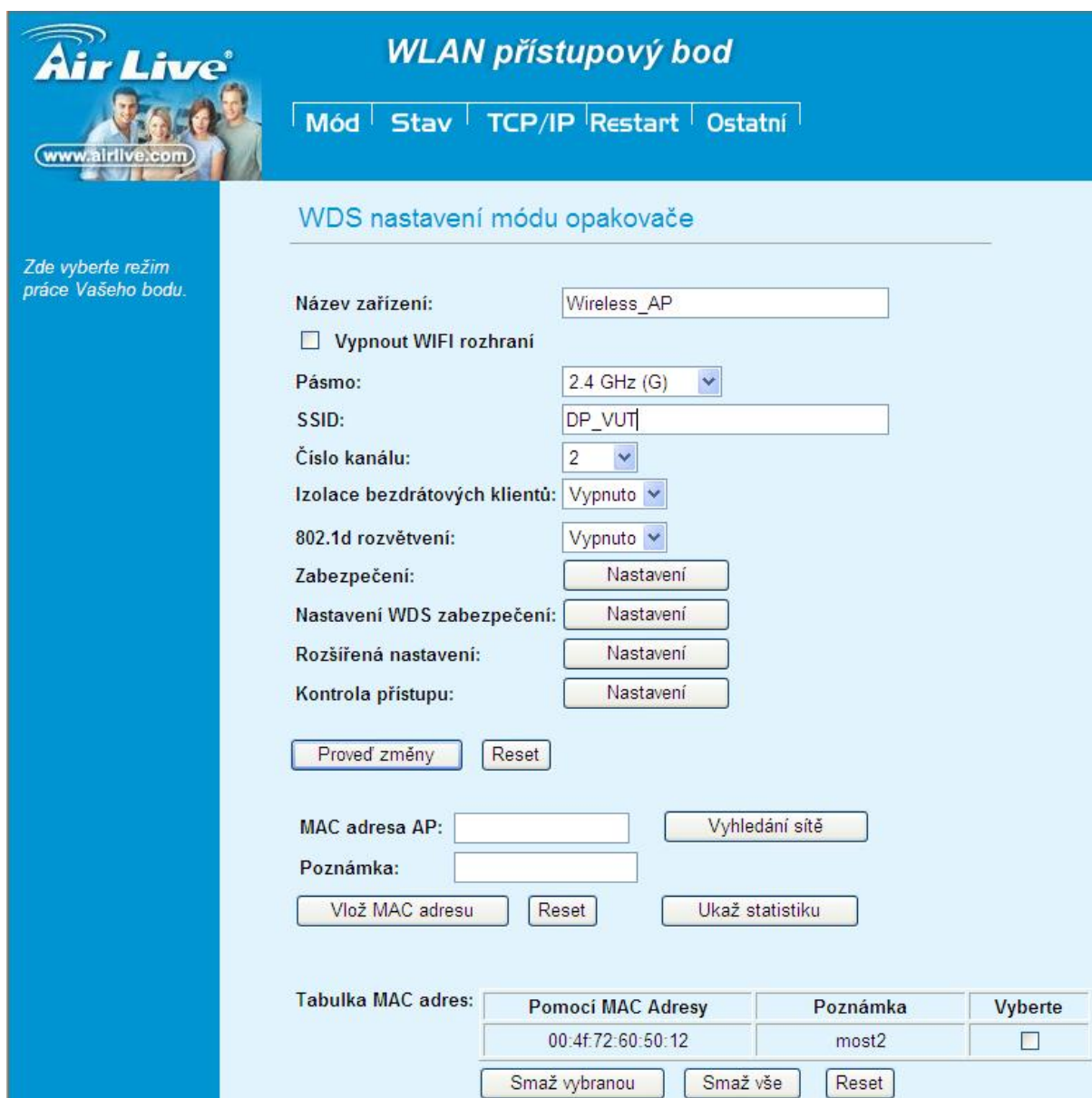
Obnov Zavři

Zde je vidět na jaké rychlosti jsou zařízení spojena, jaké je protějščí BSSID, počet paketů a jejich chybovost ve směru Tx a Rx. Toto řešení je vhodné pro použití na páteřních spojkách, kde není zarušené pásmo okolními WiFi sítěmi.

Nyní se budeme zabývat nastavením zařízení v módu WDS.

Předpokládáme, že zařízení je již do tohoto módu přepnuto a můžeme tedy začít s konfigurací WDS režimu. WDS režim jako takový je kombinace módu most a módu AP.

Na stránce výběru jednotlivých módu zařízení WL-5406AP v2 potvrdíme výběr módu WDS. Následně se nám objeví stránka pro konfiguraci tohoto módu.



The screenshot shows the 'WLAN přístupový bod' (WLAN access point) configuration page for the 'WDS nastavení módu opakače' (WDS repeater mode) configuration. The page has a blue header with the 'Air Live' logo and navigation tabs: 'Mód', 'Stav', 'TCP/IP', 'Restart', and 'Ostatní'. The 'Mód' tab is selected.

On the left side, there is a sidebar with the text 'Zde vyberte režim práce Vašeho bodu.' (Here select the operating mode of your point). The main content area is titled 'WDS nastavení módu opakače'.

The configuration fields include:

- Název zařízení:** Wireless_AP
- ☐ Vypnout WIFI rozhraní
- Pásmo:** 2.4 GHz (G)
- SSID:** DP_VUT
- Číslo kanálu:** 2
- Izolace bezdrátových klientů:** Vypnuto
- 802.1d rozvětvení:** Vypnuto
- Zabezpečení:** Nastavení
- Nastavení WDS zabezpečení:** Nastavení
- Rozšířená nastavení:** Nastavení
- Kontrola přístupu:** Nastavení

At the bottom of the main configuration area are buttons for 'Proveď změny' (Apply changes) and 'Reset'.

Below this is a section for 'MAC adresa AP:' with an input field and a 'Vyhledání sítě' (Find network) button. There is also a 'Poznámka:' (Note) field with a 'Vlož MAC adresu' (Insert MAC address) button, a 'Reset' button, and a 'Ukaž statistiku' (Show statistics) button.

At the bottom, there is a table titled 'Tabulka MAC adres:' (MAC address table):

Pomocí MAC Adresy	Poznámka	Vyberte
00:4f:72:60:50:12	most2	☐

Below the table are buttons for 'Smaž vybranou' (Delete selected), 'Smaž vše' (Delete all), and 'Reset'.

Na rozdíl od módu most navíc konfigurujeme i SSID. Toto je na všech WDS zařízeních, jenž tvoří jednu WDS síť, shodné. Dále volíme číslo kanálu, to musí být také pro všechna WDS zařízení shodné. Položka zabezpečení je stejná jako pro mód AP. Udává nám zabezpečení pro komunikaci bezdrátových klientů s jednotkou WDS. Pokud WDS síť koncipujeme pro ideální

pokrytí daného prostoru, musí být opět ve všech zařízeních shodné nastavení zabezpečení. Dále je možno nastavit zabezpečení pro propojující most mezi jednotlivými WDS zařízeními. Jak již bylo zmíněno dříve, nastavení je opět totožné jak pro mód AP. Rozšířená nastavení nám umožní konfiguraci WLAN, opět je nastavení shodné jako u předchozích dvou módů. Bohužel již v tomto módu není obsažena regulace klientů QoS. Proto řešení tohoto typu můžeme považovat za krajní řešení v rámci tvorby strukturované sítě vhodné pro pokrytí většího prostoru.

Pro vytvoření spojů mezi jednotlivými zařízeními je opět nutné zadat BSSID protějšího, případně protějších zařízení.

Příloha C

Nastavení WLA-5000AP v3 a WLA-9000 pro mód WDS bridge

Uvedená zařízení jsou koncipována primárně pro normu IEEE 802.11a fungující v pásmu 5 GHz. Většina koncových zařízení, která jsou běžně v prodeji, je pouze pro normy IEEE 802.11b a IEEE 802.11g. Proto není uvedeno nastavení do módu AP.

Uvedené konfigurace jsou prováděny pomocí webového prohlížeče. Dle výrobce je doporučen Internet Explorer 5.5 a vyšší.

WLA-5000AP v3

Multifunkční WiFi zařízení je koncipováno pro provoz v pásmech 2,4 GHz a 5 GHz. Vzhledem ke stabilitě a spolehlivosti se uvedené zařízení používá na páteřní spoje ve WiFi sítích. Konfigurace bude provedena pro normu IEEE 802.11a. Předpokládaná konfigurace je pro firmware 2.0e13, což je poslední vydaný firmware určený pro země EU. Konfigurace zařízení s jinou verzí firmware se může podstatně lišit.

Zařízení je po vybalení z přepravního boxu nastaveno přímo z výroby. Nastavení je s maximálním výstupním výkonem 17 dB, normou 802.11g, SSID airlive a TCP/IP adresou 192.168.1.2. Zařízení je v módu AP. Pro konfiguraci je tedy jako v předchozím případě nutno změnit TCP/IP adresu zařízení, z něž se budeme připojovat k WLA-5000AP v3, na IP adresu z rozsahu 192.168.1.X mimo adresy, jenž je použita WiFi zařízením. Po této změně TCP/IP adresy se můžeme pustit do konfigurace zařízení.

Do internetového prohlížeče zadáme adresu <http://192.168.1.2>. Otevře se nám konfigurační stránka.

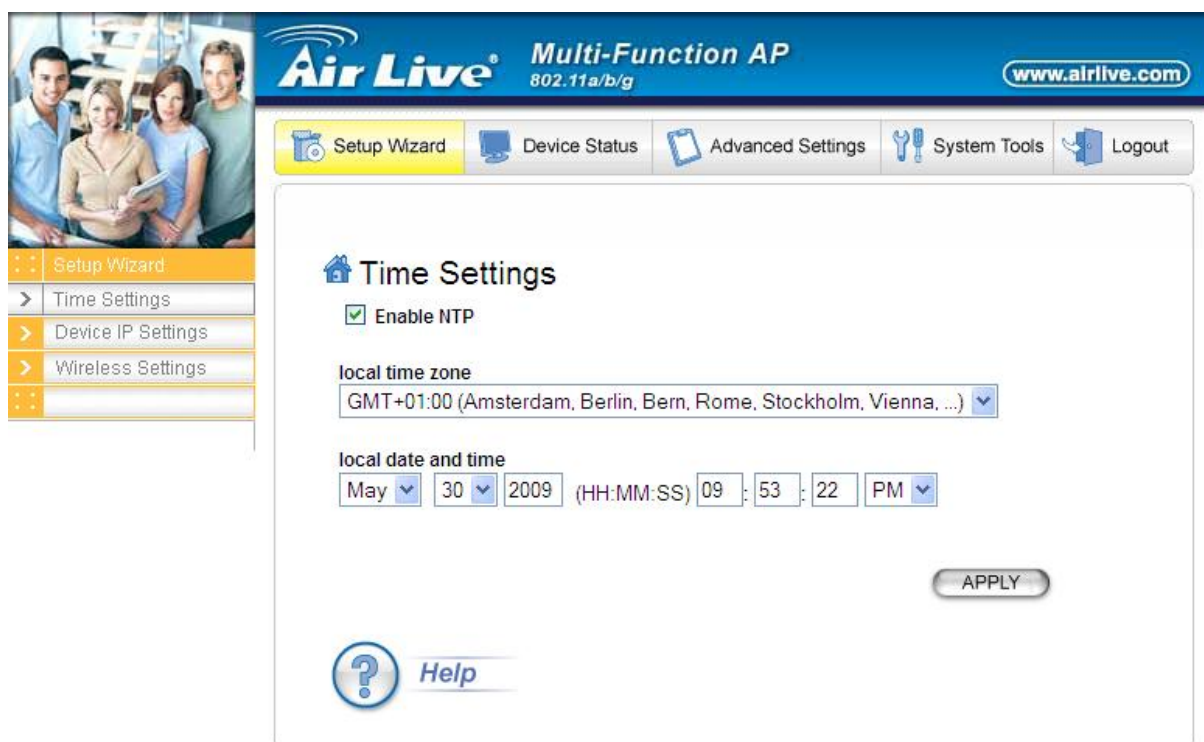


Na této stránce zvolíme položku *Setup Wizard*. Následně se otevře nová stránka, kde je vyžadován autorizovaný kód pro přístup k zařízení. Zadáme tedy kód z výroby, což je *airlive*.



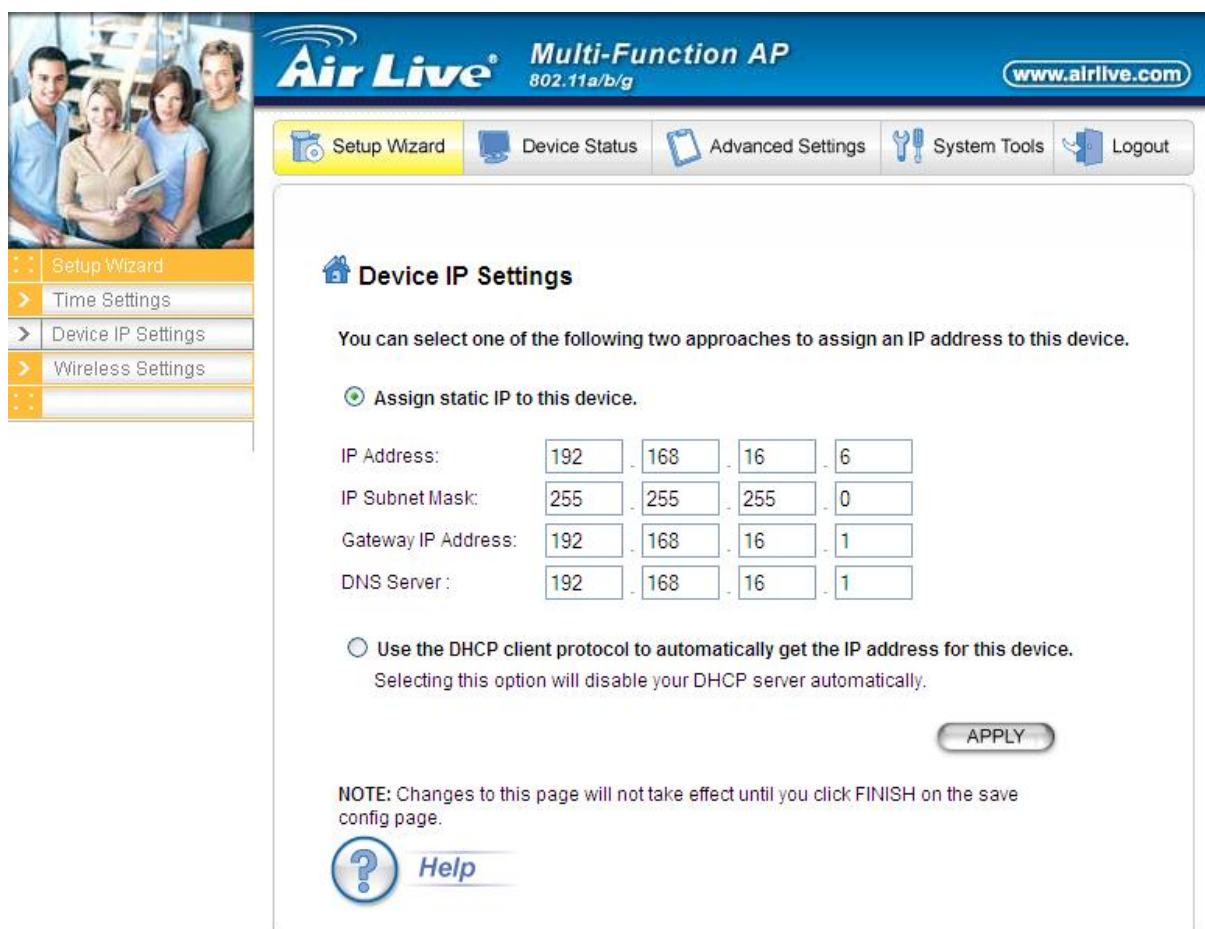
The image shows the login interface for an Air Live Multi-Function AP. At the top, there is a blue header with the 'Air Live' logo, the text 'Multi-Function AP 802.11a/b/g', and the website 'www.airlive.com'. Below the header, a white box contains the text 'Please enter your password:'. Underneath this is a password input field with seven dots and a 'LOG ON' button. At the bottom of the box, there is a link: '(Forgot your password? - see the User Guide for instructions.)'.

Po zadání hesla jsme přesměrováni na stránku *Setup Wizard, Time settings*. Na této stránce je možno nakonfigurovat synchronizaci času zařízení s časem v internetu pomocí protokolu NTP.



The image displays the 'Time Settings' page within the Air Live Multi-Function AP Setup Wizard. The top navigation bar includes 'Setup Wizard', 'Device Status', 'Advanced Settings', 'System Tools', and 'Logout'. On the left, a sidebar shows a list of options: 'Setup Wizard', 'Time Settings' (selected), 'Device IP Settings', and 'Wireless Settings'. The main content area is titled 'Time Settings' and features a checked 'Enable NTP' option. Below this, the 'local time zone' is set to 'GMT+01:00 (Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna, ...)'. The 'local date and time' is configured as 'May 30 2009 (HH:MM:SS) 09:53:22 PM'. An 'APPLY' button is located at the bottom right of the settings area. A 'Help' link with a question mark icon is at the bottom left.

Pokud potřebujeme začlenit zařízení do IP prostoru sítě, zvolíme položku *Device IP settings*. Na této stránce můžeme vybrat, zda bude adresa TCP/IP přidělena prostřednictvím DHCP serveru nebo zda bude použita statická adresa. Pro náš případ použijeme statickou adresu. Musíme tedy ještě mimo adresy zadat masku podsítě, bránu a DNS server. Poslední dvě zmiňované položky nejsou povinné. Po vložení všech údajů potvrdíme tlačítkem *Apply* uložení těchto zadaných parametrů do zařízení.



The screenshot displays the web management interface for an Air Live Multi-Function AP. The top navigation bar includes links for Setup Wizard, Device Status, Advanced Settings, System Tools, and Logout. A left sidebar shows a menu with Setup Wizard, Time Settings, Device IP Settings (highlighted), and Wireless Settings. The main content area is titled 'Device IP Settings' and provides instructions on how to assign an IP address. Two options are available: 'Assign static IP to this device' (selected) and 'Use the DHCP client protocol to automatically get the IP address for this device'. The static IP configuration fields are pre-filled with 192.168.16.6 for the IP Address, 255.255.255.0 for the Subnet Mask, 192.168.16.1 for the Gateway IP Address, and 192.168.16.1 for the DNS Server. An 'APPLY' button is located at the bottom right of the configuration section. A note at the bottom states that changes will only take effect after clicking 'FINISH' on the save config page. A 'Help' link is also present.

Air Live® Multi-Function AP
802.11a/b/g
www.airlive.com

Setup Wizard | Device Status | Advanced Settings | System Tools | Logout

Setup Wizard
Time Settings
Device IP Settings
Wireless Settings

Device IP Settings

You can select one of the following two approaches to assign an IP address to this device.

☒ Assign static IP to this device.

IP Address: 192 . 168 . 16 . 6
IP Subnet Mask: 255 . 255 . 255 . 0
Gateway IP Address: 192 . 168 . 16 . 1
DNS Server: 192 . 168 . 16 . 1

☐ Use the DHCP client protocol to automatically get the IP address for this device.
Selecting this option will disable your DHCP server automatically.

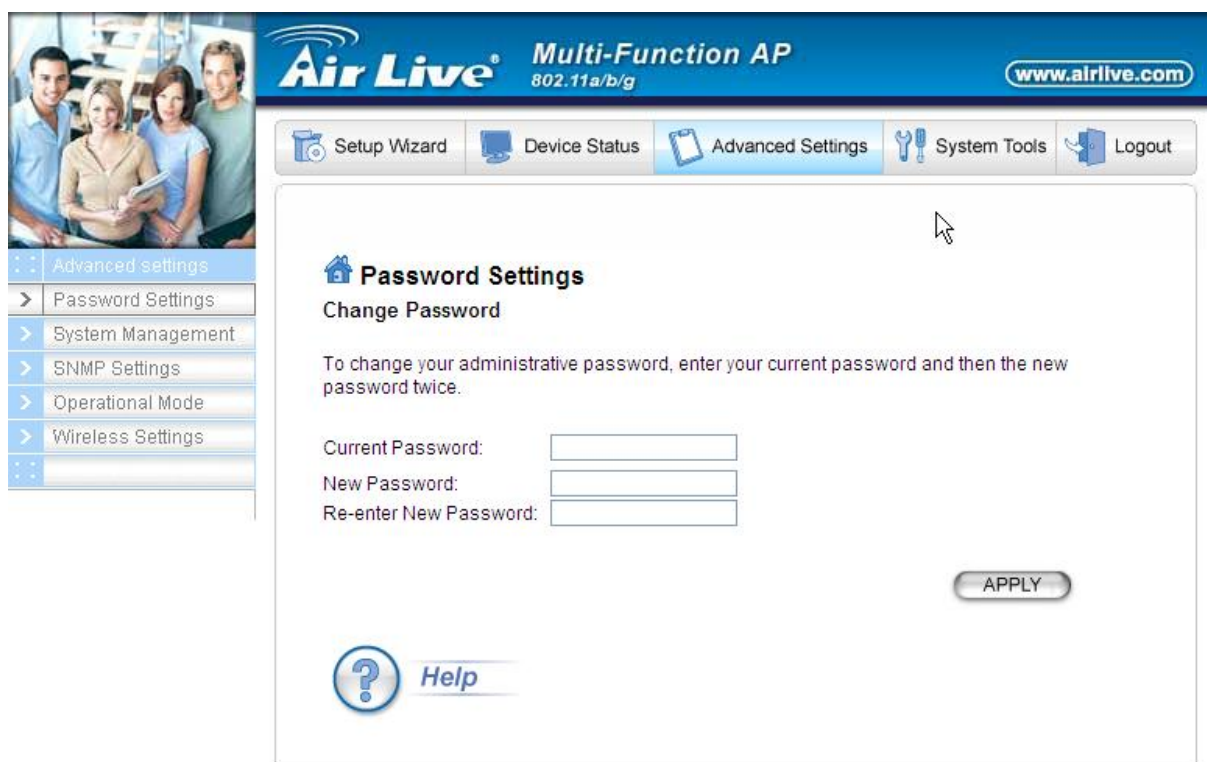
APPLY

NOTE: Changes to this page will not take effect until you click FINISH on the save config page.

Help

V dalším kroku můžeme nakonfigurovat normu, ve které bude zařízení pracovat. Ovšem tento krok je zbytečný, protože po změně módu na mód WDS dojde k přepnutí na normu 802.11b/g. Proto tento krok necháme až po přepnutí zařízení z módu AP do módu WDS.

Pokračujeme tedy dál do menu *Advanced settings*. Na uvedené stránce můžeme změnit heslo pro přístup k zařízení.



The screenshot displays the web interface of an Air Live Multi-Function AP. The top header features the 'Air Live' logo, the text 'Multi-Function AP 802.11a/b/g', and the website 'www.airlive.com'. A navigation bar includes links for 'Setup Wizard', 'Device Status', 'Advanced Settings' (which is highlighted), 'System Tools', and 'Logout'. On the left, a sidebar menu lists 'Advanced settings', 'Password Settings' (selected), 'System Management', 'SNMP Settings', 'Operational Mode', and 'Wireless Settings'. The main content area is titled 'Password Settings' with a sub-header 'Change Password'. It contains instructions: 'To change your administrative password, enter your current password and then the new password twice.' Below this are three input fields labeled 'Current Password:', 'New Password:', and 'Re-enter New Password:'. An 'APPLY' button is located at the bottom right of the form area. A 'Help' link with a question mark icon is at the bottom left.

Přejdeme do položky *Operation Mode*. Na této stránce můžeme zvolit jeden z módu WiFi zařízení. Budeme volit mód WDS bridge. Před potvrzením konfigurace můžeme zadat BSSID protějšního zařízení, na které bude spoj „ukazovat“. Pro lepší orientaci je možno zadat ještě název. Pro uložení MAC adresy je nutno potvrdit uložení tlačítkem *ADD*. Toto zařízení je schopno v tomto módu fungovat jako point to multipoint. Proto je možno zadat více MAC adres. Omezení je na 10 adres. Po vložení všech MAC adres můžeme tedy přepnout zařízení do módu WDS bridge tlačítkem *APPLY*. Následně se zařízení restartuje, což trvá 60 s. Po restartu je již zařízení v módu bridge, proto opět nejsme schopni provádět konfiguraci skrz WiFi rozhraní.



Air Live® Multi-Function AP
802.11a/b/g
www.airlive.com

Setup Wizard | Device Status | Advanced Settings | System Tools | Logout

Advanced settings
Password Settings
System Management
SNMP Settings
Operational Mode
Wireless Settings

Operational Mode

Select the operational mode

- ☐ Access Point
- ☐ Repeater
- ☒ WDS Bridge
- ☐ Client Infrastructure
- ☐ Client Adhoc
- ☐ WISP Router

APPLY

Additional configurations for WDS bridge mode:

Name:

MAC address: -----

Select Security Policy:

Select	Name	MAC Address	Security
☐	Olomoucka	00-4f-69-52-03-bd	None

DELETE SELECTED

 Help

Následně zvolíme pásmo a kanál, na kterém bude zařízení pracovat. Jak již bylo řečeno, budeme volit normu IEEE 802.11a. Po restartu zařízení se opět přihlásíme a v menu *Setup Wizard* zvolíme položku *Wireless settings*. Zde můžeme zvolit jeden z módů, v němž může zařízení pracovat. Jednotlivé módy jsou 11g/b, 11g only, 11b, SuperG without Turbo, 11a a SuperA without turbo. V našem případě zvolíme 11a. Následně musíme zvolit kanál pro komunikaci. Musíme dbát na to, zda-li je zařízení používáno uvnitř budov či venku. Dle této skutečnosti pak volíme kanál tak, aby odpovídal platné legislativě tak, jak již bylo zmíněno dříve.

Air Live® Multi-Function AP
802.11a/b/g www.airlive.com

Setup Wizard Device Status Advanced Settings System Tools Logout

Wireless Settings

Regulatory Domain: United Kingdom

WLAN Standard for Radio

Mode: 11a

Channel: 136

Select Security Policy: No

APPLY

NOTE: To access the wireless network, user must have correct SSID and encryption key, if enabled.

Help

Pro uložení parametrů použijeme tlačítko *Apply*. V případě, že spoj chceme zabezpečit, můžeme si vybrat pouze jediný typ zabezpečení a to zabezpečení WEP. Ale jak již bylo zmíněno u zařízení WL-5460AP v2, zabezpečení pro tyto typy spojů vlastně není potřebné.

Pro kontrolu zda zvolený kanál nekoliduje s kanály na nichž již fungují jiné WiFi sítě, přejdeme do menu *Device Status*, kde vybereme položku *Site Survey*. Na dalších dvou obrázcích je vyobrazen stav pro normu 802.11b/g a pro normu 802.11a.



Air Live® Multi-Function AP
802.11a/b/g
www.airlive.com

Setup Wizard | **Device Status** | Advanced Settings | System Tools | Logout

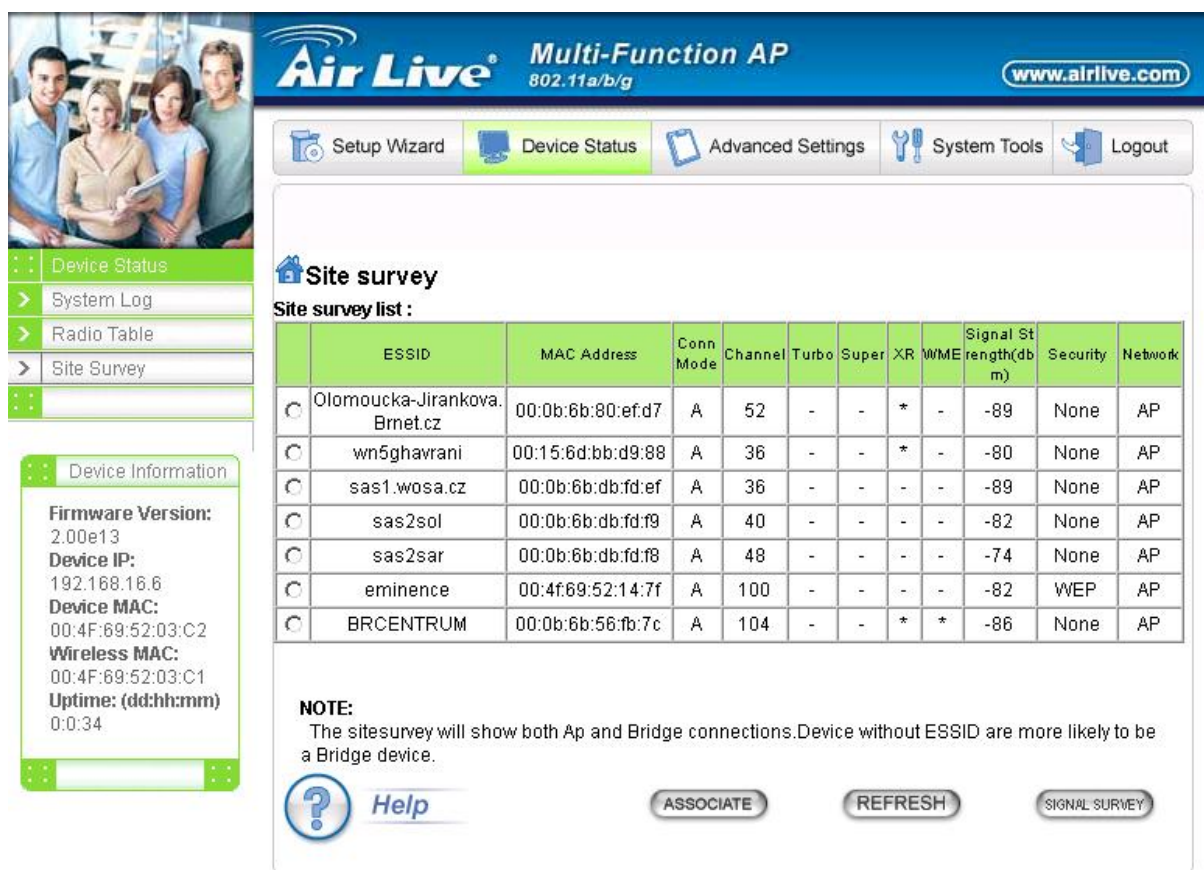
Site survey
Site survey list :

	ESSID	MAC Address	Conn Mode	Channel	Turbo	Super	XR	WME	Signal Strength (dbm)	Security	Network
☐	CZFree.Net.Cern	00:02:72:4b:96:ed	B	1	-	-	-	-	-89	None	AP
☐	CERNOVICE1	00:0b:6b:37:34:13	B	1	-	-	-	-	-92	WEP	AP
☐	RyWa.H01	00:0e:8e:7f:9c:23	G	4	-	-	*	*	-83	None	AP
☐	KR001	00:13:f7:7f:cc:e0	G	5	-	-	-	*	-91	WPA2 PSK	AP
☐	J&J	00:23:cd:c3:ab:8c	G	6	-	-	*	-	-88	WEP	AP
☐	02	00:02:cf:50:84:8c	G	6	-	-	-	-	-86	WEP	AP
☐	YVNET	00:19:e0:6e:95:4a	G	6	-	-	*	*	-86	None	AP
☐	SAS144	00:0b:6b:db:fe:24	B	7	-	-	-	-	-74	None	AP
☐	CERNOVICE	00:0b:6b:dd:be:c5	B	8	-	-	-	-	-83	WEP	AP
☐	TP-LINK	00:1d:0f:e4:87:fe	B	10	-	-	-	-	-89	WPA2 PSK	AP
☐	Olomoucka.Brnet.cz	00:0b:6b:81:37:f8	G	10	-	-	-	-	-86	None	AP
☐	Jura	00:0e:2e:64:67:4c	G	11	-	-	-	-	-92	WEP	AP
☐	moje_doma_sit	00:23:54:02:24:ee	G	11	-	-	-	-	-92	WPA PSK	AP
☐	Mikes	00:02:72:73:ad:40	G	11	-	-	-	-	-92	WPA2 PSK	AP
☐	Jirankova.Brnet.cz	00:60:b3:19:e2:47	B	13	-	-	-	-	-92	None	AP
☐	AlstomVisitors	00:1d:2e:16:5d:a8	G	1	-	-	-	*	-95	WPA PSK	AP
☐	airlive	00:4f:69:52:03:bd	G	1	-	-	-	*	-92	None	AP
☐	STAND	00:4f:62:14:b2:29	G	9	-	-	-	-	-95	WPA PSK	AP

NOTE:
The sitesurvey will show both Ap and Bridge connections. Device without ESSID are more likely to be a Bridge device.

 [Help](#) [REFRESH](#) [SIGNAL SURVEY](#)

Jak je vidět z následujícího vyobrazení stránky pro *Site survey* pro normu IEEE 802.11a, v okolí existuje velká řada WiFi sítí. Námi zvolený kanál, ale do žádné z uvedených WiFi sítí nezasahuje.



Air Live® Multi-Function AP
802.11a/b/g www.airlive.com

Setup Wizard | Device Status | Advanced Settings | System Tools | Logout

Site survey

Site survey list :

	ESSID	MAC Address	Conn Mode	Channel	Turbo	Super	XR	WME	Signal Strength (dbm)	Security	Network
☐	Olomoucka-Jirankova.Brnet.cz	00:0b:6b:80:ef:d7	A	52	-	-	*	-	-89	None	AP
☐	wn5ghavrani	00:15:6d:bb:d9:88	A	36	-	-	*	-	-80	None	AP
☐	sas1.wosa.cz	00:0b:6b:db:fd:ef	A	36	-	-	-	-	-89	None	AP
☐	sas2sol	00:0b:6b:db:fd:f9	A	40	-	-	-	-	-82	None	AP
☐	sas2sar	00:0b:6b:db:fd:f8	A	48	-	-	-	-	-74	None	AP
☐	eminence	00:4f:69:52:14:7f	A	100	-	-	-	-	-82	WEP	AP
☐	BRCENTRUM	00:0b:6b:56:fb:7c	A	104	-	-	*	*	-86	None	AP

NOTE:
The sitesurvey will show both Ap and Bridge connections. Device without ESSID are more likely to be a Bridge device.

[Help](#) [ASSOCIATE](#) [REFRESH](#) [SIGNAL SURVEY](#)

Jako poslední krok ještě musíme nastavit výstupní výkon zařízení. Toto provedeme v menu *Advanced setting*, kde vybereme položku *Wireless settings*. Na této stránce je možno nastavit velikost RTS, velikost fragmentace, snížit výstupní výkon a nastavit ACK Time Out pro jednotlivé normy.

Výstupní výkon, jak již bylo uvedeno výše, je maximálně 17 dB. Při připojení schválené externí antény jej za určitých podmínek musíme snížit. Toto je možné ve skocích po 1 dB avšak maximálně o 14 dB.

Hodnotu ACK nám pomůže vypočítat integrovaný ACK kalkulator. Po kliknutí na tlačítko *ACK Calculator* se otevře okno, kde zadáme vzdálenost jednotlivých zařízení, tu musíme prvně zjistit z mapy. Pro náš případ se jedná o vzdálenost cca 700 m. Po zadání této hodnoty je vypočtena hodnota ACK na hodnotu 28. Po uzavření okna s ACK kalkulatorem tuto hodnotu vepíšeme do příslušného pole. Jak již bylo zmíněno, pokud je tato hodnota nastavena nekorektně (platí pro obě koncová zařízení), může docházet k výpadkům spojení, nebo ke zvýšení latencí. Z této stránky vyplývá, že pokud je zařízení provozováno jak point to multipoint, musí být zařízení na jednotlivých koncích mostů zhruba ve stejné vzdálenosti. ACK se nastavuje globálně pro všechny spoje, pokud by jedno ze zařízení bylo příliš daleko a ostatní zařízení příliš blízko, docházelo by k již zmiňovaným nežádoucím efektům.



The screenshot displays the web management interface for an Air Live Multi-Function AP. The top header features the 'Air Live' logo, the product name 'Multi-Function AP', the standard '802.11a/b/g', and the website 'www.airlive.com'. A navigation bar includes links for 'Setup Wizard', 'Device Status', 'Advanced Settings' (which is active), 'System Tools', and 'Logout'. On the left, a sidebar menu lists various settings categories, with 'Wireless Settings' currently selected. The main content area is titled 'Wireless Settings' and contains several configuration fields: 'RTS Threshold' set to 2347 bytes, 'Fragmentation' set to 2346 bytes, 'Transmit Power' set to 0 dB, 'AckTimeOut (11a)' set to 28 µs, 'AckTimeOut (11g)' set to 48 µs, and 'AckTimeOut (Turbo-11g)' set to 22 µs. Each field includes its range and default value. An 'Enable STP' checkbox is present and unchecked. At the bottom right, there are buttons for 'ACK Calculator' and 'APPLY'. A 'Help' link with a question mark icon is located at the bottom left of the settings area.

Pro vytvoření spoje je tedy nutno na protějším zařízení provést stejné nastavení mimo MAC adresy protějšiho WLAN zařízení.

Pokud bychom potřebovali zálohovat či obnovit nastavení zařízení ze souboru s uloženými konfiguračními daty, tak to je možné v menu *System Tools* po výběru položky *Configuration save and restore*.

WLA-9000

Uvedené zařízení je osazeno dvěma WiFi jednotkami. Pro konfiguraci byl vybrán mód s navázáním dvou mostů na rozdílném kanále.

Zařízení je standardně dodáváno v počátečním nastavení, kdy jsou zapnuty obě rádiové jednotky. Radio1, jak je označena 1. jednotka, je nastaveno pro mód IEEE 802.11a a druhá jednotka pro mód IEEE 802.11g. Defaultní TCP/IP adresa pro konfiguraci zařízení je nastavena na 192.168.1.1. Defaultní SSID mají název airlive a zařízení se chová jako dual AP. Vzhledem k tomu, že se bude měnit mód jednotlivých WiFi zařízení tak, že následně se nepůjde připojit k zařízení klientským způsobem, je nutno konfiguraci provádět na rozhraní LAN.

Uvedená konfigurace je prováděna na zařízení s firmware 1.00e27. Při použití jiného firmware může být konfigurační postup dost odlišný!

Po zadání adresy <http://192.168.1.1> do internetového prohlížeče je zobrazena první stránka konfiguračního rozhraní. Tato stránka je velmi podobná jako u zařízení WLA-5000AP v3.



Zde vybereme položku *Wireless Setting*. Následně jsme vyzváni k zadání přístupového kódu. Defaultní heslo pro přístup je *airlive*.

Po té je stránka přeměřována do menu *Wireless settings*, kde vybereme položku *Dual WDS bridge*. Následně je zobrazena následující stránka. Zde je možno konfigurovat jednotlivá WiFi zařízení z pohledu použité normy, kanálu, zabezpečení a konfigurace jednotlivých WDS mostů.

Air Live WLA-9000AP 802.11a/b/g Dual Radio Access Point

Operation Mode | System Configuration | Device Status | Logout

Operation Mode

Dual WDS Bridge

Regulatory Domain: United Kingdom

WLAN Standard for Radio 1

☒ Enable Radio 1

Site Survey

Mode: 11a

Channel: 124

WDS Settings: Setup

Advanced Settings: Setup

LED Behavior: Traffic mode

WLAN1 Current WDS Nodes

Name	MAC Address	Security
wds1	00-4f-62-28-22-0e	None

WLAN Standard for Radio 2

☒ Enable Radio 2

Site Survey

Mode: 11a

Channel: 140

WDS Settings: Setup

Advanced Settings: Setup

LED Behavior: Traffic mode

WLAN2 Current WDS Nodes

Name	MAC Address	Security
-	-	-

Apply

NOTE: To access the wireless network, user must have correct SSID and encryption key, if enabled.

Help

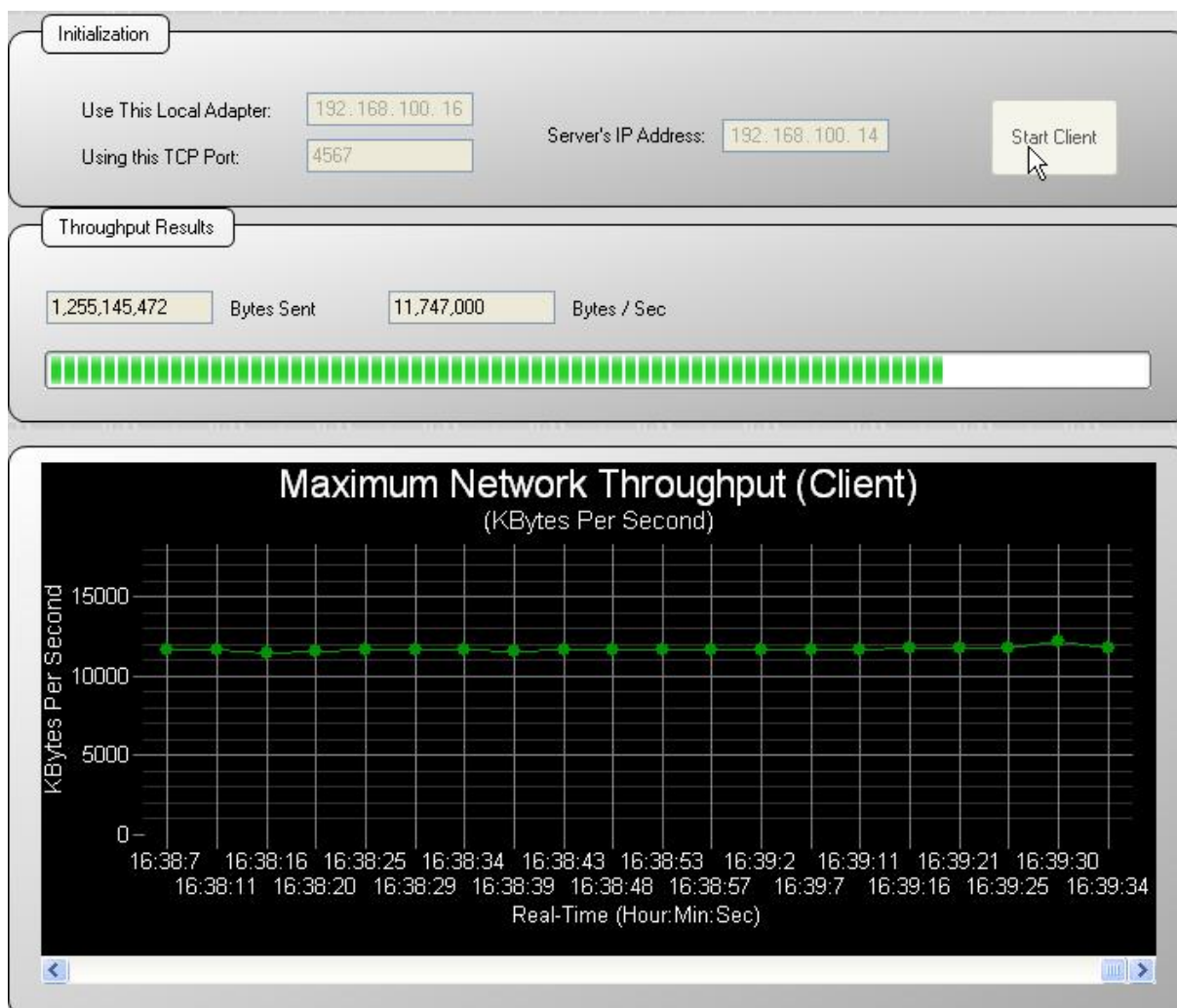
Pro možnost zjištění kanálu okolních WiFi sítí jsou zde tlačítka *Site Survey*, tak jako u předchozího popisovaného modelu.

Po zadání všech parametrů je tedy možno uložit nastavení pomocí tlačítka *APPLY*. Pokud je vše korektně nakonfigurováno dojde k vytvoření dvou WDS mostů, které mohou začít přenášet data.

D Naměřené hodnoty propustností pro spoje typu most

Kvůli objektivnosti měření byla provedena kontrolní měření mezi jednotlivými notebooky.

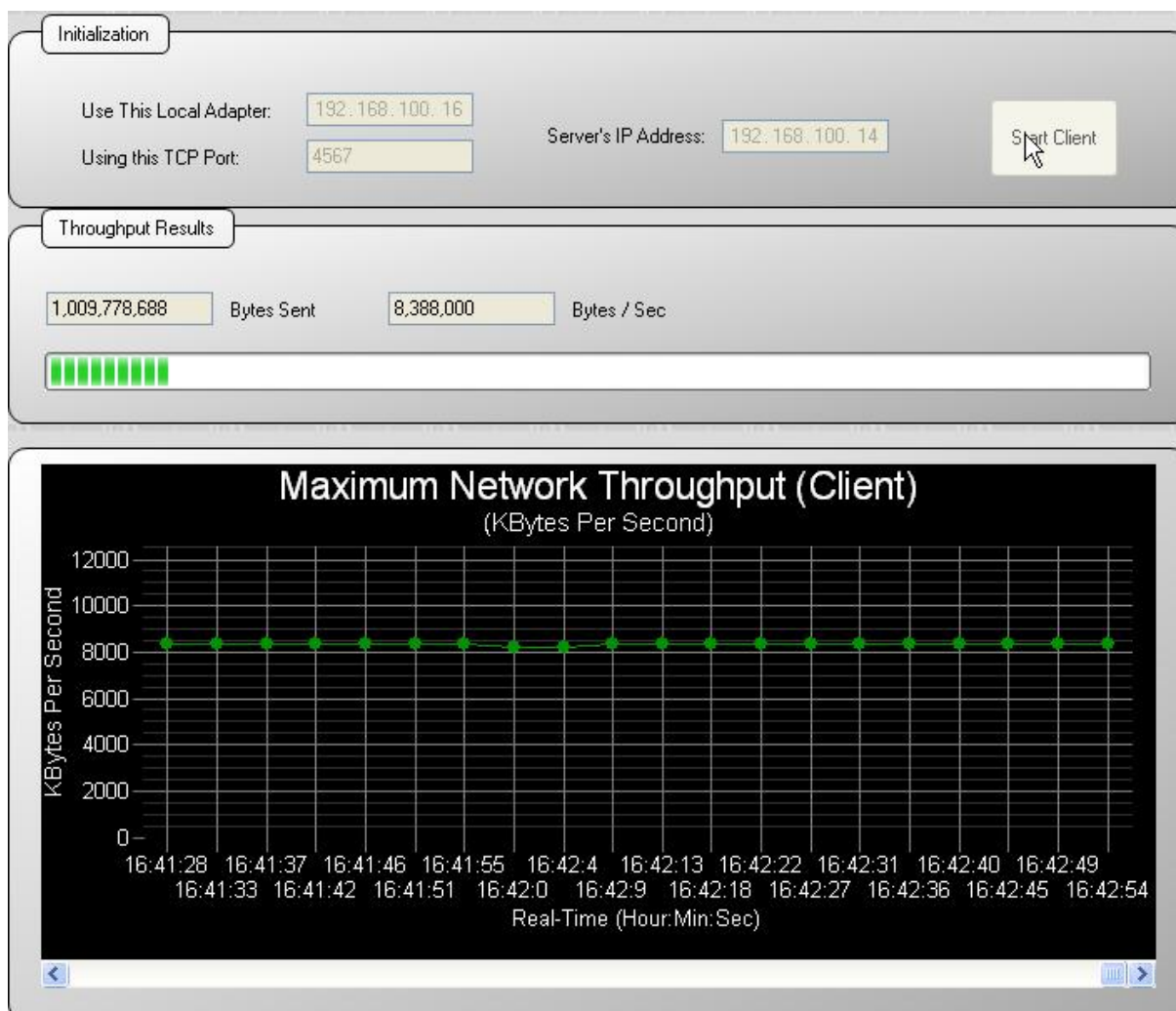
1. Spojení notebook – notebook, měření netrstress



2. Spojení notebook – notebook, měření iperf

```
[1912] local 192.168.100.10 port 1247 connected with 192.168.100.12 port 5001
[ ID] Interval      Transfer    Bandwidth
[1912] 0.0-30.4 sec  339 MBytes  93.6 Mbits/sec
```

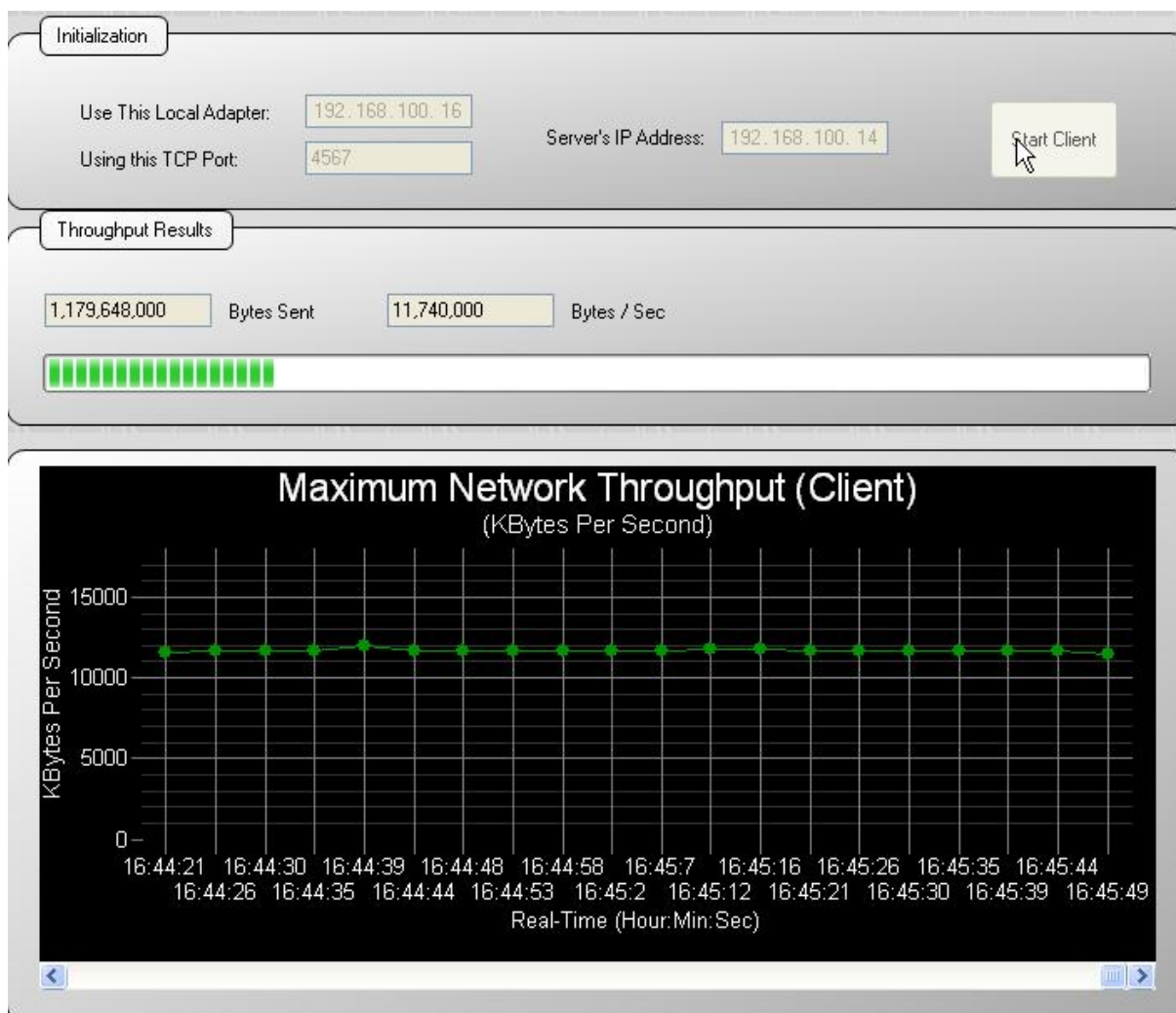
3. Spojení notebook – notebook skrz LAN ve WL-5460AP v2, měření netrstress



4. Spojení notebook – notebook skrz LAN ve WL-5460AP v2, měření iperf

```
[1912] local 192.168.100.10 port 1254 connected with 192.168.100.12 port 5001
[ ID] Interval      Transfer    Bandwidth
[1912] 0.0-30.0 sec  224 MBytes  62.5 Mbits/sec
```

5. Spojení notebook – notebook skrz LAN ve WL-5200AP, měření netrstress



6. Spojení notebook – notebook skrz LAN ve WL-5200AP, měření iperf

```
[1912] local 192.168.100.16 port 3106 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer    Bandwidth
[1912] 0.0-10.0 sec  99.1 MBytes  83.0 Mbits/sec
```


Měření v lokalitě Brno - Bohunice

Obrázek 1D – náhled do fotomapy, s vyznačeným umístěním jednotlivých zařízení.

7. Hodnoty měření pro přímý spoj v zarušeném prostředí. Použitá zařízení WL-5460AP v2, režim most, vzdálenost 110 m. Směrové antény 6 dB/30°/30°.

```
[1912] local 192.168.100.16 port 2505 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912] 0.0-10.0 sec  24.4 MBytes  20.4 Mbits/sec
```

8. Hodnoty měření pro přímý spoj. Použitá zařízení WL-5200AP, režim most, vzdálenost 110 m. Směrové antény 6 dB/30°/30°. Měřeno pro normu IEEE 802.11a.

```
[1912] local 192.168.100.16 port 2511 connected with 192.168.100.10 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912] 0.0-10.0 sec  30.1 MBytes  25.2 Mbits/sec
```

9. Hodnoty měření pro spoj s retranslací v zarušeném prostředí, lokalita Brno Bohunice. Použitá zařízení WL-5460AP v2, režim most, 1 zařízení pro retranslaci, vzdálenosti 110 m a 145 m. Směrové antény 6 dB/30°/30° pro koncové body, všesměrová anténa 8 dB pro retranslační bod.

```
[1912] local 192.168.100.16 port 2086 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912] 0.0-10.1 sec  10.8 MBytes  8.99 Mbits/sec
```

10. Hodnoty měření pro spoj s retranslací. Použitá zařízení WL-5200AP, režim most, 1 zařízení pro retranslaci, vzdálenost 110 m a 145 m. Směrové antény 6 dB/30°/30° pro koncové body, všesměrová anténa 8 dB pro retranslační bod. Měřeno pro normu IEEE 802.11a.

```
[1912] local 192.168.100.13 port 2500 connected with 192.168.100.10 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912] 0.0-10.0 sec  16.7 MBytes  14.0 Mbits/sec
```

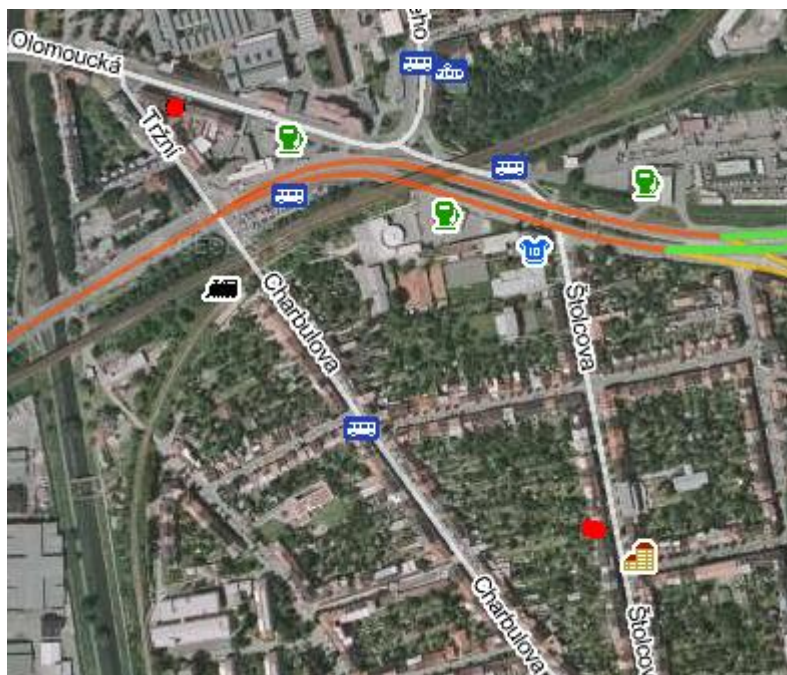
11. Hodnoty měření pro spoj s retranslací. Použitá zařízení AirMax5 jako koncová zařízení a dva kusy WLA-5200AP spojená LAN pro retranslační bod, režim most, vzdálenost 110 m a 145 m. Směrové antény 6 dB/30°/30° pro retranslační bod. Měřeno pro normu IEEE 802.11a.

```
[1912] local 192.168.100.10 port 2638 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912] 0.0-30.0 sec  84.3 MBytes  23.5 Mbits/sec
```

12. Hodnoty měření pro spoj s retranslací. Použitá zařízení AirMax5 jako koncová zařízení a WLA-9000 pro retranslační bod, režim most a dual WDS, vzdálenost 110 m a 145 m. Směrové antény 6 dB/30°/30° pro retranslační bod. Měřeno pro normu IEEE 802.11a.

```
[1912] local 192.168.100.16 port 2637 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912] 0.0-10.0 sec  28.2 MBytes  23.6 Mbits/sec
```

Měření v lokalitě Brno - Černovice



Obrázek 2D – náhled do fotomapy, s vyznačeným umístěním koncových zařízení.

13. Pro normu IEEE 802.11g bylo prováděno 20 testovacích měření. Bohužel pouze jednou se podařilo změřit propustnost spoje a to v řádu jednotek bytů za vteřinu. V ostatních případech došlo sice k navázání spojení, ale již spojem neprošel žádný ping. Důvodem bylo příliš velké zarušení okolními sítěmi.
14. Hodnoty měření pro přímý spoj. Použitá zařízení WLA-5000AP v3, režim most, vzdálenost cca 650 m. Směrové antény 8 dB/15°/15°. Měřeno pro normu IEEE 802.11a.

```
[1912] local 192.168.100.16 port 2638 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer    Bandwidth
[1912]  0.0-10.0 sec  28.1 MBytes  23.5 Mbits/sec
```

15. Hodnoty měření pro přímý spoj. Použitá zařízení AirMax5, režim most, vzdálenost cca 650 m. Měřeno pro normu IEEE 802.11a.

```
[1912] local 192.168.100.16 port 2510 connected with 192.168.100.10 port 5001
[ ID] Interval      Transfer    Bandwidth
[1912]  0.0-10.0 sec  30.0 MBytes  25.0 Mbits/sec
```

Shrnutí naměřených výsledků získaných programem IPERF

Měřené místo	Propustnost [Mb/s]
Přímé propojení notebooků	93,6
Propojení notebooků 2xLAN na WL-5460AP v2	62,5
Propojení notebooků 2xLAN na WLA-5200AP	83,0
První část spoje – Bohunice WL-5460AP v2	20,4
První část spoje – Bohunice WLA-5200AP	25,2
Kompletní spoj – Bohunice WL-5460AP v2 , retranslace jedním zařízením	8,99
Kompletní spoj – Bohunice WLA-5200AP , retranslace jedním zařízením	14,0
Kompletní spoj – Bohunice WLA-5200AP , retranslace dvěma zařízením	23,5
Kompletní spoj – Bohunice WLA-5200AP, retranslace WLA-9000	23,6
Spoj typu most – Černovice, WLA-5000AP mód 802.11g	--
Spoj typu most – Černovice, WLA-5000AP mód 802.11a	22,5
Spoj typu most – Černovice, AirMax5	25,0

E Naměřené hodnoty propustnosti pro spoje typu WDS

Měření na LAN portu jednotlivých zařízení WLA-5200AP v2 – norma IEEE 802.11g

Tato varianta zapojení je typu WDS s rozmístněním jednotlivých zařízení dle schématu uvedeném v příloze G. Zařízení byla provozována s dodávanou anténou 2 dB na kanále číslo 13. V okolí nebyly žádné rušivé WiFi sítě. Sít' nebyla zatížena jiným než testovacím datovým tokem.

1. Propustnost mezi první a druhou jednotkou.

```
[1912] local 192.168.100.10 port 2516 connected with 192.168.100.12 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912] 0.0-10.6 sec  28.5 MBytes  22.6 Mbits/sec
```

2. Propustnost mezi první až třetí jednotkou.

```
[1912] local 192.168.100.10 port 2554 connected with 192.168.100.12 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912] 0.0-10.9 sec  12.9 MBytes  9.91 Mbits/sec
```

3. Propustnost mezi první a čtvrtou jednotkou.

```
[1912] local 192.168.100.10 port 2569 connected with 192.168.100.12 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912] 0.0-10.8 sec   7.13 MBytes  5.53 Mbits/sec
```

4. Propustnost mezi první a pátou jednotkou.

```
[1912] local 192.168.100.10 port 2081 connected with 192.168.100.12 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912] 0.0-10.1 sec   8.93 MBytes  2.39 Mbits/sec
```

Níže uvedená varianta předpokládá WDS spoje mezi prvními dvěma jednotkami, pak propojení pomocí LAN s další jednotkou, jenž je nastavena v módu WDS most a je spojena s jednotkou v módu WDS. Na plánu, jenž je vyobrazen v příloze G, toto zapojení odpovídá místům umístění AP_WDS1, AP_WDS2 a AP_WDS3. Dvě zařízení, která jsou propojena LAN, jsou na místě označené AP_WDS2.

Propustnost mezi krajními jednotkami za použití dvou oddělených WDS sítí na různých kanálech s různými SSID.

```
[1912] local 192.168.100.10 port 1655 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912] 0.0-10.5 sec  22.6 MBytes  18.0 Mbits/sec
```

Shrnutí naměřených výsledků získaných programem IPERF pro normu IEEE 802.11g

Měřené místo	Propustnost [Mb/s]
Mezi první a druhou jednotkou	22,6
Mezi první a třetí jednotkou	9,91
Mezi první a čtvrtou jednotkou	5,53
Mezi první a pátou jednotkou	2,39
Řešení s retranslačním bodem řešeným dvěma zařízeními, ekvivalent spoje mezi první a třetí jednotkou	18

Měření na LAN portu jednotlivých zařízení WLA-5200AP – norma IEEE 802.11a

Tato varianta zapojení je typu WDS s rozmístněním jednotlivých zařízení dle schématu uvedeném v příloze G. Zařízení byla provozována s dodávanou anténou 2 dB na kanále číslo 44. V okolí nebyly žádné rušivé WiFi sítě. Sít' nebyla zatížena jiným než testovacím datovým tokem.

1. Propustnost mezi první a druhou jednotkou.

```
[1912] local 192.168.100.16 port 2504 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer    Bandwidth
[1912]  0.0-10.0 sec  25.3 MBytes  21.1 Mbits/sec
```

2. Propustnost mezi první až třetí jednotkou.

```
[1912] local 192.168.100.16 port 2643 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer    Bandwidth
[1912]  0.0-30.1 sec  42.7 MBytes  11.9 Mbits/sec
```

3. Propustnost mezi první a čtvrtou jednotkou.

```
[1912] local 192.168.100.16 port 2084 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer    Bandwidth
[1912]  0.0-10.1 sec  7.20 MBytes  5.99 Mbits/sec
```

4. Propustnost mezi první a pátou jednotkou.

```
[1912] local 192.168.100.16 port 2085 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer    Bandwidth
[1912]  0.0-10.2 sec  3.66 MBytes  3.02 Mbits/sec
```

Další měření je pro zapojení eliminující WDS retranslaci. Byly použity opět dva odlišné kanály (kanál 44 a 52) a dvě různá SSID.

```
[1912] local 192.168.100.16 port 2525 connected with 192.168.100.14 port 5001
[ ID] Interval      Transfer    Bandwidth
[1912]  0.0-10.0 sec  25.3 MBytes  21.1 Mbits/sec
```

VUT v Brně, Fakulta strojího inženýrství, Ústav automatizace a informatiky

Shrnutí naměřených výsledků získaných programem IPERF pro normu IEEE 802.11a

Měřené místo	Propustnost [Mb/s]
Mezi první a druhou jednotkou	21,1
Mezi první a třetí jednotkou	11,9
Mezi první a čtvrtou jednotkou	5,99
Mezi první a pátou jednotkou	3,02
Řešení s retranslačním bodem řešeným dvěma zařízeními, ekvivalent spoje mezi první a třetí jednotkou	21,1

Měření na LAN portu jednotlivých zařízení WN-300R a WN301R – norma IEEE 802.11n Draft2

Ke měření byla zapůjčena pouze 2 zařízení WN-300R a jedno WN-301R. První modelové zapojení bylo ve WDS síti s přímou viditelností mezi jednotlivými zařízeními, byla použita všechna zařízení. Pro tento model byla zařízení umístěna na pozicích AP_WDS1, AP_WDS2 a AP_WDS3.

```
[1912] local 192.168.100.10 port 2841 connected with 192.168.100.5 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912]  0.0-30.0 sec   162 MBytes   45.4 Mbits/sec
```

Další měření probíhalo už jen mezi dvěma zařízeními WN-300R, kde komunikace probíhala skrz překážku. První zařízení bylo umístěno na pozici AP_WDS3 a druhé na pozici AP_WDS4.

```
[1912] local 192.168.100.11 port 2658 connected with 192.168.100.5 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912]  0.0-30.1 sec   27.2 MBytes   7.60 Mbits/sec
```

Pro srovnání je uvedeno měření propustnosti mezi body AP_WDS3 a AP_WDS4 pro normu IEEE 802.11g na zařízení WLA-5200AP.

```
[1912] local 192.168.100.17 port 2039 connected with 192.168.100.15 port 5001
[ ID] Interval      Transfer      Bandwidth
[1912]  0.0-30.1 sec   73.1 MBytes   10.2 Mbits/sec
```

Shrnutí naměřených výsledků získaných programem IPERF pro normu IEEE 802.11n a pro IEEE 802.11g (pouze srovnávací měření)

Měřené místo	Propustnost [Mb/s]
Mezi první a třetí jednotkou	45,4
Průchod signálu překážkou	7,60
Průchod překážkou – shodné místo , norma IEEE 802.11g	10,4

F Měření síly signálu na přístupových bodech

- AP_WDS1

SSID	BSSID	Kanál	Typ	Šifrovat	Signál	Vyberte
DP_VUT AP_WDS2	00:4f:62:22:cb:4e	13 (G)	AP	no	90	☐
DP_VUT AP_WDS3	00:4f:62:21:f2:0e	13 (G)	AP	no	61	☐
DP_VUT AP_WDS4	00:4f:62:23:8d:d8	13 (G)	AP	no	52	☐
DP_VUT AP_WDS5	00:4f:62:0f:0d:88	13 (G)	AP	no	36	☐

- AP_WDS2

SSID	BSSID	Kanál	Typ	Šifrovat	Signál	Vyberte
DP_VUT AP_WDS1	00:4f:62:22:cb:06	13 (G)	AP	no	90	☐
DP_VUT AP_WDS4	00:4f:62:23:8d:d8	13 (G)	AP	no	60	☐
DP_VUT AP_WDS3	00:4f:62:21:f2:0e	13 (G)	AP	no	46	☐
DP_VUT AP_WDS5	00:4f:62:0f:0d:88	13 (G)	AP	no	20	☐

- AP_WDS3

SSID	BSSID	Kanál	Typ	Šifrovat	Signál	Vyberte
DP_VUT AP_WDS4	00:4f:62:23:8d:d8	13 (G)	AP	no	93	☐
DP_VUT AP_WDS1	00:4f:62:22:cb:06	13 (G)	AP	no	78	☐
DP_VUT AP_WDS2	00:4f:62:22:cb:4e	13 (G)	AP	no	63	☐
DP_VUT AP_WDS5	00:4f:62:0f:0d:88	13 (G)	AP	no	50	☐

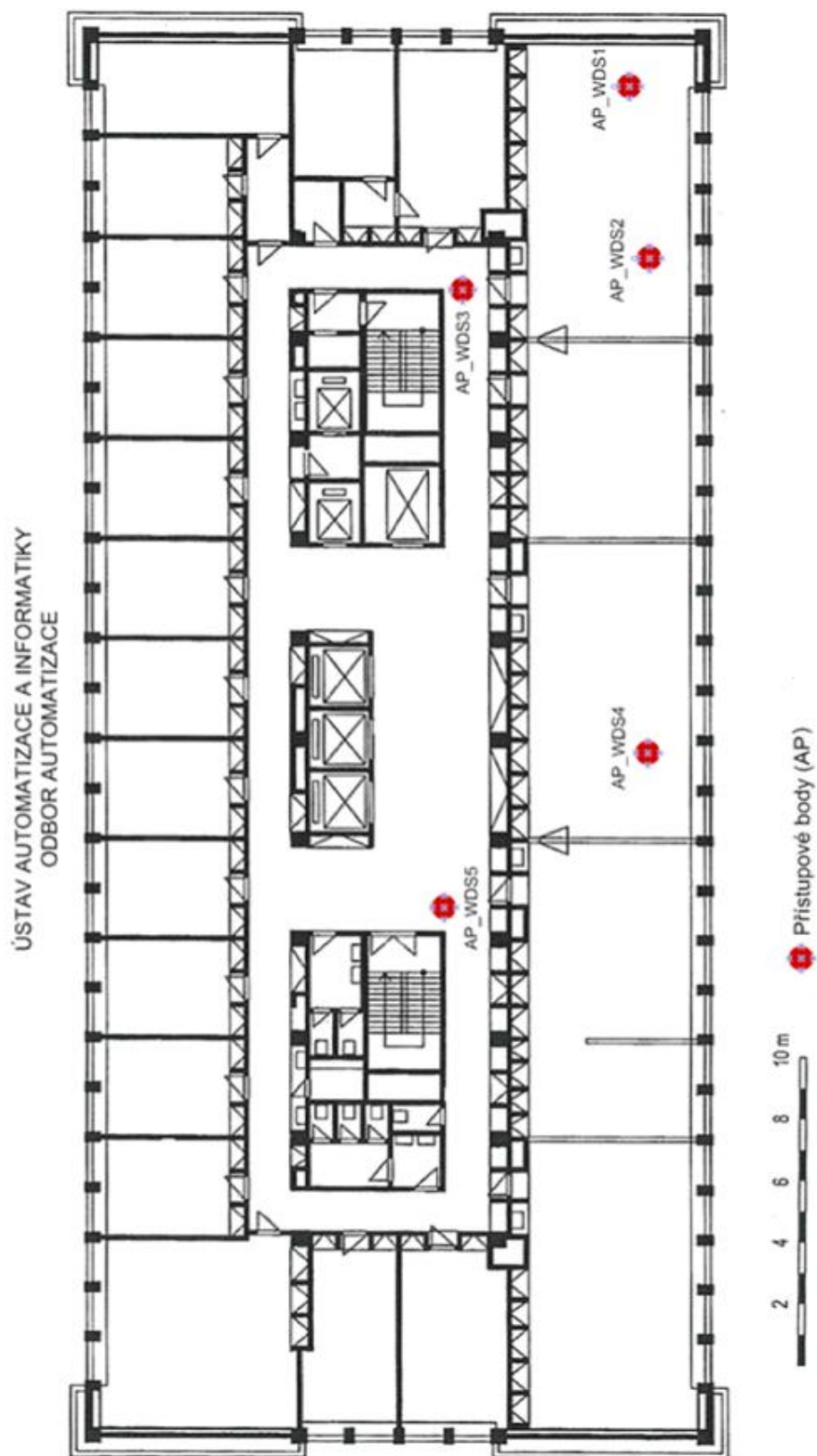
- AP_WDS4

SSID	BSSID	Kanál	Typ	Šifrovat	Signál	Vyberte
vutbrno	00:17:a4:a2:84:35	1 (B+G)	AP	no	66	☐
DP_VUT AP_WDS5	00:4f:62:0f:0d:88	13 (G)	AP	no	66	☐
lab	00:1f:c6:51:35:b1	1 (B+G)	AP	WPA-PSK	64	☐
DP_VUT AP_WDS1	00:4f:62:22:cb:06	13 (G)	AP	no	45	☐
DP_VUT AP_WDS3	00:4f:62:21:f2:0e	13 (G)	AP	no	45	☐
DP_VUT AP_WDS2	00:4f:62:22:cb:4e	13 (G)	AP	no	43	☐

- AP_WDS5

SSID	BSSID	Kanál	Typ	Šifrovat	Signál	Vyberte
vutbrno	00:17:a4:a2:84:35	1 (B+G)	AP	no	66	☐
DP_VUT AP_WDS4	00:4f:62:23:8d:d8	13 (G)	AP	no	66	☐
DP_VUT AP_WDS3	00:4f:62:0f:0d:88	13 (G)	AP	no	64	☐
DP_VUT AP_WDS2	00:4f:62:22:cb:4e	13 (G)	AP	no	33	☐

G Plánek strukturovaného prostoru



VUT v Brně, Fakulta strojního inženýrství, Ústav automatizace a informatiky

H Obsah přiloženého disku CD-ROM

Elektronická verze diplomové práce

- Žlůva Ivan_ Optimalizace bezdrátových WiFi distribuovaných sítí.pdf

Seznam technických listů jednotlivých zařízení:

- AirMax5.pdf
- MW-2000s.pdf
- WL-5460v2.pdf
- WLA-5000APv3.pdf
- WLA-5200AP.pdf
- WLA-9000.pdf
- WN-300R.pdf
- WN-300USB.pdf
- WN-301R.pdf

Seznam fotek z měření WDS sítě

- AP_WDS2_AP s OD300.JPG
- AP_WDS3_AP s OD100.JPG
- AP_WDS5_kontrola dostupnosti zarizeni.JPG
- Konfigurace AP.JPG
- Mereni propustnosti.JPG